TÜBİTAK BİLGEM
Cilt 3 Sayı 5
Ocak-Nisan 2011

BİLGEM

TÜBİTAK BİLGEM

BİLGEM Cilt:3 Sayı:5 Ocak-Nisan 2011

BİLİŞİM VE BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ

Özgürlük ve bağımsızlık benim karakterimdir.

Mustafa Kemal Atatürk

Değerli Okurlar,

2011'e merhaba derken güzel bir haberle başlamak istiyoruz. TÜBİTAK bünyesinde yer alan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) ile Bilişim Teknolojileri Enstitüsü (BTE), Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) çatısı altında birleşti. Hem kendi alanlarında, hem de birleşmeden ortaya çıkacak enerjiyle yeni alanlarda faaliyet gösterecekler. Bu oluşum aynı zamanda Türkiye'nin geleceğinin emin ellerde olacağının bir göstergesidir. Bir duyurudur, beyandır, temennidir ve geleceğe umutlu bir bakıştır. Ülkemiz adına hayırlı olsun diyoruz.

Fark etmişsinizdir; dergimizin adı değişti, fakat içeriğimiz değişmeyecek. Yayın hayatına BİLGEM Dergisi olarak devam edeceğiz.

Bu sayıdan bahsedecek olursak: İletişim ve haberleşmenin, çağımızın en önemli gerekleri arasında olduğunu biliyoruz. Peki, teknolojiyi, iletişim ve haberleşme alanlarında ileri düzeyde kullanırken acaba bilgilerimiz güvende mi? Bu soruyu irdeledik ve kapak konusu olarak "bilgi güvenliği sistemleri"ni ele aldık. Aynı konuda bir de yazı dizisine de başladık. Önceki sayıda ara verdiğimiz diğer yazı dizilerine devam ediyoruz.

Başarı öyküsü köşesinde yakın zamanda kaybettiğimiz Doç. Dr. Sayın Mustafa Aktekin'in hayat hikayesine yer verdik. Serbest kürsü bölümünde iştahla okuyacağınızı umduğumuz "Türk Mutfağı" yazısıyla karşınızdayız. Derginin son sayfalarındaki Şifresayar köşesinde yeni ödüllü soruları ve önceki soruların cevaplarını bulabilirsiniz.

Mayısta görüşmek üzere, hoşçakalın.

Dergi Yayın Kurulu

Sahibi
TÜBİTAK BİLGEM adına Merkez Başkanı
Mehmet Önder YETİŞ

Dergi Yayın Kurulu
Ahmet Serdar ADALI
Asım ALTUNBAŞ
Aziz Ulvi ÇALIŞKAN
Mustafa Ümit ÇEŞMECİ
Ersin EVİN
Cumhur Nezih GEÇKİNLİ
Fikret HACIZADE
Bilal KILIÇ
Mehmet Aydın KUBİLAY
Ahmet Hakan KUMBASAR
Hasan Berkan ÖZDEN
Levent Balamir TAVACIOĞLU
Bahattin TÜRETKEN

Kapak Tasarımı
Serkan KONAKCI

Genel Yayın Yönetmeni
Aziz Ulvi ÇALIŞKAN

Yayın Koordinatörü
Mehmet Aydın KUBİLAY

Sorumlu Yazı İşleri Müdürü
Asım ALTUNBAŞ

Edisyon-Redaksiyon
Levent Balamir TAVACIOĞLU
Cumhur Nezih GEÇKİNLİ
Bilal KILIÇ

Mali İşler Sorumlusu
Ahmet Serdar ADALI

Grafik Tasarım
Elif SÜSLER
Serkan KONAKCI
Volkan İZGİ

Yayın Türü
Dört aylık, süreli, ücretsiz

İletişim Adresi
BİLGEM Dergisi
P.K. 74, 41470 Gebze KOCAELİ

Telefon
(262) 648 1000

Faks
(262) 648 1100

Internet
www.uekae.tubitak.gov.tr/dergi

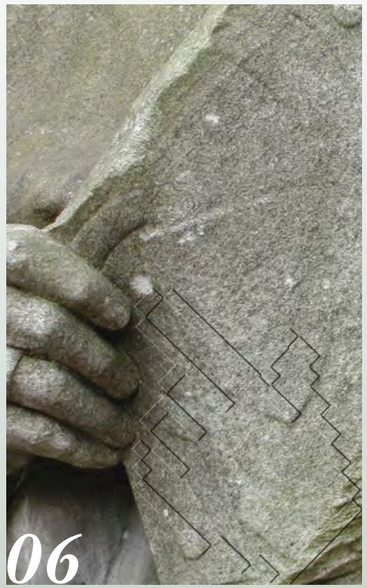
E-posta
dergi@uekae.tubitak.gov.tr

Baskı
Bilnet Matbaacılık Biltur Basım Yayın
(216) 444 44 03

Baskı Tarihi
Ocak 2011

ISSN 1309-3444

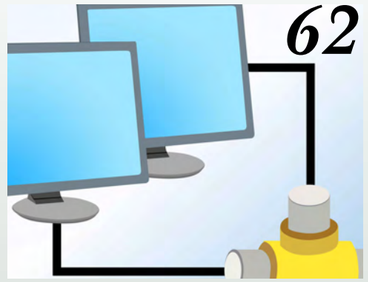
içindekiler



kapak konusu

yazı dizileri

içindekiler



makaleler

başarı öyküsü

serbest kürsü

Siber Güvenlik

"Yeni ordular kuruluyor. Silahları bilgisayar, savaş alanları internet."

Önder YETİŞ

İnternete bağlı bilgisayar ağlarının oluşturduğu elektronik ortama "siber uzay" denir ve siber uzayda 2009 yılında 2 milyar toplam internet kullanıcısı olduğu hesaplanmaktadır.

Siber uzayda rastlanan başlıca tehditler kötücül yazılımlar, hizmet dışı bırakma, yığın (spam) e-posta yollama saldırıları, ağ trafiğinin dinlenmesi, bilgi aşırma, kullanıcı şifrelerinin çalınması ve çeşitli forumlar veya oylama mekanizmalarının suiistimal edilmesidir. Tehditler ve etkileri yıllar geçtikçe değişmekte ve artmaktadır. Daha etkili saldırıların giderek daha az bilgili kimseler tarafından gerçekleştirilmesi mümkün hale gelmiştir.

Siber saldırıların en dikkati çeken özellikleri, kaynağı tespit etme zorluğu, kolay inkar edilebilirlilik, düşük maliyet, devlet destekli olup olmadığının belirlenememesi, farklı coğrafi bölgelerden katılım kolaylığı, taşeron kullanım olanağıdır. Zamanımızda, bir askeri tesis veya nükleer silah tesisi gibi klasik hedeflerin yerlerinin tespiti kolay olsa da, tehdit olarak siber saldırıların nereden yapıldığını anlamak çok zordur. Siber silah tesisinin tespit edilip yok edilmesi zor bir problemdir.

Radara yakalanmayan bir bombardıman uçağı 730 milyon dolar, radara yakalanmayan avcı uçağı 100 milyon dolar, bir Cruise füzesi 1 milyon dolar, bir siber silah ise 10 dolar ile 50 dolar arasında değişmektedir.

Bir siber saldırı sonrası internet aracılığı ile erişilen e-devlet, e-bankacılık gibi hizmetler devre dışı kalabildiği gibi e-posta iletişimi kesilebilir ve internete bağımlı kritik altyapılar çökebilir. Son yıllarda yaşadığımız en önemli siber saldırılara örnek olarak, Nisan 2007 yılında Estonya'ya, 2008'de Gürcistan'a, Litvanya'ya, Burma'ya, 2009 yılında Kırgızistan'a, Güney Kore'ye, en son Eylül 2010' da İran'a yapılan saldırıları verebiliriz. Bu saldırılar neticesinde söz konusu ülkelerde, kamu internet siteleri hizmet dışı bırakılmış, hükümet ve parlamento üyelerinin e-posta adreslerine spam saldırıları yapılmış, internet servis sağlayıcılarındaki yönlendirici cihazlar devre dışına çıkarılmış, bankacılık hizmetleri durdurulmuştur. Bu saldırılar neticesinde, açıklanmayan pek çok hasar oluşmuştur.

21. yüzyılda siber güvenlik tüm ülkeler için en önemli güvenlik unsuru, siber tehdit en önemli tehdit haline gelmiştir. Bu nedenle, bu tehdidin öneminin farkına varan ülkeler gerekli tedbirleri almakta, gerekli altyapı ve organizasyonları kurmaktadır. ABD'de, bu alanda sivil yapılanmada Ulusal Güvenlik Kurumu (National Security Agency) ve ABD Bilgisayar Olaylarına Müdahale Ekibi (Computer Emergency Response Team) önemli rol almaktadır. Askeri kesimde ise bir orgeneralin altında Siber Komutanlık (Cybercom) kurulmuştur. Kuvvet bazlarında ise çeşitli general rütbeleri altında faaliyetler yürütülmektedir.

Ülkelerin özgün işletim ve bilgi güvenliği sistemlerini geliştirmelerinin, bu alanlarda ön almış ülkelerce hoş karşılanmaması, istenmemesi, bir başka deyişle engellenmeye çalışmasının ikinci nedeni de, en az birincisi kadar, belki ondan da önemli olan güvenliktir. 21. yüzyılda siber casusluk veya siber istihbarat, güvenlik ve istihbarat faaliyetlerinde ilk sıralarda yer almaya başladı. Biraz sonra örneklerini vereceğim ülkelere baktığımızda, bu ülkelerin siber güvenlik sistemlerini, idari ve mali boyutta geliştirirken farklı organizasyon yapıları kullanabildiğini görebiliyoruz. Ancak kullanılan yazılımların, özellikle de işletim sistemlerinin milli ve özgün olması, bu faaliyetlerde ortak noktadır.

Siber casusluk ve istihbarat, bilgi sahibinin haberi olmadan kişisel, fikri mülkiyeti olan, hassas ve gizli bilgilere, kişisel, ekonomik, politik veya askeri üstünlük sağlamak amacıyla yasadışı siber yöntemlerle ulaşmak olarak tanımlanmaktadır. Ancak, günümüzde kabul gören bir husus da, casusluk ve istihbarat faaliyetlerinin, çok büyük oranda açık bilgi kaynaklarından sağlanıyor olmasıdır. Ücretsiz internet hizmet sağlayıcıları ve sosyal ağlar aracılığı ile sadece bilgi toplanmamakta, ülkelerin sosyal yapıları, toplumun karakteristiği, güçlü ve zayıf yönleri, tüketim eğilimleri vb. üzerine de araştırmalar yapılmaktadır.

Bugün hazır alınan bir yazılımın, ne zaman, nasıl çalışacağı, ne zaman çalışmaması gerektiği, ne zaman nereye veya kime bilgi aktaracağı, ancak onu geliştirenlerce kontrol edilebildiği artık bilinmeyen bir husus değildir.

Günümüzde, siber savaş, savaşın 5. boyutu haline gelmiştir. Siber savaş, bir ülkenin, başka bir ülkenin bilgisayar ve iletişim ağlarına, zarar vermek veya kullanım dışı bırakmak amacıyla illegal yöntemlerle internet, ağlar ve kişisel bilgisayarlar üzerinden müdahale etmesi olarak tanımlanmaktadır. Pentagon siber uzayın kara, hava, deniz gibi yeni bir savaş alanı olduğu doktrini kabul etmektedir. ABD'de bu alandaki en önemli darboğazın bilgisayar güvenliği uzman sayısındaki yetersizlik olduğu vurgulanmaktadır. ABD, mevcut bin civarında olan kalifiye eleman sayısını 20-30 binlere yükseltmek için gerekli eğitim programlarını hayata geçirilmeye başlamıştır.

Benzer şekilde NATO içinde de Siber Savunma Yönetim Otoritesi (NATO Cyber Defence Management Authority) altında bir yapılanma oluşturulmuştur. Dünyada mevcut siber güvenlik kurumlarına bakarsak İngiltere'de CESG, Almanya'da BSI, Fransa'da ANSSI, Çin'de PLA eliyle bu işler yürütülmektedir. Ancak, hangi ülkede, ne çeşit bir yapılanma olursa olsun, siber tehdide karşı %100 güvenlik sağlayan bir yapı ve ülke yoktur. Siber güvenlikte %100 güvenlik mümkün değildir.

Ülkemizde, ulusal düzeyde izleme ve koordinasyon, kurumsal düzeyde savunma, kurum bilgi sistemleri düzeyinde test ve denetimler, ürün düzeyinde güvenlik testleri ve kullanıcı düzeyinde eğitim ve rehberlik siber güvenliğimizi önemli ölçüde arttır. Etkin bir siber savunma için ülke içinde herkesin, kurumsal kullanıcılar, ev kullanıcıları ve diğer servis sağlayıcıları işin içinde olmalıdır.

Siber Güvenliğin sağlanmasında tüm taraflar için olay öncesinde, olay sırasında, olay sonrasında yapılacak görev ve işlemler belirlenmelidir. Olay öncesinde, kullanıcı ve kurum düzeyinde eğitim ve rehberlik verilmelidir. Kurumsal düzeyde sistemlerin düzenli test ve denetimleri yapılmalı, savunma hattı oluşturulmalıdır. Siber güvenlik koordinasyon merkezi kurulmalıdır. Siber tatbikatlar ile olaylara karşı hazırlıklı olunmalıdır.

Olay sırasında, kullanıcı ve kurum düzeyinde sürekli ve güncel bilgilendirme yapılmalıdır. Servis sağlayıcılar seviyesinde etkin iletişim ve işbirliği sağlanmalıdır. Bilgisayar olaylarına müdahale ekiplerinin çalışmaları, siber güvenlik koordinasyon merkezi tarafından eşgüdümle komuta ve kontrol edilmelidir.

Olay sonrasında, kullanıcı ve kurum düzeyinde hasar tespitinin yapılmalıdır. Siber güvenlik koordinasyon merkezi tarafından saldırı kaynaklarının tespit edilmeli, ulusal veya uluslararası hukuki mevzuat işletilmelidir. Ulaşılan sonuçların kamuoyu ve paydaş kurumlar ile paylaşılmalı ve düzeltici faaliyetler gerçekleştirilmelidir.

Bu iş ve işlemler için gerekli yasal düzenlemeler yapılmalı, teknolojik gelişmelere göre yasal güncellemelerin sürekliliği sağlanmalıdır.

Siber güvenliğin sağlanmasında ulusal düzeyde sanal ortam savunma sistemi kurulmalı, bilgisayar olaylarına müdahale ekipleri yasal zemine oturtulmalıdır. Kurum bilgi sistemleri periyodik olarak denetlenmeli, kritik kurum bilgi sistemlerin de kullanılan bilgi işlem, haberleşme ve güvenlik ürünleri güvenlik testlerinden geçirilmeli, bilgi güvenliği eğitimleri değişik seviyelerde verilmelidir.

Kamuda bilgi güvenlik ve işletim sistemlerinin milli enstitülerce geliştirilen milli sistemler olması çok büyük bir önem taşımaktadır. Bu sistemlerin yurtdışı ithalata açılması güvenliğimizi ne zaman ve hangi durumlarda tehdit edeceği öngörülememekte, bazen farkına bile varılamamaktadır.

Bu sayıdaki yazımı sonlandırırken tüm mesai arkadaşlarım adına siz değerli okurlarımıza saygılarımı sunar, keyifli okumalar dilerim.

Mehmet Önder YETİŞ
Merkez Başkanı

İnternet Güvenliğinin Tarihçesi

Bâkır EMRE

Yaşamımızın her alanına girerek, dünyamızın tümünü saran büyük haberleşme ağı internet, ülkeler arasındaki sınırları kaldırarak sanal bir dünya yaratmıştır. Ayrıca son yıllarda savaş türlerine bir yenisini, siber savaş kavramını ekleyerek bu alanda da dikkatleri üzerine çekmiştir. Tüm yönleriyle incelediğimizde son 50 yılın en büyük buluşu olarak nitelendirilmektedir.

Para çekme ve yatırma dışında her türlü finansal işlerimizi bankaya, ATM'ye gitmeden yapabildiğimiz, "Eyvah! faturanın da son günüymüş bugün" diye hayıflandığımız anda bile faturayı ödeme olanağı sunan ortamdır. Aynı zamanda yakınlarımızla haberleşme, arkadaş ya da eş bulma, ev, araba, eşya alma işlemleri internette günlük olarak gerçekleştirdiğimiz olaylardır. Bunların yanında yakın gelecekte evlenme, boşanma davalarını açabileceğimiz, çeşitli giyilebilir araçlar aracılığıyla evimizde muayene işlemlerini yürütebileceğimiz doktorunuz tarafından sağlık verilerimizin izlenebileceği bir ortam sunacaktır.

Kullanış amacına göre farklılık gösterse de internet günümüz dünyasının vazgeçilmez bir öğesi olmuş durumdadır. Eylül 2009 verilerine göre dünya üzerinde 1,966,514,816 kişi interneti kullanıyor yani dünya nüfusunun %28.7'si internet kullanmaktadır. Kullanımı her geçen gün artan kablosuz ve yeni nesil GSM ile birlikte 800 milyon civarı cihaz üzerinden erişilebilen bir ortam olmuş durumdadır.

Yazımızda internetin doğuşu, yaygınlaşması, internetteki güvenlik olaylarının geçmişi, bugünü ve geleceğini ele alınmaktadır.

İnternet'in Doğuşu

İnternet, günümüzden yarım asır öncesine dayanan bir serüvenin üründür. Zamanda bir yolculuk yapıp 1950'li yılların sonlarına gidip dünyadaki gelişmelere baktığımızda internetin nasıl doğduğuna şahit olabiliriz.

1957 yılında SSCB (Sovyet Sosyalist Cumhuriyetler Birliği)'nin yani günümüzdeki adıyla Rusya Federasyonu'nun Sputnik adlı uyduyu uzaya göndermesiyle bu alanda geriye düştüğünü düşünen ABD, ARPA'ya Advanced Research Projects Agency (İleri Araştırma Projeleri Ajansı)'nı kurmasına neden oldu. ARPA'nın amacı uzun dönem içerisinde Amerika'yı araştırma ve geliştirme alanında öne geçirmek ve aynı zamanda Sovyetlerden gelen tehditlere karşı önceden bilgilendirmekti. Bir yıl sonrasında uzay ve füze çalışmaları NASA'ya devredildi. Böylece, savunma alanındaki çalışmalardan çok araştırma çalışmalarına ağırlık verilmiş oldu. Birçok üniversitenin geliştirdiği bol riskli ama bol kazançlı projelere desteklendi.

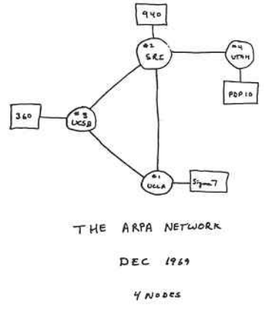
Bu strateji işe yaradı ve ARPA sayesinde birçok proje geliştirildi. Fakat ARPA içinde geliştirilen projelerin ve araştırmacıların bilgisayar kaynaklarını paylaşması o zaman için olası değildi. O devirdeki bilgisayarlar, aynı anda birden fazla kullanıcı tarafından kullanılamazdı. Yani çok görevlilik (multisaking) kavramı yoktu. Bilgisayarlar yapacakları işleri sırayla yapar, sonuçlarını bulur ve çıktıları üretirdi. Zaman paylaşımlı sistemlerin ortaya çıkmasıyla bilgisayarlar, önceleri, aynı anda birden fazla kullanıcıya servis vermeye, sonraları, aynı kullanıcıya aynı anda birden fazla iş yapmaya başladılar.

1962 yılında ARPA araştırmacılarında J. C. R. Licklider'ın "On-Line Man Computer Communications" adlı makalesi ile duyurulan Intergalactic Computer Network tanımı günümüzdeki internet'in yapı taşı olmuştur. Intergalactic Network ile, isteyen herkesin dünyanın herhangi bir yerinden çeşitli verilere ve programlara erişebilmesi öngörülüyordu.

ARPANET projesi ile ARPA içerisindeki projelerin, araştırmacıların ve bilgisayarların birbirlerine bağlanarak, birlikte çalışması amaçlandı. ARPANET'in üç değişik amaçlı bilgisayar ağ sistemi daha ortaya çıktı:

- Askeri tarafta RAND Corporation'ın oluşturduğu "askeri ağ",
- İngiltere'de National Physical Laboratoary NPL'in oluşturduğu "ticari ağ"
- Fransa'da Institut de Recherche d'Informatique et d'Automatique tarafından oluşturulmuş CYCLADES "bilimsel ağ".

ARPANET bu ağlara göre daha kullanışlı oldu ve 1969 yılında ARPANET projesi kapsamında Los Angeles'deki California Universitesi (UCLA)- Stanford Araştırma Enstitüsü (SRI) - Utah Universitesi (UTAH) ve Santa Barbara'daki California Universitesi (UCSB) arasında, 4 birimden oluşan ve 50 kbs bant genişliğine sahip bir ağ oluşturuldu. Şekil 1'de ARPANET'teki araştırmacılar tarafından çizilmiş ilk topoloji görülmektedir.



Şekil 1. *ARPANET araştırmacıları tarafından çizilen ilk topoloji.*

1972 yılında ağ üzerinden mesaj gönderebilmek için kullanılan ve posta adreslerini diğer sistemlerden ayırt etmemizi sağlayan e-posta işareti "@" Ray Tomlinson tarafından önerildi. Böylece ağ üzerinden e-posta gönderilmeye başlandı.

Şekil 2. *E-posta işareti.*

ARPANET'e bağlı ilk uluslararası bağlantı, 1973 yılında, İngiltere ile Norveç arasında gerçekleştirildi.

ARPANET üzerinde çalışan uygulamalarda dosya ve posta, NCP (Network Control Protocol) üzerinden iletiliyordu. ARPANET'in tek ağ olması ve ARPANET'e benzemeyen başka ağların da ARPANET'e bağlanabilmesini sağlamak amacıyla çeşitli çalışmalar yapıldı.

Bunlardan biri de 1974 yılında değişik cihazlar ve kurumlar arasında belirli bir standarda göre haberleşebilmesi için Vint Cerf ve Bob Kahn tarafında yayımlanan "A Protocol for Packet Network Interconnection" adlı makalesindeki TCP/IP protokolü kullanıldı. TCP/IP günümüzde de kullandığımız internetin temelini oluşturan protokoldür. Bugün kullandığımız IPv4 adresleme mekanizması, 1981 yılında, RFC (Request for Comments) 791 ile tanımlandı.

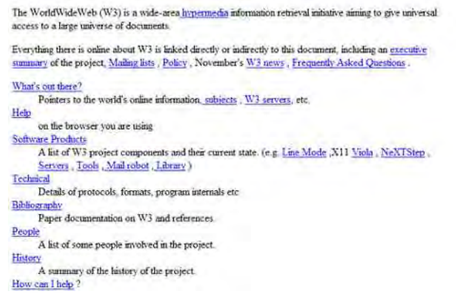
1983 yılında Alan Adı Sistemi ("Domain Name System", DNS) geliştirildi ve internet üzerinden ulaşılabilecek sistemlerden

- Eğitim kurumları için .edu,
- Devlet kurumları için .gov,
- Ticari kullanım için .com,
- Askeri kurumlar için .mil,
- Organizasyonlar için .org,
- internet servis sağlayıcıları için .net ve
- Uluslararası kurumlar için .int

Uzantıları verildi. Her bir alan adı kendisine has siteleri barındırmak üzere ayrıldı. Alan adı sisteminin de geliştirilmesi ile birlikte, "symbolic.com" ilk kayıtlı alan adı olarak tarihe geçti.

1989 yılında Tim Berners-Lee, CERN'de, World-Wide Web'i (www) geliştirmeye başladı.

1990 yılında WorldWideWeb adında metin tabanlı web tarayıcı ve CERN httpd adında bir web sunucuyu geliştirdi. Geliştirilen bu sunucu ve istemci info.cern.ch alan adı üzerinden hizmet vermeye başladı de ilk web sunucu olarak tarihe geçti (Şekil 3).


The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?

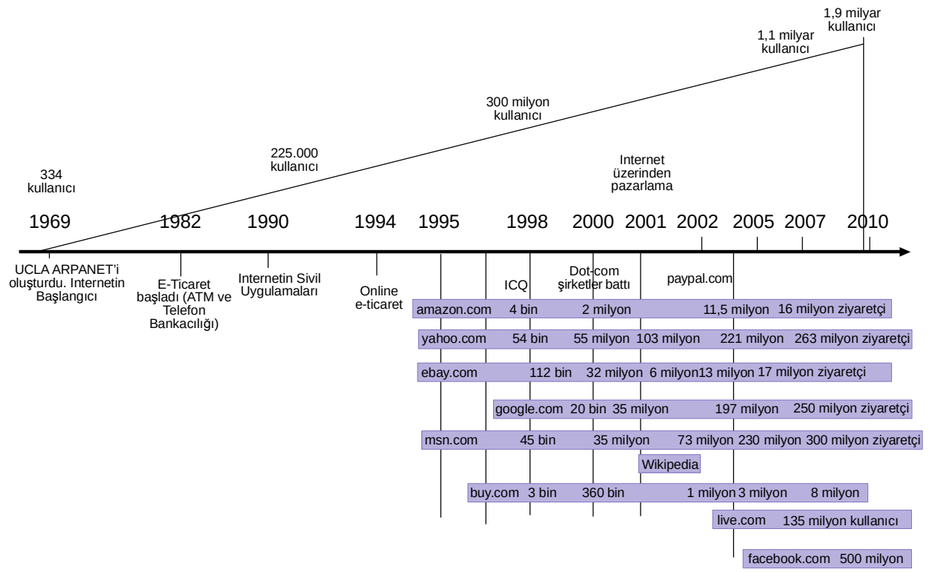
Şekil 3. *İlk web sayfası.*

İlk grafiksel web tarayıcısı Mosaic, 1993 yılında geliştirildi.

İnternet;

- 1995 yılında 45.1 milyon kullanıcıya sahip iken
- 2000 yılında bu sayı 420 milyon'a
- 2005 yılında 1.08 milyar kulancıya ve
- 2009 yılında ise 1.96 milyar kullanıcıya

ulaşmıştır (Şekil 4).



Şekil 4. *Internet kullanımı ve internetin dönüm noktaları.*

Yalnızca 2009 yılında internet üzeriden 90 trilyon e-posta gönderildi. Günlük olarak gönderilen e-posta sayısı 247 milyardır. Gönderilen e-postaların 200 milyarlık kısmı istenmeyen e-postadır(spam).

Bugüne kadar gönderilen e-postalar 1.4 milyar e-posta kullanıcısı ile gerçekleşmiştir.

İnternet üzerindeki web sitelerinin sayısı ise 2009 Aralık ayı itibari ile 234 milyona ulaşmıştır. Bu 234 milyon web sitenin bazıları ise insanların çeşitli amaçlar için kullandığı kişisel/teknik bloglardır ki bunların sayısı da azımsanmayacak kadar çoktur. Şu anda 126 milyon internet günlüğü (blog, web log olarakta bilinir) tutulmakta böylece insanlar kendi düşüncelerini bilgi birikimlerini internet üzerinden ulaşılabilir duruma getirebilmektedir.

Özellikle sosyal ağların ortaya çıkmasıyla internetin kullanımı artmıştır. Bu sitelere facebook, twitter, youtube örnek olarak gösterilebilir. Bu sitelerden twitter 2006 yılında kurulmasına ve çok küçük bir amaca hizmet vermesine karşın internet üzerinde günlük 27.3 milyon tweet (twitter adlı web uygulaması ile gönderilen mesaj) gönderilebimektedir.

Facebook.com adlı sosyal ağ sitesi ile kullanıcılar site üzerinden insanlar arkadaşlarına, yakınlarına internet üzerinden ulaşıbiliyor (Şekil 5). Bu site içerisinde dakikada 6 milyon, ayda 260 milyar, yılda 37.4 trilyon sayfa görüntülmektedir. Gösterilen bu sayfalar 500 Milyon facebook kullanıcısına ait verilerdir

Şekil 5. *Facebook.com sitesi verilerine göre Dünya üzerindeki arkadaşlık haritası.*

Youtube.com adlı site içerisinde günlük olarak 2 milyar video sunulmaktadır. Yalnızca ABD'de ayda 12.2 milyar video izlenmektedir. Sıradan bir internet kullanıcısı online video sitelerinden ayda ortalama 182 video izlemektedir.

İnsanlar arkadaşlarına, yakınlarına anlık olarak mesaj göndermek yani internet üzerinden sohbet etmek için çeşitli web araçları kullanmaktadırlar. Bu araçlardan özellikle Yahoo, Hotmail, skype, gtalk, aol Messenger gibi uygulamalar üzerinden, günde, ortalama 47 milyar ileti gönderilmektedir.

Şu anda internet üzerinde bulunan bilginin boyutu 1 zettabyte (1 milyon x 1 milyon gigabyte) olarak tahmin edilmektedir.

İnternet kullanımındaki bu umut verici istatistiklerden sonra bir de işin karanlık boyutuna bakalım. Her geçen gün sayıları artan zararlı yazılımlar, uygulama açıklıkları vb kötüye kullanım oranları şu şekildedir.

Günlük ortalama 148.000 bilgisayar köle (zombie) olarak botnetlere katılıyor. Bu köle bilgisayarlar istenmeyen e-posta göndermek için, dağıtık hizmet dışı bırakma saldırısı yapmak üzere kullanılmaktadır.

2009 yılında bilinen virüs, truva atları gibi zararlı yazılım sayısı 2.6 milyondur.. Bu oran her geçen gün artmaktadır.

Günlük gönderilen 247 milyar e-postanın 200 milyarlık kısmı yani %80 istenmeyen e-postadır.

Böylece askeri amaçlar için oluşturulan ARPA, üniversitelerdeki araştırmalar sonucu geliştirilmiş ARPANET'e yani akademik ağa dönüşmüş ve WWW geliştirilmesi ile birlikte günümüzdeki internetine dönüşmüştür. Oyunlar, kurumsal iş uygulamaları, e-ticaret, e-eğitim, e-devlet siteleri ile iş hayatımıza girmesi yanında, online mesajlaşma programları, internet üzerinden sesli ve görüntülü görüşme programları ile günlük hayatımızın vazgeçilmez bir parçası haline gelmiştir. Sosyal paylaşım siteleri, video paylaşım siteleri, sanal oyunlar (çiftlik kurma, hayvan besleme vb) uygulamalarla günlük hayatımızdaki etkinliğini artırmaya devam etmektedir.

Türkiye'de İnternetin Tarihi

12 Nisan 1993 yılında TÜBİTAK-ODTÜ (TR-NET) işbirliği ile DPT projesi çerçevesinde Türkiye global internete bağlanmıştır. 64 kbit/san hızında ki bu hat ODTÜ'den uzun bir süre ülkenin tek çıkışı olmuştur. Daha sonra Ege Üniversitesi (1994), Bilkent (1995), Boğaziçi (1995), İTÜ (1996) bağlantıları gerçekleştirilmiştir.

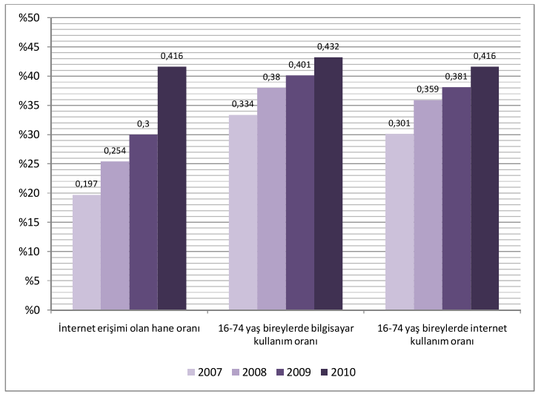
Türk Telekom'un 1995 yılında açtığı ihale ile bir konsorsiyum tarafından oluşturulan TURNET 1996 Ağustos ayında çalışmaya başlanıştır. Bunun yanı sıra Haziran 1996 tarihinde TÜBİTAK bünyesinde Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) adıyla yeni bir merkez kurulmuştur. ULAKBİM'in temel görevlerinden biri en yeni teknolojileri kullanarak Türkiye çapında tüm eğitim ve araştırma kuruluşlarını birbirine bağlayacak Ulusal Akademik Ağ (ULAKNET) adıyla hızlı bir iletişim ağı kurmak ve bu ağ aracılığı ile bilgi hizmetleri vermektir.

Sonraki yıllarda özellikle İSS (İnternet Servis Sağlayıcı) şirketlerin devreye girmesiyle internet özel şirketler, son kullanıcılar ve yeni uygulamalarla hızla büyümektedir. Türkiye'de internet bağlantı sayısının yıllara göre dağılımı Şekil 5'te görülmektedir.

Tablo1. Türkiye'de Yıllara Göre Internet Bağlantı Sayısı

	2004	2005	2006	2007	2008
ADSL	452.398	1.539.477	2.813.477	4.545.795	5.894.522
Kablo Internet	37.404	31.729	27.804	41.109	67.408
ISDN	14.005	14.298	14.535	15.297	17.096
Uydu	2.203	2.823	7.164	6.884	7.075
Toplam	*508.014*	*1.590.332*	*2.864.652*	*4.609.085*	*5.986.101*
Artış		*213%*	*80%*	*61%*	*30%*

2010 yılı Nisan ayı içerisinde gerçekleştirilen Hane Halkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre hanelerin %41,6'sı internet erişimine sahiptir. İnternet erişimi olmayan hanelerin %26,3'ü internet kullanımına ihtiyaç duymadıklarını belirtmişlerdir. ADSL %73,3 ile Türkiye'de kullanılan en yaygın internet bağlantı türüdür. Türkiye'deki internet kullanımıyla ilgili son 4 yıllık veriler Tablo 1'de görülmektedir.



Şekil 6. *Türkiye'deki internet kullanımı.*

İnternet ve Güvenlik Tehditleri

İnternetin temeli olan TCP/IP protokol ailesi daha çok veri transferi ile ilgilenmiş. Bu yüzden OSI (Open System Interconnection) referans modelinde iki katmanda bit ve paket bazında hata düzeltme düzenekleri konulmuştur. Oysa günümüz internet kullanımı dikkate alındığında, güvenlik, adres uzayı ve farklı uygulamalar için önceliklendirme yapan servis kalitesi düzeneklerinin eklenmediği görülmektedir. Sonradan bu eksiklikler için çeşitli yama çözümler geliştirilmiş olsa da bu düzeneklerin eksikliği hala hissedilmektedir. Bu makale öncelikle internette güvenlik konularıyla ilgilenmektedir.

İlk Büyük Güvenlik İnternet Olayı

ARPANET'in yaygınlaşması ve TCP/IP protokollerinin kullanmasından sonra internet üniversiteler, araştırma kurumları ve askeri birlikler tarafından kullanılmaya başlandı.

Robert Morris, NSA'de ('National Security Agency', Ulusal Güvenlik Ajansı) çalışan bir kriptografi araştırmacısı ve UNIX işletim sistemi kriptografi kütüphanesini yazan kişi olarak ünlenmiş birisi idi. Fakat ünü aynı isme sahip başka birisi tarafından ele geçirildi. Bu kişi, oğlu Robert T. Morris idi. Küçük Morris, babasının işi sayesinde küçük yaşlarda bilgisayarla oynamaya başladı. Daha sonra Harvard'ta lisans eğitimi aldı. Cornell Üniversitesinde yüksek lisans eğitimine devam ederken UNIX işletim sistemleri üzerinde çalışan fingerd, sendmail ve rsh adlı uygulamalarında bulduğu açıklar ve bazı zayıf şifreleri kullanarak uzaktaki bilgisayarlara bağlanan ve bağlandığı sistemler ile başka sistemlere bağlanabilen ve kendisini çoğaltabilen bir virüs yarattı. Bu virüs kendi kendine çoğalabildiği için daha sonra solucan (worm) olarak adlandırıldı. Türkçede de solucan ya da kurtçuk olarak adlandırılmaktadır. Morris yazdığı virüsü Kasım 1988 tarihinde MIT (Massachusetts Institute of Technology)'de önceden ele geçirmiş olduğu bir hesabı kullanarak internete bıraktı. Morris Solucanı'nın internet yoluyla yayılan ilk solucan olduğu sanılmaktadır. Solucanın MIT'den bırakılmasının nedeni; saldırının Cornell Üniversitesi üzerinden geldiğinin anlaşılmamasıydı. Solucan çalıştıktan 20 dakika sonra ARPANET öncesi internet mimarisi oluşturmaya çalışan ve savunma sanayi şirketi olan Rand Corporation'ın bilgisayarlarına bulaştı. Daha sonra Berkeley Üniversitesi ağ geçidine bulaştı. New Mexico'daki Los Alamos Ulusal Laboratuvarına ve Berkeley'deki Lawrence Livermore Laboratuarındaki ağ üzerinde bulunan cihazlara da bulaşmıştı. O devirde bu cihazlara olan bağlantı sayısı 4-5 iken saldırı sonrası bu sayı 100'e kadar çıkmıştı. Morris'in yazdığı kod aslında iyi huylu denebilecek bir koddu, çünkü hiçbir veriyi silmiyor, gizli mesajları okumuyor, yetkilendirilmiş kullanıcı hakkını almıyor ve truva atı gibi arka planda sisteme kapı açacak bir yapı sunmuyordu. Fakat ortada ters giden bir şey vardı. Burada enteresan olan gelişme Morris'in yazdığı solucan kodunun düzgün çalışmamasıydı. Fakat solucan kodundaki hata yüzünden yeni solucanlar oluşuyor, oluşan yeni solucanlar sistemin kaynaklarını tüketiyor ve yeni işlemlerin çalışmasına izin vermiyordu. Solucan çalışırken kendisini saklamak için yeni bir solucan süreci oluşturup başka sistemlere bulaşmaya çalışıyordu. Fakat ebeveyn işlem bu yeni süreç oluşturup kendisini öldürme işlemini düzgün bir şekilde yapamadığı için bir sistemde birden fazla solucan oluşuyor, oluşan her bir solucan sistem kaynaklarını daha fazla kullanmaya çalışıyordu. Böylece sistem solucanların işlerini yapmaktan kendi işini yapmaya vakit bulamıyor ve devre dışı kalıyordu. Gözden kaçan bir hata nedeniyle bilgisayarlar birçok kere enfekte oldular ve her enfeksiyon ayrı bir işlem olarak çalışarak bilgisayarı çalışamayacak kadar yavaşlattı. Bir nevi Servis dışı bırakma saldırısı (DoS Denial of Service) saldırısına maruz kaldılar. Sonuç olarak o tarihte internetin yüzde onunu oluşturan 6000 bilgisayar çalışamaz hale geldi. Tahmin edilen zarar ise 10 milyon dolar ile 100 milyon dolar arasında idi. Maddi kayıpların yanında Morris solucanının psikolojik etkisi daha büyük oldu; internete duyulan güven yıkıldı. Bu nedenle Morris solucanı, Büyük Solucan olarak da anılmaktadır. Bu olay basında da

geniş yer buldu. Amerika, Kanada ve İngiltere'deki New York Times, Toronto Star, Washington Post, London Financial Times gibi prestijli gazeteler olayı manşetlere taşıdılar.

Bir hafta içerisinde FBI ajanları Cornell Üniversitesi öğrencilerinden Robert T. Morris'ten kuşkulanmaya başladı. Burada ironik olan Morris'in babasının yine Ulusal Güvenlik Ajansı'nda bilim adamı oluşu ve birçok bilgisayar açığını bulan kişi olarak ünlenmesi idi. Oğlu da yine aynı şekilde bilgisayar ağları açıklarını bulan kişi olarak ünlendi. Ancak bu ün çok iyi bir ün olmadı. New York'taki mahkemelerce küçük Morris'e dava açıldı. Morris savunmasında "Morris solucanın amacı zarar vermek değildi, internetin büyüklüğünü bulmaya çalışıyordu. Acak koddaki hata yüzünden solucan gerektiği şekilde çalışmayıp internet üzerindeki cihazlara zarar verdi". Yerel mahkemece federal devlet bilgisayarlarına yetkisiz giriş yaptığı ve bu yetkisiz girişlerin 1000$'dan daha fazla zarara yol açtığı gerekçesiyle Morris'i suçlu buldu. Morris'e 400 saat kamu hizmeti cezası, 3 yıl gözaltında tutulma alma ve 10.050$ para cezası verdi. Robert Morris üniversiteden mezun olduktan sonra "4.2BSD UNIX TCP/IP uygulamasında zafiyet" adlı makaleyi yayınladı ve BSD UNIX'lerdeki güvenlik zayıflıklarını bildirdi. 1988 yılında internet 20 yaşında olmasına karşın varlığı kamu ve yargı sistemi yasalarınca tanınmıyordu. Morris davası ile internet şu şekilde bir tanıma sahip oldu "Morris internete (ülke içindeki üniversite, askeri ve devlet bilgisayarlarını birbirine bağlayan Ulusal ağ) bir solucan salıverdi". Soruşturmayı yönetenlerin vardığı ortak kanı ise zayıflıklar bilinen açıklardı ve bu açıkları kullanarak saldırmak için dahi ya da kahraman olmaya gerek yoktu.

Bu olaydan sonra, benzer durumlarda daha etkin çalışılıp zararlı yazılımların daha çabuk belirlenerek önlemler alabilmek için Carnegie Mellon Üniversitesi bünyesinde Bilgisayar Olaylarına Müdahale Ekibi (CERT-Computer Emergency Response Team) kuruldu.

Şekil 7. *Morris solucanı kaynak kodu.*

Bilgisayar Korsanları

Bizde bilgisayar korsanlığı olarak bilinen İngilizce'de sınırları zorlamak, olağan konsept-yapı ve kuralların dışına çıkmak anlamına gelen hacking, 1960 ve 1970'lerde MIT ve diğer bazı üniversitelerde ortaya çıkan bir terimdir.

1980'ler bilgisayar korsanı gruplarının oluşmaya başladığı yıllardı. Adını Çizgi roman kahramanı Superman'deki bir karakterden alan Lex Luthor adındaki kişi LOD (Legion of Doom) adında siber çete kurdu. Çete telefon hatlarını dinleme, telefon hatlarını kilitleme ve bilgisayarlara girme gibi birçok yasadışı faaliyetle bulundu. LOD çetesi içerisindeki anlaşmazlık sonucu ayrılanlar Masters Of Deception adıyla yeni bir siber çete kurdu. İki çete arasında 2 yıl süren siber savaşlar sonucu FBI çete üyelerini yakalayıp tutukladı.

1984 yılında bilgisayar ve telefon üzerine çeşitli alt etme yöntemleri, teknik bilgiler ve ipuçları veren ve hacker olarak bilinen kişilere ait çeşitli yazılar yayınlayan 2600 ve Phrack adlı dergiler yayın hayatına girdi.2600 dergisi adını telefon görüşmelerinin başlayabilmesi için çalan telefon sesinin frekansı olan 2600 Hz'den alıyordu.

1990 yılına gelindiğinde Amerikan Gizli Servisi bilgisayar ve telefon korsanlarına karşı Sundevil operasyonunu gerçekleştirdi. Operasyonun amacı 1980'lerin sonunda giderek artan telefon şebekesini kötü amaçlar için kullanıp kazanç sağlamak, hat kilitlemek ve telefon şebekesine bağlı olan bilgisayarları ele geçirmek anlamına gelen 'phreaking' ve bilgisayar korsanlığı etkinliklerini durdurmaktı. Zarara uğrayan telefon şirketlerinin şikâyetleri üzerine ülkenin 15 farklı kentinde kredi kartı hırsızlarını ve telefon şebekesini kötü amaçlar için kullanan kişileri yakalamak amacıyla operasyon düzenlendi ve birçok kişi yakalandı.

1994 yılında Los Angeles'taki KIIS-FM adlı radyonun kendilerini arayan 102. kişiye Porsche 944 S2 marka otomobil vereceğini duyan Kevin Poulsen adındaki phreaker telefon şebekesinde yaptığı birkaç hile ile radyoya giden bütün çağrıları kendi telefonuna yönlendirerek otomobili kazandı. Yaptığı birkaç korsanlık olayından sonra FBI tarafından yakalandı ve 51 ay cezaya çarptırıldı. Şuan da kendisi Wired.com adlı dergide güvenlik üzerine yazılar yazmaktadır.

1994 yılında Vladimir Levin adındaki matematikçi o zamana kadar internet üzerinden yapılmış en büyük soygunu yaptı. Citibank hesabından 10.000.000$ çaldı. Çeşitli kişilere ait şifre ve kullanıcı bilgilerini çalan Levin, çalınan paraları İsrail, ABD, Finlandiya, Hollanda, Almanya gibi çeşitli ülkelere aktardı. Aslında Levin bu işi mafyanın zorlamasıyla yaptı. Daha sonra İnterpol tarafından yakalandı. Paranın sadece 400.000$'ı geri alınabildi ve Vladimir Levin iki yıl hapis cezasına çarptırıldı.

"Ben bilgisayar korsanı değilim! Güvenlik Uzmanıyım." Bu sözler 90'lı yılların en çok aranan bilgisayar korsanı olan Kevin David Mitnick'indir. Mitnick, 80'lerde moda olan phreaking dalgasına takılan bir gençti. Sosyal mühendislik yönü de çok iyi idi. Sızacağı sisteme girebilmek için o şirketteki birisini arayıp kendisini aradığı kişinin üstüymüş gibi gösteriyor ve bu şekilde bilgi elde etmeye çalışıyordu. Örneğin; daha 17 yaşında iken kendisini telefonda Digital Equipments firmasının bir elemanı olarak tanıtıp, elektronik

cihazları kiralayan US Leasing firmasını arıza çözmek için arıyordu. Daha sonra sisteme girebilmek için gerekli kullanıcı adı ve şifreleri alıyordu. Böylece sisteme sızabiliyordu. Ertesi sene ise Pacific Bell adındaki bir telekom şirketine sızmaya karar verdi. Sisteme sızabilmek için çöp kutularından gerekli notları, şirket içi yazışmalardan kullanıcı adlarını elde etmeye çalıştı. Kendisini ve yakın bir arkadaşını yine Digital Equipments firmasının çalışanı gibi gösterip şirketten içeri girdi. Yöneticilerden birisinin odasından telefon veritabanına ait dokümanları çaldı. Dokümanların eksik olduğu öğrenilince polis tarafından yakalandı. Şirkete izinsiz girdiği ve doküman çaldığı için 1 yıl gözaltına tutulma cezasına çarptırıldı. University of South Carolina'daki bir terminale yasa dışı bağlandığı öğrenildiğinde ise 6 ay ıslahevinde kaldı. Cezası bitip iş hayatına başladığında yine bilgisayar üzerinden çeşitli suçlar işlemeye başladı. MIT'de çalışanları tehdit etme, kredi kartı sorgulamaları vb. nedenlerle Mitnick'e soruşturma açıldı; tutuklama kararı çıkartıldı. Mitnick olayları duyunca kaçmaya başladı. Bir müddet ortalıkta gözükmedi. Bir süre sonra NSA'in bilgisayarlarına girmeye başladı. NSA'den sonra UNIX işletim sistemi satan bir ticari şirket olan SCO'nun bilgisayarlarına girip Xenix işletim sisteminin kodlarını çalmaya çalıştı. Bu gelişmeler üzerine SCO, telekom şirketleri ile anlaşıp, Mitnick'in yerini tespit ettirdi. Polis Mitnick'i yakaladı. Dava sürerken Mitnick, SCO yönetimi ile anlaştı ve işbirliğine girdi.

Üniversite yıllarında ARPANET'i kullanarak çeşitli askeri kurumlara giriyor, çaldığı dosyaları yine ARPANET üzerindeki başka bilgisayarlar üzerinde saklıyordu. Digital Equipments firmasının işletim sistemi olan VMS'in daha duyurulmamış sürümünü elde etmeye çalıştı. Amacı işletim sisteminin kaynak kodlarını elde edip açıklıklarını bulmak ve bu işletim sistemini kullanan bilgisayarlara daha kolay erişmek idi. Nitekim öyle de oldu. VMS 5.0'ın kodlarını DEC firmasının bilgisayarlarından çaldı. Kaynak kodların büyüklüğünden dolayı kopyalamayı kendisi yapamayacaktı ve daha önce de beraber çalıştığı okul arkadaşı Lenny'den yardım istedi. Kendisine bu konuda yardım eden Lenny artık daha fazla yasa dışı iş yapmak istemediğini söyledi. Mitnick'in hırsı bitmek tükenmek bilmeyince Lenny durumu FBI'a bildirdi. Zaten Digital Equipments firması da kodların olduğu bilgisayara erişim olduğunu anlayınca durumu yetkililere bildirmişti. Yetkililer ortak bulgular sonucunda Mitnick'in yakalanması için Lenny'nin üzerine bir dinleme cihazı koyup Mitnick ile buluşmasını istediler. 1988 yılında Mitnick tutuklanarak ceza evine girdi ve bir yıl tutuklu kaldı. Ardından 6 aylık bir tedavi sürecinden geçti.


U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC) W224660021

NAME: ..... MITNICK, KEVIN DAVID
AKA(S): ..... MITNIK, KEVIN DAVID
MIRRILL, BRIAN ALLEN

DESCRIPTION:
Sex: ..... MALE
Race: ..... WHITE
Place of Birth: ..... VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ..... 5'11"
Weight: 190
Eyes: ..... BLUE
Hair: ..... BROWN
Skintone: ..... LIGHT
Scars, Marks, Tattoos: ..... NONE KNOWN
Social Security Number (s): 550-59-5695
NCIC Fingerprint Classification: DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-CI54-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia, Telephone: (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSMOOOO.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM-132 (Rev. 3/92)

Şekil 8. *Mitnick'in yakalama ilanı.*

1994 yılına gelindiğinde ise Mitnick bir hastanede çalışmaya başlamıştı. Her zamanki gibi burada da boş durmuyordu. Bu defa sisteme sızma girişimlerini Tsutomu Shimomura'nın bilgisayarında uyguluyordu. Fakat sisteme sızmak için daha önceleri çeşitli makalelerde geçen ve henüz uygulamamış olan bir yöntem denedi. Sequence number (dizi numarası) kullanarak IP spoofing (IP adresi taklit etme) yapıyordu. Sistemine sızdığı kişi bir müdahale olup olmadığını günlük sistem dosyalarından takip edebiliyordu. Fakat Mitnick, IP adresini Shimomura'nın kendi ağındaki bir bilgisayardan geliyormuş gibi gösterince, Shimomura sistemine sızan kişiyi bulamıyordu. Shimomura bu işi yapan kişiyi yakalatmak istiyordu ama elinde hiçbir ipucu yoktu. Mitnick, sızdığı bilgisayardan kopyaladığı dosyaları başka bir bilgisayara kopyalamıştı. Dosyaların kopyalandığı bilgisayarın sahibi Shimomura'ya ait dosyalar bulunca onunla iletişime geçti ve durumdan haberdar etti. Bunun üzerine Shimomura ISP firması ile iletişime geçti ve bu IP adresine ait ağ trafik kayıtlarını sniffer (ağ trafik kaydı dinleyici) yardımı ile dinlemeye başladı. Mitnick bu defa sert bir kayaya çarpmıştı. Shimomura trafik kayıtlarından birilerinin içerisinde "itni" geçen kelimeleri aradığını gördü ve bu aradığı kişinin gerçekten M"itni"ck olduğunu anladı. Trafik kayıtlarını inceleyerek saldırganın yerini belirlediler. FBI ve polisin işbirliği ile yakalanarak tutuklandı. Beş yıl hapis cezasına çarptırıldı. Mitnick; Pentagon, Sun Microsystems, Motorola gibi dünyaca ünlü kurumlara sızdığı için FBI'ın en çok aranan listesine girmiş ilk bilgisayar korsanı oldu.

Mitnick'in cezası 21 Ocak 2000'de bitti. Ama bilgisayar ve telefon kullanımına yasak getirildi. Bu süre içerisinde sadece annesi ile telefonla görüşmesine izin verildi. Bilgisayarlara yaklaşma yasağı 21 Ocak 2003'te sona erdi. Şimdilerde kendi güvenlik şirketi olan Mitnick Security Consulting'de güvenlik alanında çeşitli çalışmalar yapmakta ve dünyanın birçok ülkesinde seminerler vermektedir.

Mitnick hakkında iki film (Takedown ve Freedom Downtime) çekildi. Mitnick'e göre bu ün abartılı bir ündü. Ona göre aslında bu ününün kurbanı olmuş ve hapse girmişti.

Hapishaneden çıktıktan sonra iki de kitap yazdı: "Art of Deception" ve "Art of Intrusion". İlk kitap sosyal mühendislikle alakalıydı. İkincisi ise yaşanmış bilgisayar korsanlığı olaylarını hikâye tarzında anlatıyordu.

İlk Güvenlik Duvarı, İlk Sanal Özel Ağ

1990'lı yıllarda bilgisayar ağlarına izinsiz girişler, parolaların çalınması gibi güvenlik olayları artmaya başladığında piyasaya ticari güvenlik duvarları (firewall) çıktı. İlk güvenlik duvarları yönlendiriciler üzerinde iç ağ ve dış ağ arasındaki trafik geçişini kontrol eden paket filtreleyicilerdi. Bunlar o yıllarda genellikle Cisco, 3COM, WellFleet yönlendiriciler üzerinde çalışan uygulamalardı. İlk ticari güvenlik duvarı DEC'in SEAL ürünüydü. Bu ürün hem paket filtreleme yapıyordu, hem de uygulamalar için vekil sunuculuk (proxy) görevi göreyordu. Arkasından Raptor System, Gauntlet, Check Point gibi ticari ürünler geldi. Daha sonraki yıllarda güvenlik duvarlarının üzerine uçtan uça şifreleme yapma yeteneği ve virüs tarama yetenekleri eklendi. Günümüzde de bilgisayarların ve bilgisayar ağlarının güvenliğini sağlamada güvenlik duvarları vazgeçilmez araçlar olarak kullanılmaktadır.

Farklı coğrafyalarda ofisleri ve çalışanları olan şirketlerde ortak sisteme erişilirken parola kullanılıyordu. Bu parolalar değişik yollardan (tahmin etme, ağı dinleme vb.) bilgisayar korsanlarının eline geçiyordu. Parolaların yanı sıra güvenli erişim kartı, tek kullanımlık numaralar gibi ek güvenlik önlemleri uygulanmaya başlandı. Aynı zamanda farklı şirketler arasındaki ticaretin güvenliğinin sağlanması için gizlilik, bütünlük ve kimlik denetimi mekanizmalarını kullanan sanal özel ağ (Virtual Private Network) cihazları kullanılmaya başlandı. İlk başlarda simetrik şifreleme, daha sonradan asimetrik şifreleme algoritmaları kullanılmaya başlandı. Günümüzde ise dosya şifrelemek için PGP (Pretty Good Privacy), trafiği şifrelemek için SSL (Secure Sockets Layer) ve sayısal imza gibi günlük hayatımızı kolaylaştırılacak güvenlik çözümleri geliştirildi.

"Seni seviyorum" İmza: Virus

Bilgisayar sistemlerindeki dosyaları silerek, isimlerini değiştirerek ya da bilgisayar sistemlerinin işlemci, bellek gibi kaynaklarını tüketerek sistemin çalışmasını engellemeye çalışan zararlı yazılımlar virüs olarak adlandırılır. Bu zararlı yazılımların tarihçesi, bilgisayar tarihçesi kadar eskidir. 1971 yılında ortaya çıkan Creeper bilinen ilk bilgisayar virüsüdür. Virüslerin bugüne kadar pek çok çeşidi çıkmıştır ve verdiği zararlar artarak devam etmektedir. Günümüzde de bilgisayar güvenliği denildiğinde akla ilk gelen virüslere karşı koruma sağlayan antivirüs programlarıdır. Fakat şimdilik virüsler antivirüs programlarının bir adım önündedir. 2009 yılı içinde Microsoft'un tespit ettiği tekil zararlı yazılım sayısı 240 milyondur. Buna karşın Kaspersky antivirüs firmasının belirttiği zararlı yazılım sayısı 18 milyondur. Diğer taraftan Symantec, McAfee gibi şirketler de farklı rakamlar vermektedir. Firmalar arasında bu fark, genel bir sayı vermenin ne kadar güç olduğunu göstermektedir.

Yeni milenyumda birçok insan e-posta hesabına sahip oldu. Kişisel yazışmalarımızı yaptığımız ortamda "Seni seviyorum" başlığına sahip bir mesaj gelmesini kimse yadırgayamazdı. Nitekim 5 Mayıs 2000 yılında ortaya çıkan bu mesajın içeriğini merak eden kullanıcıları kötü bir sürpriz bekliyordu. Mesajın içeriğinde "Love-Letter-For-You.txt.vbs" adında bir dosya mevcuttu. Bu dosya bir Visual Basic Script dosyası idi. Microsoft işletim sistemlerinde, dosya isminden sonra gelen kısım (uzantı) dosyanın tipini belirtir. Seni seviyorum virüsü bu mantıktan yola çıkarak kendisinin bir "vbs" dosyası olduğunu saklıyordu. Kullanıcılar da içeriğine bakmak için dosyayı indirdiklerinde virüs aktif hale geliyordu. Kendisini bilgisayar üzerinde var olan .mp3, .jpg, .vbs, .js, .css, .wsh gibi çeşitli dosyaların üzerine yazarak yayılıyor, dosyalara erişimi engelliyordu. Daha sonra Microsoft kayıt düzenleyicisi içerisindeki kayıtlara girerek, RAM üzerinde bulunan şahıslara ait şifreleri, internetten indirdiği araçlarla yakalıyordu. Yakaladığı parolaları virüsü yazana gönderiyordu. Ayrıca virüsün başka kişilere de bulaşması için kullanıcının e-posta istemcisindeki tüm adres defterine gönderiyordu. Böylece arkadaşından "Seni seviyorum" diye bir mesaj alan herkes bu e-posta içeriğini kontrol etmeden açtı. Böylece daha fazla kişi virüsün zararlarından nasibini aldı. Virus çok hızlı bir şekilde dünya genelinde yayıldı. Tahminlere göre dünya genelinde 5.5 milyar dolarlık zarara yol açtı.

Virüsün zararlarından korunmak amacıyla Pentagon, CIA, Ford gibi büyük firmalar ve İngiltere Parlamentosu e-posta sunucularını kapattı. Virüsin yaklaşık 50 milyon bilgisayara bulaştığı zannedilmekteydi. Bu, o ana dek karşılaşılmış en büyük bilgisayar problemlerinden biriydi.

Seni seviyorum virüsünün kullandığı yöntem yeni değildi. Ondan bir yıl önce çıkan Melissa virüsü de aynı şekilde çalışıyordu: Microsoft Word kelime işlemcisi içindeki makro uygulaması ile işletim sistemi için önemli dosyaları silip ciddi zararlar veriyordu. Bununla yetinmeyip kendini kullanıcının adres defterindeki 50 kişiye daha göndererek yayılıyordu. Virüsün programcısı David L. Smith dünya genelinde 1.5 milyar dolarlık zarara neden oldu. Sebep olduğu zararlar dolayısıyla 20 ay hapis cezası aldı.

1999 yılında ortaya çıkan CIH (Çernobil) virüsü ise BIOS belleğini hedef alıyordu. O zamana kadar çıkan virüslerin çoğu yazılımlara ve dosyalara zarar verirken, CIH donanıma da zarar veren bir türdü.

2001 yılında ise CodeRed adlı solucan internet üzerinde dolaşmaya başladı. Bu solucan, Windows işletim sisteminde ağ sunumcusu olarak çalışan Internet Information Server (IIS) üzerindeki bir kütüphane dosyasının arabellek taşması

hatasından yararlanıyordu. Rastgele IP adreslerini taramaya ve bu IP adreslerindeki bilgisayarlara bir Truva atı yerleştirmeye çalışıyordu. Bu Truva atı, ayın 20'siyle 27'si arasında Beyaz Saray'ın http://whitehouse.gov adresine karşı bir hizmet dışı bırakma saldırısı (denial of service) başlatmak üzere kendisini programlıyordu.

BotNet: Robot Ağların Yükselişi

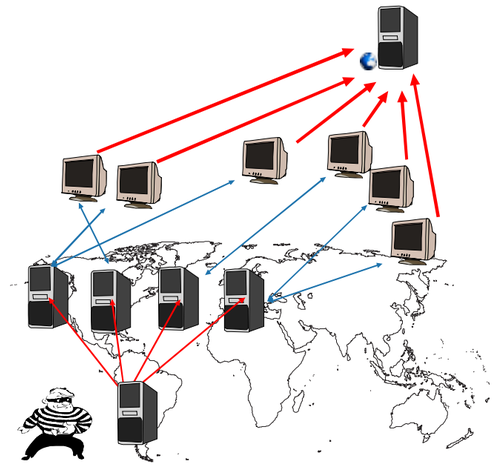
Bilgisayarlar belirli verileri girdi olarak alıp işleyerek çıktı üretir. İşlem süresi, verilerin çokluğuna ve bilgisayarın bunları işleme kapasitesine bağlı olarak değişir. Veri çok büyük ise bunu en etkin bir şekilde işlemek için, parçalara bölüp birden fazla bilgisayarda işlemek mantıklı bir çözümdür. "Dağıtık yapı" olarak bilinen bu yöntemle birden fazla bilgisayarı aynı iş için kullanıp daha erken sonuç alabilmekteyiz.

Birden fazla bilgisayarla yapılan saldırı yöntemlerinden birisi de RSA'in (Rivest, Shamir, Adleman) kırılma yöntemidir. RSA, 1977 yılında geliştirilmiş, açık anahtar altyapısına sahip bir şifreleme yöntemidir. Bu şifreleme yöntemini kırana ödül verileceği duyurulmuştur. 426 bit boyundaki bir RSA şifresi, 1994 yılında 24 farklı ülkeden 1600 farklı bilgisayarın 8 aylık ortak çalışması sonucunda kırılabildi.

BotNET diye tabir edilen sistem, "robot network" (robot ağ) kavramından türetilmiştir. Robot ağ; dağıtık halde çalışan bir ağı ve ağ içindeki binlerce köle bilgisayarı yöneten bir bilgisayardan (BotMaster) oluşur. Köle bilgisayar, işletim sistemindeki açıktan veya yazılımların güncelleme eksikliklerinden faydalanılarak ele geçirilip robot ağa dahil edilen bilgisayarlardır. Robot ağa dahil olan köle bilgisayarlar, tek bir noktadan yönetilerek, hizmet dışı bırakma saldırıları ve istenmeyen e-posta gönderileri gibi çeşitli amaçlar için kullanılır. Bu sistem mimarisi sayesinde binlerce bilgisayar tek bir bilgisayar gibi davranabilir ve hepsi aynı andan aynı işi yapabilir (Şekil 9).

Saldırı amaçlı kullanılabilen bu sistem ile ilk büyük darbe 2000 yılı Şubat ayında Yahoo portalına vuruldu. MafiaBoy lakaplı 16 yaşındaki bir genç, dağıtık hizmet dışı bırakma yöntemiyle (DDoS) 1 Gbps bant genişliğine sahip bir saldırıda bulundu: IP adresleri taklit edilmiş binlerce köle bilgisayarları kontrol ederek Yahoo'nun 3 saat boyunca hizmet dışı kalmasına neden oldu. İki gün sonra eBay, Amazon, Buy.com, ZDNet, CNN gibi birçok site de DDoS'tan nasibini aldı. Yahoo'nun %99.3'te olan erişilebilirlik oranı %3-5 seviyesine düştü. Bu saldırılar sonucu Yahoo 500.000, Amazon 600.000 dolar zarara uğradı.

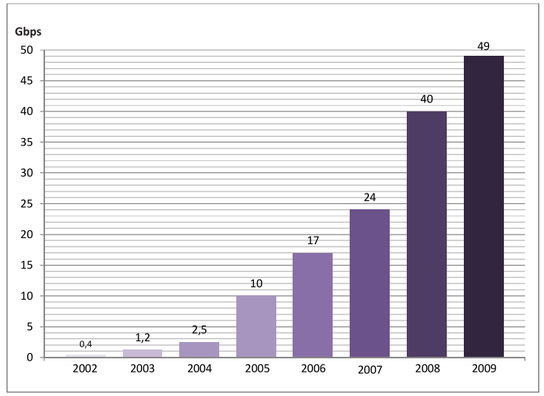
2002 yılının Ekim ayında kök DNS sunuculara karşı DDoS saldırısı düzenlendi. 13 sunucuya taklit edilmiş IP adresleriyle 1 saat boyunca büyük ICMP paketleri gönderen ping flooding



Şekil 9. *Robot ağın bir sistemi hedef alması.*

saldırısı başlatıldı. Saldırı sonucunda, internet üzerindeki IP adreslerine denk gelen domain isimlerini çözen sunuculardan 9'u hizmet dışı kaldı. Bu nedenle birçok web sayfasına ulaşılamadı.

Arbor Networks verilerine göre 2002-2009 yılları arasında gerçekleşen en büyük DDoS saldırıları Şekil 10'da gösterilmiştir.



Şekil 10. *Yıllara göre en büyük DDoS saldırıları.*

2009 yılında gerçekleştirilen en büyük DDoS saldırısı 49 Gbps olarak belirlenmiştir.

Bu saldırının bant genişliği tüketme oranlarındaki artışın önceki seneler kadar olmamasının nedeni, interneti oluşturan fiziksel altyapının kısıtlarına takılmış olmasıdır. Bu kısıtlar yüzünden 2009 sonrası yapılan saldırılar, bant genişliği tüketmek yerine daha etkin yöntemlere odaklanmaktadır.

Siber Savaşlar

Hedef seçilen ülkenin bilgi ve iletişim sistemlerine yönelik, ekonomik, politik veya askeri nedenlerle gerçekleştirilen organize saldırılara "siber savaş" denir. Özellikle rakip ülkeler arasında, kendi kaynaklarını (asker, teçhizat vb.) tüketmeden silahsız savaşla karşı tarafa zarar veren bir yöntemdir. Bu saldırıların tamamına yakını robot ağlar üzerinden gerçekleştirilir.

Siber savaşlarda kullanılan saldırı tiplerini birkaçını şöyle sıralayabiliriz:

- İnternet üzerinden karşı propaganda,
- İnternet sayfalarının ele geçirilmesi,
- Gizlilik dereceli bilginin ele geçirilmesi,
- Kritik sistemlere yönelik saldırılar (enerji altyapısı, iletişim altyapısı, kamu hizmetleri, askeri sistemler vb.),
- Dağıtık hizmet dışı bırakma saldırıları (DDoS),
- İstenmeyen e-postalar.

Şekil 11. *Bir siber savaş alanı.*

İkinci Dünya Savaşı sırasında Estonya, Sovyetler Birliği ile birlikte, Almanya'ya karşı savaşmıştı. Savaş sona erince Bronz Asker Anıtı dikildi. Bu heykel, Estonya'nın Nazi istilasından korunması amacıyla Sovyetler Birliği'nin verdiği mücadeleyi sembolize ediyordu. 26 Nisan 2007'de Estonya, Bronz Asker Heykeli'ni yerinden kaldırdı. Bir gün sonra heykelin kaldırılması Rusya tarafından kınandı. Daha sonra ise ülkede ayaklanmalar çıktı. Rusya yanlısı göstericiler ülkenin çeşitli yerlerinde gösteriler yapmaya başladı. Özellikle başkent Tallinn'de ayaklanmalar ve yağmalamalar başladı. 27-29 Nisan 2007 tarihleri arasında devletin internet sayfaları ele geçirildi; ufak çaplı DDoS saldırıları başladı; ulusal e-posta sunucularına ve haber portallerine spam saldırıları düzenlendi. Dördüncü günden itibaren, özellikle 30 Nisan-18 Mayıs tarihleri arasında daha organize saldırılar yapıldı. Ulusal bilgi sistemleri, internet hizmet sağlayıcıları, bankalara büyük zararlar veren saldırılar oldu. Ülkedeki internet sistemi çökme tehlikesiyle karşı karşıya kaldı. Saldırıların yönlendirildiği ülkeler arasında ABD ve Avrupa Birliği üyesi ülkelerin de bulunduğu tespit edildi.

Estonya'nın nüfusu 1.3 milyondur ve 1 milyondan fazla sayısal kimlik kartı sahibi vardır. Ülkede Mayıs 2007'den beri cep telefonlarında sayısal kimlik tutulmaktadır. Nüfusun %66'sı interneti sürekli kullanmaktadır. Evlerin %55'inde bilgisayar bulunmaktadır. Vergi beyanlarının %80'i internet üzerinden yapılmaktadır. Bankacılık işlemlerinin %97'si çevrim içi gerçekleştirilmektedir. Sağlık kayıtlarının tümü sayısal ortamdadır. Ülke çapında hemen her yerde kablosuz internet hizmeti sunulmaktadır ve erişim genel olarak şifresizdir. Yeni kurulan her dört şirketten biri internet üzerinde kurulmaktadır. İnternetin bu kadar çok hayatla iç içe olması Estonya'yı çok zor duruma sokmuştu. Bu durum diğer devletlere örnek oldu. E-devlet uygulamaları bürokrasiyi azaltıp hayatı kolaylaştırırken, robot ağ kaynaklı saldırıların iştahını açmaktadır.

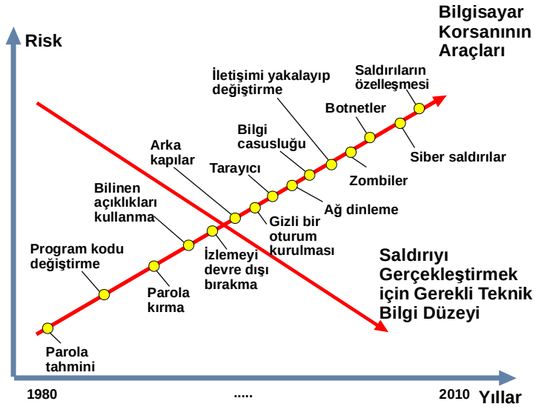
Bir başka örnek ise Gürcistan. Gürcü kuvvetler, 8 Ağustos 2008 tarihinde bağımsızlığını ilan eden Güney Osetya topraklarına operasyon düzenlediler. Rusya da bu olayın ardından 11 Ağustos 2008'de Gürcistan'a savaş açtı. Bu savaş başlamadan önce siber savaş başlamıştı. Saldırılar, 20 Temmuz 2008 tarihinde Gürcistan Devlet Başkanı Mihail Saakaşvili'nin internet sitesi olan www.president.gov.ge adresini hedef aldı. Bunlar dağıtık servis dışı bırakma saldırıları idi. Askeri harekâtın başladığı tarihte ise Gürcistan internet sitelerine yönelik saldırılar artmış, birçok siteye erişim engellenmiş ve bazı sayfaların içeriği değiştirilmişti.

Şekil 12. *Gürcistan'a karşı yapılan siber savaş sırasında devlet sitelerinden birinin içeriği.*

Siber savaşta, yardım amacıyla daha önceden benzer saldırıya maruz kalmış olan Estonyalı ve Polonyalı uzmanlar, Gürcistan'a gidip bilgi birikimlerini aktararak teknik destek sağlamışlardır. NATO, yaşanan gelişmeler karşısında "sayısal ortamda savaşı" öncelikleri arasına aldı. Bu alanda önemli bir adım atan ittifak, Estonya'da "NATO Sayısal Ortam Savunması Mükemmeliyet Merkezi"ni açtı.

Sonuç

İnternetin doğuşundan günümüze kadar birçok sayısal saldırı türü ortaya çıktı. Bu saldırılardan bazıları kişisel veya kurumsal yarar sağlamak için, bazıları ise karşı sisteme zarar vermek için kullanıldı. Önemli ölçüde maddi zarar ve iş gücü kayıpları oldu, hala da olmaya devam ediyor. Diğer taraftan güvenlikçiler de boş durmadılar; yeni çıkan açıkları kapatmak, daha güvenli sistemler geliştirmek için çalıştılar. İnternetin ya da bilgisayar haberleşmesinin sağladığı faydalar, bu saldırıların verdiği zararlardan çok fazladır. İnternete bağlı olan bilgisayar ve internette her geçen gün çıkan yeni uygulamaların sayısı bunun göstergesidir. Bilgisayar saldırılarının yıllara göre gelişimi, bu saldırıları uygulamak için gerekli bilgi seviyesi ve saldırı araçlarının yıllara göre sayısı şekil 13'te görülmektedir.



Şekil 13. *Bilgisayar saldırılarının yıllara göre gelişimi.*

Şekilden de anlaşılacağı gibi, saldırılar karmaşıklaşmakta, etkisi artmakta ve saldırı yapabilmek için gereken bilgi düzeyi azalmaktadır. Çocukların bile kullanabileceği araçlar ve programlar bulunmakla beraber gün geçtikçe bu araçların sayısı da artmaktadır.

TÜİK'in (Türkiye İstatistik Kurumu) 2010 Ağustos ayı verilerine göre son on iki ay içerisinde kişisel amaçla internet kullanan bireylerin %47'si güvenlik sorunu ile karşılaşmıştır. Bireylerin karşılaştığı en önemli sorunların başında %36 ile bilgi veya zaman kaybına neden olan virüs ve benzerleri gelmektedir. İstenmeyen e-postalar %32 ile ikinci sıradadır. İnternet kullanan bireylerin %58'i kişisel amaçla kullandığı bilgisayarlarını ya da verilerini korumak için bir güvenlik yazılımı veya aracı kullanmıştır.

Aynı şekilde sosyal ağların artması da internet üzerinden gelebilecek tehditleri arttırmaktadır. Kişisel verilerin internet üzerinden daha da kolay elde edilmesi, bu verilerin kullanılarak o kişiye ait internet üzerinden suç işlenmesine de olanak tanımaktadır.

Estonya örneğinde olduğu gibi ülkeler arasındaki savaş belki de siber suçlardan olacak ya da savaşlar siber savaşlar haline gelecektir!

KAYNAKÇA

[1] Internet Usage Statistics. http://www.internetworldstats.com/stats.htm.
[2] L.E. DeNardis, *The History of Internet Security.* Information Security Project. Yale University.

KRİTİK ALTYAPILAR

DÜNYA VE TÜRKİYE

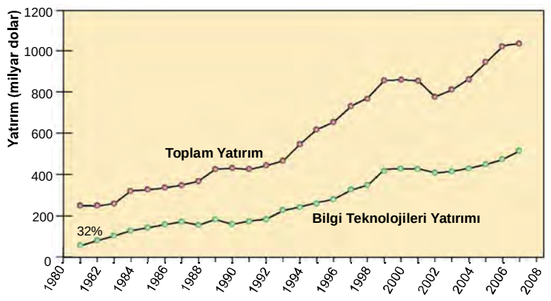
ÖZETİ

Bilge KARABACAK

Kritik altyapılar devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasından bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir. Kritik altyapıların korunması, gelişmiş ülkelerin önemli gündem maddelerinden birisi olarak karşımıza çıkmaktadır. Bu ülkeler, kritik altyapıların korunması ile ilgili yasal, teknik, idari, kurumsal ve dokümanter çalışmalarda ciddi yol almışlardır. Ülkemizde, bu konuda 2009 senesinde bazı resmi başlangıç çalışmaları yapılmıştır ancak Türkiye'nin önünde uzun bir yol olduğu söylenebilir. Makalede öncelikle anahtar kavramların tarihsel gelişimleri aktarılmış ve tanımlamaları yapılmıştır. Kritik altyapılar konusunda Dünya'da ve Türkiye'de yaşanan güvenlik olaylarına yer verilmiştir. Gelişmiş ülkelerin yaptığı çalışmalar ayrıntılı olarak aktarılmış, ülkemizde yapılan başlangıç çalışmaları hakkında bilgi verilmiştir. Makalenin son bölümünde, Türkiye'nin bu konuda atması gereken adımlara yer verilmiştir.

1. Giriş

Ülkelerin, kurumların, toplumların ve bireylerin bilgi ve iletişim teknolojilerine bağımlılığı gün geçtikçe artmaktadır. Amerikan Ticaret Bakanlığı'nın bir araştırması, gelişmiş ülkelerde, kurumların gerçekleştirdiği yatırımların yarısının bilgi ve iletişim teknolojilerine yapıldığını göstermektedir [1].



Bilgi ve iletişim teknolojilerin sağladığı birçok yararın yanı sıra bu teknolojiler ile birlikte yeni bir tehdit türü olan sayısal tehditler hayatımıza girmiştir. Sayısal tehditlerden korunmak için bireyler seviyesinden ülkeler seviyesine kadar alınması gereken karşı önlemler bulunmaktadır. Ülke seviyesinde gerçekleştirilmesi gereken önemli çalışmalardan birisi de, kritik altyapıların korunması (Critical Infrastructure Protection-CIP) konusudur. Bu kapsamda bir devlet politikası olarak belirlenen adımlar kamu kurumları ve özel şirketler tarafından gerçekleştirilmektedir. "Kritik altyapı" terimi ilk defa Ekim 1997 tarihli "Amerika Birleşik Devletleri Başkanlık Komisyonu'nun Kritik Altyapıların Korunması Hakkında Raporu"nda kullanılmıştır [2]. 192 sayfa ve 12 bölümden oluşan söz konusu raporda temel tanımlamalar ve durum analizi yapılmış, alınması gereken önlemler listelenmiştir.

Yeni bir kavramı tanıtmak amacıyla hazırlanan bu rapordan yedi ay sonra, 18 sayfalık "Başkanlık Karar Direktifi", dönemin Amerikan Başkanı Bill Clinton tarafından 22 Mayıs 1998 tarihinde imzalanmıştır [3]. Bu direktif, ABD'nin kritik altyapılarını işleten ve ulusal güvenlikten sorumlu tüm kamu kurumlarına gönderilmiştir. Söz konusu direktifte başkanın hedefi, ulusal hedefler, kritik altyapıların listesi, kurumların gerçekleştirmesi gereken adımlar, eşgüdüm ile ilgili hususlar, yeni yapılanmalar ve ulusal koordinatör ile ilgili bilgilere yer verilmiştir. Başkanlık karar direktifinde, silahlı kuvvetlerin ve ekonominin, kritik altyapılara ve sayısal sistemlere, artan bir hızla bağımlı olduğunun altı çizilmiştir. Kritik altyapılar, ekonominin ve hükümetin sağlıklı bir şekilde işlemesi için çok önemli fiziksel ve sayısal sistemler olarak tanımlanmıştır. Kritik altyapıların kamu kurumları veya özel sektör tarafından işletilebildiğinin altı çizilmiş, iletişim, enerji, bankacılık, ulaşım, su sistemleri ve acil durum servisleri örnek kritik altyapılar olarak zikredilmiştir. Geçmiş senelerde, kritik altyapıların fiziksel ve mantıksal olarak ayrı ve bu nedenle bağımlılığı olmayan sistemler olduğu belirtilmiş, bilgi teknolojilerindeki gelişmelerin hem altyapıların kendisini etkilediğini hem de altyapılar arasındaki ilişkileri ve bağımlılığı önemli bir biçimde belirtilmiştir.

Kritik altyapı kavramının ortaya çıkmasının en önemli nedeni bilgi teknolojilerinin yaygın bir şekilde kullanılmasıdır. Kritik altyapılar ve bilgi teknolojileri birçok yönden kesişmektedir. Bu kesişimler bilgi teknolojilerinin önemini çok açık bir biçimde göstermektedir. Bu önem, "kritik bilgi altyapıları" teriminin ortaya çıkmasına yol açmıştır. OECD, kritik bilgi altyapılarını, işlevini yitirmesi durumunda sağlık hizmetlerine, toplumsal emniyet ve güvenliğe, vatandaşların ekonomik refahına veya hükümetin/ekonominin verimli çalışmasını büyük ölçüde etkileyen bilgi ağları ve sistemleri olarak tanımlamaktadır [4]. Diğer taraftan, kritik bilgi altyapıları terimi ülkelerin ulusal politikalarında ve stratejilerinde daha az kullanılan bir terimdir.

İkinci bölümde, kritik altyapıların ve kritik bilgi altyapılarının daha ayrıntılı tanımları yapılmıştır. Üçüncü bölümde, kritik altyapılara yönelik olarak gerçekleştirilmiş sayısal saldırı olaylarına yer verilmiştir. Bu örnekler verilirken aynı zamanda kritik altyapılar, kritik bilgi altyapıları ve SCADA kavramları birbirleri ile ilişkilendirilmiştir. Dördüncü ve beşinci bölümde, sırasıyla kritik altyapıların korunması konusunda Dünya'da ve ülkemizde gerçekleştirilen çalışmalara yer verilmiştir. Altıncı bölümde, ülkemizde gerçekleştirilmesi gereken çalışmalar özetlemiştir. Makalenin yedinci bölümü sonuç bölümüdür.

2. Tanımlar

Kritik altyapılar devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasından bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir.

Günümüzde hemen hemen bütün kritik altyapılar, bilgi ve iletişim teknolojilerini az veya çok içermekte ve bu teknolojiler ile değişik şekillerde kesişmektedir [5]. Barajlar, enerji üretim ve dağıtım santralleri gibi kritik altyapılar bilgi teknolojileri tarafından kontrol edilmekte ve izlenmektedir. Telekomünikasyon gibi kritik altyapılar ise tümüyle bilgi ve iletişim teknolojilerinden oluşmaktadır. Giriş bölümünde de belirtildiği gibi, kritik altyapı kavramı bilgi ve iletişim teknolojilerindeki gelişmelerden sonra tanımlanmıştır. Bu tanımlamadan sonra, bilgi ve iletişim teknolojilerinin önemini vurgulamak amacıyla kritik bilgi altyapısı kavramı tanımlanmış ve kullanılmaya başlanmıştır. Kritik bilgi altyapıları,

a. Kritik altyapıları destekleyen bilgi ve iletişim teknolojilerinin unsurları olabilir;

b. Ulusal ekonomi ve devlet fonksiyonlarının düzgün işlemesi için gerekli bilgi ve iletişim teknolojilerinin altyapıları olabilir.

Bu genel kapsam OECD tarafından belirlenmiş bir çerçevedir [4]. Bu tanım şu şekilde örneklendirilebilir:

a. Telekomünikasyon altyapısı gibi kritik altyapılar tümüyle bilgi ve iletişim teknolojilerinden oluşurlar.

b. Enerji üretim ve dağıtım sistemleri, su ve kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesini sağlayan SCADA (Supervisory Control And Data Acquisition) sistemlerinin bir bölümü, bilgi ve iletişim teknolojilerinden oluşur.

c. Finans sistemi, güvenlik servisleri gibi kritik altyapılar bilgi ve iletişim teknolojilerini yoğun şekilde kullanırlar.

Üç farklı örnekte kendisine yer bulan tüm bilgi ve iletişim teknolojileri, "kritik bilgi altyapıları" olarak adlandırılmaktadır. Kritik bilgi altyapılarının da aslında bir kritik altyapı olduğu söylenebilir. İnternet de başlı başına bir kritik altyapı olarak değerlendirilmekte ve bu konuda bilimsel çalışmalar yapılmaktadır [6]. Özellikle son birkaç yıldır daha sık sözü edilmeye başlanan bulut bilgi işlem (Cloud Computing) ile birlikte hem veriye hem de uygulamalara erişim internet üzerinden gerçekleştirilebilmektedir [7]. Bu da internetin önemini artıran bir diğer etkendir.

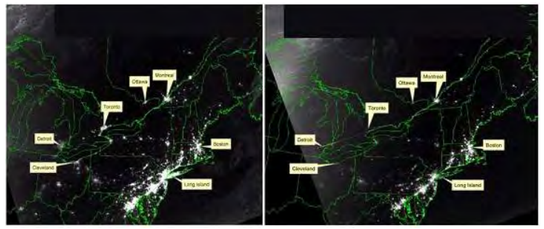
Kritik altyapılar arasında çok sayıda ve karmaşık bağımlılıklar, ilişkiler bulunmaktadır [8]. Bilgi ve iletişim teknolojileri bazı kritik altyapılar arasındaki bağımlılıkları başlatmış, var olan bazı bağımlılıkları ise önemli ölçüde artırmıştır. Örneğin barajlardaki bir arıza, elektrik üretiminin durmasına, elektrik üretimindeki problemler internet altyapısının işlevselliğinin bozulmasına neden olabilir. İnternetteki kesintiler ise başta bankacılık olmak üzere birçok kritik altyapıyı etkileyecektir. Bir sonraki bölümde kritik altyapıların bilgi ve iletişim teknolojileri ile kesişimi örnekler verilerek detaylandırılmıştır.

3. Örnekler ve İhlaller

Barajlar, termik santralleri, enerji dağıtım üniteleri gibi geçmişte tümüyle fiziksel unsurlardan ve bağıntısı olmayan endüstriyel kontrol sistemlerinden oluşan kritik altyapıların birçoğu günümüzde bilgi ve iletişim teknolojileri ile yönetilebilir ve izlenebilir duruma gelmiştir. Kritik altyapıların yönetimi ve izlenmesinde uzun yıllardan bu yana SCADA olarak adlandırılan endüstriyel kontrol sistemleri kullanılmaktadır [5]. Geçmişte, başka ağlar ile bağlantısı olmayan, bilgi ve iletişim teknolojileri içermeyen veya altyapıya özel olarak geliştirilmiş teknolojileri içeren SCADA sistemleri, günümüzde yaygın olarak kullanılan ve bilinen yazılım, donanım ve ağ protokollerini barındırmaya başlamıştır. Ayrıca, kritik altyapıları yöneten ve izleyen birçok SCADA sistemi kurumsal ağlara ve internete bağlantılı hale gelmeye başlamıştır [9].

Sonuç olarak, SCADA sistemleri sayısal savaşa ve sayısal terörist ataklarına çok daha fazla bir şekilde açık duruma gelmiş ve güvenlikleri geçmişe göre önemli biçimde sorgulanmaya başlamıştır [10], [11]. 2003 senesinde ABD'nin sekiz adet eyaletinde 50 milyon kişiyi etkileyen, bazı şehirlerde 2 gün süren, 11 kişinin ölümüne ve 6 milyar dolar zarara yol açan ve tarihe "2003 Northeast Blackout" olarak geçen ABD tarihinin en önemli elektrik kesintisinin nedenlerinden birisinin elektrik dağıtımında kullanılan yazılımdaki bir hatanın olduğu saptanmıştır.

Günümüz bilgi teknolojilerini kullanan örnek bir SCADA sistem tasarımı[1]



"2003 Northeast Blackout" uydu görüntüleri

Ekim 2003'de ABD'nin en yoğun limanlarından olan Houston Limanı'nın bilgisayar sistemi saldırıya uğramış ve limanın bir süre hizmet vermesi engellenmiştir. Saldırının İngiltere'nin Shaftesbury isimli küçük bir kasabasındaki bir bilgisayardan yapıldığı anlaşılmıştır. Ancak, bir süre sonra, bilgisayarın sahibinin suçsuz olduğu, bilgisayarın sayısal teröristlerin kontrolüne geçmiş bir zombi bilgisayar olduğu anlaşılmıştır. Bu olay sayısal teröristlerin ne derece profesyonel çalıştıklarını göstermektedir.

Rus bilgisayar korsanlarının Estonya'nın bilgi ve iletişim sistemlerine karşı gerçekleştirdiği sayısal saldırılarda, saldırı yapan bilgisayarların birçoğunun ABD'de ve ülkemizde olduğu tespit edilmiştir. Sayısal savaşlarda, bu örneklerde olduğu gibi zombi durumuna getirilmiş bilgisayarlar kullanılmaktadır. Zombi bilgisayarların kullanıcıları genellikle bilgisayarlarının başkaları tarafından kötü amaçla kullanıldığının farkına varacak bilgiye ve tecrübeye sahip değillerdir. Son örnek olarak, Ağustos

Houston Limanı

2003'te Ohio'da faaliyet gösteren, Davis-Besse nükleer santralinin izole bilgisayar ağına Slammer solucanı bulaşmış ve santralin izleme sistemini beş saat boyunca çalışamaz duruma getirmiştir. İnternet kaynaklı bilgisayar solucanlarının izole ağlara bulaşması, bu ağların ne derece izole olduğunun sorgulanmasına yol açmaktadır.

Ohio David-Besse Nükleer Santrali

ABD, etkin ve verimli kullanım için kritik altyapıları yöneten SCADA sistemlerini büyük oranda standartlaştırmış ve ortak ağlardan ulaşılabilir duruma getirmiştir. Bu nedenle verilmiş olan tüm örnekler, ABD'nin sahibi olduğu kritik altyapılar ile ilgilidir. Ancak, dünyadaki gelişmiş diğer ülkeler ile beraber ülkemizin de güncel teknolojiyi SCADA sistemlerine adapte etmeye başladığı söylenebilir. Adana ilindeki Sugözü Termik Santrali'nin bilgisayar sistemleri aracılığıyla 24 saat izlendiği, TÜBİTAK'ın desteği ile barajlar için Türkçe yazılım geliştirildiği, Akköprü Barajı'nın uydu bağlantılı bilgisayar sistemi ile yönetildiği, Batman Barajı'nın bilgisayarlarının Alman firması tarafından parasını alamadığı gerekçesiyle kilitlendiği medyada yer alan bazı haber başlıklarıdır. Bu haberlere yazılı basının internet arşivlerinden erişilebilir. Batman Barajı örneği, milli yazılımın önemini gösteren bir haber olarak dikkat çekmektedir.

Milliyet

Batman Barajı şifrelendi

Batman Barajı Hidroelektrik Santralı'nın yapımını üstlenen Alman Noel Şirketi, 1 milyon dolar alacağını tahsil edemediği gerekçesiyle şirketin bilsayarlarını şifre ile kilitleyip, kenti terketti. Şifreleme nedeniyle santralın üç ünitesinde de enerji üretimi durdu.

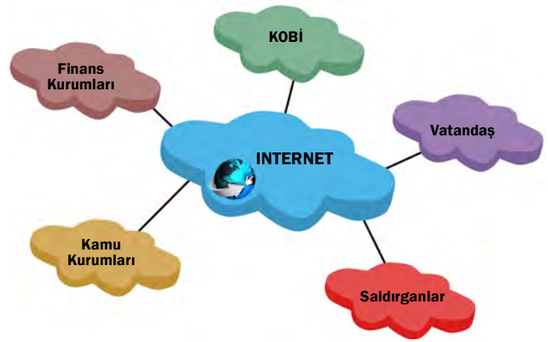
Bilgisayarların şifrelenerek kilitlenmesi nedeniyle Batman Barajı'nda enerji üretimi yapılamadığını söyleyen DSİ yetkilileri, bu nedenle Batman'ın bazı ilçeleri ile Şırnak ve Cizre'ye kesintili olarak elektrik verebildiklerini belirttiler.

Barajın yeniden elektrik üretimine başlaması için şifreyi çözmek üzere Türkiye Elektromekanik Sanayi uzmanları da yoğun çalışmalarını sürdürüyor. Uzmanlar bir yandan şifreyi çözmeye, bir yandan da Alman firması yetkililerine ulaşmaya çalışıyor.

Teknolojiyi çok hızlı bir şekilde adapte eden ve kullanan Türkiye, günümüzde en yeni teknoloji, kablosuz SCADA sistemlerini kullanmaya başlamıştır. Gazetelerde çıkmış olan haberler bu durumu doğrulamaktadır. Önümüzdeki yıllarda, ülkemizin sahip olduğu kritik altyapılarda daha yaygın şekilde son teknoloji SCADA sistemlerini kullanması kaçınılmazdır.

Telekomünikasyon altyapısı (sabit telefon ve cep telefonu operatörleri, internet altyapısı), e-devlet uygulamaları ve bankacılık gibi kritik altyapıların bilgi ve iletişim teknolojileri ile ilişkisi bir önceki paragrafta anlatılan kritik altyapılardan (barajlar, santraller v.b.) oldukça farklıdır. Bu tip kritik altyapılar çok büyük oranda bilgi ve iletişim teknolojilerinden oluşmaktadır, bazılarının varlık sebebi ise bilgi ve iletişim teknolojileridir.

2007 Nisan ve Mayıs aylarında, Rus bilgisayar korsanlarının Estonya bilgi sistemlerine sızması, bu sistemlerin faaliyetlerini durma noktasına getirmesi ve sonuç olarak Estonya'nın ekonomik ve toplumsal zararlar yaşaması birçok ülkenin gündeminde aylarca yer almıştır. Sayısal ataklardan dolayı Estonya hükümeti ülkenin bankacılık sisteminin, medyasının ve e-devlet hizmetlerinin kontrolünü hemen hemen kaybetmiştir. Estonya Savunma Bakanlığı 3 haftalık saldırı süresince, hükümetin faaliyetlerini yürütemediğini deklere etmiştir [12]. Bu örnek, bir ülkenin internet altyapısının önemli bir kritik altyapı olduğunu göstermektedir. Estonya'nın ekonomik ve toplumsal düzeninin sayısal saldırılardan etkilenmesinin en önemli nedeni bu ülkenin çok büyük bir oranda e-devlet yapısına geçmiş olması ve birçok kamu hizmetinin internet üzerinden gerçekleştirilmesidir. İlerleyen senelerde birçok ülke ve Türkiye en az Estonya kadar internete bağımlı hale gelecektir. Burada dikkat çeken diğer bir husus bir kritik altyapı olarak internetin sahip olduğu özel durumdur. İnternet, ülkelerin hayati fonksiyonlarının bağlı olabileceği bir kritik altyapıdır, internet aynı zamanda saldırganların da kullandığı ve yer aldığı bir ortamdır [6], [9].



Internet: Hem kritik altyapı hem de saldırganların bulunduğu ortam

Bir sıcak savaş senaryosu olarak bir ülkenin diğer ülkenin barajını bombalanması dünya konjonktüründe rahatlıkla yapılabilecek bir saldırı değilken, sayısal savaşçıların internet üzerinden barajın SCADA sistemine erişip barajın kapaklarını açması daha kolay yapılabilir. Diğer taraftan, internet üzerinden bir SCADA sisteminin kontrol altına alınması zor veya internet bağlantısı yoksa imkânsız olabilir. Bunun yerine kolay olduğundan ve hızlı sonuç verdiğinden dolayı ülkenin internet altyapısının öncelikle hedef alınması çok daha büyük bir ihtimaldir. Bir ülkenin internet çıkışını servis dışı bırakmak, e-devlet uygulamalarını hizmet veremez duruma getirmek, bankacılık ve borsa sistemlerini çalışmasını engellemek, ana yönlendirici (router) cihazlarını ele geçirmek, ülkenin en üst seviye DNS (Alan Adı Sistemi) sunucusunu ele geçirmek ve kritik servisleri yanlış internet sayfalarına yönlendirmek kolaylıkla yapılabilen, geçmişte sıklıkla yaşanmış ve Estonya gibi internete yüksek seviyede bağımlılığı olan ülkelerde ciddi ekonomik ve toplumsal sonuçları olmuş sayısal saldırı örnekleridir.

İMKB (İstanbul Menkul Kıymetler Borsası), Türkiye ekonomisi için büyük öneme sahip olan bir kritik altyapı olarak nitelendirilebilir. 29 Kasım 2007'de yol çalışması yapan bir kepçenin fiber kabloyu koparması sonucunda borsa ilk seansı gerçekleştirememiş ikinci seansa ise yarım saat geç başlamıştı. Borsanın işlem yapmaması her ne kadar bir sayısal saldırının sonucu olmasa da, bilgi teknolojisindeki bir arızanın ekonomik karşılığını görmek açısından önemli bir örnektir. 30 Ocak 2009'da birçok ülkenin bilgisayar sistemine yayılan ve önemli zararlar veren Conficker virüsü Atatürk Havalimanı'nın dış hatlar terminalinde çalışan bilgisayarları da etkilemiştir. Yaşanan aksaklıklardan dolayı birçok yolcunun bagajı işleme konamamış, uzun kuyruklar oluşmuştur. Her iki olayın ayrıntılarına gazete arşivlerinden ulaşılabilir.

Radikal

260 milyar dolarlık borsa bir kepçe darbesiyle çöktü

Yol yapım ve inşaat çalışmaları nedeniyle Türkiye dünyada eşi benzeri görülmeyen olaylara sahne oluyor. Geçen yıl bir inşaatın yapımı nedeniyle metronun tavanı delinirken, dün ise son dronemin gözde alışveriş merkezi İstinye Park'ın önündeki yolun genişletme çalışması İMKB'nin hayat damarını kopardı. Toplam 319 şirketin işlem gördüğü ve 260 milyar dolarlık (313 milyon YTL) toplam piyasa değerine sahip bulunan İMKB de böylece bir kepçenin ucuna takıldı.

Borsaya veri akışını sağlayan fiberoptik kabloların kopması yüzünden dün İMKB'de ilk seans gerçekleştirilemezken, Saat 14.00'te başlaması gereken seans ise 14.30'da başlayıp 17.30'da sona erdi.

HABER TÜRK

Atatürk Havalimanı'nda virüs kabusu

TÜBİTAK'ın uyardığı "downadup" adındaki "networm" virüsü Atatürk Havalimanı Dış Hatlar Terminali'ndeki sistemleri de etkiledi. Bilet ve bagaj işlemlerinin yapıldığı SITA-CUTE sistemleri bozulunca işlemler elle yapıldı. Birçok yolcunun bagajları havalimanında kaldı TAV, virüs nedeniyle sistem problemi yaşandığını doğruladı.

TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) bünyesinde faaliyet gösteren Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME), bilgi sistemlerinde hızla yayılan yeni bir solucanı "acil" koduyla bildirdi.

TR-BOME'den yapılan bildirimde, Microsoft'un 23 Ekim 2008'de Windows 2000, Windows XP ve Windows 2003 işletim sistemlerini etkileyen, çok acil olduğunu bildirdiği MS08-67 kodlu güncellemeyi yayınladığı belirtilerek, dünyada 15 milyon bilgisayara bulaştığı tahmin edilen "Confickr" isimli solucanın, bu güncellemenin uygulanmamış olduğu sistemlerde etkin olduğu bildirildi.

Solucanın son sürümü, zayıf şifrelere sahip kullanıcı hesaplarını, ağ üzerindeki paylaşımları ve solucanın bulaştığı bilgisayarlara takılan harici taşınabilir bellekleri kullanarak yayılıyor. Bu açıklamanın ardından önceki gün, virüsün İstanbul Atatürk Havalimanı Dış Hatlar Terminalinde biniş işlemlerinin yapıldığı SITA-CUTE sistemlerini etkilediği tespit edildi.

Bilgisayar güvenliği konusunda yazılımlar üreten ve hizmet veren Symantec firması tarafından hazırlanan Nisan 2009 tarihli İnternet Güvenliği Tehdit Raporu'nda Türkiye spam e-postanın kaynaklandığı ülkeler arasında Dünya'da üçüncü sırada yer almıştır. Spam e-postaların çoğunlukla başkalarının eline geçmiş zombi bilgisayarlar tarafından gönderildiği düşünülürse bu durum Türkiye'deki zombi bilgisayarların yoğunluğu hakkında bir fikir vermektedir. Firmanın 2007 senesinde yayınladığı raporda ise zombi bilgisayar sayısı dikkate alındığı zaman Ankara EMEA bölgesinde (Avrupa, Orta Doğu ve Afrika) yer alan şehirler içerisinde yedinci sırada yer almıştır. Aynı raporda, Ankara spam e-posta gönderen şehirler içerisinde altıncı sırada yer almıştır. Sonuç olarak, Türkiye sınırları içerisinde yer alan ve Türk vatandaşlarının kullandığı ancak zombi duruma gelmiş olan binlerce bilgisayar, kritik bilgi sistemi olarak tanımlanabilecek e-devlet uygulamalarımızı ve çoğunlukla özel sektörün işlettiği finans sistemlerini hedef alabilirler. Başka ülkelerin hükümetleri tarafından desteklenen sayısal teröristlerin kontrolünde olması uzak bir ihtimal olmayan bu bilgisayarlar olası bir sayısal savaşta başrol oynayacaklardır.

Tablo 1. Şehirlere göre köle bilgisayar sıralaması.

Bölgesel Sıra	Önceki Sıra	Şehir	Ülke
1	1	Madrid	İspanya
2	9	Petah Tiqwa	İsrail
3	7	Roma	İtalya
4	5	Milan	İtalya
5	2	Londra	İngiltere
6	3	Paris	Fransa
7	4	Ankara	Türkiye
8	8	Lizbon	Portekiz
9	6	Varşova	Polonya
10	12	Hayfa	İsrail

Tablo 2. En çok yığın (spam) e-posta gönderen şehirler.

Bölgesel Sıra	Önceki Sıra	Şehir	Ülke
1	1	Madrid	İspanya
2	4	Petah Tiqwa	İsrail
3	8	Milan	İtalya
4	6	Moskova	Rusya
5	-	İstanbul	Türkiye
6	3	Ankara	Türkiye
7	13	Budapeşte	Macaristan
8	10	Varşova	Polonya
9	15	Katowice	Polonya
10	21	Poznan	Polonya

Tablo 3. Ülke bazında zararlı faaliyetler.

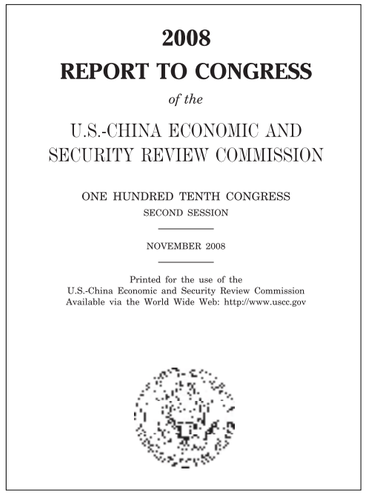
2008 Sırası	2007 Sırası	Ülke	2008 Yüzdesi	2007 Yüzdesi
1	1	ABD	%29	%45
2	8	Rusya	%6	%3
3	15	Türkiye	%5	%1
4	2	Çin	%4	%4
5	12	Brezilya	%4	%2
6	7	İngiltere	%3	%5
7	6	Almanya	%3	%3
8	9	İtalya	%3	%2
9	5	Polonya	%2	%3
10	10	İspanya	%2	%2

BABD'de bir hükümet kuruluşu olarak faaliyet gösteren ABD-Çin Ekonomik ve Güvenlik İnceleme Komisyonu'nun (USCC) 2008'de hazırladığı ve Amerikan Kongresi'ne sunduğu raporda çok çarpıcı ifadeler yer almaktadır [13]. Raporda yer alan bazı ifadeler şunlardır:

- Çin'in dünyanın herhangi bir yerine ve herhangi bir zamanda sayısal operasyon yapacak niyeti ve kabiliyeti bulunmaktadır.
- Çin'de 250 adet sayısal korsan grubu yer faaliyet göstermektedir. Bu gruplar Çin Hükümeti tarafından bilgisayar ağlarına girmesi ve zarar vermesi için desteklenmektedir.
- Çin Hükümeti aktif bir sayısal casusluk programını yürütmektedir.
- Çin'in sayısal savaş teknikleri ABD'nin karşı koyamayacağı hatta fark edemeyeceği kadar karmaşık ve ileri düzeydedir.

Tablo 4. En çok yığın (spam) e-posta gönderen ülkeler.

2008 Sırası	2007 Sırası	Ülke	2008 Yüzdesi	2007 Yüzdesi	Zararlı Kod Sırası	Spam E-posta Sırası	Yemleme Sitesi Sırası	Köle Bilgisayar Sırası	Saldırı Kaynağı Sırası
1	1	ABD	%23	%26	1	3	1	2	1
2	2	Çin	%9	%11	2	4	6	1	2
3	3	Almanya	%6	%7	12	2	2	4	4
4	4	İngiltere	%5	%4	4	10	5	9	3
5	8	Brezilya	%4	%3	16	1	16	5	9
6	6	İspanya	%4	%3	10	8	13	3	6
7	7	İtalya	%3	%3	11	6	14	6	8
8	5	Fransa	%3	%4	8	14	9	10	5
9	15	Türkiye	%3	%2	15	5	24	8	12
10	12	Polonya	%3	%2	23	9	8	7	17



2008

REPORT TO CONGRESS

of the

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ONE HUNDRED TENTH CONGRESS
SECOND SESSION

NOVEMBER 2008

Printed for the use of the
U.S.-China Economic and Security Review Commission
Available via the World Wide Web: http://www.uscc.gov

Güvenlik alanında faaliyet gösteren Northrop Grumman firması tarafından ABD-Çin Ekonomik ve Güvenlik İnceleme Komisyonu için hazırlanan 9 Ekim 2009 tarihli raporda ise Çin'in sayısal casusluk tehdidinin gün geçtikçe arttığı ifade edilmiştir. Raporda, 2007 senesi itibarıyla ABD devlet ve savunma birimlerinin ağlarına girilmesi sonucunda 10 ile 20 terabayt arası verinin dışarıya sızdırıldığı ifade edilmiştir [14].

Ülkemiz, henüz gelişmiş Avrupa ülkeleri ve özellikle ABD seviyesinde sayısal sistemlere geçmiş değildir. Ancak hızla bu yolda ilerlemektedir. ABD gibi uzun yıllardır sayısal güvenlik konusunda çok ciddi çalışmalar yapan ve bu konuya önem veren bir ülke bile sayısal saldırılara karşı çaresiz kalabilmektedir. Bu nedenle, ülkemizde bir devlet politikası olarak sayısal güvenlik benimsenmeli ve bu yönde ciddi çalışmalar başlatılmalıdır.

4. Dünya'da Gerçekleştirilen Çalışmalar

Hemen hemen tamamı aynı zamanda OECD üyesi olan gelişmiş ülkeler kritik altyapıların korunması ile ilgili olarak yasalarını düzenlenmiş, bu ülkelerde yeni kurumlar kurulmuş, hâlihazırdaki kurumlarda değişiklikler yapılmış, koordinatörler belirlenmiştir. Bu faaliyetler bizzat devlet başkanlarının direktifi ile başlatılmış ve himayesinde devam etmektedir. Bu ülkeler aynı zamanda devlet başkanı himayesinde ve bilgisinde hazırlanmış ulusal bilgi güvenliği siyasası belgesine sahiptirler. Söz konusu siyasa belgelerine de bakıldığı zaman kritik altyapı teriminin sıklıkla kullanıldığı görülmekte, sayısal savaşta öncelikli hedef olacak bu altyapıların etkilenmesi durumunda ülke ekonomisinin ve toplumsal düzenin ciddi zararlar göreceği belirtilmektedir. Kritik altyapıların korunması, ulusal seviyede bir güvenlik kültürünün oluşmasının temel etkenlerinden birisi olarak görülmektedir. Sonuç olarak, gelişmiş ülkeler kritik altyapıların korunması ile ilgili programını oluşturmuş ve bu program çerçevesinde çalışmalarını sürdürmektedir. Makalenin dördüncü bölümü altında yer alan alt bölümlerde bazı gelişmiş ülkelerin, Avrupa Birliği'nin, OECD'nin ve NATO'nun gerçekleştirdiği çalışmalara hakkında bilgi verilmiştir.

4.1. ABD'nin Gerçekleştirdiği Çalışmalar

ABD'nin başlatmış olduğu çalışmalara makalenin giriş kısmında yer verilmiştir. 2009'daki gelişmelerden bahsedilecek olursa; Amerikan Başkanı Barack Obama 9 Şubat 2009 günü, ulusal güvenlik yetkililerinden Amerika'nın sayısal ortamı için 60 günlük bir güvenlik gözden geçirmesi yapmalarını talep etmiştir. Gözden geçirme raporu Beyaz Saray'ın sayfasında yayınlanmıştır. Otuz bir defa "kritik altyapılar" ifadesinin kullanıldığı raporda, sayısal güvenlik konusunda tam yetkili koordinatörün atanması, "sayısal ortamın güvenliği için ulusal strateji"nin güncellenmesi gibi 10 adet maddenin yer aldığı yakın zamanlı bir eylem planı yer almıştır. Raporda ayrıca kritik altyapıların korunması konusunda gerçekleştirilmesi gereken adımlara yer verilmiştir. Sağlam ve esnek kritik altyapılar için kurumlar arası bilgi paylaşım yeteneklerini artırıcı yasal önlemlerin alınması gerektiği bildirilmiştir. Özel sektörün işlettiği kritik altyapıların korunması için hükümetin özel sektörle kamu-özel sektör ortaklıklarındaki rol ve sorumlulukları tanımlamak amacıyla çalışması gerektiği bildirilmiştir. Diğer taraftan Obama, 29 Mayıs 2009 günü Beyaz Saray'da yaptığı 15 dakikalık konuşmada Amerika'nın sayısal altyapısının güvenliğinin son derece önemli olduğunu belirtmiş ve konusu sayısal ortamda güvenlik olan bu konuşması basında geniş yankı bulmuştur. Konuşmanın metni Beyaz Saray'ın internet sayfasında yer almaktadır.

Yedi sene öncesine gidersek; Beyaz Saray Şubat 2003'te Sayısal Ortamın Güvenliği için Ulusal Strateji belgesini yayınlamıştır. Belge, ABD'nin sayısal savunma alanındaki faaliyetlerine ilişkin temel bir belgedir. Belgede kritik altyapıların korunması ile ilgili birçok husus da yer almaktadır. Bu belge, bilgi ve iletişim teknolojileri ile kritik altyapıları çok sıkı bir şekilde ilişkilendirmekte ve sayısal ortamın kritik altyapıların sinir sistemi olduğunu ifade etmektedir. Strateji belgesi, federal yönetimin, yerel makamların ve özel sektörün gerçekleştirmesi gereken aktiviteleri içeren ulusal nitelikte hazırlanmış bir belgedir. Belgede aynı zamanda kendi görev alanları itibarıyla öncü rol üstlenecek devlet kurumlarının

hangileri oldukları ve bu devlet kurumlarının rol ve sorumlulukları da belirtilmektedir. Sayısal Ortamın Güvenliği için Ulusal Strateji belgesinin Başkan Barack Obama'nın talep ettiği güvenlik gözden geçirmesi çerçevesinde güncellenmesi kararı alınmıştır. Strateji belgesinde ayrıca Anayurt Güvenliği Bakanlığı'na sayısal savunma konusunda önemli sorumluluklar verilmiştir. Strateji belgesi, Temmuz 2002'de yayınlanan Anayurt Güvenliği için Ulusal Strateji belgesinin uygulama boyutunu oluşturmaktadır. Anayurt Güvenliği için Ulusal Strateji belgesi Beyaz Saray tarafından hazırlanmış, Amerikan Başkanı tarafından imzalanmış ve 2002 Temmuz ayında yayınlanmıştır. Bu dokümanda, özel sektörün rolü, altyapıların direnci, kritik altyapılara yapılacak atakların engellenmesi, koruyucu önlemler alınması ve olaydan geri dönüş kabiliyetleri gibi hususlar yer almaktadır. Strateji belgesi aynı zamanda Kritik Altyapıların Fiziksel Korunması için Ulusal Strateji belgesini de tamamlayıcı niteliktedir. 2002 yılında çıkartılan anayurt güvenliği kanunu ile Anayurt Güvenliği Bakanlığı kritik altyapıların korunması ile ilgili ulusal çalışmaları bilgi ve iletişim teknolojilerini de kapsayacak şekilde hem kamu sektörü hem de özel sektör kapsamında koordine etmekten sorumlu olmuştur. Bakanlık bünyesinde Ulusal Siber Güvenlik Birimi bulunmaktadır.

THE WHITE HOUSE
Office of the Press Secretary

For Immediate Release May 29, 2009

REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE
East Room

11:08 A.M. EDT

THE PRESIDENT: Everybody, please be seated. We meet today at a transformational moment -- a moment in history when our interconnected world presents us, at once, with great promise but also great peril.

Now, over the past four months my administration has taken decisive steps to seize the promise and confront these perils. We're working to recover from a global recession while laying a new foundation for lasting prosperity. We're strengthening our armed forces as they fight two wars, at the same time we're renewing American leadership to confront unconventional challenges, from nuclear proliferation to terrorism, from climate change to pandemic disease. And we're bringing to government -- and to this White House -- unprecedented transparency and accountability and new ways for Americans to participate in their democracy.

But none of this progress would be possible, and none of these 21st century challenges can be fully met, without America's digital infrastructure -- the backbone that underpins a prosperous economy and a strong military and an open and efficient government. Without that foundation we can't get the job done.

It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives.

It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history.

So cyberspace is real. And so are the risks that come with it.

It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox -- seen and unseen -- is something that we experience every day.

It's about the privacy and the economic security of American families. We rely on the Internet to pay our bills, to bank, to shop, to file our taxes. But we've had to learn a whole new vocabulary just to stay ahead of the cyber criminals who would do us harm -- spyware and malware and spoofing and phishing and botnets. Millions of Americans have been victimized, their privacy violated, their identities stolen, their lives upended, and their wallets emptied. According to one survey, in the past two years alone cyber crime has cost Americans more than $8 billion.

4.6. Avrupa Birliği'nin Gerçekleştirdiği Çalışmalar

Avrupa Birliği kritik altyapıların korunması ile ilgili ilk adımı 2004 senesinde atmıştır. Bu kapsamda, 2004 Haziran ayında Avrupa Konseyi'nden gelen talep doğrultusunda Avrupa Komisyonu 20 Ekim 2004'de "Terörle Mücadele için Kritik Altyapı Korunması" başlıklı bir belge yayınlamış ve bu belgeyi Avrupa Konseyi ve Avrupa Parlamentosu'na göndermiştir. Hazırlanan 11 sayfalık belgede, kritik altyapıların tanımı yapılmış, tehditler tanımlanmış ve bu konuda yapılması gereken çalışmalar özetlenmiştir. Bu raporun ardından, "Kritik Altyapıların Korunması için Avrupa Programı-EPCIP" başlıklı bir program açılmıştır.

17 Kasım 2005'te Avrupa Komisyonu EPCIP'in kurulması ile ilgili politika unsurlarının yer aldığı dokümanı yayınladı. Nisan 2007'de, Avrupa Konseyi üye ülkelerin kendi sınırları içerisindeki kritik altyapıları korumaktan sorumlu olduğunu belirterek EPCIP'ın tamamlandığını duyurdu. Bu tarihten sonra, Avrupa Komisyonu Avrupa'daki kritik altyapıların belirlenmesi ve saldırılara karşı korunması ile ilgili prosedür geliştirmeye başladı. Prosedür tamamlandıktan sonra Avrupa Konseyi'nin 2008/114/EC kodlu direktifi yayınladı. Direktif, bilgi ve iletişim teknolojilerini göz ardı etmeyen ancak enerji ve taşımacılık sektörlerine ağırlık veren bir direktif olarak yayınlandı. Kritik altyapılar korunması konusunda hazırlanan son doküman 30 Mart 2009'da yayınlanmıştır. Doküman Avrupa Komisyonu tarafından hazırlanmıştır.

4.7. OECD'nin Gerçekleştirdiği Çalışmalar

OECD bünyesinde faaliyet gösteren Bilginin Güvenliği ve Mahremiyeti Çalışma grubu kritik bilgi altyapılarının korunması ile ilgili üye ülkelere yol gösterecek dokümanlar hazırlamaktadır. Söz konusu çalışma grubu "Kritik Bilgi Altyapılarının Korunması Hususunda Konsey Tavsiyeleri" başlıklı dokümanı Ocak 2008'de hazırlamıştır [4]. Avrupa Komisyonu, çalışmalarında bu dokümandan faydalanmıştır. OECD'nin bu dokümanı kritik bilgi altyapılarının korunması ile ilgili hem üye ülkelere hem de dünyadaki diğer ülkelere kılavuzluk yapmak amacıyla hazırlanmıştır. Dokümanda yer alan tavsiyeler iki ana gruba bölünmüştür. Birinci grup ülkelerin kendi sınırları içerisinde kalan kritik bilgi altyapılarının korunması ile ilgili tavsiyeleri içermektedir. İkinci grup ise ülkeler arası koordinasyon hususlarını içermektedir. Böylelikle doküman hem ulusal politikalar için hem de uluslar arası işbirliği için kılavuzluk yapmaktadır. Bu doküman, yedi OECD üyesi ülkenin kritik bilgi altyapıları konusunda yapmış olduğu çalışmaların karşılaştırmalı çalışmasında yer alan iyi pratiklerden üretilmiştir. Bu ülkeler Avustralya, Kanada, Kore, Japonya, Hollanda, İngiltere ve ABD'dir.

OECD Bilgi Güvenliği ve Mahremiyeti Çalışma Grubu üyelik için başvuran ülkelerden temel bilgi güvenliği pratiklerinin uygulanmasını zorunlu tutmaktadır. Bilgi güvenliği pratikleri

içerisinde kritik bilgi altyapılarının korunması da yer almaktadır. OECD'nin kurucu ülkesi olarak Türkiye'nin kritik bilgi altyapılarının korunması ile ilgili hususlara uyumu yoktur. Kritik bilgi altyapılarının korunması ile ilgili aday ülkelerin cevaplaması talep edilen sorular aşağıda listelenmiştir:

- Hükümetiniz kritik bilgi altyapılarının korunması ile ilgili bir siyasa ve strateji oluşturdu mu?
- Hükümetiniz kritik bilgi altyapılarının kamu, özel sektör ve bireyler nezdinde korunması konusunda liderlik ve katılım gösteriyor mu?
- Hükümetiniz kritik bilgi altyapılarının korunması ile ilgili rol ve sorumlulukları belirleyip atamaları yaptı mı?
- Hükümetiniz kritik bilgi altyapılarının korunması ile ilgili değişik yönleri içine alan bir yönetim yapısı oluşturdu mu?
- Hükümetiniz kritik bilgi altyapılarının korunması ile ilgili kamu kurumlarını, özel sektörü ve bireyleri kapsayan bir bilinçlendirme ve eğitim faaliyeti uyguluyor mu?

4.8. NATO'nun Gerçekleştirdiği Çalışmalar

NATO da OECD gibi kritik altyapılardan ziyade kritik bilgi altyapılarına yönelik çalışmalar yapmaktadır. NATO, kendi bilgi sistemlerini kritik bilgi altyapısı olarak değerlendirmekte ve bununla ilgili özellikle Estonya'ya yapılan saldırılardan sonra ciddi çalışmalar yapmaktadır. NATO bilgi sistemlerine karşı yapılan sayısal ataklar ilk defa 1990'ların sonunda NATO'nun balkanlara yaptığı operasyonlar sırasında raporlanmıştır. Bundan sonra, birçok güvenlik olayı NATO web sitelerinin içeriğinin değiştirilmesi ve e-posta sunucularını ele geçirilmesi şeklinde gerçekleşmiştir. Ayrıca, NATO bilgi sistemleri kapsamındaki sayısal iletişimlerin kontrol altına alınması, operasyonel servislerin kesintiye uğratılması çok ciddi kaygılar uyandırmıştır.

Sonuç olarak, 2002 yılındaki Prag Zirvesinde, NATO üyesi ülkelerin devlet başkanları "NATO bilgi sistemlerinin sayısal ataklara karşı savunma yeteneklerinin güçlendirilmesi" konusundaki deklarasyona imza attılar.

2002'deki Prag zirvesinde imzalanan deklarasyon birliğin sayısal güvenlik ile ilgili durumunu geliştirici bazı dahili NATO aktivitelerinin başlatılmasını sağlamıştır. En önemli ve kapsamlı çalışma NATO Bilgisayar Olaylarına Müdahale Yeteneği kurulması (NCIRC Computer incident response capability) projesinin 2003 senesinde başlatılmasıdır. NCIRC, 2006 senesinden bu yana faaliyet göstermekte; NATO bilgisayar ağlarına yönelik sayısal ataklara müdahale etmektedir.

2007 senesine kadar, NATO sayısal savunma konusunda resmi bir siyasa belgesine sahip değildi. Sonuç olarak sayısal savunma konusunda özelleşmiş bir kılavuz doküman bulunmuyordu. Böyle bir resmi siyasa belgesinin yokluğunda, NATO'nun kendi sayısal savunması, NATO'nun Güvenlik Siyasası'nın bir parçası olarak ele alınıyor ve sadece teknik ve bilgisayar ağlarının yönetimi ile ilgili bir konu olarak görülüyordu.

Nisan ve Mayıs 2007'de Estonya bilgi sistemlerine karşı gerçekleştirilen sayısal ataklar sonucunda sayısal savunmanın tüm ülkeyi ilgilendirdiği ve ulusal bir konu olduğu görülmüştür. Bu nedenle, konunun siyasa ve stratejik seviyede de ele alınması gerektiği ortaya çıkmıştır. 2007'de Estonya bilgi sistemlerine yönelik gerçekleştirilen sayısal ataklardan sonra, NATO'ya üye ülkeler olayın değerlendirmesine yapmak üzere bir araya gelmeye ve NATO'nun sayısal savunma yeteneklerini artırmak için gerekli adımları atmaya karar vermişlerdir.

Bu kapsamda, 20 Aralık 2007'de "NATO sayısal savunma siyasa" belgesi yayınlanmıştır. 17 Nisan 2008 ise " NATO sayısal savunma yönetim otoritesi – CDMA kurulmuştur. 2009 senesi başında, CDMA için operasyon konsepti (Concept of Operations - CONOPS) geliştirilmiş ve kabul edilmiştir.

NATO'da yeni yaklaşım doğrudan teknik ve operasyonel desteğin sağlanmasını da içermektedir. NATO sayısal savunma hızlı reaksiyon takımının sayısal ataklara maruz kalan üye ülkeye ülkenin talep etmesi durumunda gönderilmesi buna bir örnek olarak verilebilir.

NATO'nun sayısal savunma yeteneğinin asıl sorumluluğu görevleri desteklemek için NATO tarafından işletilen bilgisayar ağlarını korumaktır. NATO şu an, eğer sayısal atak altında ise üye ülkeyi korumakla ve ülkeye yardım teklif etmekle yükümlüdür [12].

5. Ülkemizde Gerçekleştirilen Çalışmalar

Estonya bilgi sistemlerine Rus bilgisayar korsanları tarafından Nisan ve Mayıs 2007'de gerçekleştirilen koordine ataklardan sonra hazırlanan "NATO sayısal savunma siyasa" belgesine göre NATO üyesi ülkeler, CDMA'ya ulusal temas noktalarını bildirmişlerdir. Yine NATO Sayısal Savunma Konsepti'ne göre NATO üyesi ülkeler ulusal sayısal ortam savunma politikalarını hazırlamaya başlamışlardır. Dışişleri Bakanlığımız TÜBİTAK-UEKAE'yi (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) NATO'ya ulusal temas noktası olarak bildirmiştir. NATO'nun sayısal ortam güvenlik politikası hazırlanması talebi Dışişleri Bakanlığı tarafından Başbakanlık'a iletilmiş, Başbakanlık Mayıs 2008'te söz konusu politikanın UEKAE koordinasyonunda hazırlanmasını resmen talep etmiştir. Politika dokümanı UEKAE ile birlikte 19 adet kamu kurumunun katılımı ile hazırlanmıştır. Bu kurumlar, Cumhurbaşkanlığı, Başbakanlık, Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Adalet Bakanlığı, Milli Savunma Bakanlığı, Maliye Bakanlığı, Ulaştırma Bakanlığı, İçişleri Bakanlığı, Devlet Planlama Teşkilatı Müsteşarlığı, Dış Ticaret Müsteşarlığı, Hazine Müsteşarlığı, Merkez Bankası, Milli Güvenlik Kurulu Genel Sekreterliği, Milli İstihbarat Teşkilatı Müsteşarlığı, Bankacılık Düzenleme ve Denetleme Kurumu, Emniyet Genel Müdürlüğü ve Bilgi Teknolojileri ve İletişim Kurumu'dur. Politika belgesi hazırlanması çalışmalarına katılacak kurum listesi, Başbakanlık tarafından koordinatör kurum olarak UEKAE'ye bildirilmiştir. Politika dokümanı, Temmuz 2008 – Kasım 2008 ayları arasında hazırlanmış; bu sürede tüm kurumların katıldığı üç adet toplantı gerçekleştirilmiştir. Hazırlanan politika dokümanı beş sayfadan oluşmaktadır. Üçüncü toplantının ardından, politika belgesinde son düzenlemeler yapılmış, katılımcı kamu kurumlarının çoğunluğunun onayı ile belge Başbakanlık'a Ocak 2009'da resmi olarak teslim edilmiştir. Halihazırda, Başbakanlık'ın belgeyi onaylaması beklenmektedir. Ülkemizde kritik altyapıların güvenliği ile ilgili atılmış ilk adım bu politika belgesidir. Politika belgesinde "Kritik bilgi ve iletişim sistem altyapılarının güvenliği sağlanmalıdır. Ülke içerisindeki kritik bilgi ve iletişim sistem altyapıları, bunların birbirleriyle ilişkileri, kritiklik seviyeleri ve sorumluları tespit edilmelidir. Tespit edilen kritik bilgi ve iletişim sistem altyapıları sanal ortamdan gelebilecek tehditlere karşı korunmalıdır" ifadeleri yer almaktadır.

Ülkemizde kritik altyapılar ile ilgili daha yakın bir gelişme 2009 Sonbaharı'nda gerçekleşmiştir. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü bünyesinde oluşturulan ve çalışmalarına fiilen 3 Mart 2009 tarihinde başlayan e-Mevzuat Çalışma grubu, 7 Ağustos 2009 tarihi itibarıyla "e-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı"nı hazırlamıştır. E-devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı'nda kritik altyapı ve kritik bilgi altyapısı terimleri geçmemektedir. Bununla beraber taslak içerisinde "Kritik Bilgi Sistemi"nin tanımı "İşlevlerinin tamamen veya kısmen yerine getirilememesi halinde kamu güvenliği ve düzenini önemli derecede etkileyen bilgi sistemleri" olarak tanımlanmıştır. Kanunda geçen "Bilgi Toplumu Ajansı" içerisindeki "Bilgi Toplumu Dairesi"nin görevlerinden bir tanesi de "kritik bilgi sistemlerini belirlemek ve bu sistemler için uygulanacak asgari güvenlik standartlarını tespit etmek" şeklinde belirtilmiştir.

Bu iki taslak çalışma dışında ülkemizde kritik altyapılar konusunda resmi bir çalışma bulunmamaktadır. İkinci taslak çalışmanın 2010 Ocak ayı içerisinde rafa kaldırıldığı ile ilgili haberler internet sitelerinde yer almıştır. Sonuç olarak, Türkiye kritik altyapıların korunması ile ilgili çalışmaların henüz başındadır.

6. Ülkemizde Yapılması Gereken Çalışmalar

Kritik altyapıların korunması ile ilgili olarak gelişmiş ülkelerde olduğu gibi ülkemizde de resmi çalışmaların başlatılması gerekmektedir. Resmi çalışmaların ana çerçevesinin sayısal güvenlik olması ve kritik altyapıların korunmasının bu ana çerçevenin bir alt maddesi olması bazı gelişmiş ülkelerin izlediği ve ülkemize de uygun bir yapıdır. Bu kapsamda:

Ulusal Sanal Ortam Güvenlik Politikası'nın resmiyet ve işlerlik kazanması gerekmektedir. Bu politika belgesini takip eden strateji belgesinin ve eylem planının da hazırlanması sıradaki önemli adımlardır. Bütün bu belgeler için destekleyici mevzuat hazırlanmalı, güncellenmesi ve değiştirilmesi gereken halihazırdaki mevzuat tespit edilmeli ve değişiklikler yapılmalıdır.

Sayısal savunma ile ilgili çalışmaları organize edecek bir ulusal yürütme organı oluşturulmalıdır. Yürütme organının asıl sorumluluğu koordinasyon olmalıdır. Kritik altyapıları işleten kamu sektörüne ve özel sektöre yapılması gereken çalışmaları bildirmelidir. Yürütme organı, devletin belirlediği politikaları uygulatan bir kurum olmalıdır.

Sayısal savunma ve kritik altyapıların korunması ile ilgili ulusal bilincin oluşturulması adına çalışmalar gerçekleştirilmelidir. Kritik altyapıları işleten kurumların gerçekleştirmesi gereken çalışmalardan vatandaşın yapması ve yapmaması gerekenlere kadar birçok konuyu kapsayan bilinçlendirme programı için ulusal medya, internet siteleri gibi kaynaklar kullanılmalıdır.

Sayısal ihlallere karşı tepki yeteneği geliştirmek amacıyla ulusal bilgisayar olaylarına müdahale ekibinin yetenekleri geliştirilmelidir. Kritik altyapıları işleten kurumlar da etkin bilgisayar olaylarına müdahale ekiplerini oluşturulmalıdırlar. Ayrıca farklı bilgisayar olaylarına müdahale ekipleri arasında koordinasyon yeteneği oluşturulmalıdır.

İnternet altyapısının güçlü ve alternatifli bir duruma getirilmesi dağıtık servis dışı bırakma saldırılarından en az seviyede zarar görmek için gereklidir. Telekomünikasyon altyapısı ve internet önemli kritik altyapılardır. Bu bağlamda, internet servis sağlayıcıları ile koordinasyon diğer önemli bir husustur.

Son olarak, ülkemiz sayısal savaş konusunda uluslararası işbirliğine önem vermelidir. Gelişmiş ülkeler ve OECD, NATO gibi organizasyonlar sayısal güvenlik ve sayısal savunma konusunda oldukça fazla yol almışlardır. Türkiye bu tecrübelerden faydalanmalıdır. Tüm dünyayı içine alan ve sınırları olmayan devasa bir ağ durumundaki internet sayısal saldırıların da kaynağıdır. Ülkemiz bilgi

sistemlerine yapılacak bir sayısal saldırının kaynağı herhangi bir ülkedeki bilgisayarlardan kaynaklanabilir. Uluslar arası işbirliğinin önemi saldırılara karşı önlem alma noktasında önemli bir diğer husustur.

Bu bölüm iki farklı listeden oluşmaktadır. İlk liste, Türkiye'nin atması gereken öncelikli teknik olmayan prosedürel adımlardan oluşmaktadır. İkinci liste ise daha teknik adımlardan oluşan bir listedir. İlk numaralandırılmış listedeki adımlara tamamlanmadan ikinci listedeki adımların başarısızlıkla sonuçlanması kaçınılmazdır [15]. Her iki liste de gelişmiş ülkelerin ve uluslararası organizasyonların hazırlamış oldukları kılavuz dokümanlardan faydalanılarak hazırlanmıştır.

6.1. Türkiye'nin Gerçekleştirmesi Gereken Temel Adımlar

- Üst seviye yürütmeden (Örn: Başbakanlık) destek ve katılım
- Destekleyen mevzuatın hazırlanması ve yürürlüğe girmesi
- Ulusal Sanal Ortam Güvenlik Politikası'nın resmiyet kazanması
- Ulusal Sanal Ortam Güvenlik Stratejisinin ve Eylem Planı'nın hazırlanması (Politika belgesinin resmiyet kazanmasının ardından)
- Kritik altyapıların korunması ile ilgili politika belgesi hazırlanması
- Çalışmalar için yeterli seviyede bütçe ayrılması

6.2. Temel Adımların Ardından Gerçekleştirilmesi Gereken Çalışmalar

Bu başlık altındaki adımların başarıyla tamamlanması için gerekli öncül çalışmalar bir önceki başlıkta listelenmiştir. Bir önceki başlıkta listelenen adımlar gerçekleştirilmediği takdirde, aşağıdaki adımlar kapsamında çalışmaya başlanılsa bile çalışmanın sonuçlandırılması oldukça güçtür [15].

- Özel sektör ile iş birliği ve koordinasyon
- Kritik altyapılar ile ilgili çalışmaları koordine edecek bir merkezin kurulması
- Rol ve sorumlulukların belirlenmesi ve atanması
- Kritik altyapıların ve aralarındaki bağımlılıkların belirlenmesi için ülke çapında risk analizi yapılması
- OECD ilkelerine uyumun sağlanması
- Bilgi paylaşımı için hükümet ile kritik altyapı işleticileri (özel veya kamu) arasında ortaklık kurulması
- Açıklıkları belirlemek ve önlem almak için periyodik güvenlik testleri ve tatbikatlar düzenlenmesi
- Güvenle sayısallaşmış bir ulusun bilgi ve bilinç seviyesini artırmak için eğitim ve bilinçlendirme faaliyetleri düzenlenmesi
- Diğer ülkeler ve uluslar arası organizasyonlarla iş birlikleri geliştirilmesi
- Araştırma ve geliştirme faaliyetlerinin desteklenmesi
- Güçlü ve ülke çapında faaliyet gösteren Bilgisayar Olaylarına Müdahale Ekibi (BOME)
- Güçlü ve alternatifli internet altyapısının oluşturulması
- İnternet servis sağlayıcılarının etkin yönetimi ve koordinasyonu [12]

7. Sonuç

Makalede öncelikle, Türkiye için yeni bir kavram olan kritik altyapılar konusunda bilgilendirme yapılmış, kritik altyapıların bilgi ve iletişim teknolojileri ile ilişkisi ve bu teknolojilere bağımlılığı örnekler ile gösterilmiştir. Makalede ayrıca, gelişmiş ülkelerin ve organizasyonların bu konuda yaptığı çalışmalar özetlenmiştir.

Her ülkenin olduğu gibi ülkemizin de bilgi ve iletişim teknolojileri ile kesişimi olan kritik altyapıları bulunmaktadır. Ancak, ülkemizde kritik altyapıların korunması konusunda resmi bir programı bulunmamaktadır. Ülkemizde kritik altyapıların korunması ile ilgili bir program başlatılması ve bunu destekleyen yasal altyapının oluşturulması gerekmektedir. Ülkemizin de üyesi olduğu OECD ve NATO'nun bu konudaki çalışmaları ve işbirliği fırsatları uzmanların göz ardı etmemesi gereken hususlardır.

Diğer taraftan, makalede yer verilen sayısal saldırıların başarıya ulaşmış olmasının en önemli nedeninin yönetimi sağlıklı bir şekilde yapılmayan bilgi ve iletişim teknolojileridir. Kritik altyapıların güvenliğinin sağlanmasında insan faktörü ve güvenlik bilinci en önemli parametrelerin başında gelmektedir. Bilgi ve iletişim sistemlerinin güvenlik hedefleri göz önüne alınarak yönetilmesi ve temel güvenlik önlemlerinin alınması durumunda sayısal güvenliğin büyük oranda sağlanacağı ve sistemlerin sayısal saldırılara karşı korunaklı duruma geleceği şüphesizdir.

KAYNAKÇA

[1] U.S. Department of Commerce, Bureau of Economic Analysis, "National Income and Product Accounts", 2008.

[2] The Report of the President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, 1997

[3] USA Presidential Decision Directive/NCS-63, "http://www.fas.org/irp/offdocs/pdd/pdd-63.htm", 1998 (18 Şubat 2010'da erişildi)

[4] OECD, Working Party on Information Security and Privacy, "Recommendations of the Council on the Protection of Critical Information Infrastructures", Ocak 2008

[5] Jayawickrama, W., "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001", Book Chapter: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Cilt 4277/2006, s. 565-574, 2006

[6] Beltran F., Fontenay A., Alameida M. W., "Internet as a critical infrastructure: lessons from the backbone experience in South America", Communications & Strategies, No. 58, 2005

[7] Mathat T., Kumaraswamy S., Latif S., "Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance", O'reilly, 2009

[8] Lewis T. G., "Critical Infrastructure Protection In Homeland Security - Defending A Networked Nation", A John Wiley & Sons, Inc., Publication, 2006

[9] Fischer W., Lepperhoff N., "Can Critical Infrastructure rely on the Internet", Computers & Security, Cilt. 24, s. 485-491, 2005

[10] Shea D. A., "Report for Congress, Critical Infrastructure: Control Systems and the Terrorist Threat", 2003

[11] Lemos R., "SCADA system makers pushed toward security". SecurityFocus. http://www.securityfocus.com/news/11402, 2006 (18 Şubat 2010'da erişildi)

[12] Anıl Süleyman, Cyber Security in NATO and Nations, Cyber Warfare Symposium, 10 December 2009, Ankara

[13] USCC 2008 Annual Report, 2008 Report to Congress of the U.S.-China Economic and Security Review Commission, Kasım 2008

[14] Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Prepared for The US-China Economic and Security Review Commission, Ekim 2009

[15] Karabacak B., Özkan S., "Critical Infrastructure Protection Status and Action Items of Turkey", International Conference on eGovernment Sharing Experiences, eGovShare2009, 8-11 December 2009, Antalya

Kurumsal bilgi güvenliğine ışık tutan standartlar

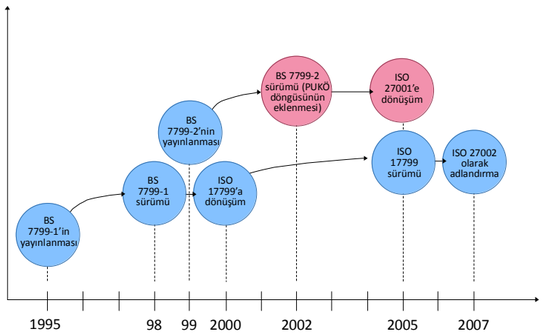
Fikret OTTEKİN

1. Giriş

Günümüzde bilginin hem kişiler için, hem kurumlar için en büyük sermaye durumuna geldiği bir gerçektir. Bilginin doğru şekilde kullanılması, doğru zamanda doğru ellerde bulunması için çok sayıda yaklaşım geliştirilmiş [1], yurdumuz da içinde olmak üzere dünyanın pek çok yerinde kurumsal iş süreçlerinin bu yaklaşımlar uyarınca tanımlanması için yüksek düzeyde işgücü harcanmıştır. Bu çabanın kökeninde kurumsal verimliliği arttırma düşüncesi olduğu gibi, müşteri beklentisi, yasal yükümlülükler ve benzeri etmenlerin de bulunabildiğini görüyoruz.

Sözü edilen yaklaşımlar bilginin etkinlik, verimlilik, gizlilik, bütünlük, erişilebilirlik, uygunluk ve güvenilirlik yönlerinin bir veya birkaçı ile ilgili olarak yapılabilecek düzenlemeleri tanımlamaktadır. COBIT, COSO, ITIL, CMMI bilginin yönetilmesi ile ilgili olarak akla gelen ilk yaklaşımlardır.

ISO 27001 standardı ise bilgi güvenliğine, yani bilginin gizlilik, bütünlük ve erişilebilirliğine odaklanmıştır. Makalemizde bu standardın (ISO 27001:2005) ve eki durumundaki ISO 27002:2005 standardının kurumsal bilgi güvenliğindeki yerini ve birbirleri ile ilişkilerini açıklamaya çalışacağız. Standartların geçmişine baktığımızda, "British Standards Institute (BSI)" tarafından hazırlandıklarını, daha sonra "International Standards Organization (ISO)" tarafından uluslararası standart olarak benimsendiklerini görüyoruz (Şekil 1).



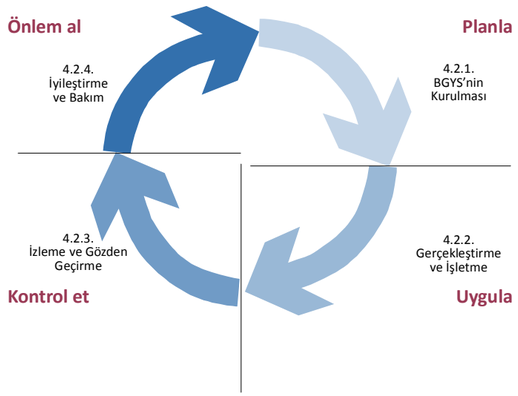
Şekil 1. *ISO 27001 ve 27002 standartlarının tarihsel gelişimi.*

2. ISO 27001 Standardı

ISO 27001 standardı, yaşayan bir bilgi güvenliği sistemi kapsamında gerçekleştirilmesi gereken işlevleri tanımlar. "Yaşayan sistem" ile demek istenen, kurumdaki bilgi güvenliği sürecinin değişen dünyaya ve gereksinimlere, tehdit ve saldırılara karşılık verme, kendini yenileme ve hatalarını düzeltme yeteneklerine sahip olmasıdır.

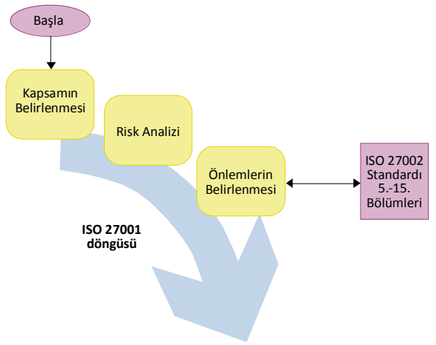
ISO 27001'de tanımlanan yaklaşıma göre, bilgi güvenliğinin bir süreç olarak gerçekleştirilmesi ve sürecin planlama, uygulama, kontrol etme ve önlem alma adımlarından oluşan bir döngü şeklinde çalıştırılması gerekir [2]. Yaşayan bir bilgi güvenliği sistemi ancak PUKÖ döngünün çalıştırılması ile mümkün olabilir (Şekil 2). Türkçe kaynaklarda Planla – Uygula – Kontrol Et – Önlem Al sözcüklerinin kısaltması olarak yerleşmiş PUKÖ'nün aslı İngilizce Plan – Do – Check - Act deyimidir. Planla – Uygula – Denetle – Düzelt çevirisinin daha uygun olduğu kanısında olsak da makale boyunca klasik çeviriye sadık kalacağız.

PUKÖ döngüsünün bilgi güvenliği sürecine özgü olmadığını, akvaryum temizliğinden pizza pişirmeye kadar her türlü sürecin aynı ilkelerle yönetilmesi gerektiğini belirttikten sonra PUKÖ adımlarına biraz daha yakından bakalım:



Şekil 2. *ISO 27001 standardında bilgi güvenliği döngüsünün alt başlıkları.*

Planlama adımında, kurumda bilgi güvenliği şemsiyesi altında bulunan varlıklara yönelik risklerin analiz edilmesi, bu çalışmanın sonuçlarına göre ISO 27002 standardında yer alan önlemlerden kurum için gerekli olanların seçilmesi ve uygulanması önerilmektedir (Şekil 3).



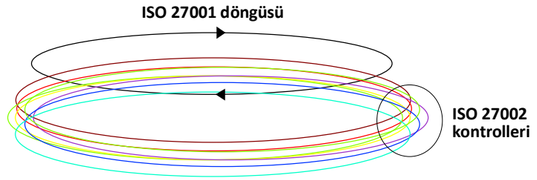
Şekil 3. *ISO 27001 döngüsünün planlama aşamasında ISO 27002 kontrollerinin seçilmesi.*

Böylece, ISO 27001 ve ISO 27002 standartları arasındaki ilişki kurulmuş olmaktadır. Şöyle ki, ISO 27001 standardında tanımlanan döngü, ISO 27002 standardından seçilen önlemler için çalıştırılarak bilgi güvenliği süreci gerçekleştirilmiş ve yaşatılmış olmaktadır.

Bilgi güvenliğinde asıl olanın ISO 27001 süreci olduğu, bu süreçten kopuk, dolayısıyla ölçüm, tetkik ve gözden geçirmelerin yapılmadığı, kayıtların oluşturulmadığı, düzeltici ve önleyici faaliyetlerin gerçekleştirilmediği bir sistemde alınan önlemlerin kuruma hizmet etmeyeceği söylenebilir.

3. ISO 27002 standardı

ISO 27002 standardı, bilgi güvenliği sürecinde işletilebilecek önlemleri içeren bir havuzdur [3, 4]. Giriş bölümünde, bilgi güvenliğinin ISO 27002 standardından seçilen önlemler aracılığıyla gerçekleştirileceği, her önlem için uygulama, izleme ve iyileştirme çalışmalarının yapılması gerektiği belirtilerek ISO 27001 döngüsüne gönderme yapılmaktadır (Şekil 4).



Şekil 4. *ISO 27001 döngüsü ve ISO 27002 kontrolleri.*

Özetle, önlemler ISO 27002 standardında, önlemlerin nasıl yaşatılacağı ise ISO 27001 standardında yer almaktadır.

4. ISO 27000 standartları ve bisiklet örneği

İki standart arasındaki ilişki Şekil 5'teki fotoğrafa göre açıklandığında, bisikletin parmaklığa kablo ile bağlanmasına karar verilmesi, kablonun seçilmesi, bisikletin bağlanması, daha sonra bağlantının ve kablonun gözden geçirilmesi ISO 27001 döngüsüne, seçilen kablonun kendisi ise belirlenen ISO 27002 önlemlerine benzetilebilir.

Şekil 5. *Güvenlik önlemleri alınmış bisiklet ve bilgi güvenliği standartları.*

Fotoğraftan, önlemleri alan kişinin bisikletin çalınmasından çok korktuğu açıkça görülmektedir. Kablolara harcanan para ve kabloların bisikletin park edileceği yere taşınması için harcanan çaba göz önünde bulundurulduğunda, alınan önlem ile gereksinim arasındaki dengenin kurulamadığı düşünülebilir. Bu durum, hem harcanan kaynak hem de kullanım açısından olumsuz sonuçlar doğuracaktır.

Bu örnekte gerekenden kalın kablo kullanılması, risk analizi yapılmadan bütün ISO 27002 önlemlerinin gerçekleştirildiği bir bilgi güvenliği sistemine benzetilebilir. Tüm önlemlerin gerçekleştirilmesi bütçeye önemli bir yük getirecek, gereğinden fazla insan kaynağı kullanılmasına neden olacak, ayrıca bilginin erişilebilirliğini de azaltacaktır.

Böylece ISO 27002 önlemlerinden kuruma gerçekten hizmet edecek olanların seçilmesinin ne kadar önemli olduğunu görmüş olduk. Bu seçimin doğru yapılabilmesi için risk analizi gerekir. [5, 6]

Kurumda uygulanacak önlemler belirlenirken, risk analizine ek olarak ISO 27002 standardının kendi önlemleri arasında gerçekleştirdiği önceliklendirme de göz önünde bulundurulabilir.

ISO 27001 standardını ve bilgi güvenliği sürecini daha sonra incelemek üzere kapatalım ve ISO 27002 standardında yer alan belli başlı önlemlere bir göz atalım.

5. ISO 27002 önlemlerinin standart içindeki organizasyonu

Bağlama halatı veya kablosu nasıl hiyerarşik bir yapı içerisinde gittikçe incelen kablolardan oluşuyorsa, ISO 27002 standardında yer alan önlemler için de aynı durum söz konusudur. (Şekil 6)

ISO 27002 standardında, onbir gruba ayrılmış 133 güvenlik önlemi yer alır. Bu önlemler kurumun yasal yükümlülüklerinin belirlenmesinden insan kaynakları güvenliğine kadar geniş bir yelpaze oluşturmaktadır.

Standardın hemen başında, "0.6 Bilgi güvenliğine giriş" başlığı altında bu 133 güvenlik önleminden on tanesinin hemen her kurum için gerekli ve öncelikli olduğu belirtilmektedir.

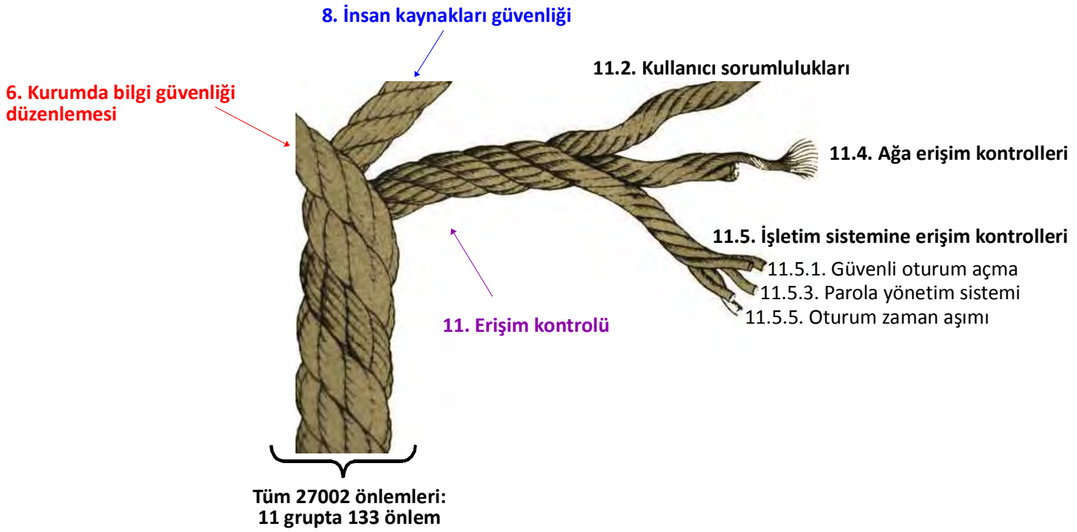
6. ISO 27002'deki öncelikli güvenlik önlemleri

ISO 27002'deki öncelikli güvenlik önlemlerinin ilk üçü, kurumun yasalardan ve sözleşmelerden kaynaklanan yükümlülüklerini gözden kaçırmaması ile ilgilidir. Bunlar, standardın

1. Verinin korunması ve kişisel bilgilerin gizliliği (ISO 27002 15.1.4),

2. Kurumsal kayıtların korunması (ISO 27002 15.1.3),

3. Fikri mülkiyet hakları (ISO 27002 15.1.2),



Şekil 6. *ISO 27002 önlemlerinin gruplara ayrılması.*

başlıkları altında açıklanmaktadır. Bu önlemlerde, özetle, uzman hukukçular yardımı ile kurumla ilgili mevzuatın ve kurumu bağlayan sözleşmelerin incelenmesi ve kurumun bilgi güvenliği yükümlülüklerinin belirlenmesi gerektiği belirtilmektedir. Daha sonra da bu yükümlülüklerin yerine getirilmesi için politika ve yöntemlerin geliştirilmesi ve kurumda uygulanması gerekir.

Diğer yedi önlem ise bilgi güvenliği konusunda yaygın olarak kullanılan ve standardın hemen her kurum için gerekli olduğunu belirttiği önlemlerdir:

4. Bilgi güvenliği politikası (ISO 27002 5.1.1),

5. Bilgi güvenliği sorumluluklarının atanması (ISO 27002 6.1.3),

6. Bilgi güvenliği eğitimi ve bilinçlendirme (ISO 27002 8.2.2),

7. Uygulamaların doğru çalışması (ISO 27002 12.2),

8. Teknik açıklık yönetimi (ISO 27002 12.6),

9. İş sürekliliği yönetimi (ISO 27002 14),

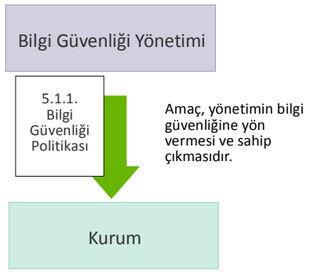
10. Bilgi güvenliği olaylarının yönetilmesi (ISO 27002 13.2).

7 ve 8 numaralı önlemler standardın 2005 sürümünde öncelikli uygulamalar arasına eklenmiştir. Bu durum dünyada gerçekleşmekte olan bilgi güvenliği olaylarının gidişini ortaya koyma açısından da önemlidir.

Şimdi 4-10 numaralı önlemleri biraz daha yakından inceleyelim.

Bilgi güvenliği politikası (ISO 27002, 5.1.1)

Bilgi güvenliği politikası aracılığı ile kurum yönetimi, yasal mevzuat ve diğer bilgi güvenliği ihtiyaçları uyarınca kurumda bilgi güvenliğini sağlamayı üstlenir [7] (Şekil 7).



Şekil 7. *Bilgi güvenliği politikası.*

Bilgi güvenliği politikası, kurumsal yaklaşımı tanımlayarak bilgi güvenliği konusunda yükümlülüklerin nasıl gerçekleştirileceğine ilişkin çerçeveyi oluşturur.

Politika üst yönetim tarafından onaylanır, yayımlanır ve tüm kurum çalışanları bilgi güvenliği politikası konusunda bilgilendirilir. Bilgi güvenliği politikası, belgenin sahibi tarafından periyodik olarak gözden geçirilir.

Bilgi güvenliği politikası aşağıdaki konuları içermelidir:

a. Bilgi güvenliği politikasının genel tanımı, amacı ve kapsamı.

b. Üst yönetimin bilgi güvenliği ile ilgili niyeti, hedefi ve desteği.

c. Riskin yönetilmesi ve bilgi güvenliği önlemleri ile ilgili genel çerçeve.

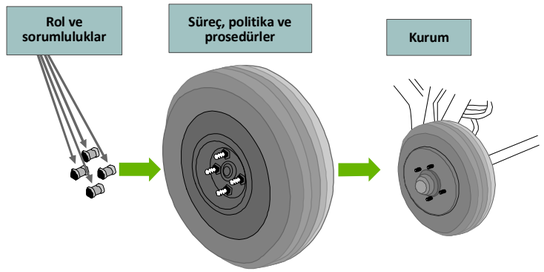
d. Kurum için önem arz eden mevzuat, standart ve ilkeler.

e. Çeşitli bilgi sistemleri ve süreçleri ile ilgili olarak hazırlanacak alt politika ve prosedürlere göndermeler. (Erişim kontrolü, Fiziksel güvenlik, Şifre politikası gibi konularda alt politika ve prosedürler düzenlenecektir).

f. Bilgi güvenliğinin yönetilmesi ile ilgili sorumlulukların tanımları.

Bilgi güvenliği sorumluluklarının atanması (ISO 27002, 6.1.3)

Bilgi güvenliği ile ilgili rol ve sorumlulukların tanımlanması, politika, alt politika ve prosedürlerde belirtilen işlevlerin hayata geçirilmesini sağlayan başlıca etkendir (Şekil 8). Rol ve sorumlulukların tanımlanmaması durumunda, hazırlanan politika ve prosedürlerin kağıt üstünde kalması sürpriz olmayacaktır.



Şekil 8. *Kurumda rol ve sorumlulukların atanmasının önemi.*

Kapsam içindeki tüm bilgi sistemleri için;

1. Varlıklar ve bilgi güvenliği süreçleri açıkça belirlenir,

2. Her bir varlık ve süreç için sorumlu belirlenir, sorumluluğun içeriği ve ayrıntıları belgelenir.

Güvenlik sorumluluğuna sahip personel, görevini bir başkasına verse de sorumluluğunu aktaramaz.

Bilgi güvenliği eğitimi ve bilinçlendirme (ISO 27002, 8.2.2)

Kapsam içindeki tüm çalışanlar, üçüncü taraf kullanıcıları ve personeli, bilgiye veya bilgi servislerine erişim hakkı verilmeden önce kurumun bilgi güvenliği politika ve beklentileri konusunda eğitilir. Eğitim ve bilinçlendirme çalışmaları, bilgi güvenliğinin en zayıf halkası olan kullanıcılardan kaynaklanan hataların en alt düzeye indirilmesi açısından son derece önemlidir [8].

Bilgi güvenliği eğitimi ve bilinçlendirme süreci aracılığı ile kullanıcıya

1. Kurumun bilgi güvenliği ile ilgili politika ve prosedürleri,

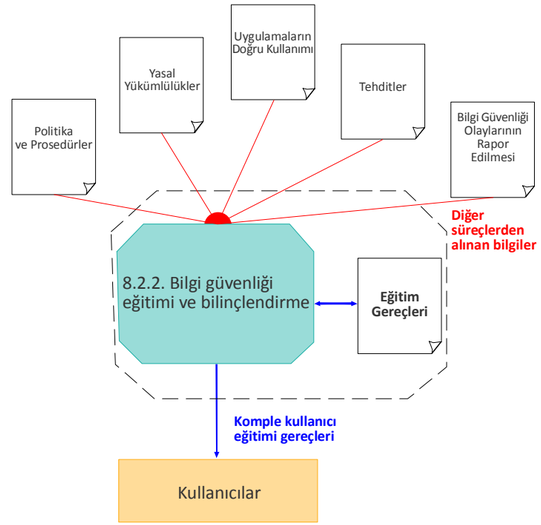
2. Bilgi güvenliği ile ilgili yasal yükümlülükleri,

3. Bilgi servislerinin ve uygulamaların doğru kullanımı (oturum açma işlemleri ve benzeri),

4. Bilinen tehditler,

5. Bilgi güvenliği olaylarının algılanması ve bildirilmesi

ile ilgili bilgiler aktarılır (Şekil 9).



Şekil 9. *Bilgi güvenliği eğitimi ve bilinçlendirme çalışmaları.*

Eğitim çalışmaları periyodik olarak tekrarlanarak personele hem güncel bilgiler aktarılır, hem de personelin bilgi güvenliği kültürünü benimsemesi sağlanır.

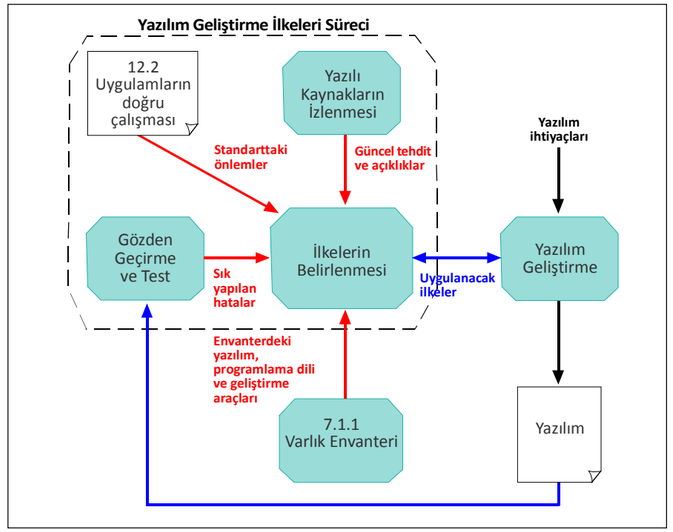
Uygulamaların doğru çalışması (ISO 27002, 12.2)

Yazılım teknolojisi dünyada en hızlı değişen ve gelişen teknolojilerin başında gelir. Programlama dilleri, iletişim ve işlemci teknolojilerinde yaşanan gelişim, sektörde hemen her kurumda rastlanan personel yetersizliği ve zaman baskısı ile birleşerek yazılımı hataya en açık alanlardan biri durumuna getirir. Bu duruma ek olarak, yazılım açıklarını kullanarak bilgi sistemlerine yetkisiz erişim gerçekleştirme, yeni bir uzmanlık alanı olarak ortaya çıkmış, bu konuda çalışma yapan nerede ise bir sektör oluşmuş durumdadır. Bu bilgiler ışığında 27002 standardının 2005 sürümünde "12.2 Uygulamaların doğru çalışması" başlığının "olmazsa olmaz"lar arasına eklenmesi son derece doğaldır.

Bu güvenlik önleminin hayata geçirilmesi için

1. ISO 27002 standardının 12.2.x başlıklarında açıklanan önlemlerin gözden geçirilmesi,

2. Kullanılan programlama dilleri de göz önünde bulundurularak, bu dillerle geliştirilen uygulamalarda karşılaşılan açıklıkların ve bunlardan korunma yollarının değerlendirilmesi ve sektörel yayınların izlenmesiyle "Güncel tehdit ve açıklıklar"ın belirlenmesi,



Şekil 10. *Uygulamaların doğru çalışması.*

3. Geliştirilen yazılımlarda, çapraz gözden geçirme ve test yapılarak sıkça yapılan hataların belirlenmesi,

4. İlk üç maddede elde edilen veriler göz önünde bulundurularak güvenli yazılım geliştirme ilkelerinin belirlenmesi ve

5. Belirlenen ilkelerin kurumda yazılım geliştiren tüm personele bildirilmesi

işlerini gerçekleştiren bir "Yazılım Geliştirme İlkeleri Süreci" (Şekil 10) oluşturulmalıdır.

Teknik açıklık yönetimi (ISO 27002, 12.6)

Teknik açıklık yönetimi kısaca "Teknik açıklıklardan kaynaklanan risklerin yönetilmesi" olarak tanımlanır [9]. Teknik açıklıklar, sunucu bilgisayarlarından çeşitli ağ birimlerine kadar uzanan geniş bir yelpaze üstünde çalışan yazılımların yama yönetimi, yapılandırma ayarları ve diğer teknik özelliklerinden kaynaklanan açıklıklardır. Bunların izlenmesini ve kapatılmasını konu alan 12.6 maddesi de ISO 27002 "12.2 Uygulamaların doğru çalışması" maddesi gibi standardın 2005 sürümünde en önemli güvenlik uygulamaları arasına katılmış olup bu iki başlıkta ele alınan konular birbirini tamamlar niteliktedir.

Bu alanda zayıflık oluşmaması için "Teknik açıklık yönetimi"nin ilgili kurumda bir süreç olarak oluşturulması gerektiği standart tarafından belirtilmektedir. Sürecin başarı ile çalışabilmesi için varlık envanterinin güncel ve eksiksiz olarak (yazılım içeren varlıkların üstündeki yazılımlar, bu yazılımların sürümleri, envantere girme tarihi ve benzeri) tutulması gerekir [5]. Teknik açıklık yönetimi süreci kapsamında aşağıdaki işlemler gerçekleştirilir:

1. Her süreçte olduğu gibi rol ve sorumlulukların belirlenmesi,

2. Kurum varlıklarının ve bilgi sistemlerinin önemi göz önünde bulundurularak belirlenecek bir sıklıkta "Teknik Güvenlik Testleri"nin yinelenmesi,

3. Envanterdeki varlıkların açıklıkları ile ilgili bilgi üreten kaynakların belirlenmesi, (uygulama yazılımı konusunda olduğu gibi bu konuda da dünyada son derece aktif bir saldırı ve savunma sektörü oluşmuştur), güncellenmesi ve izlenmesi,

4. Belirlenen açıklıkları içeren varlıkların sahipleri ile eş güdüm

5. Yama vb. önlemlerin test edilmesi ve varlık sahipleriyle eş güdümlü olarak uygulanması (Şekil 11).

Şekil 10 ve 11'in incelenmesiyle standardın 12.2 ve 12.6 maddelerindeki güvenlik önlemlerinin gerçekleştirilmesi için benzer yapılanmalara gereksinim olduğu görülür. Varlık envanterinin, test sonuçlarının ve yazılı kaynakların izlenmesini gerçekleştirecek bir "Bilgi Güvenliği Teknoloji Sorumlusu", her iki sürecin sorumluluğunu üstlenebilir.

Bilgi güvenliği olaylarının yönetilmesi (ISO 27002, 13.2)

ISO 27002 uyarınca, rapor edilen bilgi güvenliği olaylarına hızlı ve etkili karşılık verebilmek için tutarlı bir yaklaşımın oluşturulması, prosedür ve sorumlulukların tanımlanması, bilgi güvenliği olaylarıyla ilgili izleme, değerlendirme, müdahale ve gerektiğinde kanıt toplama çalışmalarının bir süreç yaklaşımı içerisinde (gözden geçirilerek ve iyileştirilerek) gerçekleştirilmesi gerekir [10].

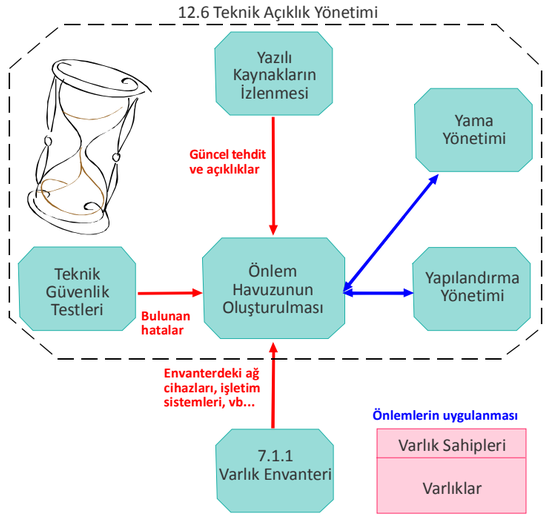
Bilgi güvenliği olaylarına müdahale ile ilgili olarak

1. Bilgi sistemi arızası,

2. Virüs saldırısı,

3. Servis dışı bırakma saldırısı,

4. Eksik veya hatalı veri girişi,



Şekil 11. *Teknik açıklık yönetimi.*

5. Gizlilik ve bütünlüğü bozan ihlaller,

6. Bilgi sisteminin kötüye kullanılması

ve gerekli görülen diğer durumlarda çalıştırılacak prosedürler oluşturulur. Bunlara ek olarak;

1. Olayın nedeninin belirlenmesi ve tekrarına engel olmak için düzeltici faaliyetlerin gerçekleştirilmesi,

2. Kanıt toplama ve ilgili makamlara iletme,

3. Canlı sisteme yalnızca yetkili personelin müdahale etmesi,

4. Yapılan müdahalenin belgelenmesi,

5. Müdahalelerin düzenli olarak yönetime bildirilmesi ve yönetim tarafından gözden geçirilmesi

6. Bilgi sistemlerinin bütünlüğünün en az gecikme ile sağlanması

konuları da prosedürler çerçevesinde düzenlenir. Bilgi güvenliği olaylarının algılanması konusunda

a) Olay ve zayıflıkların rapor edilmesine (ISO 27002, 13.1 alt başlığı) ek olarak

b) Sistem kullanımının düzenli olarak gözlenmesi de (ISO 27002, 10.10.2 alt başlığı)

önemlidir (Şekil 12).

Şekil 12. *Bilgi güvenliği olaylarının algılanması ve yönetilmesi.*

İş sürekliliği yönetimi (ISO 27002, 14)

İş sürekliliği yönetimi, büyük arıza, sabotaj veya doğal afetlerin kurum bilgi sistemlerinde yaratacağı olumsuz etkileri önleyici ve giderici eylemlerin belirlenmesi ve bu önlemlere ait atama, tatbikat, belgeleme ve diğer çalışmaların kurum bünyesinde bir süreç olarak yaşatılması anlamına gelir [11] (Şekil 13).

Kuruma ait bilgi sistemleri gözden geçirilerek önemli iş süreçleri ve bilgi varlıkları belirlenir ve kurumun iş sürekliliği konusundaki gereksinimi gerçekçi bir biçimde belirlenir.

Bu kapsamda;

1. Kritik iş süreçlerinin ve bunlarla ilgili varlıkların belirlenmesi, bunları etkileyecek tehditlerin ve gerçekleşme olasılıklarının belirlenmesi,

2. Bu risklerin azaltılmasını sağlayacak önlemlerin belirlenmesi, bunlar için parasal ve kurumsal kaynak ayrılması (Kurumda belirlenen önlemlerin var olan önlemlerle karşılaştırılması),

3. İş sürekliliği planlarının geliştirilmesi ve belgelenmesi,

4. Planların düzenli olarak test edilmesi ("tatbikat" olarak da adlandırılabilir) ve güncellenmesi sağlanır.

Şekil 13. *İş sürekliliği yönetimi.*

7. Bilgi Güvenliği Yönetim Sistemi ve Süreç Yaklaşımı

ISO 27002 standardında yer alan belli başlı güvenlik önlemlerini gördükten sonra tekrar 27001'e dönelim ve standardın çizdiği büyük resmi görmeye çalışalım. İlk iş olarak şunu vurgulayalım: ISO 27001 standardı Bilgi Güvenliği Yönetim Sistemi (BGYS)'nin süreçlerden oluşan bir sistem olarak algılanması gerektiğini vurgular. Buna ek olarak, BGYS'nin kendisi de bir süreçtir.

ISO 27001 standardına göre süreç, "Girdileri çıktıya çevirmek için kaynak kullanan ve yönetilen çalışmalardır." Dolayısıyla, sürecin

- Girdisi,
- Çıktısı,
- Girdiyi çıktıya dönüştürmekte kullandığı bilgisi ve yöntemi

vardır. Bunlara ek olarak süreç çalışırken kaynak kullanır. Standarttaki "yönetilen çalışma" ifadesinden

- Yönetim tarafından tanımlanmış veya onaylanmış etkinliklerin
- Yönetim tarafından belirlenmiş roller ve atanmış sorumlular

tarafından gerçekleştirilmesi anlaşılmaktadır.

BGYS sürecinin girdisi "Bilgi güvenliği gereksinimi ve beklentileri", çıktısı ise "Yönetilen bilgi güvenliği"dir.

Süreci oluşturan çalışmalar dört adım altında toplanabilir. Bu dört adım PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) döngüsünü oluşturur. Bu adımlar ve standardın ilgili başlıkları Tablo – 1'de verilmektedir.

Bu dört adımın gerçekleştirilmesi ile PUKÖ döngüsü tamamlanmış olur. Ancak, "Planlama" adımı yalnızca 4.2.1 başlığı, "Kontrol Et" adımı yalnızca 4.2.3 başlığı ile sınırlı olamaz.

4.2 başlığı altında BGYS döngüsünün çok yoğun bir özeti yapılmaktadır. Bu başlık altından standardın "belgeleme gereksinimleri", "yönetim sorumluluğu", "iç tetkik", ayrıca ISO 27002 kontrollerinin özetlendiği "Ek A. Kontrol Amaçları ve Kontroller" bölümlerine göndermeler yapılmaktadır. Bu bölümlerde de PUKÖ döngüsü altında sözü geçen çalışmalar ayrıntılı olarak açıklanmaktadır.

8. Uygulayıcılar: Kurum ve Yönetim

Bu çalışmaları yerine getirenler konusunda standart, kimi zaman "Kurum..", kimi zaman da "Yönetim.." "..aşağıdaki çalışmaları gerçekleştirir" ifadesini kullanmaktadır. Yönetim kurumun dışında yer alan bir öğe olamayacağına göre "Yönetim" ifadesinden "Yalnızca Yönetim", "Kurum" ifadesinden ise "Kurum içinde yönetim tarafından görevlendirilmiş birimler ve gerekiyorsa yönetim temsilcisi" anlaşılmalıdır. (Şekil 14)

Standart, "5 Yönetim Sorumluluğu" başlığı altında yönetimin sürecin tamamında devrede olduğunu çeşitli etkinlikler aracılığıyla kanıtlanması gerektiğini ifade ederek "Kurum" ve "Yönetim" kavramlarını yukarıdaki gibi tanımlamamızı sağlamaktadır.

Özetle "Yönetim", tüm süreç boyunca işin içindedir, çeşitli adımlarda çalışmalara katılarak veya kaynak sağlayarak BGYS sürecine katkıda bulunur.

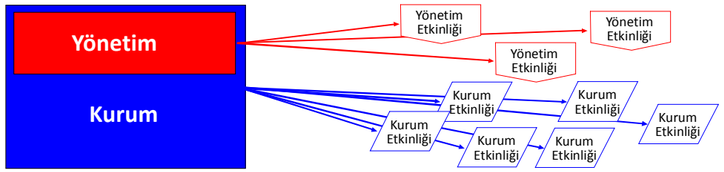
"Kurum" ve "Yönetim" etkinliklerine ek olarak standartta dikkat çeken bir etkinlik türü de belgeleme ve kayıt çalışmalarıdır. Bu konu "4.3 Belgeleme Gereksinimleri" başlığı altında işlenmektedir. Bu başlık altında üretilmesi zorunlu olan belgelerin PUKÖ döngüsünün hangi etkinlikleri ile ilişkili olarak geliştirileceği ve belgelerle ilgili olarak yönetimin üstüne düşenler açıklanmaktadır.

9. Kurum, Yönetim ve Belgeleme çalışmaları

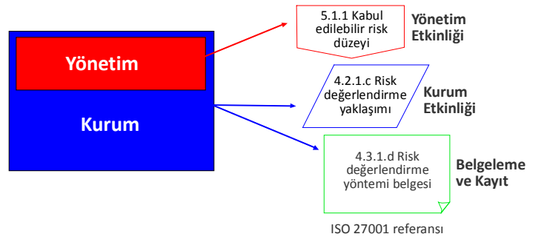
PUKÖ döngüsünde bulunan herhangi bir kurum etkinliği için bu etkinliğe paralel olarak gerçekleştirilmesi gereken bir yönetim etkinliği ve etkinliklerin çoğu için oluşturulması gereken belge veya kayıtlar belirtilmektedir. Örnek olarak "4.2.1.c Risk değerlendirme yaklaşımının tanımlanması" etkinliğini inceleyelim. Bu etkinlik ile ilgili olarak yönetimin 5.1.f başlığında belirtilen "Riskleri kabul etme ölçütlerini ve kabul edilebilir risk düzeylerini belirleme" etkinliğini gerçekleştirmesi beklenmektedir. Aynı etkinlikle ilgili olarak 4.3.1.d başlığında "Risk değerlendirme yöntemi tanımı"nın belgelenmesi gerektiği belirtilmektedir (Şekil 15).

Tablo1. PUKÖ Adımlarının Standart Alt Başlıkları İle ilişkisi

Adım	Standardın ilgili başlığı
Planla	4.2.1 BGYS'nin kurulması
Uygula	4.2.2 BGYS'nin gerçekleştirilmesi ve işletilmesi
Kontrol Et	4.2.3 BGYS'nin izlenmesi ve gözden geçirilmesi
Önlem Al	4.2.4 BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi



Şekil 14. *BGYS etkinlikleri, "Kurum" ve "Yönetim".*



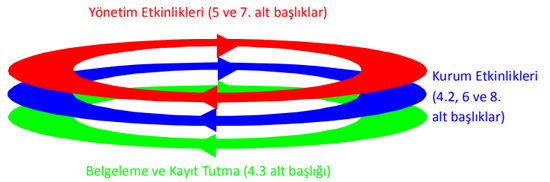
Şekil 15. *4.2.1.c faaliyeti, eşlik eden yönetim etkinliği ve belgeleme.*

10. Yönetim ve belgelemenin oluşturduğu paralel döngüler

Standardın "4.2 BGYS'nin kurulması ve yönetilmesi" başlığı, esasen "PUKÖ döngüsü"nün tamamını içerir, BGYS süreci çerçevesinde gerçekleştirilecek kurum etkinlikerine değinirken yönetim çalışmalarına ve belgelemeye de göndermeler yapar. Kurum çalışmalarının bir kısmı ise - "6 İç tetkik" ve "8 BGYS'nin iyileştirilmesi" - daha sonra ayrıntılarıyla açıklanmaktadır.

Ardından gelen 4.3 başlığı, süreç boyunca üretilecek belgelere, 5 ve 7 numaralı başlıklar ise yönetim çalışmalarına ilişkin bilgiler verir.

Bu bölümlerin içerikleri PUKÖ döngüsüne eşlik eden yönetim ve belgeleme döngülerini tanımlamaktadır. Bu üç paralel döngünün bir araya gelmesiyle çok katmanlı BGYS süreci oluşmaktadır (Şekil 16).



Şekil 16. *Üç katmanlı BGYS döngüsü.*

Şekilde de görüldüğü gibi

- Yönetim etkinlikleri üst katmanı,
- Kurum etkinlikleri orta katmanı,
- Belgeleme ve kayıt tutma ise alt katmanı oluşturmaktadır.

BGYS sürecinin tüm etkinlikleri için üç katmanda birden çalışma olduğunu söylemek mümkün olmasa da çoğu için mümkündür. Örneğin yönetim katmanının katkısının bazı aşamalarda yalnızca kaynak sağlamak olduğu, diğer bazı aşamalar için ise standardın belge üretilmesini istemediği söylenebilir. Gene de Şekil-16'de resmedilen çok katmanlı BGYS döngüsünün bilgi güvenliği sürecine ilişkin oldukça gerçekçi bir model oluşturduğu söylenebilir.

Çok katmanlı yapıların hemen hepsinde olduğu gibi burada da üst katmanın çıktısı bir alttaki katmanın girdisini oluşturmaktadır. Kurum etkinlikleri nin sonucunda oluşan belgeler ise çoğunlukla sürecin bir sonraki etkinliği için girdi olmaktadır.

Örnek olarak yine Şekil 15'e dönecek olursak,

Bir yönetim etkinliği olan kabul edilebilir risk düzeyinin belirlenmesi (5.1.f), kurum etkinliği olan risk değerlendirme yaklaşımının belirlenmesine (4.2.1.c) girdi oluşturur. Bu etkinlik sonucunda belgeleme katmanında yer alan risk yöntemi belgesi (4.3.1.d) üretilir. Bu doküman, sürecin bir sonraki etkinliği olan risk analizi çalışmaları (4.2.1.d-f) için girdi oluşturur.

11. Katmanlar arası senkronizasyon ve BGYS süreç özeti

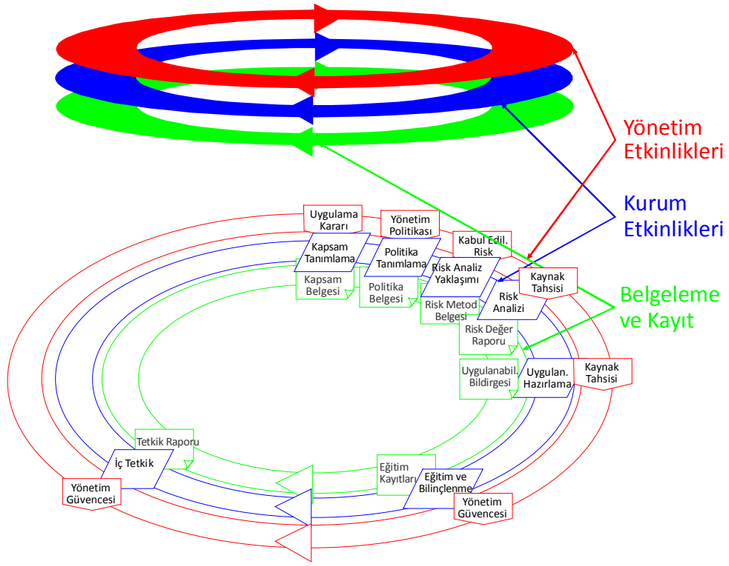
Standartta bulunan tüm göndermelerin incelenmesi sonucunda farklı katmanlardaki etkinliklerinin ilişkilendirilmesi ve katmanlar arası senkronizasyonun sağlanması mümkündür. Böylece standartta karışık olarak yer alan BGYS sürecinin tüm katman ve etkinlikleri tek şekilde toplanabilir. (Bu özet Şekil 18'de gösterilmiştir.) Ancak önce bunun nasıl yapılacağını açıklayalım. Şekil 17 aslında Şekil 16'nın ayrıntılı biçimi olmakla birlikte yer darlığı yüzünden Şekil 16'daki derinlik ve çok katmanlı yapı duygusunu verememektedir.

Standartta yer alan tüm etkinliklerin BGYS döngüsüne ayrıntılı bir biçimde yerleştirilmesiyle hem süreçte yer alan etkinliklerin tamamı, hem de bu etkinlikler arasındaki ilişkiler gözler önüne serilmektedir. (Şekil 18)

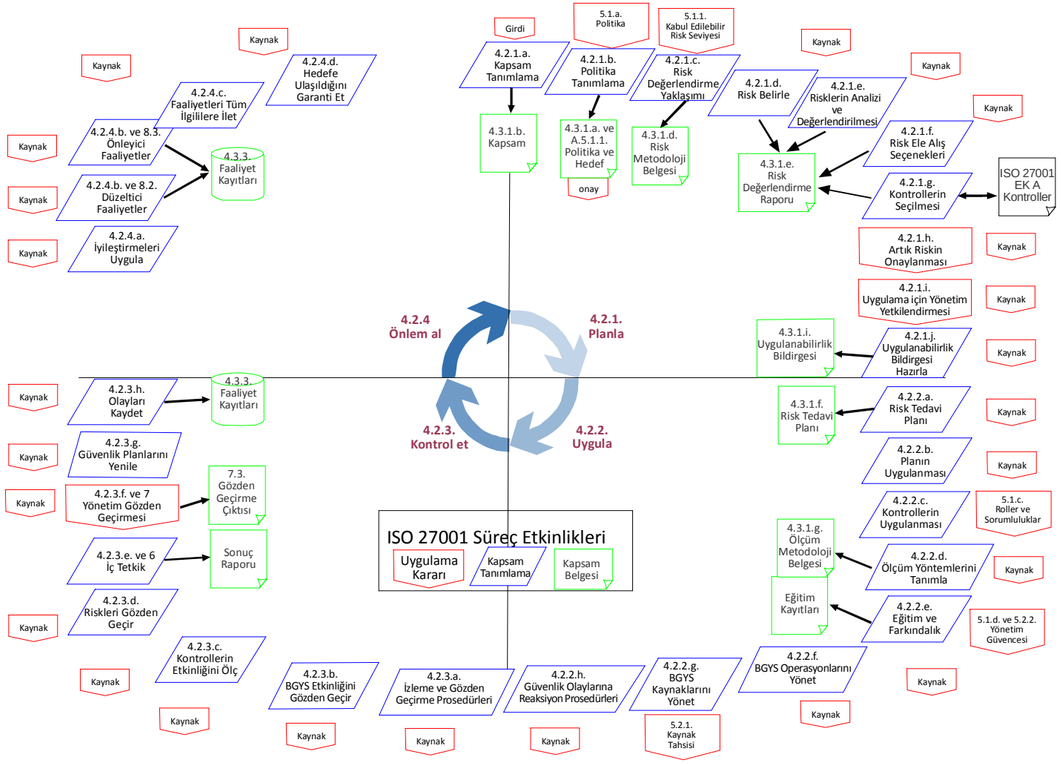
12. Tarihsel gelişim ve öneriler

Bilgi güvenliği, ISO 27001 standardında tanımlanan döngünün ISO 27002 standardında açıklanan önlemler için çalıştırılması ile sağlanmaktadır. Bu konuda temel olanın 27001 süreci olduğunu, risk analizi gerçekleştirilmeden alınan önlemlerin kuruma yararlı olmasının rastlantıya bağlı olacağını söylemek yanlış olmaz.

Bununla birlikte, ISO 27002 standardında açıklanan önlem havuzunda yer alan 133 maddeden on tanesinin öncelikli olduğu ve başlangıç aşamasında bile gerçekleştirilmesinin gerektiği ISO 27002 standardında vurgulanmaktadır. Bu uyarının de gözden kaçırılmaması gerekir. ISO 27002 standardında açıklanan öncelikli önlemlerden kurumsal gereksinimleri karşılayanların uygulanması ile bilgi güvenliğine katkı sağlanabilir.



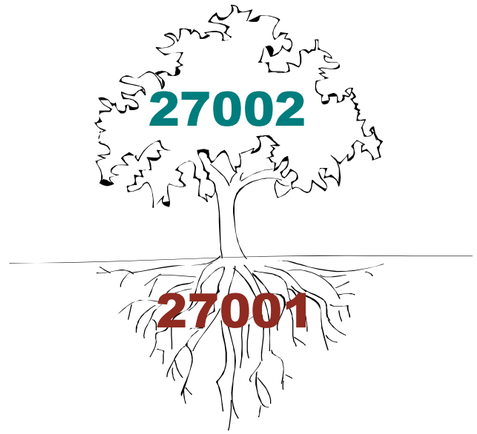
Şekil 17. *Çok katmanlı BGYS döngüsünün ayrıntılı açıklaması.*



Şekil 18. *Ayrıntılarıyla açıklanmış üç katmanlı BGYS süreci.*

27001 ve 27002 standartlarının tarihsel gelişimi göz önünde bulundurulduğunda, önlem havuzu durumundaki 27002'nin ilk sürümünün 7799-1 adı ile 1995'de yayımlandığı görülmektedir. Bilgi güvenliği sürecini tanımlayan 27001 standardı ise 2005 tarihinde yayımlanmıştır. Bu tarihlerin ve deneyimlerin ışığında önlem havuzuna dalıp gitmenin yeterli olmadığı, asıl güçlüğün bunları yaşatmak olduğunu, 27001'in bu arayışın sonucu olarak ortaya çıktığı söylenebilir.

Dolayısıyla önemli olan, i) Risk analizi, ii) Önlemlerin belirlenmesi ve uygulanması, iii) İç tetkik, iv) Yönetim gözden geçirmesi ve v) Düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi adımlarından oluşan 27001 sürecinin kurum tarafından işletilmesidir. Dar bir kapsamda veya kısıtlı bir önlem seti için bile olsa, bilgi güvenliği sürecinin çalıştırılması, kurumda bilgi güvenliğinin temelinin sağlam bir biçimde atılmasını sağlar (Şekil 19). Bizim tüm kurumlara önerimiz, öncelikle bu temelin atılmasıdır. Temel sağlam olarak atıldıktan sonra kapsam da güvenlik önlemleri de genişletilebilir.



Şekil 19. *Bilgi güvenliği sürecini (27001) ve önlem havuzunu (27002) tanımlayan standartlar.*

KAYNAKÇA

[1] "COBIT Mapping. Overview of International IT Guidance, 2nd Edition" http://www.isaca.org/

[2] International Standard *ISO/IEC 27001*, Information technology – Security techniques – Information security management systems – Requirements.

[3] International Standard *ISO/IEC 27002*, Information technology – Security techniques – Code of practice for information security management.

[4] Fikret Ottekin, "ISO 27001 Denetim Listesi", http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=154

[5] Fatih Koç, "Varlık Envanteri Oluşturma Kılavuzu" http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=223

[6] Doğan Eskiyörük, "BGYS Risk Yönetim Süreci Kılavuzu", http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=148

[7] Günce Öztürk, "Bilgi Güvenliği Politikası Oluşturma Kılavuzu", http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=155

[8] Dinçer Önel, "Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu" http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=150

[9] Hayretdin Bahşi, "Teknik Açıklık Yönetimi", http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=90&Itemid=6

[10] "Olay Müdahale Koordinasyonu", http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=69&Itemid=6

[11] Ziya Gökalp, "İşin sürekliliği adına 'Bilgi Güvenliği'", http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=256&Itemid=6

BİLİŞİM SİSTEMLERİ GÜVENLİĞİNDE

TÜBİTAK

BİLGEM

Tahsin TÜRKÖZ

Hepimizin bildiği gibi, bilişim sistemleri son 15 yılımıza damgasını vurdu. Kâğıt üzerinden yürüyen pek çok iş gerek kolaylığı gerekse getirdiği diğer faydalar nedeniyle sanal ortamlara taşındı. Uzun yıllar içerisinde oluşmuş birikim ve tecrübelerimizi küçücük depolama alanlarında taşıyabilir hale gelmemiz, iş gereksinimlerimizin neredeyse tamamına yakınını cep telefonları ile karşılayabiliyor olmamız, bu değişimin ne kadar hızlı ve hayrete düşürücü olduğunun en önemli göstergelerinden.

Ünlü psikolog Abraham Maslow, bazı eleştirilere rağmen bugün hâlâ kabul gören kuramında, insanoğlunun beslenme ve uyuma gibi fizyolojik ihtiyaçlarından sonra kendini güvende hissetmek ve tehlikeden uzak durmak içgüdülerinin ağır bastığından bahseder. Tarih, yakın çağımıza kadar bu kuramın en önemli kanıtı niteliğindeydi. Fakat güvenliğin hep arka planda kaldığı bilişim sistemlerindeki gelişmeler Maslow'u yalancı çıkardı. Özellikle son on yıl içerisinde bilişim sistemlerinde saptanan açıklıklara karşı savunmasızlığımız, güvenlik bilincinin ancak yaşanılan acı tecrübelerin bir bileşkesi ile oluşması, bu noktadaki zafiyetlerimizi ortaya koydu.

Şekil 1. *Maslow Üçgeni.*

Dünden Bugüne

Ulusal bilgi güvenliğinin sağlanmasını ve bu konularda ülkemizin kendi ayakları üzerinde durmasını kendisine misyon edinmiş TÜBİTAK BİLGEM, bilgi güvenliğinin sadece şifreleme ile sağlanamayacağını, bilişim sistemleri ve ağ düzeyindeki saldırıların da önemsenmesi gerektiğini ve bu alanda uzmanlaşmış bir bölüme ihtiyaç olduğu düşüncesini 1997 yılında hayata geçirdi. İlk yıllarında **Ağ Güvenliği Grubu** adıyla yürütülen çalışmalarda kapsamlı bir test laboratuvarı kuruldu. Laboratuvar ortamında *Microsoft* ve açık kaynak kodlu işletim sistemleri, bunların üzerinde çalışan e-posta sunucu, veritabanları gibi popüler uygulamalar, aktif ağ cihaz ve kutuları, saldırı tespit sistemleri gibi savunma ürünleri güvenlik bakış açısı ile değerlendirildi. Önemli bir bilgi birikimi sağlandı.

2001 yılında Genelkurmay Başkanlığı'nın da desteğiyle gerçekleştirilen Ortak Kriter Test Merkezi (OKTEM) kurulması projesi ile bu bilgi birikimi, uluslararası kabul gören standartların gerçeklenmesi amacıyla kullanıldı. Bilişim sistemi ürünlerinin belirli güvenlik kriterlerine göre değerlendirilip sağlamış olduğu güvenlik seviyelerinin belirlenmesi temel ilkesine dayanan Ortak Kriterler (*'Common Criteria', CC*) değerlendirmeleri, ülkemiz laboratuvarlarında yapılabilir hale geldi. Laboratuvar sonraki yıllarda kripto cihazları için gerçeklenebilir olan *COMSEC* (Haberleşme Güvenliği) testlerini de kabiliyetleri arasına ekledi. 2006 yılından günümüze akıllı kart güvenliği ile ilgili çalışmalarını yoğunlaştırarak, özellikle Yan Kanal Çözümlemesi (*Side Channel Analysis*) ve Tersine Mühendislik (*Reverse Engineering*) konularında uzmanlık kazandı. Bu alanda sahip olduğu altyapı ile dünyada önemli test merkezlerinden biri haline geldi.

Geçtiğimiz yıl Ortak Kriterler belgelendirmesi konusunda meydana gelen bir gelişme ile sevindik. Bu konuda paydaş durumunda olan TÜBİTAK BİLGEM ve TSE'nin işbirliğiyle, üretilen sertifikaların uluslararası tanınırlığa sahip olması için yapılan uzun ve zorlu yolculuk tamamlandı. 12-16 Nisan tarihlerinde TSE'de uluslararası denetçiler tarafından gerçekleştirilen ve OKTEM tarafından üretilen değerlendirme raporlarının da dikkatle incelendiği tetkik başarı ile sonuçlandı. Sonrasında, Türkiye'nin kabulüne yönelik başlatılan idari süreç tüm diğer sertifika üreticisi ülkelerin onayı ile tamamlandı. Böylelikle Türkiye, "Sertifika Üreticisi Ülke" statüsüne sahip 14 ülkenin yanına adını yazdırmış oldu.

Ağ Güvenliği Grubu, kuruluşundan bugüne Türk Silahlı Kuvvetleri'nin bilişim sistemleri güvenliği alanındaki gereksinimlerini karşılamak üzere pek çok proje gerçekleştirdi. Güvenlik mimarilerinin tasarımı, sistemlerin güvenli kurulumu, güvenlik testleri, risk çözümleme çalışmalarının gerçekleşmesi gibi alt başlıklar altında ele alınabilecek projelerle Ağ Güvenliği Grubu, ülkemizin özellikle geleceği adına oldukça önemsenmesi gereken bilişim güvenliği alanında söz sahibi bir otorite konumuna geldi.

Eldeki bilgi birikiminin paylaşımı ve ülke genelinde bilgi güvenliği konusundaki bilincin artırılması amacıyla yüzünü diğer sektörlere de çeviren Ağ Güvenliği Grubu, kamu kurumları ve kritik özel sektör kurumları ile bazı projeler gerçekleştirdi. Güvenlik testleri ile başlayan, daha sonra Risk Analizi, Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulumu/danışmanlığı ile devam eden bu çalışmalarda kurumların önemli kazanımları oldu. Bazı kamu kurumları, yönetim hiyerarşisindeki etkin noktalara, bilgi güvenliği sağlanmasına yönelik birimler entegre ederek konuyu en üst düzeyde ele almaya gayret gösterdiler.

Özel sektörde gerçekleştirilen projeler genellikle bankacılık, telekomünikasyon ve otomotiv alanlarında çalışan firmalarla yürütüldü. Bunlar mali kazanımların arka planda kaldığı, eldeki bilgi birikiminin geliştirilmesi ve yeni teknolojilerden haberdar olabilme amacıyla yürütülen projelerdi. Müşterilerimizin proje çıktılarından memnun kalarak çok yüksek oranda yeni proje önerilerinde bulunmalarının doğru yolda olduğumuzun göstergelerinden biri olduğunu düşünüyoruz.

Devlet Planlama Teşkilatı Bilgi Toplumu Dairesi'nin 2005 yılında başlatmış olduğu **Bilgi Toplumu Stratejisi** isimli çalışma ülkemizde bilişim sistemleri adına önemli bir milat oldu. Çalışma, ülkemizin bilgi toplumu olması yolunda önemli mesafeler kat etmek ve bilgi teknolojilerinden etkin olarak yararlanılmasını sağlamak amacıyla gerçekleştirildi. Çalışmanın bir maddesini de **Bilgi Sistemleri Güvenlik Programı** oluşturuyordu. TÜBİTAK BİLGEM Ağ Güvenliği Grubu tarafından yürütülen ve halen devam eden bu program ile, başta kamu kurum ve kuruluşları olmak üzere ülkemizin bilgi sistem güvenliğiyle ilgili gereksinimlerinin karşılanması hedeflenmekte. Program kapsamında pek çok kamu kurumunda pilot çalışmalar gerçekleştirildi. Bu çalışmalar ile kurumların bilgi güvenliği problemlerini minimize etmek ve kurumsal bilgi güvenliği bilinci kazandırmak adına gayret gösterildi. Kritik kamu kurumlarımızda çalışan personele, üniversitede bilişim sistemlerinin yönetimiyle görevli kişilere eğitimler verildi.

Bilgi Sistemleri Güvenlik Programı'nın önemli hedeflerinden birisi de, ülkemizde bilgisayar ortamlarında yaşanabilecek bilgi güvenliği olaylarına doğru ve sağlıklı müdahaleyi gerçekleştirmek amacıyla gerekli altyapıyı oluşturmaktı. Bu amaçla yine TÜBİTAK BİLGEM bünyesinde Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME) kuruldu. Bu ekip kritik kamu kurumlarında BOME yapılanmasının kurulabilmesi için gerekli eğitim ve eşgüdüm faaliyetlerini yürüttü. Kasım 2008'de gerçekleştirilen tatbikat ile kurumlara, bilgi güvenliği sorunlarına hızla tepki gösterebilme kabiliyeti kazandırıldı. Halen BOME konularında kamu kurumları ile sıkı ilişkiler içerisindeyiz. Ayrıca, ülkemizi ilgilendiren ve bilişim sistemleri kaynaklı güvenlik sorunlarında ulusal irtibat noktası olarak pek çok yurtdışı kurumla ortak çalışmalar yürütmekteyiz.

Ülke içerisindeki çalışmalarımız devam ederken, bir taraftan da bilgi birikimimizin vermiş olduğu özgüvenle yurtdışında benzer hizmetleri gerçekleştirme konusunda bazı gayretlerimiz oldu. Özellikle Bilgi Güvenliği Yönetim Sistemi, İş Sürekliliği gibi alanlarda başarıyla sonuçlanan projelere imza atıldı. Türkiye'nin yakın ilişkiler içerisinde olduğu ülkelere bilgi güvenliğine yönelik eğitimler verildi. Bu çalışmaların önümüzdeki yıllarda artan sıklıkla devam edeceğini öngörüyoruz.

Yıllar geçtikçe kabuğunu kıran ve Türkiye'nin önde gelen bilişim sistemleri güvenliği merkezlerinden biri haline gelen Ağ Güvenliği Grubu ismiyle de bir değişim yaşadı ve **Bilişim Sistemleri Güvenliği Bölümü** adını aldı. Bölüm halen TSK, kamu kurumları, özel sektörden firmalar ile gerek yurtiçi gerekse yurtdışında projeler gerçekleştiriyor. Her geçen yıl büyüyen, konusunda uzman kadrosuyla, oldukça geniş bir yelpazede kurumların bilgi güvenliği gereksinimlerini karşılamaya gayret gösteriyor.

Bilgi Paylaşınca Güzeldir

Özellikle Bilgi Sistemleri Güvenlik Programı'nda yürüttüğümüz çalışmalarımızın ana hedefi, var olan bilgi birikimimizi ülkemizin faydasına sunabilmekti. Bu amaçla kurumlar ve bu alanda çalışan kişiler ile ortak bazı faaliyetler yürüttük. Örneğin biri Ankara'da diğeri de İstanbul'da olmak üzere yılda iki kere gerçekleştirdiğimiz etkinliklerde bilgi güvenliğindeki eğilimler, güncel tehditler gibi konularda paylaşımlarda bulunduk. Ülkemiz için üzerinde durulması gereken bilgi güvenliği konularını masaya yatırarak çözümler üretmeye çalıştık.

Belirli bir kurum ile gerçekleştirilen çalışmaların o kuruma sağlayacağı faydayı inkâr etmek mümkün değil. Aynı şekilde, içi dolu bir etkinliğin katılımcılarına sağlayacağı katma değeri de... Fakat genel kamu yararını düşündüğümüzde, bu faydaların oldukça dar kapsamda kaldığını söylemek mümkün. Bu felsefeden yola çıkarak, bilgi paylaşımını daha etkin gerçekleştirmenin yollarını aradık ve **Ulusal Bilgi Güvenliği Kapısı** (http://www.bilgiguvenligi.gov.tr) *web* portalini kurmaya karar verdik. İki yıldır faaliyetlerini sürdüren bu ortamda bilgi birikimimizi, bilgi güvenliğine destek veren diğer gönüllü uzmanların da katkılarını tüm Türkiye ile paylaşmaya gayret gösteriyoruz.

Kuruluşundan itibaren bilişim sistemleri güvenliği konusunda uzman pek çok kişinin takdirini ve desteğini alan Ulusal Bilgi Güvenliği Kapısı interaktif altyapısı ile katılımcı bir içerik

sunuyor okurlarına. 2500'e yakın kullanıcı, 100'den fazla yazara sahip sitede güncel bilgi güvenliği konularını ele alan teknik yazılar, bilgi güvenliği varlıklarının güvenliğinin sağlanmasını amaçlayan kapsamlı kılavuz dokümanlar ciddiyet ve özenle hazırlanıyor. Bilişim sistemlerinde yeni ortaya çıkarılan güvenlik açıkları takip edilerek önem düzeyi ve ülkemizdeki yaygınlığına göre okuyucularına ulaştırılıyor.

Bugüne kadar 1000'e yakın içeriğe yer veren Ulusal Bilgi Güvenliği Kapısı'nda 5.000.000'u aşkın sayfa görüntülendi. Kurulduğundan bu yana hızla artan ilgiye layık olabilmek için aynı ciddiyetle çalışmalarımıza devam etme niyetindeyiz. Ülkemizde bir benzeri olmadığını düşündüğümüz bu bilgi paylaşım platformunun dünyada da emsalleri ile yarışabilir olduğunu görmek bizi çok memnun ediyor.

Bilişim Sistemleri Güvenlik Testlerine Nasıl Bakıyoruz?

İnternetin günümüzde en önemli bilgi kaynağı haline gelmesi bize birçok kolaylık sağlarken bazı yan etkileri de beraberinde getirdi. Artık merak ettiğimiz bir konu hakkında pek çok dokümana hızlı bir biçimde ulaşabiliyor ve kısa sürede o konunun uzmanı (!) haline geliveriyoruz. Bilgi Güvenliği sektörü de bundan nasibini alıyor tabii. Özellikle konunun ilgi çekici olması, saldırganların paylaşımcılığa önem vermesi ve topluluk çalışmaları sonucunda üretilen araçlar ve platformlar ile pek çok saldırının kolayca gerçekleştirilebilir olmasından ötürü bu işe soyunanların sayısı az değil. Yapılan iş çok önemli bir sermaye gerektirmiyor. Bir internet bağlantısı, test için kullanabileceğiniz bilgisayarlar ve ikna kabiliyetiniz ile "ben de bu işi yapabiliyorum" dememeniz için bir neden yok.

Son yıllarda bilişim sistemleri güvenlik testlerine rağbetin artması, BDDK gibi bazı düzenleyici kurumların güvenlik testlerini zorunlu kılması işin ehli olmayan kişilerin iştahını kabarttı. Diğer taraftan, kurumların ihtiyaç duydukları güvenlik testleri için hazırladıkları şartnamelerin işin niteliğini tarif edememesi kolay yoldan para kazanmak isteyenlerin ekmeğine yağ sürdü. Bu anlamda gerçekleştirmiş oldukları güvenlik testi projelerinden verim alamayan, kendilerine hiçbir katma değer sağlayamayan birçok kurumun yetkilileriyle dertleşme imkânımız oldu.

Bu konuda kurumlara tavsiyemiz, kalitesinden şüphe ettikleri güvenlik testi firmalarına bir ön test yapma zorunluluğu getirmeleri. Ayrıca, hazırlanmış örnek bir Türkçe test sonuç raporu istemeleri. Bu şekilde hem testlerin kalitesini bir nebze olsun ölçme olanağına kavuşurlar hem de oluşan raporun bazı araçlar tarafından otomatik hazırlanan raporların bileşkesi olmadığından emin olurlar.

Konunun özüne gelecek olursak... Sağlıklı bir güvenlik testi nasıl yapılmalı? Şu ana kadar gerçekleştirmiş olduğumuz güvenlik testleri başarının üç sihirli kelimede saklandığını gösterdi: Kapsam, insan etkileşimi ve raporlama.

Öncelikle güvenlik testlerinin tüm kritik bilgi sistemi varlıklarını kapsadığından emin olunmalı. Varlıklar ağ, işletim sistemi, platform ve uygulama düzeyinde ele alınıp, güvenlik bakış açısıyla incelenmedikçe sağlıklı bir sonuç elde etmek mümkün değil. Örneğin, uygulamada alınan bir güvenlik önlemi ağ katmanındaki bazı zafiyetler nedeniyle işlevselliğini yitirebilir. Tabii böyle bir çalışmayı gerçekleştirebilmek konunun temeline hâkim olmayı gerektiriyor.

Otomatik güvenlik testi araçlarıyla gerçekleştirilen çalışmaların etkinliği konusu da üzerinde durulması gereken bir diğer başlık. Ürettikleri yanlış uyarılar ve test uzayını doğru tespit edememe gibi eksiklikler, bu araçların etkinliği konusunda ciddi soru işaretleri oluşturuyor. Her bilgi sistemi, kendine özgü kurulum ve yapılandırması ile farklı karakteristiğe sahiptir. Bu nedenle güvenlik testlerinde farklı yöntemlerin kullanılması ve insan zekâsının dahil edilmesi oldukça önemli. Tabii ki bu tespit, otomatik araçların hiç kullanılmaması anlamına da gelmiyor.

Üçüncü kritik nokta ise raporlama. Özellikle kurumların en çok dert yakındıkları konuların başında, güvenlik testi projeleri sonucunda üretilen raporların kurumları daha güvenli bir noktaya taşıma noktasındaki eksiklikleri geliyor. Raporlar test bulgularını ayrıntılı olarak ele alırken çözüme yönelik tavsiyeleri de içermeli. Hatta testler sırasında kurum personeli ile ortak çalışma yürüterek açıklıkların daha net anlaşılması sağlanmalı. Kurumların almış oldukları ek güvenlik önlemleri de göz önünde bulundurularak risk değerleri gerçekçi bir biçimde belirlenmeli.

Kurumların Bilgi Güvenliğine Bakışları Nasıl Olmalı?

Ülkemizde bilgi sistemlerinin güvenlik testlerine ilişkin, oturmaya başlayan bir kültür var. Bu oldukça güzel bir gelişme. Fakat bilgi güvenliğinin kurumsal bir politika olarak ele alınmadığı ortamlarda sadece testler ile bu ihtiyacın karşılanmaya çalışılması yeterli değil. Firmaların büyük çoğunluğu önemli yatırımlar yapmadan önce gerekli fizibilite çalışmalarını, risk hesaplamalarını yapmaktalar. Özellikle prestij ve maddi kayıpların olabileceği alanlardan da kaçınmaktalar. Aynı modelin, gerçekleştirdiğimiz işlerle doğrudan ilişkili bilişim sistemlerinde de uygulanması gerekiyor. Bu amaçla Bilgi Güvenliği Yönetim Sistemi kurulumu, İş Sürekliliği için gerekli plan ve altyapıların hazırlanması gibi projeler hayata geçirilmeli ve kurumsal bir kültür oluşturulmalı. Bu konuyu önemsemeyen firma ve kurumların önümüzdeki yılların rekabet ortamında gerilerde kalacağını düşünüyoruz.

Bilgi Güvenliği Alanında Ar-Ge Çalışmaları

Bilişim Sistemleri Güvenliği Bölümü olarak geçtiğimiz on yılı aşkın sürede çok önemli bilgi birikimleri elde ettik. Gelecek yıllara bu bilgi birikimimizi güncel bir şekilde taşıyabilmemiz için Ar-Ge çalışmalarımıza hız kesmeden devam etmenin doğru olacağını düşünüyoruz. Ülkemizde TÜBİTAK BİLGEM ve benzeri kurumlar pek çok Ar-Ge faaliyetine imza atarak bu anlamda önemli kazanımlar elde ettiler. Bizim de hedefimiz, özellikle bilgi güvenliği alanında çözüm bekleyen sorunlara eğilmek. Bu nedenle işi sadece Ar-Ge yapmak olan personel istihdam ediyor ve geniş olanaklar sağlamaya gayret gösteriyoruz.

İlk Ar-Ge çalışması olarak Milli Güvenlik Duvarı projesini gerçekleştirdik. Dağıtık (*distributed*) yapıda çalışabilen, aynı anda onlarca noktanın tek merkezden yönetimine olanak sağlayan, yüksek kapasiteli hatlarda üst düzey performans gösteren bir ürün ile sonuçlanan bu proje ülkemiz adına önemli bir kazanım oldu. 200'den fazla kritik noktada çalışan Milli Güvenlik Duvarı, ülkemizin farklı kurumlarında siber savunma kalkanı olarak görev yapıyor. Güvenlik ürünleri alanında dış ülkelere olan bağımlılığımızı azaltmak adına da güzel bir örnek oluşturuyor.

Akıllı kartlar için gerçekleştirdiğimiz Yan Kanal Çözümlemesi çalışmaları da üzerinde durulması gereken bir diğer Ar-Ge faaliyetimiz. Kredi kartları, vatandaşlık kartları gibi yaşamın pek çok alanında kullanılmaya başlayan akıllı kartların güvenliği oldukça önemli bir konu. Akıllı kartların çalışması sırasında ortaya çıkardığı güç, elektromanyetik alan ve işlem zamanı gibi bilgilerle kartın barındırdığı *PIN* numarası, gizli anahtar gibi kritik bilgilerin açığa çıkarılması hedefli yürütülen bu testlerde oldukça başarılı sonuçlara ulaştık. Bu testleri şu an yapabiliyor olmamız gelecekte kullanacağımız akıllı kartların seçiminde veya tasarımında yanlış adımlar atmamamıza imkân tanıyacak.

Bu iki Ar-Ge faaliyetimize benzerlerini eklemek amacıyla 2009 yılında yoğun bir çalışma gerçekleştirdik. Araştırmalarımız, ülkemizde bilgi güvenliğinin sağlanması yolunda, üzerinde durulması gereken onlarca konu olduğunu ortaya koydu. Çalışmalarımızı belirli alanlarda yoğunlaştırabilmek için, potansiyel konuları önceliklendirmeye çalıştık. Sonuçta, beş ana konuda çalışmalara başlayarak, yakın gelecekte somut çıktılar ortaya koymayı kendimize hedef seçtik.

Birincisi, sanal ordular olarak da nitelendirilen '***botnet***'ler. İhtiyaç durumunda, yönetenleri tarafından bir hedefe saldırabilecek biçimde hazırolda bekleyen '*botnet*'ler, önümüzdeki yıllarda gerçekleşeceği tahmin edilen siber savaşların önemli bir enstrümanı olarak görülüyor. Ülkemizde '*botnet*'lere karşı alınan önlemlerin eksikliği ve uygulanabilecek önlemlerin de yetersiz olması bizi bu alanda çalışmalar yürütmeye itti. Amacımız özellikle ülkemizdeki kritik noktalar için '*botnet*'leri saptayan, faaliyetlerini engelleyen ve tespiti sırasında diğerlerini uyarabilen sistemler geliştirmek ve faaliyete geçirmek.

Üzerinde çalışmalar gerçekleştirdiğimiz bir diğer alan ise zararlı yazılımlar. Son yıllarda bilişim sistemlerine gerçekleştirilen saldırılar irdelendiğinde zararlı yazılımların yüksek oranlarda kullanıldığını görüyoruz. Özellikle, bilinen zararlı yazılımların saldırganlar tarafından değiştirilerek tespit edilmesinin zorlaştırılması, önleyici sistemleri çaresiz bırakıyor. Bu anlamda, ülkemizde zararlı yazılımların tespit ve çözümlemesini gerçekleştirecek altyapının oluşturulmasını ihtiyaç olarak görüyoruz.

Yürüttüğümüz diğer bir Ar-Ge çalışması da veri kaçağı önleme mekanizmaları üzerine. Özellikle son iki yılda kurumlardan kontrolsüz bilgi çıkışı ile ilgili pek çok haber kulağımıza çalındı. Dünyada da bu konunun popüler hale gelmesiyle, özellikle anti-virüs firmalarının bazı ürünler çıkardığını söylemek mümkün. Öte yandan, bu ürünleri incelememiz sonucunda bulduğumuz, özellikle Türkçe dokümanlarda yer alan içeriğin anlamlandırılması ve gizlilik düzeyinin saptanmasına yönelik kullanılan yöntemlerdeki önemli eksiklikler bizi bu alanda çalışmaya teşvik etti.

Önemsediğimiz bir başka konu da açık kaynak kodlu sistemler. Yine TÜBİTAK BİLGEM tarafından desteklenen Pardus işletim sisteminin her geçen gün daha fazla ilgi görmesi, açık kaynak kodlu sistemlerin güvenliğinin sağlanması adına bazı çalışmaların gerçekleştirilmesini gerekli kıldı. Özellikle merkezi yönetim ve güvenlik yönetimi konularında Pardus projelerine önemli katkılarda bulunuyoruz.

Kimlik yönetimine dayalı bir güvenlik sisteminin, kurumları pek çok bilgi güvenliği tehdidi karşısında güçlü kılacağını düşünüyoruz. Bu nedenle, bu alandaki çalışmalarımızı yoğunlaştırdık. Kurumsal uygulamalarda kimlik doğrulama ve yetkilendirme gibi fonksiyonların ayrı sistemler üzerinden gerçekleştirilmesi, kullanıcı hesaplarının tekil olarak oluşturulması, uygulamalar arasında tümleşik kimlik doğrulama ile geçişlerin gerçekleştirilebilmesi, İnsan Kaynakları Bölümleri ile bütünleşerek yetki verilmesi ve iptali işlemlerinin otomatize edilmesi gibi konularda kurumların gereksinimlerine göre projeler gerçekleştirmekteyiz.

Özetleyecek olursak, günümüze değin gerek Bilişim Sistemleri Güvenliği Bölümü gerekse ülkemiz adına, bilgi güvenliği konusunda önemli mesafeleri kat ettiğimizi söyleyebiliriz. Bundan sonra da aynı motivasyon içerisinde ve büyüyerek çalışmalarımıza devam etmeyi hedefliyoruz. Bir taraftan ülkemizin bilgi güvenliği konusunda bilinçlenmesi adına yüklenmiş olduğumuz misyonu yerine getirirken diğer taraftan Ar-Ge çalışmalarımız ile geleceğimizi aydınlatmak istiyoruz.

BULUT BİLİŞİM

YAKUP KORKMAZ, MUHARREM AYDIN, BİLGE KARABACAK

1. Giriş

Bilişim uzmanları, interneti doğumundan bugüne kadar üç evreye ayırmakta ve bulut bilişimi[1] internette üçüncü evre olarak nitelendirmektedir. Birincisi, herkesin bilgisayarında çalıştığı ve internette sınırlı sayıda bilgiye ulaştığı evreydi ve diğer bir ifadeyle internetin başlangıcıydı. Bu evre, doksanlı yılların ortasına kadar sürdü. İkincisi, internetin yaygınlaşması evresiydi. Doksanların ortasında başlayıp günümüze kadar sürdü. Üçüncüsü ise, bulut bilişim evresidir. Her ne kadar, Amerika Birleşik Devletleri epey yol aldıysa da, dünya hatta gelişmiş ülkeler ortalamasına baktığımız zaman, ülkelerin bu evrenin başında olunduğu söylenebilir. Birinci evrede, hem veri hem de yazılımlar bilgisayarlarda tutuluyordu. İkinci evrede, yazılımlar hala bilgisayarlarda tutulmakla beraber, verinin büyük çoğunluğu artık internetteydi. Üçüncü evrede ise, hem veri hem de yazılım internetten sunulmaktadır [1].

Bulut bilişimin temel mantığını ifade eden kısa cümleler: "bilgisayarınıza yazılım kurmayın, fazla depolama alanına da gereksiniminiz yok, yazılım lisanslarına para ödemeyin, bilgisayarlarınız çok düşük donanım özelliklerinde olabilir, basit bir internet gezinti aracı (örn: firefox) ile internete erişin; hem yazılımlarınız hem de verileriniz internette" şeklinde verilebilir.

çizerken, internet ortamını ve internet altyapısını "bulut" şeklinde göstererek soyutlarlar. Bulut bilişim kavramındaki "bulut" ifadesi de, benzer mantıkla hem yazılım hem de donanım araçlarına sahip olma zorunluluğunun azalması, kullanıcının kullandığı sistemin iç yapısındaki karmaşıklıktan soyutlanması ve bu gereksinimlerin birer "hizmet" olarak temin edilmesi olarak düşünülebilir [2].

"Her şey hizmet" sloganı, en az kelimeyle bulut bilişimi ifade etme amacıyla kullanılabilir. Bulut bilişim çok temel olarak, bilgi teknolojileri kaynak ve kabiliyetlerinin hizmet olarak sunulmasıdır. Bulut bilişimi bugüne kadar süregelmiş yaklaşımlardan ayıran temel unsurlar, bu kaynak ve yeteneklere kolaylıkla erişilip, kolaylıkla yönetilebilmesi şeklinde özetlenebilir. Bulut bilişimde uygulama, veri saklama, bilgi işleme, uygulama geliştirme, iletişim kaynakları ve altyapılar gibi, hemen hemen tüm bilgi teknolojileri kaynak ve yetenekleri hizmet olarak sunulabilmektedir.

Kapsamı biraz daha genişleterek bulut bilişimi, "çok hızlı bir şekilde ve minimum yönetim çabasıyla kullanıma sunulabilen, özellikleri değiştirilebilir bilişim kaynaklarını (sunucular, depolama alanları, uygulamalar) barındıran bir paylaşım havuzuna istek olduğunda, pratik bir şekilde ağ üzerinden erişmeye imkân sağlayan model" olarak tanımlayabiliriz [1].

Faaliyetlerine bir arama motoru olarak başlayan Google, bulut bilişime ciddi yatırım yapmaktadır. Google'ın dünyanın dördüncü büyük sunucu üreticisi olduğu, New York Times gazetesinin 3 Temmuz 2006 tarihli sayısında çıkan haberde, Martin Reynolds isimli bir Gartner çalışanı tarafından ifade edilmiştir.

Bilişim sektöründe, 2009 yılı içinde yaşanan gelişmeler sıralanırken, bulut bilişim ve uygulamaları ilk sıralarda kendisine yer bulmaktadır. ABD kaynaklı "The New Media" şirketler birliği ve "Educause Learning Initiative" kuruluşunun birlikte hazırladığı 2009 Gelecek Raporu (The Horizon Report 2009) bulut bilişimin, bir sene veya daha kısa bir süre içerisinde, yoğun bir şekilde benimseneceğini ifade etmektedir [3]. Sektöründe lider bazı kuruluşların tahminlerine göre, önümüzdeki 5-10 yıl içinde bilişim işlemleri ve veri depolamanın yarısından çoğu "bulut"un içinde olacaktır [2]. Bulut bilişimin hizmet sağlayıcı açısından önemli bileşenlerinden

Google, Chrome isimli işletim sistemini Temmuz 2009'da duyurdu ve 2010 yılının ikinci yarısında kullanıma hazır olacağını belirtti. Bu işletim sistemi, aslında internetten sunulan hizmetlere erişim için geliştirilmiş en az özelliklere sahip bir "bulut istemcisi" olarak tasarlanmıştır. İşletim sisteminin yapacağı en önemli işlem, internet tarayıcısını (browser) çalıştırmaktan ibarettir. Google şirketinin bütün bu hazırlıklarının nedeni, internetin üçüncü evresinde en önde olmak olarak özetlenebilir.

[1] "Cloud Computing" kavramının Türkçe karşılığı, bilişim sektörü çalışanları arasında tartışılmaya devam ediyor. "Bulutsu Bilişim", "Kümesel İşlem", "Sis Bilişimi" gibi öneriler ortaya atılsa da en yaygın kabul gören öneriler "Bulut Bilişim" ve "Bulut Bilgi İşlem" oldu. Bu yazıda "Bulut Bilişim" terimi kullanılmıştır.

Google şirketinin yapmış olduğu duyurular temel alınarak hazırlanan ve şirketin teknik altyapısının tanıtıldığı "Google Platform" wiki sayfasında, ilginç bilgiler yer almaktadır. Wiki sayfasına göre, Google şirketinin 450.000'den fazla sunucusu bulunmaktadır.

birisi olan "sanallaştırma"nın pazar payı, 2008 yılına oranla 2009'da %40'tan fazla büyüme kaydetmiştir [4]. Gartner araştırma şirketine göre, 2013 yılına gelindiğinde bulut bilişim sektörünün, 150 milyar dolarlık bir hacme ulaşması beklenmektedir [5].

HP, Microsoft, Google gibi şirketler, internet üzerinden hizmet satışı yapmak için, 'Neden ciddi yatırımlar yapıyorlar?' 'Gerçekten tahminler tutacak mı?' gibi sorulara yanıt vermek için, duruma bir de bulut bilişimden yararlanacak kurumlar tarafından bakmakta yarar vardır. Günümüzde kurumların hangi alanlarda çalışma yaptıklarına bakılmaksızın, bir ürün ortaya koymak veya bir hizmet sunmak için, donanımsal ve yazılımsal olarak, teknolojik bir altyapıya sahip olmaları gerektiği görülmektedir. Bununla beraber, kurumların son dönemde giderek artan şekilde, yalnız uzmanlaştıkları alanlarda ve iş kollarında çalışmayı, oluşan diğer tüm gereksinimlerini ise, dışarıdan kendi alanında uzmanlaşmış kuruluşlardan sağlamayı tercih ettikleri gözlemlenebilir.

Bunların sonucu olarak giderek daha fazla kurum, ekonomik faaliyetlerini gerçekleştirebilecek teknolojik altyapı ihtiyaçlarını karşılamak için gerekli olan veri merkezlerini, kurum içinde kurmak ve yönetmek yerine, bu ihtiyaçlarını dışarıdan "bulut bilişim hizmet sağlayıcı" şirketlerden elde etme yolunu seçiyor. Böylece kurumlar uzmanlaştıkları ana iş kollarına odaklanıp, daha yaratıcı ve verimli çalışmaktadırlar. Bulut bilişim firmalarının, büyük ölçekte ve yüksek hacimde veri merkezleri kurup yönetmesi sonucu müşteri kurumlar; yönetim, ağ ve depolama teknolojileri ihtiyaçlarını daha düşük birim maliyetlerde elde edebilmektedirler. Büyük ölçekteki veri merkezleri (50.000 sunucu kapasiteli), orta büyüklükteki veri merkezlerine (1.000 sunucu kapasiteli) göre, yönetim ve ağ teknolojisi birim maliyetlerini yedi kat, depolama teknolojisi maliyetlerini ise beş kat düşürebilmektedirler [6]. Ayrıca elektrik maliyetinin veri merkezlerinin toplam maliyetlerinin 1/3'ünü oluşturduğu bilinmektedir [7]. Bulut bilişim hizmet sağlayıcıları, bölgeler arasında büyük fark gösteren elektrik birim fiyatları sebebiyle (ABD içinde bölgeler arası altı kata varan fiyat farkı bulunmaktadır [8]), elektrik maliyetlerinin en düşük olduğu bölgelerde kümelenerek, genel harcamalarda da büyük oranda indirime gidebilmektedirler. Kurumlar, teknoloji altyapılarını oluşturmak için teknolojik altyapı yatırımlarında bulunup, yüksek sermaye maliyetlerine katlanmak yerine, operasyon maliyetleri ile iş yapmaya ve arta kalan sermayelerini asıl çalışma yaptıkları ana iş kollarına aktarabilmektedirler. Anlık veya dönemlik oluşabilecek iş yoğunluğu durumlarında, bulut bilişim hizmet sağlayıcılarının gerektiği anda gerektiği kadar kaynak ayrılmasını sağlayan teknolojileri sayesinde, kurumların her türlü yoğun kullanım durumunda, aynı performansta hizmet sunmalarına imkân tanımakta ve kurumların kaynak israfına yol açan, bu durumlara özel fazladan sunucular bulundurmalarının önüne geçilmektedir. Kurumların bu teknolojiden yoksun olan kendi veri merkezlerinde, sunucularının ortalama kapasite kullanım oranlarının %5 ile %20 arasında değiştiği hesaplanmakta ve kaynak israfının boyutları gözlenebilmektedir [9, 10].

2. Neden Bugün?

George Lucas'ın, Yıldız Savaşları serisini tasarlarken ilk üç bölümü o zamanın teknolojisiyle çekemeyeceği düşüncesiyle ertelediği ve bu nedenle ilk olarak dördüncü bölümü çektiği söylenir. Son yıllarda yoğun şekilde konuşulmaya ve

Google sunucuları, ABD'nin değişik eyaletlerindeki on iki farklı yerleşkede ve Avrupa'da yer almaktadır. Google şirketinin en büyük veri merkezlerinden biri, hidroelektrik santrallerinden sağlanan enerjinin ucuz olması nedeniyle, Oregon eyaletindeki The Dalles şehri yakınlarında Kolombiya nehri kıyısında kurulmuştur. Her biri futbol sahası büyüklüğünde iki adet binanın yanında, iki adet dört katlı bina yüksekliğinde soğutma kuleleri bulunmaktadır.evresinde en önde olmak olarak özetlenebilir.

gerçeklenmeye başlanan bulut bilişim için de, durum buna benzemektedir. 1960'lı yıllarda ARPANET'in geliştirilmesinden sorumlu olan Licklider, "İntergalaktik bilgisayar ağı" fikrini ortaya attı. Bu düşünceye göre dünyadaki herkes birbiriyle bağlantılı olacak ve programlara ve verilere herhangi bir yerden erişebilecekti [11]. Günümüze kadar bulut bilişim değişik evrelerden geçti. Değişik nedenlerle başarılı olamayan bu evreler, bugünkü bulut yaklaşımının da hazırlayıcısı oldu. Grid computing ve yarar bilişimi (utility computing) bu evreler arasında en çok bilinenlerdir. Bulut bilişim fikri çok eskilere dayanmasına rağmen uygulamalarının yeni başlamasının en önemli nedenleri şunlardır:

- Sağlam ve yüksek hızlı ağların yaygınlaşması,

- Açık arayüzlü sunucu donanımlarının farklı markalardaki bileşenlerin birbirine bağlanmasına olanak tanıması; bu sayede marka bağımlılığının ortadan kalkması ve farklı ihtiyaçlar için farklı donanımlar kullanılabilmesinin önünün açılması,

- Açık kaynak kodlu yazılımların (Örn: Linux, Apache) sunulacak hizmetlerin maliyetini düşürmesi,

- Bulut içindeki uygulamaların geliştirilmesini son derece hızlandıran açık Web 2.0 ve benzeri standartlar.

3. Bulut Bilişimin Anahtar Özellikleri ve Üstünlükleri

Makalenin bu bölümünde bulut bilişimin birçok üstünlüğü maddeler halinde sıralanmıştır [1].

- Bulut bilişiminden yararlanan kurum (tüketici), istediği hizmeti bulut hizmet sağlayıcısından herhangi bir insan iletişimine gerek duymadan alabilir, kullanmadığı hizmeti de geri verebilir. Hizmet, bir yazılım olabileceği gibi, işlemci ve boş disk alanı gibi kaynaklar da olabilir.

- Hizmet sağlayıcılar, tüketicinin arzu ettiği yetenekleri hızla ve düşük maliyetle sunabilme kapasitesine sahiptir. Hizmet sağlayıcı kullanılmayan hizmetleri, tüketicinin kullanımına hazır halde bir havuzda tutar.

- Hizmetler ve kaynaklar ortak ulaşılan bir ağ üzerinden, (ör. internet) kullanıma hazır durumdadır ve ağ bağlantısı olduğu müddetçe hizmetlere tüm platformlardan erişilebilir. Hizmet alan kullanıcı, ağa bağlanabildiği her yerden gereksinim duyduğu veri ve hizmetlere kolayca ulaşabilir.

- Tüketiciye sunulan yetenekler, hizmet sağlayıcı tarafından sunulan araçlarla kontrol edilebilir. Yeteneklerin kullanımı izlenebilir, kontrol edilebilir ve hem tüketiciye, hem de hizmet sağlayıcıya rapor olarak sunulabilir.

- Tüketici, gereksinimi olan kadar hizmeti kiralar ve kiraladığı kadar ödeme yapar. Örneğin finansal kurumlar, ayın belli günlerinde yoğun bir bilgi işlem gücüne gereksinim duyarken, çoğu günler daha az seviyede bilgi işlem gücü ile çalışmalarını sürdürebilirler. Bu durumda, kurumlar yoğun günleri dikkate alarak, ciddi yatırım yaptıkları bilgi işlem altyapısını, büyük oranda kapasitesinin altında kullanmış olurlar. Tüketici, bulut hizmet sağlayıcıdan ayın belli günleri için daha çok işlemci ve disk alanı kiralayarak, gereksinimini daha ucuz bir şekilde karşılamış olur.

- Bütün veri uzak bilgisayarlarda tutulduğu için, son kullanıcılar için sabit disklerin bozulmasının veya dizüstü bilgisayarlarının çalınmasının, veri kaybı ve güvenliği konusunda ciddi sonuçları olmayacaktır (Bulut bilişimin ortaya çıkardığı veri mahremiyeti riskine makalenin altıncı bölümünde yer verilmiştir).

- Bulut bilişim, bilgi ve uygulamaların çevrimiçi paylaşımına olanak sağladığı için, yeni "birlikte çalışma" modelleri sunar. Bu açıdan değerlendirildiği zaman, özellikle akademik kurumlar ve üniversiteler için, yeni işbirliği olanaklarının kapısı aralanmaktadır.

- Bulut bilişim, hem sıradan hem de kişiye özel bilişim sorunlarının çözümleri için, yapılacak harcamaları ve çözüm karmaşıklığını azaltabilecek gerekli potansiyele sahiptir. Güçlü sistemleri, bugüne kadar olduğundan çok daha düşük maliyetle kullanıma sunan bulut bilişim, araştırmacılara bugüne kadar başarılamamış gen araştırmalarını, çevresel modellemeleri, yaşayan sistemlerin analizini ve daha birçok alandaki araştırmaları gerçekleştirme olanağı sunmaktadır.

- Bulut bilişim ile birlikte, hem kurumlar hem son kullanıcılar için, güçlü bilgisayarlara duyulan gereksinim ortadan kalkmaktadır. Basit donanımda bir kişisel bilgisayar ile, hatta bir cep telefonu ile, gereksinim duyulan hizmetlere erişilebilir. Bu yönüyle bulut bilişim, özellikle gelişmekte olan ülkelerde, bilişim hizmetlerinin yaygınlaşması adına büyük olanaklar sunmaktadır.

- Her kullanıcının bilgisayarına tek tek kurulması gerekmediğinden, bulut bilişim uygulamalarının bakımı çok daha kolaydır. Değişiklikler kullanıcıya anında yansıyacağından, teknik destek büyük ölçüde kolaylaşır.

- Bulut bilişimin şirketler ve organizasyonlar için en büyük yararlarından biri, bilişim sistemlerinin yönetim zorluklarını ve yönetim maliyetlerini çok büyük oranda azaltmasıdır. Bu durum özellikle üst düzey bilişim sistemlerini ve iyi yetişmiş bilişim yöneticilerini istihdam etme zorluğu çeken kamu kurumları ve kâr amacı gütmeyen kurumlar için önem taşımaktadır. Bilişim teknolojileri alanında eğitim görmüş nitelikli eleman bulma konusunda sıkıntı yaşayan kurumlar, bulut bilişimin gelişmesinden en üst düzeyde yararlanacaklardır. Aynı durum gelişmekte olan ülkeler için de geçerlidir. Bir internet bağlantısı ve bulut sayesinde az gelişmiş ülkelerdeki araştırmacılar, hükümet yetkilileri ve girişimciler, nerede olduklarının bir önemi olmaksızın en iyi bilişim yeteneklerine erişebileceklerdir.

- Bulut bilişim, büyük şirketlerin sahip olduğu karmaşık bilişim sistemlerine sahip olma gücü olmayan küçük ve orta bütçeli işletmelerin (KOBİ), hareket alanlarını alabildiğine genişletmektedir. Bulut bilişim sayesinde KOBİ'ler uzmanlaştıkları konularda, diğer şirketlerin hizmetlerinin bir parçası olarak hizmet verebilecek durumda olacaklar. Aynı şekilde, dünyanın her köşesindeki uygulama geliştiren bireysel girişimciler, herhangi bir yerdeki ortaklarla işbirliği yapabilecek, fikirlerini paylaşabilecek ve böylece ufuklarını alabildiğine genişletmiş olacaklar.

- Bulut bilişim, dayanıklılığı ve güvenliği artırması, bakım maliyetlerini azaltması ve daha çok esneklik sağlaması nedeniyle, devlet yönetimleri için özel olarak çekicilik taşımaktadır. Yüzlerce farklı sistem yerine, devlet yönetimi işlemlerini tek bir bulut içinde çalıştırmak, daha dayanıklı, daha güvenli, daha az masraflı ve çok daha kolay yönetilir sistemlere sahip olmayı sağlayacaktır.

- Kurumların bilgi işlem altyapısındaki cihazların tükettiği enerjiden çok daha fazlası, cihazların bulunduğu ortamı soğutmak için kullanılmaktadır. Küresel ısınmayla mücadele konusunda, bilişim dünyası adına atılabilecek en önemli adım bulut bilişimdir. Özellikle sadece belli zaman aralıklarında bilgi işlemi yoğun şekilde kullanan kurumların bulut bilişimden faydalanmaları çok önemli enerji tasarruflarının da önünü açacaktır.

- Bulut bilişim, kurumlar için önemli bir bütçe kalemi olan yazılım lisans maliyetlerini, büyük ölçüde düşürme potansiyeline sahiptir. Benzer durum son kullanıcılar için de geçerlidir. Bulut bilişim, ayrıca son kullanıcılar için korsan yazılım kullanımını ciddi oranda azaltabilir.

4. Bulut Bilişim Gerçekleştirme Modelleri

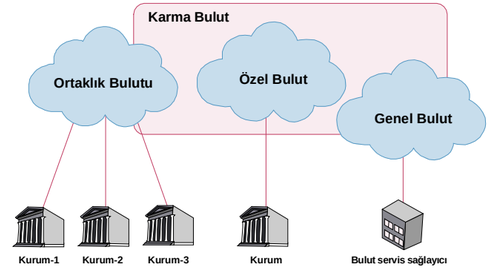
Bulut bilişim için farklı senaryolar ve gereksinimler göz önüne alınarak oluşturulmuş dört farklı gerçekleştirme modeli bulunmaktadır [12]. Bunlar Şekil-1'de gösterilmiştir.

- Genel Bulut (Public Cloud): Bulut altyapısı, internet üzerinden genel kullanıcılara ya da çok geniş bir endüstri grubunun kullanımına açıktır. Bulut hizmetlerinin satın alındığı organizasyon tarafından yönetilir. İyi ölçeklendirilmiş web hizmetleri, internet üzerinden tüketiciye sunulur. Örneğin Google birçok uygulamasını, genel bulut üzerinden son kullanıcıların hizmetine sunar.

- Ortaklık Bulut'u (Community Cloud): Bulut altyapısı, ortak ilgileri (ör: görev tanımı, ortak güvenlik ihtiyaçları) olan birden çok kurum tarafından paylaşılır. Gerçekleştirme, kurumlar tarafından yönetilebilir veya bu kurumlar dışındaki bir hizmet sağlayıcı da yönetimi yapabilir. Masraf tüketiciler arasında paylaşıldığı için genel buluta göre daha pahalı bir çözümdür. Diğer taraftan daha yüksek bir güvenlik, mahremiyet ve politika uyumluluğu bu yolla sağlanabilir. Google, ABD'de kamu kurumları için ortaklık bulut modeli geliştirmiştir [1].

- Özel Bulut (Private Cloud): Bulut altyapısı sadece bir kurum için ve kurumun yönetimindeki özel ağ (veya kiralık hatlar) üzerinde çalışır. Bu model, özellikle güvenlik ve mahremiyet ile ilgili riskleri büyük ölçüde düşüren bir çözümdür. Özel bulut, ülkemiz için özellikle taşra teşkilatı olan kamu kurumları için uygun bir çözüm olabilir.

- Karma Bulut (Hybrid Cloud): Gereksinime göre değişik modellerinin farklı kombinasyonlarda kullanılmasından oluşur. Birden fazla ağ içi ve/veya dışı hizmet sağlayıcı karma bulut çözümü içerisinde yer alabilir. Benzer şekilde birden fazla kurum da, karma bulut hizmetinden yararlanabilir. Örneğin, güvenlik gerekliliği yüksek olan veriler için ortaklık bulutundan hizmet alınırken, internet kullanımı gibi rutin faaliyetler için genel bulut kullanılabilir.



Şekil 1. *Bulut hizmet gerçekleştirim modelleri.*

5. Bulut Hizmet Seviyeleri

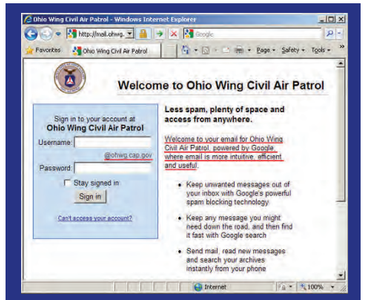
Şekil-2'de gösterildiği gibi, bulut bilişim hizmetleri üç temel katmana ayrılmaktadır. Bir bulut hizmet sağlayıcı, donanımları (işlemci, bellek, disk alanı) hizmet olarak sunabilir. Bu durumda müşteri kurumdaki ağ mimarları, bu donanımları hizmet sağlayıcı tarafından sağlanan yönetim arayüzleri ile, kurum gereksinimlerini dikkate alarak kullanabilir duruma getirecektir. Yine kurumdaki bilişim uzmanlarının, donanımların üzerinde çalışacak olan işletim sistemlerini ve yazılımları kurmaları gerekecektir. Diğer taraftan, bulut hizmet sağlayıcı, uygulama geliştirme platformunu hizmet olarak sunabilir. Bu durumda da kurum donanım mimarisi ile uğraşmayacak, ancak kurumdaki uygulama geliştiricileri, hizmet sağlayıcı tarafından verilen teknik imkanları kullanarak, uygulamaları geliştireceklerdir. Hizmet sağlayıcı, kurumun kullanacağı

yazılımları hizmet olarak sunabilir. Bu durumda kurumun yapacağı tek işlem, ilgili yazılımı satın almak ve ortak ağ üzerinden kullanmak olacaktır. Makalenin bu bölümünde, özetlemiş olduğumuz bu üç farklı hizmet seviyesi ayrıntılandırılmıştır.

5.1. Bir Hizmet Olarak Yazılım (Software as a Service –SaaS) SaaS, bir yazılım şirketi tarafından geliştirilen ve yönetilen, müşterilerinin ise internet üzerinden kullanabildiği bir yazılım olarak özetlenebilir. Kullanıcı tarafından bilgisayarlara veya sunuculara kurulan geleneksel paket uygulamaların aksine, yazılımın sahibi bulut hizmet sağlayıcıdır. Yazılımı kendi veri merkezlerindeki bilgisayarlarda çalıştırır. Müşteri ise, yazılıma sahip değildir ama, genellikle aylık bir ücret karşılığı kiralar. SaaS "istek üzerine yazılım" olarak ta ifade edilmektedir.

SaaS uygulamaları yerinde kurulumdan daha ucuzdur. İşletmeler, yazılımları çalıştırmak için ek donanım veya altyapı almak zorunda değillerdir. Dolayısıyla SaaS'da sermaye harcamaları yoktur. Geleneksel kurumsal yazılımlarda olduğu gibi, yazılımın kurulması, yaygınlaştırılması, bakımı ve desteği için kaynak harcamaya gerek yoktur.

Hizmet olarak sunulan yazılımlar çok geniş bir yelpazeye hitap etmektedir. internetten kitap satışı ile faaliyete başlayan Amazon.com'un, S3 isimli çevrimiçi depolama hizmetini bir web hizmeti olarak kullanıcılara sunmaktadır. Google şirketinin docs.google.com adresinden sunduğu "dokümanlar" hizmeti de, senelerdir kullandığımız Microsoft Ofis paketinin, en bilinen öğelerinin eşdeğerlerini çevrimiçi olarak sunmaktadır. Hemen hemen herkesin, yıllardır kullandığı Hotmail, Gmail gibi e-posta hizmetleri de, aslında birer SaaS olarak nitelendirilebilir.



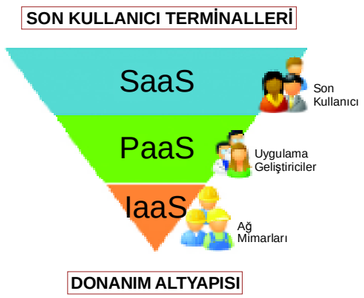
Hizmet olarak yazılım şeklinde Google şirketinin ücretsiz e-posta hizmetinin yanı sıra, takvim ve ofis uygulamaları gibi ücretsiz uygulamalarını da internet üzerinden kullanıyoruz. Amerika Birleşik Devletleri'nde birçok hükümet birimi ve kamu kurumu, e-posta hizmetini Google şirketinden kurumsal olarak almaya başlamıştır. Hükümet birimi böylece, e-posta hizmeti için sunucu işletmekten kurtulmuş, belli bir ücret karşılığında bu hizmeti Google şirketinden almaya başlamıştır. Tabi ki, Google şirketinin ABD hükümet birimine verdiği bu hizmet, kuruma özeldir ve ücretsiz hizmetlerden faydalanan internet kullanıcılarında çıkan reklamlardan arındırılmış bir hizmettir. Ekran görüntüsü, Amerikan Hava Kuvvetleri'ne bağlı olarak Ohio'da faaliyet gösteren bir kamu kurumunun, http://mail.ohwg.cap.gov adresinden aldığı e-posta hizmetinin ana sayfasının görünümüdür.

5.2. Bir Hizmet Olarak Platform (Platform as a Service – PaaS)

PaaS seviyesinde hizmet sağlayıcı, uygulama geliştirme ortamını, uygulamanın çalışacağı ortamı, tamamlayıcı hizmetleri ve altyapıları (ör. oturum yönetimi, kimlik doğrulama, versiyon yönetimi, ölçeklenebilirlik) tasarlayıp kurar. Müşteri kurumdaki uygulama geliştiriciler, uygulamaları bu platforma göre geliştirir. Böylece bulut uygulamalarının hayata geçirilmesi için, gerekli tüm donanım ve yazılım katmanlarının, ayrı ayrı satın alınıp yönetilmesine ihtiyaç kalmaz. Bu platformlara, Microsoft'un Windows Azure Platformu, code.google.com adresinden erişilen Google App Engine ve Adobe firmasının ColdFusion çözümü örnek olarak verilebilir.

5.3. Bir Hizmet Olarak Altyapı (Infrastructure as a Service – IaaS)

SaaS seviyesinde müşteri kurum, işlemci gücü, veri saklama ve ağ kaynaklarını hizmet olarak kullanır. SaaS büyük oranda sanallaştırma teknolojisine dayanmaktadır. VmWare, Microsoft'un geliştirdiği Hyper-V ürünü ve açık kaynak kodlu Xen, en yaygın kullanılan sanallaştırma araçlarıdır. Acil olarak bir sunucuya ihtiyaç duyan kurumun, hizmet sağlayıcıya internet üzerinden üye olması ve on dakika içinde istediği özellikte bir sunucuyu oluşturup, bu sunucuya SSH hizmeti ile erişmesi, IaaS kullanımına örnek olarak verilebilir. Kurumun işi bittiği zaman yapması gereken, işlem hesabından sunucuyu silmesi olacaktır. Amazon.com'un EC2 isimli yaygın olarak kullanılan bir IaaS hizmeti bulunmaktadır. Amazon EC2 ile sanallaştırılmış bir sunucu, saati 0.1 USD fiyatla kiralanabilmekte ve bu sanal makine üzerinde istenilen yazılım yüklenip hizmete sunulabilmektedir. Diğer taraftan, Amazon'a göre daha az bilinen RackSpace, benzer bir hizmeti saati 0.015 USD fiyatla sunmaktadır [13].



Şekil 2. *Bulut hizmet seviyeleri ve her bir seviyedeki roller.*

ABD Hükümeti, bulut bilişim ile ilgili teknolojik gelişmeleri yakından takip etmektedir. Kurumsal e-posta örneğinde olduğu gibi, ABD Hükümeti'nin yoğun olarak bulut bilişime yatırım yaptığı ve giderek artan şekilde bulut bilişim hizmetlerini tercih ettiği görülmektedir. Amerikan Hükümeti bilgi sistemleri yöneticisi (CIO) Vivek Kundra, 75 milyar USD teknoloji harcamasıyla, Amerikan Hükümeti'nin teknoloji firmalarının en büyük müşterisi konumunda olduğunu belirtmektedir. Bunun en son örneği, ABD Hükümeti tarafından açılan ve www.apps.gov adresinden hizmet veren sitedir. Bu internet sayfasından, güvenilir bulut bilişim hizmet sağlayıcıları tarafından sunulan hizmetlerin tanıtımı ve satışı yapılmaktadır. ABD Hükümeti'nin bu siteyi oluşturmaktaki amacı, birçok bulut bilişim hizmet sağlayıcısını ve hizmetlerini tek bir noktadan sunmak ve bu sayede kamu kurumlarını bulut bilişim hizmetlerine yönelmeye özendirmek ve bu hizmetlere geçişe teşvik etmektir. Bu siteyi oluşturarak amaçlanan diğer bir fayda ise, resmi devlet kurumlarının güvenlik ve teknik yeterlilik konusundaki tereddütlerini gidermek ve bulut bilişim hizmet alımında oldukça uzayan bürokratik işlemleri kısaltarak, geçişi hızlandırmaktır. Ayrıca, Kundra'nın belirttiğine göre, Amerikan Hükümeti ilerleyen aşamalarda kendine ait bulut bilişim altyapısını ve hizmetleri oluşturacak ve hizmetlere bu site üzerinden erişilebilecektir. ABD Hükümeti'nin henüz yeni sayılabilecek olan bulut bilişim teknolojisine yaptığı yatırımlar, bulut bilişim hizmetlerinin yaygınlaşması yönünde önemli göstergelerden birisi olarak sayılabilir.

6. Bulut Bilişim'in Riskleri

Sunduğu geniş olanakların ve esnekliğin yanında, bulut bilişim beraberinde belirli riskleri de getirmektedir. Bu bölümde, riskler üzerinde durulurken unutulmaması gereken nokta, her riskin bir fırsat ile eşlenmiş olduğu; bulut bilişim tarafından sunulan fırsatların getirisi ile, göze alınan riskin sonucunda karşı karşıya kalınabilecek zararın değerlendirmesinin, her kurumun kendine özel şartları, dinamikleri ve çalışma alanları göz önünde bulundurularak iyi yapılmış olmasıdır. Ayrıca risklerin değerlendirilmesi sırasında dikkat edilmesi gereken bir diğer nokta da, bulut bilişimin içerdiği riskler ile hali hazırda kullanılan geleneksel çözümlerle devam edilmesi durumunda, karşı karşıya kalınabilecek risklerin karşılaştırmasının doğru olarak yapılmış olmasıdır [14]. Belirli riskler sadece bulut bilişime özel olmakla birlikte, bazı riskler geleneksel yöntemlere göre, bulut bilişimde daha fazla veya daha az olabilecektir. Bulut bilişimin barındırmadığı ve sadece geleneksel yöntemlerde rastlanabilecek riskler de mevcuttur. Yapılacak risk değerlendirmesinin sağlıklı olabilmesi için, tüm bunların göz önünde bulundurulması gerekmektedir.

Makalemizin bu bölümünde bulut bilişimin beraberinde getirdiği yedi adet riske yer verilmiştir. Bu bölüm altında yer alan alt bölümlerde, her bir risk kendi içinde farklı açılardan incelenmiş, risklerin azaltılabilmesi için yapılması gerekenlere veya hali hazırda yapılmakta olan çalışmalara yer verilmiştir. Bulut bilişim ile ilgili riskler yedi alt başlık altında incelenmiştir:

1. Hizmet Devamlılığı ve Kullanılırlığı
2. Veri Güvenliği ve Gizliliği
3. Veri Denetlenebilirliği, Uygunluğu ve Yasal Düzenlemeler
4. Hizmet Sağlayıcı Bağımlılığı ve Veri Kilitlenmesi
5. Yönetim Ara yüzü ve Uzaktan Erişim
6. Bant Genişliği ve Veri Transferi
7. Yazılım Lisanslama

6.1. Hizmet Devamlılığı ve Kullanılırlığı

Bulut bilişim, hizmet sağlayıcılarda hizmet kesintisine neden olabilecek bir sorun yaşanması durumunda, bu hizmet sağlayıcıdan hizmet alma yoluna gitmiş tüm kurumlar birden bundan etkilenecek ve kesinti sonuçlanana kadar, kurumların hizmet veremez hale gelmelerine neden olacaktır. Eğer kurumlar tüm teknolojik altyapı ve hizmetleri tek bir bulut bilişim hizmet sağlayıcıdan temin ediyorlarsa, oluşabilecek bir kesinti, kurumun tüm işletme ve ekonomik faaliyetlerinin durmasına neden olabilir. Her ne kadar bulut bilişim hizmet sağlayıcı firmalar bu tür durumlara karşı hazırlıklı ve çok geniş teknolojik altyapılara sahip olsalar da, Haziran 2008'de Google AppEngine'de meydana gelen bir programlama hatasından dolayı 6 saat, Temmuz 2008'de ise Amazon S3'te tek bir bit hatasından kaynaklanan bir hata nedeniyle de,8 saatlik hizmet kesintileri yaşanmıştır [15, 16].

Tek bir hata noktasına (single point of failure) dayanmaktan kaçınarak, kurumların ihtiyaç duydukları hizmetleri farklı hizmet sağlayıcılardan tedarik

etmeleri, kurumların riski dağıtmasına, hizmet sağlayıcılarda oluşabilecek kesintilerden ve hatta hizmet sağlayıcıların iflası gibi durumlardan en az düzeyde etkilenmelerini sağlayacaktır [7].

Bulut bilişim hizmet sağlayıcılarında meydana gelebilecek hizmet kesintileri, hizmet sağlayıcıları içindeki yazılımsal, donanımsal ya da mimari bir hatadan kaynaklanabileceği gibi, dışarıdan gelebilecek saldırılardan da kaynaklanabilir. Bu tür dışarıdan yapılan saldırılar genelde, dağıtık hizmet dışı bırakma saldırıları (DDoS) tabir edilen, birçok bilgisayardan aynı anda aynı noktaya isteklerin yönlendirilip, sunucuların bu isteklere yanıt veremez hale getirilmesi ilkesine dayanan saldırılardır. Bilgisayar korsanları, "DDoS" saldırıları düzenleyip, bulut bilişim hizmet sağlayıcıların hizmetlerini kesintiye uğratacakları tehdidi ile hizmet sağlayıcı firmalardan para talep edebilmektedirler [7]. Bu saldırılarda kullanılan bilgisayarlar "bot" adı verilen, bilgisayar korsanları tarafından zararlı yazılımlar yüklenip ele geçirilmiş ve kullanıcısının farkında olmadan istenildiği an istenen bir noktaya saldırması sağlanan bilgisayarlardır. İnternet üzerinde karaborsada, ele geçirilmiş bir bilgisayarın (bot) 0.03 USD gibi düşük bir fiyatla, bir hafta süreyle kiralanabildiği bilinmektedir [17]. Bu sayede kolay bir şekilde, düşük bir harcama ve çok büyük sayıda ele geçirilmiş bilgisayar kullanılarak (bot), etkili hizmet dışı bırakma saldırılarının (DDoS) düzenlenebilmesi, hizmet sağlayıcılar için önemli tehlike ve risk oluşturmaktadır. Fakat bulut bilişim hizmet sağlayıcılarının bu tür saldırılara karşı koyacak koruma mekanizmalarını oluşturma yoluna gitmesi, gereksinim anında hızlı ve dinamik kaynak ayırabiliyor olmaları sayesinde, gelen "DDoS" saldırılarına karşı koyabilmeleri ve saldırının geldiği noktaları belirleyip engelleyebilmeleri mümkün olmaktadır [7].

6.2. Veri Güvenliği ve Gizliliği

Bulut bilişim hizmetlerindeki önemli kaygılardan birini de, hizmet sağlayıcılara teslim edilen özel ve gizli bilgilerin, bulut içindeki diğer hizmet kullanıcısı olan kurumlardan nasıl korunacağı, veri gizliliğinin nasıl sağlanacağı konusu oluşturmaktadır. Bulut içindeki bir kullanıcı için, mümkün olan veri gizliliği seviyesi çoğu durumda, masaüstü uygulama kullanıcılarına göre daha düşük olmaktadır [18].

Bulut bilişim hizmetlerinin aynı anda birçok kullanıcı tarafından kullanılması ve fiziksel kaynakların tüm kullanıcılar tarafından ortak olarak kullanılıyor olması, veri gizliliği ve güvenliği için riskler barındırmaktadır. Bulut içindeki farklı kullanıcıların, ortak kaynaklar üzerindeki depolama, bellek alanlarını birbirinden ayırmaya yarayan iç mekanizmalarda ortaya çıkabilecek açıklık ve hatalar, yapılacak saldırılar sonucu kullanıcıların özel ve gizli verilerinin ele geçirilmesine sebebiyet verebilir.

Ayrıca bulut bilişimde, kaynakların dinamik olarak ayrılıp bırakıldığı düşünüldüğünde, çoğu işletim sisteminde uygulandığı gibi, silinen verilerin fiziksel olarak silinmeyip sadece mantıksal seviyede silinmesi durumunda, bırakılan depolama kaynağının başka bir kullanıcıya verilmesi sonucu, bu fiziksel olarak silinmeyen verinin başka kullanıcılar tarafından ele geçirilmesi mümkün olabilmektedir.

Bulut bilişimin dağıtık mimaride olması nedeniyle, içerisinde hizmetler arası yoğun veri trafiği ve veri iletişimi gerektirmektedir. Bunun sonucu olarak, bulut içinde bulunabilecek kötü niyetli kullanıcılar, zararlı yazılımlar çalıştırıp, açık kapı (port) taraması yaparak elde edeceği bilgilerle, korsan saldırılarda bulunabilir ve olası veri kaçaklarını ve veri iletişimini dinleyip, gizli verileri ele geçirebilirler [14].

Bulut bilişim, hizmet sağlayıcı firmaların, belirli özelleşmiş görevleri dışarıdan üçüncü parti firmalardan tedarik yoluna gitmesi, hizmet sağlayıcıların aldıkları tüm güvenlik önlemlerine rağmen, sistemlerinin güvenlik seviyesini, üçüncü parti firmalarla kurulan bağlantının ve bu firmaların sistemlerinin güvenlik düzeyüne bağlı hale getirerek, veri güvenliğinin ve veri kontrolünün kaybedilmesine neden olabilir.

Yukarıda sayılan veri gizliliğine zarar verebilecek davranışların büyük bölümü, bulut içinde verileri şifreli şekilde saklama, sanal yerel ağlar kullanımı ve ağ içi güvenlik duvarı kullanımı yöntemleri ile engellenebilir. Örnek olarak, verilerin bulut bilişim hizmet sağlayıcısına şifrelenip gönderilmesi yöntemi, hastaların hassas sağlık bilgilerine sahip olan, TC3 adlı bir sağlık firması tarafından başarıyla kullanılmıştır [19]. Diğer taraftan, özel bulut veya ortaklık bulut gerçekleştirme modellerinin kullanımı, veri güvenliği ve gizliliği ile ilgili birçok risk bertaraf edilebilir.

6.3. Veri Denetlenebilirliği, Uygunluğu ve Yasal Düzenlemeler

Belirli alanlarda çalışma yapan kurumlar, sertifikasyonu sağlamak, rekabet üstünlüğü elde etmek, endüstri standartlarını karşılamak veya yasal zorunluluklardan dolayı, belirli standartlara uyma konusunda büyük yatırımlar yapmaktadırlar. Fakat bulut bilişim hizmet sağlayıcılarının, bu standartların gereklerini yerine getirmeye yönelik, kendi uygunlukları (compliance) konusunda kanıt sunamamaları ve bulut kullanıcılarına bunlara ilişkin denetim izni vermediği durumlarda, yapılan yatırımlar riske atılmış olabilir. Örnek olarak, Amazon EC2 hizmet sağlayıcısı kullanıcılarını, platformları üzerinde PCI veri güvenlik standardına uygunluğu sağlamada zora düşebilecekleri konusunda uyarmaktadır. Bu nedenle, EC2 üzerinde faaliyet gösteren hizmetler, kredi kartı işlemlerini yerine getirememektedir [14].

Bulut bilişim hizmetlerinin dağıtılmış olarak çalışan küresel hizmetler olduğu düşünüldüğünde, farklı ülkelerden kullanıcılar, farklı iş kültürlerine ve yasal düzenlemelere sahip olarak iş görmektedirler. Bulut bilişim hizmet sağlayıcılarının, farklı ülkelerde ve bölgelerde veri merkezleri bulundurması, bulunduğu ülkedeki yasal düzenlemelere de uyum sağlamasını gerektirebilir. Veri gizliliği ve denetimi konusunda, ülkelerin farklı yasal düzenlemelere sahip olması, bulut bilişim hizmet sağlayıcılarının hizmetlerini yerine getirirken, farklı yasal düzenlemelere uyum sağlamada sorunlara neden olabilir. Avrupa Birliği ülkeleri ve Amerika Birleşik Devletleri arasında bile, kişisel gizlilik ve kişisel gizliliği koruma türleri konusunda, belirgin farklılıklar bulunmaktadır [20]. Ayrıca, bulunduğu ülke dışındaki başka bir ülkede, yerleşik bir bulut bilişim hizmet sağlayıcısından hizmet alan kurumlar, dolaylı olarak bu ülkenin yasalarının kapsamına girdiği için, burada saklanan verilerine, hizmet sağlayıcının bulunduğu ülke tarafından adli yargı yoluyla erişilebilir ve verilerinin gizliliği tehlikeye girebilir. Örnek olarak, Amerika Birleşik Devletleri hükümeti, ABD Vatanseverlik yasası ve Yurtiçi Güvenlik yasası, benzeri yasaları kullanarak, gelişmiş bilgi toplama teknolojilerinin yardımıyla, her türlü bağlamdaki elektronik veriye erişebilmektedir [21]. Dolayısıyla Avrupa'da bulunan bir kullanıcı, ABD merkezli bir bulut bilişim hizmet sağlayıcıdan hizmet temin etme kararı alırken, bu ülkedeki yasal düzenlemeleri göz önünde bulundurması gerekmektedir.

Bulut bilişim mimarisine, veri denetimi özelliği kazandırabilmek ve bu yolla belirli standartları ve yasal zorunlulukları sağlayabilmek için, sanal misafir işletim sisteminin erişemeyeceği, ayrı bir veri denetimi katmanı eklenebilir. Bu sayede veri denetimi ve uygunluğu, merkezileştirilmiş tek bir mantıksal katman üzerinden sağlanabilir [7].

6.4. Hizmet Sağlayıcı Bağımlılığı ve Veri Kilitlenmesi

Bir bulut bilişim hizmet sağlayıcısından diğerine geçiş yapmak istenmesi durumunda, bulut bilişim hizmet sağlayıcılarının; yazılım geliştirme ara yüzlerini (API) istenen seviyede standartlaştırmamış olmaları, verilerin hizmet sağlayıcılara özel veritabanı şemalarında tutulmaları gibi nedenlerle, veri ve yazılımların taşınmasında büyük zorluklarla karşılaşılmaktadır. Bunun sonucu olarak kurumların, bulut bilişim hizmet sağlayıcılarına, bir anlamda bağımlı duruma geldikleri görülmektedir. Bu bağımlılık, farklı hizmet modelleri için farklı şekillerde olabilmektedir. Hizmet olarak Yazılım (SaaS) modelinde, kurum verilerinin, hizmet sağlayıcının tasarladığı özel bir veri tabanının şemasında saklanması, verinin taşınmasını; belirli alanda uzmanlaşmış uygulamalarının bulunması, kurumların uygulama değiştirmelerini zorlaştırmaktadır. Hizmet olarak Platform (PaaS) modelinde ise, kurumlar hizmet sağlayıcıların yazılım geliştirme ara yüzlerine (API) ve bileşenlerine bağımlı hale gelirken, Hizmet olarak Altyapı modelinde (IaaS) ise, kullanılan donanımsal kaynaklara bağımlı hale geldikleri görülmektedir [14].

Bir bulut bilişim hizmet sağlayıcısına, depolanan veri ve kullanılan uygulamalar dolayısıyla bağımlı olmak, uygulanan fiyat politikalarına karşı esnek olamamaya, hizmet sağlayıcısının mimarisinde var olabilecek açıklık ve zayıflıklar sonucu oluşabilecek arıza ve saldırılardan dolayı veri kaybına uğramaya neden olabilir. Ayrıca, bir bulut bilişim hizmet sağlayıcısının, bir diğeri tarafından satın alınması sonrasında, gerçekleşebilecek olan hizmet veya kullanım şartnamesi değişiklikleri, kurumları zora sokabileceği gibi; bir hizmet sağlayıcının yaşadığı teknik ve ekonomik zorluklar sonucu iflas etmesi, hizmet alan kurumların büyük veri ve itibar kaybına uğramalarına neden olabilir. Her ne kadar bu zor bir olasılık olarak görülse de, Linkup adlı çevrimiçi veri depolama hizmetinin, 8 Ağustos 2008 tarihinde, müşteri verilerinin %45'ini kaybettikten sonra batması, bu riskin var olduğuna örnek olarak verilebilir [22].

6.5. Yönetim Ara yüzü ve Uzaktan Erişim

Bulut bilişim hizmet sağlayıcıların, kullanıcılarının hizmetlerini yönettikleri ara yüzler, internet üzerinden erişilebilir olmaları ve geniş yönetim olanakları içermeleri nedeniyle, internet tarayıcıların ve uzaktan erişimin zayıflıkları düşünüldüğünde, yüksek güvenlik riski taşımaktadırlar. Uzaktan erişim sırasında, saldırganlar tarafından koklama (sniffing), yanıltma (spoofing) ve araya girme (man-in-the-middle) gibi saldırı yöntemleri kullanarak, iletişimin ve taşınan verinin dinlenmesi, kullanıcı oturumunun elde edilmesi ve kullanıcı şifrelerinin çalınması mümkün olabilmektedir [14]. Eğer saldırgan kullanıcı şifre ve bilgilerini ele geçirirse, yapılan işlemleri izleyebilir, verileri silebilir, veriler üzerinde oynayabilir, hatalı veri döndürülmesine neden olabilir ve hatta müşterileri zararlı sitelere yönlendirebilir. Ayrıca saldırgan, ele geçirdiği kullanıcı hesabını veya kullanılan hizmetleri, daha ileri ve geniş saldırılar yapmak için bir merkez olarak kullanıp, kullanıcıya duyulan güveni ve kullanıcının itibarını kullanarak, başka kişiler ve bulut bilişim hizmet sağlayıcısını da etkileyebilecek, daha büyük saldırılar gerçekleştirebilmektedir [23].

Bulut bilişim hizmet sağlayıcılar tarafından, bulut temelli güvenlik modeli oluşturulmasına başlanıp, bulut bilişim kullanıcılarının anti virüs ve güvenlik yazılımları kurmasına gerek bırakmayan, bulut-içi (in-the-cloud) tarama hizmetleri başlatılmıştır. Bu sayede, bulut kullanıcılarının zararlı yazılımlara, sistemdeki açık kapılara (loophole), zayıflıklara ve araya girme saldırılarına karşı korunmasına, bulut içindeki saldırıların engellenmesine çalışılmaktadır [24].

6.6. Bant Genişliği ve Veri Transferi

Bulut bilişimin temelinde yatan ana fikirlerden biri olan, kullanıcıların veri işleme ve saklama faaliyetlerinden arındırılıp, verilerin merkezi bir bulut içine toplanması ve buradan gerekli işlemlerin yapılabilmesi fikri, uygulamaların giderek daha yoğun veri kullanmaya başlamasıyla, verilerin

kullanıcıdan bulut bilişim hizmet sağlayıcısına taşınmasında zorluklara neden olmaktadır. Bulut bilişim hizmet sağlayıcısına geçiş sırasında, kurumların tüm verilerini hizmet sağlayıcısına taşıması gerekliliği, kullanılabilir bant genişliğinin sınırlı olması, veri transferinin uzun sürmesi ve veri transfer maliyetlerinin yüksek olması, kurumların bulut bilişim yoluyla hizmet almasının önündeki önemli engellerdendir. Örnek olarak, Amazon S3 hizmet sağlayıcısına, veri transferinde ortalama bant genişliğinin 5 ile 18 Mbit arasında olduğu ölçülmüştür [25]. Bu durumda, 10 TB'lık bir veriyi, ortalama değerin üzerinde, 20 Mbit/saniye hızda, S3 hizmet sağlayıcısına gönderilmesi işlemi, 45 günden fazla sürecektir [7].

Bant genişliğinin belirli düzeyin üzerine çıkamaması, dolayısıyla büyük veri transferlerinin çok uzun sürmesi ve maliyetinin yüksek olması gibi sorunlara karşı, veri disklerinin kargo şirketleri tarafından bir günde teslim edilmek üzere fiziksel olarak yollanması gibi çözümler önem kazanmıştır.

Bulut bilişim hizmet sağlayıcılarının düzenli bir internet bağlantısına ve yüksek bant genişliğine gereksinim duymaları sebebiyle, bulut bilişim hizmet sağlayıcılarına gerekli internet altyapısını ve bant genişliğini sağlayan İnternet hizmet sağlayıcılar (ISP), uyguladıkları fiyat politikaları yoluyla, bulut bilişim hizmet sağlayıcılarını ekonomik olarak baskı altına alabilirler. Hatta bazı İnternet hizmet sağlayıcılar, hali hazırda büyük ağ ve veri merkezleri bulundurma, kendi veri iletişim altyapılarına sahip olma, yüksek bant genişliği kullanabilme gibi üstünlükleri nedeniyle, haksız rekabete yol açabilecek şekilde, bulut bilişim hizmetlerini verme yoluna gidebilirler [21].

6.7 Yazılım Lisanslama

Günümüzdeki yazılım lisanslama uygulaması, yazılımların çalışacağı bilgisayarların sayısını ve hangi bilgisayarlarda çalışabileceğini kısıtlarken, çevrim içi lisanslama denetimi yaparak, kullanılan lisanslarla yazılımların yüklendiği bilgisayarları eşlemektedir. Bulut bilişim hizmet yapısında ise, işlemci, bellek ve depolama alanları dinamik olarak değişebildiği, dinamik olarak makine eklenebildiği için, yazılım lisanslaması karmaşık hale gelmektedir. Örnek olarak, kullanılan kopya (instance) sayısına göre lisanslama yapan bir yazılımda, çalışan hizmette kullanılmak üzere yeni bir makine eklendiğinde, bu makine üzerinde yeni bir yazılım kopyası (instance) oluşturulup, lisanslaması ayrı olarak yapılacaktır. Fakat bulut bilişimde, makinelerin dinamik olarak eklenip çıkarılabildiği düşünüldüğünde, çıkarılan bir makine yerine yenisi eklendiğinde, toplamda makine sayısı aynı da kalsa, klasik lisanslama mantığında her yeni makine için yeni bir lisans kullanılması gerekeceği için, lisans sayısı makine sayısının çok üzerine çıkabilir [14]. Bu durumda kullanılan yazılımların çeşidi ve sayısına göre, kurumların katlanmak durumunda kalacakları bulut bilişim hizmet maliyeti çok yükselebilir ve kurumlar için bulut bilişim hizmet tedariki yapmak cazip olmaktan çıkabilir.

Ayrıca lisanslama ve kullanıcı anlaşmaları, ulusal pazarlarda değişebildiği ve bazı ürünlerin sadece belirli ülke pazarlarında kullanılabildiği düşünüldüğünde, bulut bilişim hizmet sağlayıcıları içinde yazılımların yönetimi ve denetimi karmaşık hale gelip, bu konuda sorunlar ortaya çıkabilir.

Bulut bilişim hizmetlerinde, yazılım lisanslamada sorunlar yaşanması, hizmet sağlayıcılar tarafından açık kaynak kodlu yazılımların kullanılmasına neden olması üzerine ve bulut bilişim pazarının ticari olarak oldukça büyümesinin de yardımıyla, büyük ticari yazılım firmaları kullandıkça-öde (pay-as-you-go) mantığında çalışan lisanslama yöntemleri geliştirmeye başladılar. Son olarak, Microsoft yazılım firması, Amazon EC2 bulut bilişim hizmet sağlayıcısı üzerinde, kullandıkça-öde lisanslama imkânları sağlayıp, Windows Server ve SQL Server yazılımlarını kullanılmasına olanak sağlamıştır. Örnek olarak, Microsoft Windows Server işletim sisteminin saatlik kullanım bedeli olarak 0.15 USD belirlenmişken, açık kaynak kodlu denklerinin saatlik kullanım bedelleri 0.10 USD olmaktadır [7].

7. Türkiye için Fırsatlar

Son yıllarda ülkemizde, gerek kamu kurumları bünyesinde gerekse özel kurumlarda, büyük çaplı sanallaştırma projeleri gerçekleştirilmektedir. Bu projeler kapsamında kurumlar, fiziksel sunuculara dağıtılmış şekilde çalışan bilgi işlem hizmetlerinin, sanal sunuculara geçişini yapmaktadırlar. Sanallaştırma projeleri, "özel bulut" gerçekleştirmenin hayata geçirilmesi ve kurumların merkezi bilgi işlem birimlerinin, bulut hizmet sağlayıcı olarak hizmet vermesi yönünde, önemli bir aşama olarak görülmektedir. Özellikle taşra teşkilatı olan kamu kurumlarının ve üniversitelerin önünde, bu bağlamda ciddi fırsatlar bulunmaktadır. Bilgi işlem hizmetlerini sanal sunucular üzerinde yapılandırmış olan kurumlar, web uygulamaları geliştirerek taşradaki personeline daha sürekli ve güvenilir hizmetler verebilirler.

Ülkemizde "özel bulut" modelinin uygulanabileceği üç temel profil bulunmaktadır. Bunlar askeri bulut, kamu bulutu ve bilim bulutu olarak isimlendirilebilir.

Tüm Türkiye'ye yayılmış TAFICS altyapısını kullanan Türk Silahlı Kuvvetleri, bilgi sistemlerinin belirlenen bileşenlerinin, merkezi karargâhlardaki bilgi işlem altyapıları üzerinden, bir hizmet olarak tüm Türkiye'deki birliklere sunulmasının önemli yararları olacaktır.

Kamu kurumları için de benzer bir durum söz konusudur. Taşra teşkilatına sahip olan Adalet Bakanlığı, Maliye Bakanlığı, Tarım ve Köy İşleri Bakanlığı gibi birçok kamu kurumu için, bulut bilişim büyük üstünlükler getirecektir. Bu kurumların merkezlerinde oluşturulacak bir altyapı ile birlikte taşraya yapılan bilişim harcamaları azalacak, taşradaki teknik personele duyulan ancak nitelikli eleman bulunmadığından dolayı karşılanamayan gereksinim ortadan kalkacaktır.

Üçüncü olarak, ULAKBİM yönetiminde ve öncülüğünde, üniversiteler için oluşturulacak bir bulut altyapısının da, son yıllarda kurulan ve bilgi işlem personeli

istihdamı konusunda zorluklar çeken üniversitelerin, bilişim gereksinimlerine yanıt vereceği düşünülmektedir.

Kısaca söz edilen bütün çözümler için ortak gereklilik, iletişim altyapısının hızlı ve yedekli bir yapıda olması gerekliliğidir. Makalenin riskler bölümünde de söz edildiği gibi, altyapıdan kaynaklanabilecek bir sorunda, uçlardaki kullanıcılar hem uygulamaya hem de veriye ulaşamayacaklardır.

8. Sonuç

Bulut bilişim getirdiği üstünlükler ve esnekliklerin yanı sıra, riskleri de beraberinde taşımaktadır. İnternet altyapısının çok güçlü olduğu ABD'de, kamu kurumlarını da içine alan geniş bir yelpazede, kurumlar bulut bilişimin üstünlüklerinden yararlanmaya başlamışlardır. Diğer taraftan, bilişim uzmanları ve politika belirleyiciler, bulut bilişimin riskleri konusunda tartışmaya devam etmektedir.

Ülkemizde de bilişim uzmanları, gün geçtikçe daha sık bir şekilde bulut bilişimden söz etmekte, bir çok kurum bilgi işlem hizmetlerini, sanal sunucular üzerinde çalıştırmaya başlamaktadır. Teknolojiye büyük bir hızla uyum sağlayan ve kullanan kurumlarımız, çok geçmeden bulut bilişimin üstünlüklerinden yararlanmaya başlayacaklardır.

Henüz bulut bilişim ile ilgili yaygın ve kurumsal kullanım gerçekleşmemişken, ülkemizin gereksinim duyduğu çalışma, bulut bilişimin risklerini dikkate alan ve bu risklerin bertaraf edilmesi yönünde, teknik, idari ve yasal karşı önlemler ortaya koyan araştırma ve geliştirme çalışmalarıdır. TÜBİTAK-BİLGEM bünyesinde bu kapsamda çalışmalar sürmektedir.

KAYNAKÇA

[1] ICCP, Technology Foresight Forum - "Cloud Computing: The Next Computing Paradigm?", Ekim 2009

[2] Scanlon H., Wieners B., "The Internet Cloud", Eylül 1999, http://www.thestandard.com/article/0,1902,5466,00.html (29 Mart 2010'da erişildi)

[3] Johnson, L., Levine, A., & Smith, R., The 2009 Horizon Report, Austin Texas, The New Media Consortium, 2009

[4] İlkay Zaman, IT Advisor Dergisi, Ocak 2010

[5] Gartner, Forecast: Sizing the Cloud; Understanding the Opportunities in Cloud Services, Mart 2009

[6] Hamilton J., Internet-Scale Service Efficiency, In Large-Scale Distributed Systems and Middleware (LADIS) Workshop, Eylül 2008

[7] Armbrust et. al., Above the Clouds: A Berkeley View of Cloud Computing, Şubat 2009

[8] Administration E. I., State Electricity Prices, 2006, http://www.eia.doe.gov/neic/rankings/stateelectricityprice.htm (29 Mart 2010'da erişildi)

[9] Rangan K., The Cloud Wars: $100+ billion at stake, Tech. rep., Merrill Lynch, Mayıs 2008

[10] Siegele L,. Let It Rise: A Special Report on Corporate IT, The Economist, Ekim 2008

[11] Arif Mahomed, A History of Cloud Computing, ComputerWeekly, Mart 2009

[12] Mell, P., Grance T., The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Information Technology Laboratory, Ekim 2009

[13] Orhan Alkan, Cloud Computing: Altyapı Hizmetleri (http://www.computerworld.com.tr/cloud-computing-altyapi-hizmetleri-detay_3964.html)

[14] Enisa, Benefits, risks and recommendations for information security, Kasım 2009

[15] Wilson S., AppEngine Outage, CIO Weblog, Haziran 2008, http://www.cio-weblog.com/50226711/appengine_outage.php (29 Mart 2010'da erişildi)

[16] The Amazon S3 Team, Amazon S3 Availability Event: July 20, 2008, Temmuz 2008, http://status.aws.amazon.com/s3-20080720.html (29 Mart 2010'da erişildi)

[17] Paxson, V., Private Communication, Aralık 2008

[18] Delaney, K. J., & Vara, V., Google plans services to store users' data, Wall Street Journal, Kasım 2007, http://online.wsj.com/article/SB119612660573504716.html?mod=hps_us_whats_news (29 Mart 2010'da erişildi)

[19] Total Claims Capture & Control, TC3 Health Case Study: Amazon Web Services, http://aws.amazon.com/solutions/case-studies/tc3-health/ (29 Mart 2010'da erişildi)

[20] Sunosky, J. T., Privacy online: A primer on the European Union's Directive and the United States' Safe Harbor privacy principles, Currents: International Trade Law Journal,9, 80-88, 2000

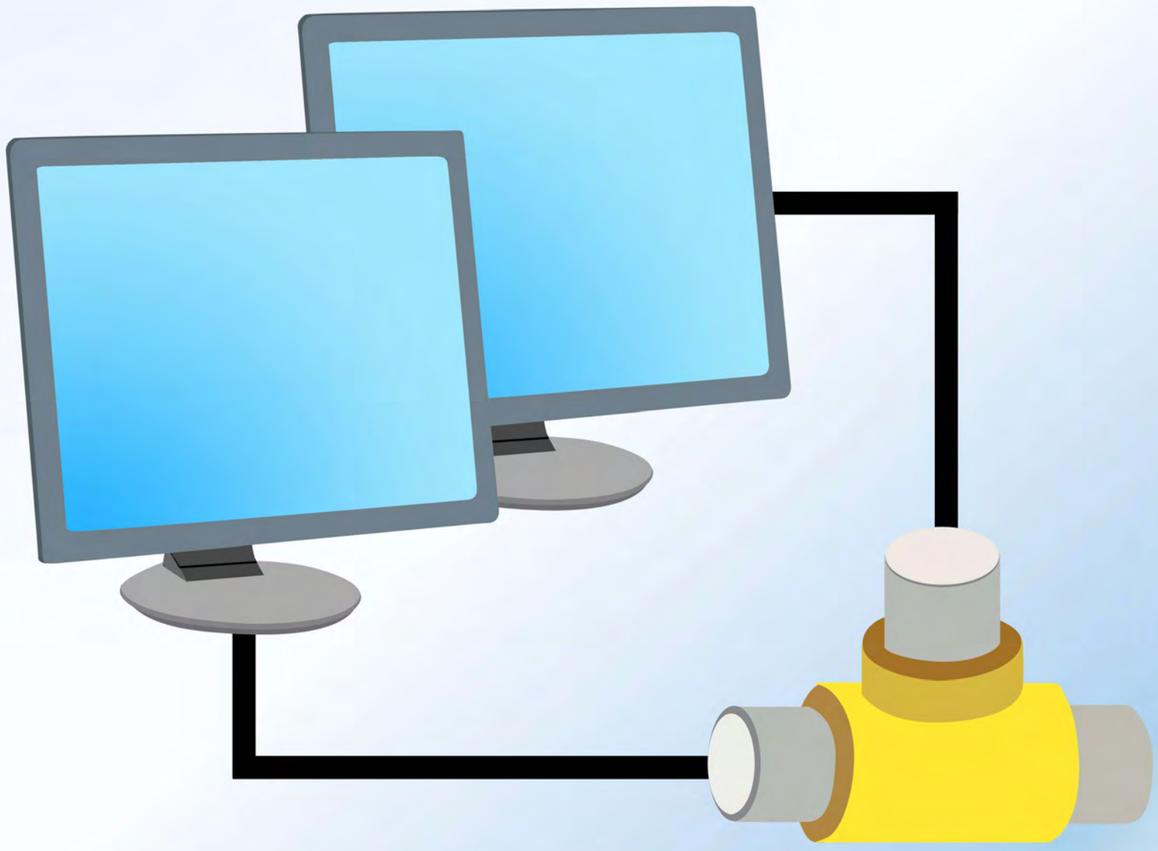
[21] Jaeger et. al., Cloud Computing and Information Policy: Computing in a Policy Cloud?, 2008

[22] Brodkin, J., Loss of customer data spurs closure of online storage service 'The Linkup', Network World, Ağustos 2008.

[23] CSA, Top Threats to Cloud Computing V1.0, Mart 2010

[24] Ragragio & Radu, The Cloud or the Mist?, Eylül 2009

[25] Garfinkel, S., An Evaluation of Amazon's Grid Computing Services: EC2, S3 and SQS, Tech. Rep. TR-08-07, Harvard University, Ağustos 2007



BİLİŞİM GÜVENLİĞİ SİSTEMLERİ

YENİ NESİL İNTERNET PROTOKOLÜ IPV6

Mehmet KARA

İnternetin temel iletişim protokolü olan TCP/IP (Transmission Control Protocol/Internet Protocol) protokol ailesi 1969 yılından beri kullanılmaktadır. 1981 yılında RFC(Request For Comments) 791'le yayınlanmış olan IPv4 protokolü bazı değişikliklerle günümüze kadar internet trafiğini başarıyla olarak taşımıştır. Fakat, o günün koşullarında IPv4'ün tasarımında adres uzayı, servis kalitesi ve güvenlik önlemleri yetersiz kalmıştır[1].

Aktif kullanılan IPv4 adres sayısı her geçen gün azalmaktadır. Yapılan tahminlere göre Ekim 2011 yılında IPv4 adreslerinin tükenmesi beklenmektedir[2]. Son yıllarda, internetin hızla büyümesi sonucunda gelişen ülkelerde, yeterince IPv4 adres alamama sıkıntısı yaşanmaktadır. Her ne kadar 1980'li yıllardan sonra adres dağıtım politikasında yapılan değişikliklerle kıtaların ve ülkelerin IPv4 adres dağılımları dengelenmeye çalışılsa da hala ABD merkezli bir yapı olduğu görülmektedir. Örneğin başlangıçta ABD IP adreslerinin %55'ini elinde tutarken, bugün bu rakam %37'lere gerilemiştir. Aynı şekilde Çin'in IP adreslerinin sayısı ayrı ayrı MIT ve Stanford üniversitelerinde daha azken, bugün %8'lere ulaşmıştır. IPv4 adresleri 32 bit uzunluğundadır. 32 bitlik adreslerle 2^{32}= 4,294,967,296 tane farklı adres üretilebilir. Yani dünyada kişi başına bir IP adresi bile düşmemektedir. Oysaki bu adreslerin bir kısmı iç ağ kullanımları, yerel çevrimler (loopback), çokluyayın (multicast) ve araştırmalar için kullanılmaktadır. Bunun yanında IPv4 adres dağıtımında etkili bir yöntem izlenmediğinden, yeni kullanımlar için IP adresleri hızla tükenmektedir. Diğer yandan internete bağlı makinelerin hızla artması ve yeni uygulamaların (3G, 4G, VoIP, GPRS, IPTV, NGN) devreye girmesi, evlerdeki su sayacı, elektrik sayacı, doğalgaz sayacı, kontrol sistemleri gibi çeşitli cihazlara IP adresi verilmesinin istenmesi IP adresi ihtiyacını daha da artırmaktadır. IP adreslerinin etkin kullanımı için süreç içerisinde değişken boyutlu alt ağ maskesi, ağların alt ağlara bölünmesi, ağ adres çevrimi (Network Address Translation) gibi çözümler üretilse de bunlar bazı sorunları da beraberinde getirmektedir. Bu yüzden her bir cihazın kendi gerçek IP adresini kullanabileceği yeni uygulamaları (3G, 4G, VoIP, GPRS, IPTV, NGN) problemsiz olarak destekleyecek IP adresleme düzenine ihtiyaç vardır.

IPv4 adres sayısının yetersiz olması, ilk önce, gelişmiş, gelişmekte olan ve nüfusun fazla olduğu ülkelerde hissedilmeye başlanmıştır. Bunlar arasında Çin, Japonya, Hindistan ve Güney Kore başta gelmektedir. IPv4 adreslerinin başlangıçta küresel olarak adil dağıtılmaması, sorunun temelini oluşturmaktadır. İnternetin yaygınlaşmasıyla birlikte IPv4 adreslerinin daha dengeli dağıtımı için çeşitli politikalar geliştirilmiştir. Bu çerçevede IP adresi dağıtımında çeşitli düzenlemeler yapılmıştır. Türkiye IP adreslerinin %0.45'sine sahiptir. Nüfuslar karşılaştırıldığında ve teknolojik gelişmelerin artık sınır tanımadığı düşünüldüğünde, bu tablonun biran önce düzeltilmesi gerektiği görülebilir. IPv6 ile bu adres kıtlığının çözülmesi ve şu anda çalışan ilgili küresel otoritelerce adres dağıtımının daha düzenli olarak yönetilmesi beklenmektedir.

Amerika Birleşik Devletleri Kamu Kurumları, NASA, Savunma Dairesi ve benzeri kuruluşlar 30 Haziran 2008'de resmi olarak IPv6'ya geçmiş olacağını duyurmuştur. Windows Vista, IPv6 teknolojisini desteklemektedir. Bu desteğin IPv6 geçişini hızlandıracağı tahmin edilmektedir. Şubat 2007'de 2 milyon Windows Vista lisansının satıldığı belirtilmiştir. Bu durum, IPv6'nın kısa zamanda, en azından uç birimlerde yaygın olarak hazır olacağını açıkça ortaya koymaktadır.

IMS (IP Multimedia Subsystem), NGN (Next Generation Networks), Wimax, Wi-Fi, 3G, IPTV kurulumları ve servisleri gün geçtikçe artmaktadır. Terminal çeşitliliği ve sayısı hızla artmaktadır. Örneğin, Strategy Analytics şirketinin bir araştırmasına göre 2010'da 3G kullanıcı sayısının 1 Milyarı geçeceği öngörülmektedir. Bu sayının da telsiz iletişim terminallerinin sadece üçte birini oluşturacağı tahmin edilmektedir.

Şu anda kullanılan IPv4 protokolü tasarlanırken veri taşıyacağı düşünülerek ona uygun bir protokol yapısı geliştirilmiştir. Bu yapıda daha çok verilerin bir noktadan başka bir noktaya hatasız bir şekilde iletilmesi amaçlanmıştır.. Zamanla, internet üzerinden ses, görüntü gibi yapı olarak farklı türdeki bilgilerin de taşınmasına ihtiyaç duyulmuştur. Bu görüntü

ve ses trafikleri bilginin hatasız iletilmesinden çok, belli bir zaman içerisinde karşı uca varmasını hedefler. Bu da internet yapısında farklı servisler için farklı önceliklendirmeleri (Quality of Service) gerektirir. IPv4'te çok sınırlı yeteneklere sahip bir önceliklendirme düzeneği vardır, ancak bu özellik internet üzerinde çalışmamaktadır. Daha sonradan eklenen kimi araçlarla servis kalitesi ayarlanmaya çalışılsa da servis kalitesi içerisine gömülü bir protokolün etkinliğine ulaşamamaktadır. Farklı servisler için farklı önceliklendirmeleri destekleyecek bir protokole ihtiyaç vardır.

TCP/IP protokol ailesi ARPANET projesi çerçevesinde geliştirilirken öncelikle protokolün hatasız çalışması hedeflenmiştir. Bu yüzden veri bağlama katmanında ve iletim katmanında hata kontrolü yapılmaktadır. Fakat protokol ailesinin yapısında güvenliğe karşı bir önlem alınmamıştır. İnternetin yaygın olarak kullanılmasıyla, bilerek ya da bilmeyerek kullanıcılar bilgisayarların sürekliliğine, gizliliğine ve bütünlüğüne zarar vermişlerdir. Ağ üzerinde yapılan bu saldırılara ya da yanlış kullanımlara karşı güvenlik duvarı, kimlik doğrulama, yetkilendirme, izleme, saldırı tespit/önleme sistemleri gibi çözümler geliştirilmiştir. Günümüzde çok sayıda yeni saldırı ve bu saldırılara karşı güvenlik önlemleri ortaya çıkmaktadır.

IPV6'NIN TEKNİK ÖZELLİKLERİ

IPv6 protokolü, IETF (Internet Engineering Task Force) tarafından yayınlanmış olan bir dizi RFC dokümanı vasıtasıyla tanımlanmıştır. Bu RFC'lerin en temel olanlarına IETF IPv6 Çalışma Grubu sayfasından ulaşılabilir[3].

IPv6'yı IPv4'ten ayıran en önemli özellik 128 bitlik genişletilmiş adres alanıdır. Bu genişlemenin sağlamış olduğu teorik adreslenebilir düğüm sayısı 340,282,366,920,938,463,463,374,607,431,768,211,456'dır. Bu dünyada merter kareye 1 molden ($6.02x10^{23}$) daha fazla IP adresi geldiği anlamına gelir. Böylesine geniş bir adres alanının şu an yaşanan adres sıkıntısını çözmesinin yanında, İnternet uygulamalarında yeniliklere de yol açması beklenmektedir. Öte yandan, IP üzerinde yapılan değişiklikler yalnızca bununla da kalmayıp, protokolün tam anlamıyla yeniden gözden geçirilmesi ve yenilenmesi de söz konusu olmuştur. Bunlar arasında basitleştirilmiş ve 64 bitlik işlemcilere göre düzenlenmiş paket başlığı, paket bölünmesinin sadece uç noktalarda yapılacak olması yönlendiricilerin veri trafiğini daha seri bir şekilde işleyebilmesi için yapılan değişikliklerdir. Temel IP başlığının yanı sıra ihtiyaca göre eklenebilir uzantı başlıklarının tanımlanabilmesi protokolün esnekliğini arttıran bir etmen olmuştur. Güvenlik için IPSec (IP security protocol) şartı da IPv6 ile gelen özellikler arasında yer almaktadır [4].

IPv6 adresleri bağ içi (link-local) ve evrensel (global) olmak üzere iki çeşittir. Bağ içi adresler yalnızca özel amaçlarla kullanılır ve bu adresleri taşıyan paketler yönlendiriciler tarafından asla diğer bağlara iletilmezler. IPv4'te sıkça kullanılan genel yayın (broadcast) adresleri, görevleri çoklu yayın (multicast) adresleri tarafından üstlenildiği için IPv6 mimarisinde yer almaz. Herhangi birine yayın adresleri (anycast) IPv6'nın getirmiş olduğu yenilikler arasındadır. Bu tip adreslere gönderilen paketler, bu adresi kullanan birden çok düğümden sadece birine varacak şekilde yönlendirilir. Kullanımda birden çok düğümün aynı adresi paylaşması açısından çoklu yayın adreslerine benzemekle birlikte, paketin sonunda yalnızca tek bir düğüme ulaşması açısından tekli yayını andırırlar.

Otomatik adres yapılandırması IPv6'nın getirmiş olduğu önemli yeniliklerdendir. Ağ üzerindeki adres atama görevini üstlenmiş bir DHCP(Dynamic Host Configuration Protocol) ya da PPP (Point to Point Protocol) sunucusu olmaksızın ağa bağlı düğümlerin kendilerince adres edinmelerine olanak tanır. Bunun da temelinde, ağdaki yönlendiricilerin gerekli adres bloğunu anons etmeleri ve düğümlerin de bu bloğa kendilerinden 64 bitlik bir değer eklemeleriyle adres oluşturmaları yatar. Bu şekilde oluşturulan adreslerin kullanılmadan önce tekillik testinden geçirilmesi gerekir. Düğümler, bir adresi başkalarının kullanmadığını tespit ettiklerinde kullanıma alabilirler.

IP protokol başlığında ise büyük değişiklikler olmuştur. IPv4'te var olan protokol başlık büyüklüğü, kimlik bilgisi, paket parçası bilgisi, başlık sağlama toplamı kaldırılmış, IPv6 başlığına yeni olarak akış bilgisi eklenmiştir. Tipik 20 bayt genişliğindeki IPv4 başlığının yerini 40 baytlık IPv6 başlığı almıştır. Temel IPv6 başlığına ek olarak, kendince özel amaçlara yönelik yönlendirme, paket bölmesi, şifreleme ve gezici (mobil) uzantı başlıkları tanımlanmıştır. Zaman içerisinde ihtiyaç oldukça bunlara yenileri eklenebilir.

Yönlendirme alanında temel ilkelerde bir değişiklik olmamakla birlikte var olan RIP (Routing Information Protocol), OSPF(Open Shortest Path First), IS-IS(Intermediate System-Intermediate System), MP-BGP (Multi Protocol- Boarder Gateway Protocol), PIM-SM(Protocol Independent Multicast - Sparse-Mode), PIM-SSM(Protocol Independent Multicast Source Specific Multicast) gibi protokoller IPv6 adreslerini işleyebilecek şekilde güncellenmiştir. Çoklu yayın için kullanılan IGMP(Internet Group Management Protocol)'nin yerini yeni geliştirilen MLD(Multicast Listener Discovery) almıştır.

Alan adlarının kaydından sorumlu DNS(Domain Name Service), IPv4 adreslerin yanı sıra IPv6 adreslerini de barındıracak şekilde düzenlenmiştir. IPv4 adresleri A tipi kayıtlarda saklanırken, AAAA tipi kayıtlar IPv6 adreslerine ayrılmıştır. IPv6'yı destekleyen bir DNS sunucusu üzerinde bir alan adı aynı zamanda hem IPv4 hem de IPv6 adreslerine atanabilir.

IPv4'ün hareketlilik protokolü Mobil IPv4'e karşılık olarak Mobil IPv6 geliştirilmiştir. Aralarında uygulamada öne çıkan faklılıklar olmasına rağmen bu iki protokol ana hatlarıyla birbirlerine benzemektedir.

IPV6'YA GEÇİŞ VE IPV4-IPV6 UYUMLULUĞU

IPv6'ya geçiş son yıllarda özellikle Asya ve Avrupa'da artmıştır. IPv6 pek çok önemli özelliği de beraberinde getirmektedir. Bu özelliklerden en önemlisi IP adres uzayının büyük ölçüde artmasıdır. Ancak IP adres uzayındaki artış değişik adres şekillerinin ve ifadelerinin ortaya çıkmasına sebep olmuştur. Bu durum sadece ağ katmanını değil aynı zamanda uygulamaları da etkilemektedir.

Şu anda IPv4 ağları ile çalışan organizasyonlar, IPv6'ya sorunsuz olarak kolay bir biçimde nasıl geçilebileceklerini araştırmakta ve IPv6'ya geçiş planları yapmaktadır. IPv6'ya geçişte en kolay ve etkili yol, şimdiki durumda var olan IPv4 ağlarına IPv6 ile çalışan cihazlar eklemek ve zaman geçtikçe IPv6 ağırlığını artırarak nihayetinde bütün ağların IPv6 ile çalışır duruma gelmesini sağlamaktır. Yani IPv4 ağlardan tamamen IPv6 ağlara geçiş kısa bir zaman aralığı değil, uzun vadeli bir süreç olacaktır.

Geçiş Teknolojileri

IPv6'ya geçişte pek çok teknoloji kullanılabilir. Genel olarak bu teknolojiler [8]:

İkili Yığın (Dual Stack): Ağ cihazlarında hem IPv4, hem de IPv6'nın birlikte çalışması;

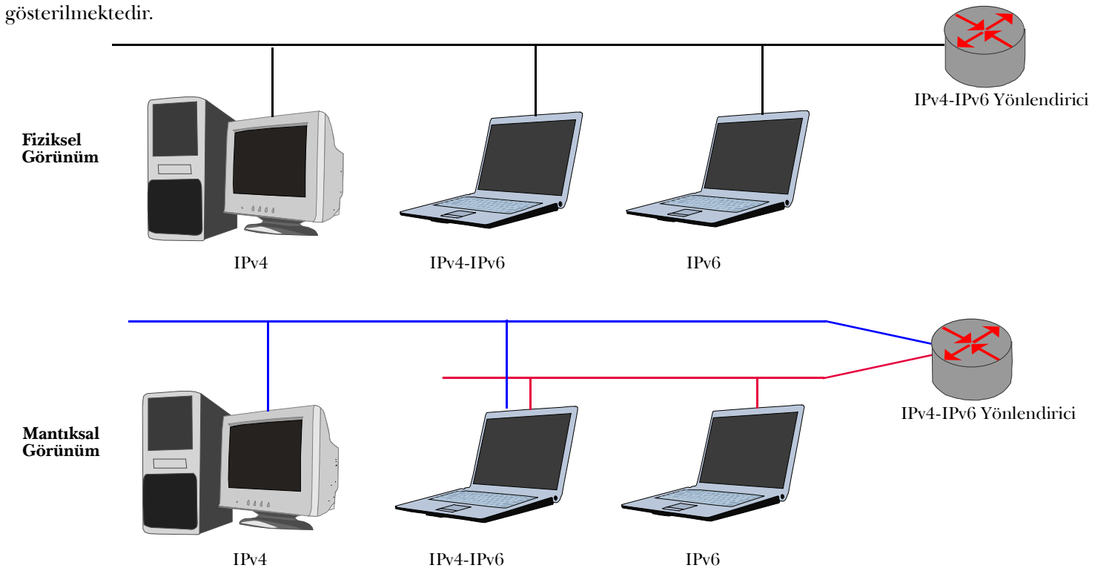
Tünelleme: IPv6 paketlerin IPv4 paket formatına dönüştürülerek, IPv4 ağ üzerinden gönderilmesi;

Dönüşüm: Ağ geçidi veya yönlendirici tarafından yapılan adres ve port dönüşümü.

İkili Yığın Yaklaşımı

İkili yığın teknolojisinde, ağ cihazları hem IPv4'ü hem de IPv6'yı desteklemektedir. Böylece IPv4-IPv4 iletişimler ve IPv6-IPv6 iletişimler aynı ağ üzerinden gerçekleşmektedir. Bu teknolojinin uygulanabilmesi için yönlendirici gibi ağ katmanında çalışan ağ cihazları ve son kullanıcı bilgisayarları hem IPv4 hem de IPv6 teknolojisini desteklemelidir. Örneğin bir ağ yöneticisi IPv4 adreslerinin, IPv4 ile çalışan DHCP üzerinden dağıtımını sağlayabilir. Aynı zamanda IPv6 adreslerin otomatik olarak ayarlanması gerçekleştirilebilir.

Ortak bir ağ altyapısında çalışan IPv4 ve IPv6 teknolojisinin ikili yığınla çalışan cihazlarda uygulanması, hem IPv4 hem de IPv6'nın aynı fiziksel bağlantılardan iletilmesini gerektirmektedir. Dolayısıyla ethernet ve ikinci katmanda çalışan diğer teknolojiler hem IPv4 hem de IPv6'yı desteklemelidir. IPv4 ve IPv6'yı destekleyen cihazların, her iki teknolojiyle de çalışabilmesi için, bu tür fiziksel bağlantıları da desteklemesi gerekmektedir. Bu yaklaşım Şekil 1'de gösterilmektedir.

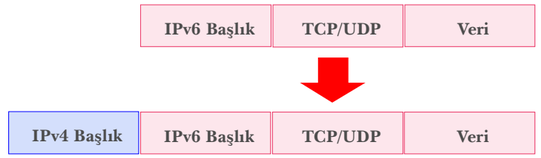


Şekil 1. *IPv6 ve IPv4'ün beraber çalışması.*

Tünelleme Yaklaşımı

IPv4 üzerinden IPv6 paketlerini veya IPv6 üzerinden IPv4 paketlerini iletmek için kullanılabilecek pek çok tünelleme teknolojisi bulunmaktadır. Yani IPv4 paketi içerisine IPv6 paketi konulup belli bir noktaya kadar öyle taşınır belli bir noktadan sonra paket açılarak IPv6 paketi çıkarılır ve IPv6 olarak işlenir. Ya da tam tersi yapılabilir. Bu yapı ile IPv4 ve IPv6 ağlar içi içe kullanılabilir. Bu teknolojiler, genel olarak, ayarlanmış ve otomatik olmak üzere, iki şekilde ifade edilebilir. Ayarlanmış tüneller önceden tanımlıdır.

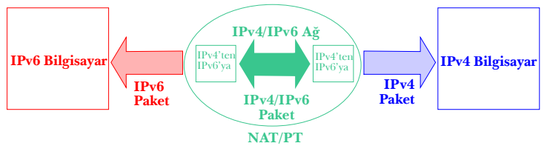
Genel olarak IPv6 paketlerinin IPv4 ağı üzerinden tünellenmesi, her bir IPv6 paketin başına IPv4 başlığı eklenmesiyle gerçekleştirilir. Bu işlemle birlikte tünellenmiş IPv6 paketlerinin IPv4 cihazlar tarafından iletilmesi sağlanır. Tünelin başlangıç ve bitiş noktaları yönlendirici veya son kullanıcı olabilir. Kaynağın IPv4 adresi olarak tünel başlangıcındaki cihazın IPv4 adresi, hedefin IPv4 adresi olarak da tünel bitişindeki cihazın IPv4 adresi verilir. Tünelin çıkış noktası IPv4 başlığını açarak IPv6 paketi ortaya çıkarır ve gerekli yönlendirmeleri yaparak bu paketin hedefine ulaşmasını sağlar.



Şekil 2. *IPv4 başlığı eklenmesi.*

Ağ ve Port Adres Dönüşümü Yaklaşımı

IPv6 paketleri, IPv4 paketlere ya da IPv4 paketleri IPv6 paketlere dönüştürerek iletmek mümkündür. Bu dönüşümler Ağ Adres Dönüşümü ve Port Dönüşümü (PT) ile yapılır.



Şekil 3. *Ağ ve port adres dönüşümü.*

Geçiş Teknolojilerinin Karşılaştırılması

İkili yığın yöntemi, kullanımı kolay ve esnek bir çözümdür. Ancak bu yöntem, IPv4 ve IPv6 yığınlarını bir arada çalıştırmak zorundadır. Bu yüzden daha çok bellek ve işlemci gücü gerektirmektedir. Ayrıca bu yöntemde kullanılan uygulamalarda, bilgisayarların IPv4'le mi yoksa IPv6'yla mı çalıştığını belirlemek gerekir.

Tünelleme yöntemi, herhangi bir ISS desteği olmasa da, IPv6 protokolüyle iletişim yapılabilmesini sağlar. Bütün bir ağda sadece iki bilgisayar IPv6 teknolojisi içeriyorsa, IPv4 ağı üzerinden bu iki bilgisayarın IPv6 ile haberleşebilmesi tünelleme yöntemiyle mümkündür. Bu yöntemin olumsuzlukları, diğer tünelleme düzeneklerinde olduğu gibi, tünel giriş ve çıkış noktalarında çalışan cihazların fazladan iş yapması ve tekil arıza noktaları içermesidir.

Dönüşüm yöntemleri ise sadece özel ihtiyaçlar halinde kullanılır. Bu yöntem, IPv6 teknolojisiyle gelen bazı özelliklerin kullanılamamasına neden olmaktadır.

Her dönüşüm yönteminin iyi ve kötü yanları olmasına karşın uygulanacak ağın durumu hangi yöntemin seçileceğinde önemli bir rol oynamaktadır. Etkin bir geçiş yöntemi için ağ analiz edilmeli, ihtiyaçlar belirlenmeli ve ona uygun bir geçiş yöntemi seçilmelidir.

IPV6 TEKNOLOJİSİNİN DURUMU

Dünyadaki Durum

IPv6 teknolojisinin uygulanmasında ilk adım olarak 1999 yılında kurulan IPv6 forumu dikkat çekmektedir. IPv6 forumunun görevi genel olarak internet kullanıcılarını IPv6 teknolojisinin avantajları konusunda bilgilendirmek ve bu protokolün dünyada yaygınlaşmasını sağlamaktır. IPv6 forumunun üyeleri arasında donanım/yazılım üreticileri, sektöründe lider telekomünikasyon firmaları, internet servis sağlayıcılar, internet çözüm üreticileri, danışmanlık şirketleri, ar-ge enstitüleri gibi pek çok kuruluş yer almaktadır.

Dünyanın değişik bölgelerinde IPv6 teknolojisinin durumu, teknolojinin geleceği için umut verici olmakla birlikte, gelecekte, bilişim dünyasında yaşanacak gelişmelerin de habercisidir.

6NET projesi IPv6 sürümü ile internetin büyümesini ve IPv6'ya geçişi göstermek için Avrupa Birliği tarafından oluşturulmuş 18 milyon Euro bütçesi olan üç yıllık bir projedir. Projeye üniversiteler, araştırma enstitüleri ve özel sektörden otuz beş kurum katılmıştır. Proje 2002 yılında başlamış ve 30 Haziran 2005'te sonlandırılmıştır [5]. Bu proje ile ilgili dokümanlar ve konu ile ilgili kılavuzlar http://www.6net.org/ adresinden izlenebilir. 6NET projesi iki buçuk yıl süreli başka bir Avrupa Birliği projesi olan DISS ile devam etmiştir. DISS projesinde hedefler: IPv6 kurulum ve geçiş planları konusunda bilgi değişiminin sağlanması, IPv6 konusunda çalışmalar yapan Çin ve Hindistan'la bilgi değişimi sağlamak, IPv6 konusunda elde edilen bilgi ve birikiminin etkin olarak yayınlanmasını sağlamak, Avrupa Birliği'ne üye ve aday ülkelerin araştırma geliştirme faaliyetlerini ilerletmek, IPv6 konusunda mükemmeliyet merkezleri oluşturmak olarak tanımlanmıştır. Proje Eylül 2007'de tamamlanmıştır. Fransa'nın başkenti Paris ve Belçika'nın başkenti Brüksel'de kurdukları laboratuarlarla IP ürünlerinin uyumluluk testlerine ve kurumları bilinçlendirme faaliyetlerine devam etmektedirler [7].

www.go6.net IPv6 konusunda bilgi vermek amacıyla kurulmuş bir internet sitesidir. IPv6form, Hexago ve VSNL International tarafından desteklenmektedir.

ABD: ABD hükümeti sivil ve askeri bütün kuruluşların uyması gereken, 30 Haziran 2008'e kadar IPv6'ya geçiş konusunda bir kanun yayınlamıştır [8]. Aralık 2009'da yeni alınacak ürünlerde IPv6 uyumluluk olması şartını getirmiştir. Bu düzenlemeler ABD'de IPv6'nın hızlı bir şekilde yaygınlaşmasını sağlamaktadır.

Kanada: Kanada'da faaliyet gösteren Viaginie kuruluşu, IPv4 bilgisayarlarının IPv6 ağa bağlanabilmesi için bir tünel sunucusu geliştirmiştir. ABD ve bazı ülkelerle IPv4 tüneller üzerinden yerel IPv6 ağa bağlantı kurulmuştur. Kanada'da ayrıca IPv6 destekleyen kök DNS sunucusu DNS sorgularına cevap vermektedir.

Japonya: Japonya'da bulunan tüm ISP'ler IPv6 servislerine başlamıştır. IIJ (Internet Initiative Japan) kuruluşu 1998'de tünelleme yoluyla ilk IPv6 servisini kurmuştur. Bu servisi halen yaklaşık 100 müşteri kullanmaktadır. NTT Telekomünikasyon şirketi 2001 yılında ilk ticari IPv6 servisini hizmete sokmuştur. Hitachi, Fujitsu, NEC, Furukawa Electric, Yamaha gibi önemli yönlendirici üreticileri IPv6 protokolünü destekleyen yönlendiriciler geliştirmiştir. Powered Com, Japan Telekom, KDDI gibi önemli servis sağlayıcılar mobil telefon, çevrimiçi oyun, sağlık gibi sektörlerde IPv6 teknolojisini deneme çalışmalarına başlamıştır. 370 firma IPv6 ürünün üretimi yapmaktadır. Güney Kore ve Çin bunun ancak uyarısını

yapabilmektedir. ABD'de ise daha düşük olduğu tahmin edilmektedir. Japonya'ya ait NNT haberleşme şirketi tek başına ABD ISS'larının tamamından fazla IPv6 müşterisine sahiptir.

Tayvan: Tayvan'da 7 büyük internet servis sağlayıcısı IPv4-IPv6 geçişi için kurumlara donanım dağıtmış ve IPv6 ile çalışan binlerce VoIP telefonu kamu çalışanlarına verilmiştir. Arabalar, kampüsler ve kişisel elektronik cihazlar için IPv6 teknolojisi kullanılmaya başlanmıştır. Tayvan en detaylı IPv6 projelerinden birini yapmaktadır.

Güney Kore: Diğer bir Asya ülkesi olan Güney Kore'de faaliyet gösteren Kore Telekom yeni bir IPv6 denemesi başlatmıştır. Kore hükümeti bu deneme için maddi destek sağlamaktadır. Almanya ve Avrupa Birliğinden sonra en çok IP adresi Güney Kore tarafından alınmıştır. Samsung ve LG gibi teknoloji şirketleri IPv6 destekli ürünler çıkarmaya çalışmaktadır.

Çin: IP adres sayısından fazla insanın yaşadığı tek ülke Çin'dir. Bu yüzden Ipv6'ya geçiş Çin'de oldukça önemsenen bir konudur. Çin hükümeti yıllardır IPv6 çalışmaları için maddi destek ve fon sağlamıştır ve sağlamaya devam etmektedir. Çin'de göze çarpan başka bir olay IPv6 teknolojisiyle oluşturulan Çin Yeni Nesil Internet CNGI(China Next Generation Internet) projesinin başlamış olmasıdır. Çin'de IPv6 teknolojisinin yaygınlaşması için itici güç olmuş ve IPv6 için en büyük test Pekin olimpiyatlarında yapılmıştır. Kamera ve ışık sistemi IPv6 ile kontrol edilmiştir. %10 civarında bir enerji tasarrufu ağlanmıştır. Çin IPv6 geçişi konusunda öncülüğünü sürdürmektedir.

Ülkelerin yanında birçok organizasyonda IPv6'ya geçiş ve yeni ürünlerin IPv6 protokolü ile uyumlu çalışacak şekilde üretilmesi konusunda açıklamalar yapmışlardır. Aşağıda bunlara ait bir kaç örnek verilmiştir [9].

- 3GPP, IMS ürünleri için özellikle IPv6 kullanılmasını zorunlu tutmuştur (http://www.3gpp.org).
- Telecommunications Industry Association (TIA), 3G Multimedya System (IMS)'i Next Generation Networks platformu olarak seçmiştir.
- Eylül 2000'de Japonya başbakanı IPv6'yi e-Japan 2005'in kritik parçası olarak tanımlamıştır. Japon hükümeti IPv6 uyumluluğunu yapan şirketlere vergi kolaylıkları sağlamıştır.
- 2003 Haziran'da ABD savunma bakanlığı Haziran 2008'e kadar IPv6'ya geçişi zorunlu tutmuştur. 2005 Haziran'da Beyaz Saray Yönetim Ofisi (White House Office of Management (OMB)) devlet kurumlarının 2008'e kadar olan geçişin temel adımlarını tanımlamasını istemiştir. (http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf). Geçişlerin bir kısmı yapılmış bir kısmı da yapılmaktadır.
- Avrupa Uzay Ajansı IPv6'ya desteğini ilan etmiştir.
- The Japanese Intelligent Transport System (ITS) projesi ve Avrupa Car2Car konsorsiyumu gelecek Car2car uygulamalarında IPv6'nın kullanımını tavsiye etmişlerdir.
- The Digital Video Broadcasting (DVB-S) konsorsiyumu IPv6'ya geçişe karar vermiştir.
- Çin hükümeti CNGI'i kurmuş ve parasal olarak desteklemiştir. Çin'in internet omurgası IPv6 olarak tasarlanmıştır.
- GRID kendi Globus Toolkit 4 ürününü IPv6 uyumlu hale getirilmiştir. (http://www.gridtoday.com/05/0117/104472.html)

TÜRKİYE'DEKİ MEVCUT DURUM

Türkiye'de IPv6 konusundaki ar-ge çalışmalarına 2003 yılı başında TÜBİTAK – ULAKBİM başlamıştır. ULAKBİM, Avrupa Akademik Ağı GEANT'a olan İnternet bağlantısındaki hazırlıklarını tamamlayarak 2003'te ULAKNET'e bağlı olan tüm üniversitelerin ve araştırma kurumlarının GEANT'a saf IPv6 bağlantısı yapabilmesi için gereken omurga altyapısını oluşturmuş; 2004 yılının başından itibaren talep eden üniversitelere IPv6 adreslerini tahsis edebilecek duruma gelmiş; ve Şubat 2004'te düzenlenen Akademik Bilişim'de tüm üniversitelere IPv6 teknolojisinin tanıtımını yapmıştır. IPv6 protokolünün gelişimini, IPv6'ya geçişte yaşanacak sorunları ve çözüm yollarını, ve dünyadaki IPv6 ar-ge çalışmalarını takip eden TÜBİTAK - ULAKBİM, 2006 yılı sonunda 6 üniversitenin de katılımıyla ULAK6NET Görev Gücü'nü oluşturmuştur.

Telekomünikasyon Kurumu tarafından hazırlanan "Mobil IP: Mevcut Düzenlemeler ve Türkiye Önerileri" başlıklı kurum tezinde IPv6 konusu ağırlıklı olarak işlenmiş; tez çalışması kapsamında, İşletmeciler ve ISS'lara 2004 yılında yapılan anket çalışması sonucunda, ISS'ların bir bölümünün IPv6 uyumlu donanım altyapısına sahip oldukları ve geçişe istekli oldukları öğrenilmiştir. Bilgi Teknolojileri ve İletişim Kurumu, ULAKBİM, Gazi Üniversitesi ve Çanakkale Üniversitesi mevcut altyapının IPv6 uyumluluğunun tespit edilmesi, geçiş planlarının çıkarılması için hali hazırda bir proje yürütmektedir.

Bu gelişmeler yanında Türkiye IPv6 destekli ürün üretme, teknoloji geliştirme ve güvenliğini test etme bakımından öncelikle uzakdoğu ülkeleri başta olmak üzere diğer ülkeler kadar ileri gidemediği görülmektedir. Türkiye'de henüz IPv6 teknolojisini destekleyen ürünlerin uyumluluk testlerini yapabilen, IPv6 geçişi için test ortamları hazırlayıp geçiş planları çıkaran, ürünlerin IPv6 performansını değerlendirebilen, IPv6 güvenli yapılandırma kılavuzlarını çıkaran bir kurum ya da kuruluş yoktur.

Genel olarak Türkiye'de yer alan 23 kuruluş (ULAKBİM, SUPERONLINE, ESERTELEKOM, TÜRK TELEKOM, KOÇNET vb…) RIPE'tan IPv6 adres uzayı satın almıştır. Bunlardan sadece 3 tanesi aktif olarak kullanmaktadır. IPv6 adresi alan kuruluşlara iat tablo Şekil 4 görülmektedir.

SONUÇ

Yakın gelecekte IPv4 adreslerinin bitecek olması, IPv6 protokolünün bünyesinde yeni özellikler barındırması, yeni teknolojilerin IPv6 destekli olarak gelmesi dünyada IPv6'ya geçişi hızlandırmaktadır. IPv6 protokolünün ortaya çıkmasıyla birlikte dünyadaki birçok ülke IPv6 geçiş çalışmalarına, üreticiler de IPv6 uyumlu ürünler üretme konusunda çalışmaya başlamışlar ve bu çalışmalar son yıllarda hız kazanmıştır.

Türkiye'deki kurum ve kuruluşların bir kısmı yeni teknolojilerin IPv6 destekli olmasından dolayı bir kısmı da adres sıkıntısından dolayı IPv6'ya geçmek durumunda kalacaklardır. Bunun için öncelikle internet servis sağlayıcıların sonra da interneti kullanan kurumların IPv6 altyapısını oluşturma çalışmalarına başlamaları gerekmektedir. Diğer taraftan ilgili kurumların IPv6 ve IPv6'ya geçiş, IPv6 güvenliği konularında kurum ve kuruluşlarda bilinç oluşturması gerekmektedir.

IPv6 destekli teknolojiler ve ürünler üretmek, belli alanlarda teknolojik liderliği ele geçirmek için önemli bir fırsat olacaktır. Bu fırsatın değerlendirilebilmesi için IPv6 konusunda politikalar geliştirilmeli ve çalışma alanları belirlenerek bu alanlarda yapılacak araştırmalar çeşitli fonlarla desteklenmelidir.

Tablo 1. Türkiye'de IPv6 adresi almış kurumlar.

Adres	Sahibi	Rezervasyon	İlk Bağlantı	Son Bağlantı
2001:930::/32	KocNET	2002-10-04	2009-06-22	2010-12-28
2001:a98::/32	Ulakbim	2003-01-14	2003-05-30	2010-12-28
2001:1b68::/32	Eser Telekom	2004-05-07		Bağlanılmadı
2a00:de8::/32	TR.NET Orta Dogu Yazilim	2008-11-07		Bağlanılmadı
2a00:1880::/32	Vodafone Turkey IPv6 Allo.	2009-12-15		Bağlanılmadı
2a00:1d30::/32	TTNet A.S.	2010-03-12		Bağlanılmadı
2a00:1d58::/32	Turksat Uydu Haberlesme	2010-03-15		Bağlanılmadı
2a00:1f90::/32	Is Net A.S.	2010-04-22		Bağlanılmadı
2a00:dc00::/32	SiNET Telekomunikasyon Ltd.	2010-12-23		Bağlanılmadı
2a01:188::/32	Superonline International.	2006-08-07		Bağlanılmadı
2a01:358::/32	Turk Telekom	2007-05-16	2008-04-25	2010-12-28
2a01:718::/32	Borusan Telekom ve Ile.	2007-12-28		Bağlanılmadı
2a01:720::/32	ADA-NET Internet ve Ile.	2007-12-31		Bağlanılmadı
2a01:730::/32	Teletek Telekomunikasyon.	2008-01-08		Bağlanılmadı
2a01:748::/32	Meteksan Net Iletisim Hi.	2008-01-14		Bağlanılmadı
2a01:790::/32	Radore Hosting	2008-01-23		Bağlanılmadı
2a02:50::/32	Ihlas Net	2008-02-15		Bağlanılmadı
2a02:e0::/32	Tellcom Iletisim Hiz.	2008-02-27	2010-05-12	2010-12-21
2a02:178::/32	HSBC İnternet Ve Telekomu	2008-03-17		Bağlanılmadı
2a02:268::/32	Garanti Technology	2008-04-09		Bağlanılmadı
2a02:480::/32	DORUK-NET	2008-06-06		Bağlanılmadı
2a02:4e0::/32	Turkcell Iletisim Hiz.	2008-06-18		Bağlanılmadı
2a02:f80::/32	Maya Iletisim Ticaret Lim.	2009-06-02		Bağlanılmadı
2a02:ff0::/32	TurkNet Iletisim Hiz.	2009-06-15		Bağlanılmadı
2a02:2010::/32	Avea Iletisim Hiz.	2010-06-25		Bağlanılmadı
2a02:2020::/32	Cizgi Bilgisayar Sistemleri	2010-06-28		Bağlanılmadı
2a02:2460::/32	Oger Telecom Yonetim Hiz.	2010-09-20		Bağlanılmadı
2a02:26b0::/32	Hosting Internet Hiz.	2010-10-21		Bağlanılmadı
2a02:26c0::/32	Enson Net Ltd.	2010-10-21		Bağlanılmadı
3ffe:82d0::/28	OXYGEN/TR	2001-12-04		2005-04-15

KAYNAKÇA

[1] Introduction to IPv6, Microsoft Corporation, January 2008

[2] http://www.potaroo.net/tools/ipv4/index.html

[3] http://ietf.org/html.charters/ipv6-charter.html

[4] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November, 1998.

[5] Tim Rooney, "IPv6 to IPv4 Transation Strategies", BT Diamond, 2007

[6] http://www.6net.org/overview.html

[7] http://www.6diss.org/

[8] http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf

[9] Jim Bound, Yanick Pouffary, Yurie Rich, David Green, "IPv6 Form Roadmap&Vision", 2006

ELEKTRONİK İMZA

E-imza Oluşturma Araçları

Ersin GÜLAÇTI

Dizimizin dördüncü yazısında e-imza araçları konusunu yazılım, donanım, işletim sistemleri ile entegrasyon ve yazılım geliştirme araçları boyutlarıyla ele alacağız. Ayrıca en güvenli ve yaygın kullanılan e-imza oluşturma aracı olan akıllı kartların güvenliğinden de bahsedeceğiz.

1. GİRİŞ

E-imza ve diğer açık anahtar altyapısı hizmetlerinden yararlanırken her elektronik sertifika sahibi kendisine ait özel ve açık anahtarları kullanır. Açık anahtar verisi elektronik sertifikanın içine yerleştirilen ve herkesle paylaşılan bir bilgidir, ancak özel anahtar bilgisi kişiye özel olan ve başka kimseyle paylaşılmaması gereken bir veridir.

E-imza oluşturma ve doğrulama işlemlerinde yazılım ve donanım bileşenleri beraber kullanılır. Bu bileşenler genellikle kişisel bilgisayar sistemleriyle beraber çalıştırılır. Özel anahtarların üretim anından itibaren yaşam döngüsünün tamamında güvenli olarak saklanması ve kullanılması gerekir. Bu zorlu görevi yerine getirmek için kullanılan akıllı kartları ve diğer bileşenleri ilerleyen kısımlarda daha yakından tanıyacaksınız.

Bu yazıda geçen kavramların daha iyi anlaşılması için yazı dizimizin önceki yazılarının okunması yararlı olacaktır.

2. AKILLI KARTLAR

Akıllı kartlar, genelde kredi kartı boyutlarında plastik ve bezneri malzemeden üretilmiş, içerisinde işlemci, RAM ve ROM belleği bulunan gömülü bir mikroişlemciye sahip donanımlardır. Üzerinde manyetik şerit, barkod, temassız radyo frekans vericileri gibi farklı teknolojileri bulundurabilirler. Günümüzde kapı geçiş kontrolü, elektronik ticaret, kimlik doğrulama, e-imza vb gizlilik ve güvenlik gerektiren bir çok uygulamada çok yaygın olarak akıllı kartlar kullanılmaktadır. Akıllı kartlar açık anahtar altyapısının ürettiği sertifikaların ve bunlarla ilişkili olan özel anahtarların taşınması için kullanılan en yaygın ve güvenli cihazlardır.

Akıllı kartlar elektronik devre yapılarına, veri aktarım tipine ve boyutlarına göre farklılıklar gösterirler. Akıllı kartlar veri tipine göre aşağıdaki gibi sınıflandırılabilirler:

- Bellek kartları
  - o Güvenlik donanımlı
  - o Güvenlik donanımı olmayan
- İşlemcili Kartlar
  - o Kripto işlemcili
  - o Kripto işlemcisi olmayan

Akıllı kartlar üzerinde bulunan mikroişlemcinin dış dünya ile haberleşme yöntemine göre "temaslı" ve "temassız" olmak üzere iki ana sınıfa ayrılır. Bazı kartlar temaslı ve temassız ara yüzleri üzerinde iki ayrı mikroişlemci taşıyarak sunabilir. Bu tür kartlara hibrid kart adı verilir. Bu özelliğin aynı mikroişlemci üzerinde birleştirildiği kart tipine ise dual kart adı verilir.

Açık anahtar altyapısı ve e-imza sistemlerinde kullanılabilecek akıllı kartlar kripto işlemcili akıllı kartlar sınıfında yer alırlar. Bu akıllı kartlar, programlanabilir alanları olan, dayanıklı, taşınabilir bilgisayarlar olarak tanımlanabilir. Bu kartların başlıca teknik özellikleri şöyle sıralanabilir:

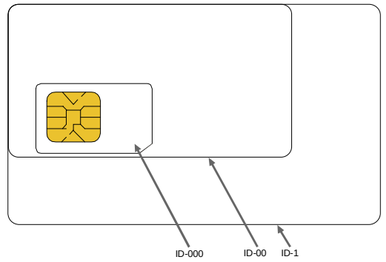
- Mikroişlemciye sahiptir. (8, 16 ve 32 bit modeller vardır)
- Bir işletim sistemine sahiptir. (AKIS, CardOS, Multos vb.)
- RSA, DSA, ECDSA gibi asimetrik algoritmaları çalıştırabilen yardımcı kripto işlemcisine sahiptir.
- İşletim sistemi ve kripto kütüphanesi mikroişlemcinin ROM belleğinde saklanır.
- Kripto anahtarlarını ve sertifikaları saklamak için yeterli büyüklükte EEPROM belleğe sahiptir. (Tercihen 8kb ve üstü)
- Özel anahtarlar kart içinde üretildikten veya kart içine yerleştirildikten sonra asla dışarı çıkarılamaz.
- Kart içindeki özel anahtarla işlem yapmak için karta PIN kodu girilmesi zorunludur.

Yukarıdaki özelliklere sahip bir akıllı kart aşağıdaki hizmetleri sunar:

- Kart üzerinde şifreleme ve şifre çözme,
- Kart üzerinde imzalama ve imza onaylama,
- Kart üzerinde özel ve açık anahtarların tutulması,
- Kart içine bilgi yazabilme,
- Kartın parola (PIN kodu) ile korunması.

Akıllı kartların özel ve açık alanları vardır. Özel alanlarda anahtar üretimi, imzalama, şifre çözme gibi işlemler yapılır, bu alanlara dışarıdan yetkisiz erişim yasaklanmıştır. Açık alanlara genel bilgiler yazılır. Akıllı kart yönetim yazılımı yardımıyla buradaki bilgiler görülebilir.

Akıllı kartın boyutları, uluslararası ISO-7810 standardına göre belirlenir. ISO-7816 standardı ise çalışma sıcaklıkları, esneklik, elektriksel temasın pozisyonu ve mikroişlemcinin dış dünya ile nasıl bağlantı kuracağı gibi özellikleri kapsayan, kartın fiziksel karakteristiğini de belirler. ISO 7816'da tanımlanan kart biçimleri Şekil 1'de verilmiştir.



Format	Boyutlar (GXY) mm	Örnek
ID-1	85,6 x 54	Kredi kartı
ID-00	66 x 33	-
ID-000	24 x 15	SIM kart

Kart kalınlığı: 0,76 mm

Şekil 1. *ISO 7816'ya göre Akıllı Kart boyutları.*

3. AKILLI KART OKUYUCULAR

Akıllı kartların kendi enerji kaynakları olmadığı için ancak bir okuyucu terminale bağlanarak kullanılabilirler. Bu terminallere akıllı kart okuyucu adı verilir. Akıllı kart okuyucuların bağlandıkları bilgisayarda kullanılabilmesi için sürücü yazılımlarının o bilgisayara yüklenmiş olması gerekir. Değişik akıllı kart okuyucu tipleri aşağıda anlatılmaktadır.

Masaüstü Akıllı Kart Okuyucular

Bu kart okuyucular en yaygın kullanılan modellerdir. Kredi kartı boyutundaki akıllı kartlarla kullanılırlar. Bilgisayara USB veya seri bağlantı ile bağlanırlar. Üzerinde yer alan ışık sayesinde kart ile işlem yapılıp yapılmadığı gözlenebilir.

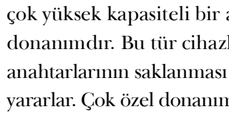
Tuş Takımlı Akıllı Kart Okuyucular

Bu tip okuyucular akıllı kart parolasını (PIN) kendi üzerlerindeki tuş takımı aracılığıyla alabilirler. Böylece kart parolası başka bir cihaza (örneğin bilgisayara) iletilmez. Bu yöntem diğer okuyuculara göre daha güvenli çalışmasını sağlar. Bazı modeller tuş takımının yanı sıra LCD ekran da içerir. Bilgisayara USB veya seri bağlantı ile bağlanırlar. Diğer okuyucu tiplerine oranla fiyatları daha yüksektir.

Akıllı Çubuk Şeklinde Kart Okuyucular

Bu tür kart okuyucular USB kapısından bilgisayara bağlanır ve SIM Kart boyutundaki akıllı kartlarla çalışırlar. Fiyatı en ucuz olan okuyucu tipidir.

PC Kart Seklinde Kart okuyucular



Genellikle bu okuyucular taşınabilir bilgisayarların PCMCIA yuvalarına takılarak kullanılır. ID-1 (kredi kartı) boyutunda kartları okumak için kullanılırlar. Taşınabilir bilgisayarlar ile kullanımı çok kolaydır.

Klavye ile Bütünleşik Kart Okuyucular

Bu tür okuyucular bilgisayarlar için üretilen klavyelere bütünleşiktir. Bu tip klavyeler normal klavyelerden daha pahalıdır. Eğer klavyedeki tuşlar bozulursa kart okuyucu kısmı sağlam bile olsa klavyenin değiştirilmesi gerekir. Bu da maliyeti yükseltici bir etkendir.

Disket Sürücü Şeklinde Kart Okuyucular

Bu tür okuyucular bilgisayarların 3.5" veya 5.25" genişleme yuvasına monte edilir ve bilgisayarın ana kartına bağlanır. Var olan bilgisayarlara takılması ayrı bir işgücü gerektirdiği için, çoğu kişi tarafından kullanışlı bulunmamaktadır.

4. GÜVENLİ DONANIM MODÜLLERİ (GDM)

Güvenli donanım modülü (HSM: Hardware Security Module) çok yüksek kapasiteli bir akıllı kart gibi iş gören özel bir donanımdır. Bu tür cihazlar da akıllı kartlar gibi kripto anahtarlarının saklanması ve cihaz vasıtasıyla kullanılması işine yararlar. Çok özel donanımlar oldukları için maliyetleri oldukça yüksektir. Bu cihazlar hem daha uzun anahtarlar kullanılmasına (4096 bit RSA gibi) yarar, hem de çok yüksek başarımla kripto işlemi yapabilirler. Bazı modellerde saniyede 2000 adet 1024 bit RSA işlemi yapılır.

GDM donanımları, çok sayıda e-imza işlemi yapan kurumların tercih ettiği, e-imza oluşturma araçlarıdır. Örneğin elektronik sertifika hizmet sağlayıcıları, aboneleri için e-fatura üreten firmalar GDM kullanırlar.

Donanım güvenlik modülleri iki temel tipte yer alır:

Adanmış modeller : Bu modeller sadece bir bilgisayara bağlı olarak çalışır. PCI kart seklinde veya bilgisayardaki bir SCSI kontrol kartına bağlanan, harici cihaz seklinde olan modeller vardır.

Ağ modelleri : Bu tür GDM'ler kendi başlarına çalışan ve ağ ara yüzüne sahip cihazlardır. Genellikle bir yerel alan ağı (LAN) üzerinde çalışan birden fazla bilgisayar tarafından kullanılırlar.

5. GÜVENLİK

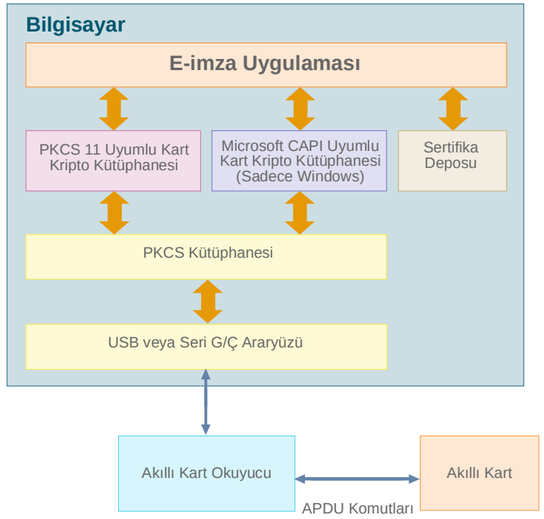
Akıllı kartların ve güvenli donanım modüllerinin e-imza, şifre çözme vb kripto işlemlerinde kullanılan özel anahtarları güvenli olarak saklamaları ve kullandırmaları çok önemlidir. Bu nedenle bu tür ürünlerin çeşitli güvenlik testlerinden geçmeleri ve bu durumu belgelendirmeleri istenir. Bu güvenlik testlerinin en bilinenleri Ortak Kriterler (Common Criteria) ve FIPS (Federal Information Processing Standards) olarak sayılabilir. Ortak Kriterler testleri, Türkiye'nin de sertifika üreticisi olarak içinde bulunduğu uluslar arası bir anlaşmaya taraf 15 üretici ve 11 tüketici ülke tarafından kabul görmüştür. FIPS ise ABD tarafından ortaya konan standartları tarif eder.

Bir akıllı kartın veya GDM'nin ne ölçüde güvenliğe olduğu sahip olduğu Ortak Kriter veya FIPS sertifikasına bakılarak anlaşılabilir. Türkiye'deki e-imza mevzuatına göre bir e-imza oluşturma aracının en az Ortak Kriterler EAL4+ düzeyinde veya en az FIPS 140-2 Level 3 düzeyinde olduğunu belgelendirmek zorunludur.

Akıllı kartların ve GDM'lerin güvenlik testleri yapılırken çok çeşitli yöntemler kullanılır. Bu yöntemler arasında tasarım ve kaynak kod gözden geçirme, nüfuz testleri (penetration test), fiziksel saldırı (örneğin: odaklanmış iyon demedi - focused ion beam), yan kanal analizi vb sayılabilir.

6. İŞLETİM SİSTEMLERİ İLE ENTEGRASYON

Akıllı kartların ve kart okuyucuların işletim sistemleri ile beraber çalışabilmesi için Şekil 2'de gösterilen mimariye benzer bir yapı kullanılır.



Şekil 2. *AkıllıKart - İşletim Sistemi ilişkisi.*

Bir akıllı kartın işletim sisteminde kullanılabilmesi için aşağıdaki yazılımların yüklenmiş olması gerekmektedir.

Akıllı Kart Okuyucu Sürücüsü: Bilgisayara bağlanan tüm cihazlar gibi akıllı kart okuyucu için de bir sürücü yüklenmesi gereklidir. Bu sürücü bilgisayarın giriş-çıkış sistemi üzerinden haberleşmeyi sağlar.

İşletim Sistemi Akıllı Kart Bileşenleri: Windows işletim sisteminde ve Linux dağıtımlarında hazır olarak gelen akıllı kart erişim altyapısı kullanılır. Bu altyapı için PC/SC standardı kabul görmüştür.

Akıllı Kart Kripto Kütüphanesi: Programcının akıllı karta erişmesini sağlayan, imzalama, şifreleme gibi işlemleri yaptırabileceği fonksiyonların bulunduğu kütüphanelerdir. Bunlardan en yaygını olan PKCS#11 [2] standardı ile uyumlu kütüphane genellikle açık kaynak kodlu ürünlerin ve Java platformunun akıllı karta erişim için tercih ettiği kütüphane tipidir. PKCS#11 kütüphaneleri, platform bağımsız akıllı kart uygulaması geliştirmek için Windows, Linux, Mac OS gibi farklı ortamlarda kullanılabilir. Diğer kütüphane tipi ise Microsoft CAPI uyumlu kütüphanedir. Bu tip kütüphaneler, Microsoft Windows işletim sistemi üzerinde kullanılmak üzere, Microsoft firması tarafından tanımlanmış standarda uygun yazılmıştır.

[1] Personal Computer Smartcard Consortium tarafından yayınlanmış standarttır. Daha fazla bilgi için: http://www.pcscworkgroup.com/.

[2] Public Key Cryptography Standards: RSA firması tarafından yayınlanmış ve 1'den 15'e kadar numaralandırılmış açık anahtar altyapısı ile ilgili standartları ifade eder. Daha fazla bilgi için: http://www.rsa.com/rsalabs/node.asp?id=2124.

Şekil 2'de gösterilen kart okuyucu-akıllı kart haberleşmesi APDU komut seti ile yapılır. APDU (Application Protocol Data Unit) okuyucu ile akıllı kartın arasındaki haberleşmeyi sağlayan bir veri yapısıdır. APDU'nun yapısı ISO-7816 standartında tanımlanmıştır.

7. YAZILIM GELİŞTİRME

E-imza oluşturmak için yazılım geliştirenlerin en temel ihtiyacı, bilgisayara takılı akıllı kart okuyucuları ve bunların içindeki akıllı kartları doğru bir şekilde tespit edip kullanmaktır. Bilgisayara takılı kart okuyucular genellikle PC/SC katmanının sunduğu fonksiyonlar ile tespit edilebilir. Akıllı kart okuyucular tespit edildikten sonra akıllı karta erişilmek istendiğinde iki seçenek karşımıza çıkar. Bunlar; APDU komutları ve kart kripto kütüphanesidir.

Uygulama geliştiriciler herhangi bir Akıllı Kart Kripto Kütüphanesi kullanmadan doğrudan APDU komutlarıyla akıllı karta hükmedebilirler. Ancak bu yöntem, farklı akıllı kartların komut setlerine göre, farklı işlemler yapmayı gerektirir. Bu nedenle genellikle en yaygın kart kripto kütüphanesi tipi olan PKCS#11 kütüphaneleri üzerinden akıllı kartların yönetilmesi tercih edilir. Ayrıca HSM cihazlarının genellikle APDU komut seti desteği yoktur. Bu nedenle, GDM cihazlarına erişimde de, Akıllı Kart Kripto Kütüphanesi kullanılması yaygın bir yaklaşımdır.

PKCS#11 kütüphaneleri her ne kadar kullanılan akıllı kart markasından bağımsız olarak yazılım geliştirmeyi mümkün kılsa da çok basit bir yapıya sahip değildirler. Bu nedenle, e-imza yazılımı geliştirenlerin, PKCS#11 standardını çok iyi öğrenmeleri ve kullanmaları veya bu arayüzü geliştirilen yazılımdan soyutlayan yardımcı kütüphaneler kullanmaları gerekir.

Akıllı Kartlar ve Uygulamaları

ORTAK KRİTER GÜVENLİK SERTİFİKASININ ALINMASI

Mustafa BAŞAK

Günümüzde geniş bir kullanım alanına sahip olan akıllı kartlar, her geçen gün daha da yaygınlaşmaktadır. Elektronik ortamda verilen hizmetlerin çeşitliliği ve kalitesi, akıllı kart kullanımı sayesinde giderek artmaktadır. Yazı dizimizin bu bölümünde, çeşitli akıllı kart uygulamaları ve güvenlik sertifikası alınması hakkında bilgi verilecektir.

Akıllı kart uygulamaları, vatandaşın kamu veya özel kurum hizmetlerinden yararlanması için kullanılan kimlik tabanlı uygulamalar ve mali işlemlerde kullanılan ödeme sistemleri uygulamaları olmak üzere iki grupta toplanabilir. Bu uygulamalar, yazıda ayrıntılı olarak açıklanmıştır.

1. PKI (AAA) Uygulaması

Akıllı kart kullanılarak gerçekleştirilen PKI (Public Key Infrastructure - Açık Anahtar Altyapısı - AAA) uygulamaları ile ilgili teknik bilgiler, yazı dizimizin dördüncü bölümünde ayrıntılı olarak verilmişti. Bu bölümde, uygulamada akıllı kart üzerinde gerçekleştirilen işlemler ele alınacaktır.

PKI uygulaması, dokümanların elektronik ortamda sayısal imza (elektronik imza) ile imzalanması ve/veya imzalanmış dokümanların geçerlenmesi için tasarlanmış bir akıllı kart uygulamasıdır. Bu uygulamanın amacı, elektronik ortamdan gelen bir dokümanın doğru kişiden ve değişikliğe uğramadan geldiğinden emin olunmasıdır. Sayısal imza, ıslak imzadan daha yüksek bir güvenlik sağlar.

Sayısal imza, imzalanacak dokümanın (veya mesajın), imzalayan kişinin asimetrik özel anahtarıyla kriptolanması ile elde edilir. Sayısal imza, elektronik ortamdaki dokümanın sonuna eklenir ve aşağıdaki özelliklere sahiptir:

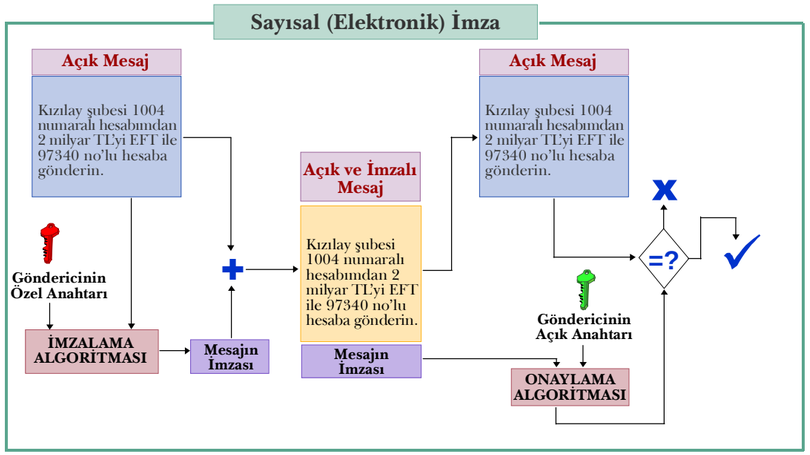
- Elektronik ortamdaki dokümanın gönderildiği kişinin, mesajı gönderenin kimliğini doğrulamasını ve dokümanın değiştirilmediğini teyit edebilmesini sağlar,
- İnkâr edilemezlik hizmeti sağlar,
- Asimetrik şifreleme yöntemi ile elde edilir.

Şekil – 1'de, sayısal imza atılması ve bu imzanın doğrulaması adımlarının uygulandığı bir sayısal imzalama .akışı verilmiştir.

PKI uygulaması, kişiye güvenilir ve hukuksal geçerliliği bulunan bir kurum tarafından sayısal imza sertifikası verilmesi ile başlar. Kurum tarafından verilen elektronik imza sertifikasının kullanılabilmesi için, bir akıllı kart içerisine güvenli olarak yüklenmesi gerekir. Yüklenen sertifika ile kişiselleştirilen akıllı kartın sahibi tarafından kullanılabilmesi için PIN (Personal Identification Number – Kişisel Tanımlama Numarası) koruması uygulanır. Kişinin atacağı sayısal imzanın yalnızca sertifika sahibinin bileceği bir bilgi olan PIN girildikten sonra atılabilmesi imzayı atan kişiye sorumluluk yükler. Kullanıcının, kişisel PIN numarası ve sertifikası ile imzalanmış bir belgeyi inkar etmesi, hukuksal bir geçerlilik taşımaz.

PKCS#15 veri yapısının, sayısal imza uygulama yazılımının, hukuksal geçerliliği olan X509 standardında bir sertifikanın, kişinin asimetrik özel anahtarının ve PIN akıllı kart içerisine yüklenmiş olması, kişinin doküman imzalayabilmesi veya imzalanan bir dokümanı onaylabilmesi için yeterlidir. Ancak, akıllı kartı kullanarak imzalama veya imza onaylama işlemini gerçekleştirecek olan yazılımın (cihazın) bu işlemi yaptırabilmesi için, PKCS#11 sayısal imza arayüz standardını desteklemesi gerekir.

Akıllı kartlarda, işletim sistemi tarafından çalıştırılacak olan PKI uygulama yazılımının da güvenliği belgelenmiş bir yazılım olması ve akıllı kart dışında bulunan yazılımsal arayüzlerinin de güvenlik kriterlerine uygun şekilde tasarlanmış olması gerekir.



Şekil 1. *Sayısal imzalama tekniği.*

2. Vatandaşlık Kartı (e-kimlik) Uygulaması

Vatandaşlık kartı uygulaması, vatandaşın devlet hizmetlerinden kolaylıkla yararlanmasını sağlamak amacıyla gerçekleştirilen bir uygulamadır. Bu uygulamada vatandaşlık kartı, vatandaş ile devleti birbirine bağlayan bir araçtır. Bu aracın çalınmaya ve kopyalanmaya karşı güvencede olması, önde gelen gereklerden biridir. Vatandaşlık kartı uygulamasının, üzerinde e-kimlik uygulaması olan güvenli bir akıllı kart ile sağlanması önerilir. Bu nedenle akıllı kart üzerindeki e-kimlik uygulaması, ülkeler için önemli bir gereksinim olarak ortaya çıkmaktadır. Bu uygulamanın güvenliğini sağlamak, kartın sağlayıcısı olan devlete düşmektedir. Ayrıca, bazı evrensel uygulamalarda ülkelerin başka ülke vatandaşlarının kimliklerini doğrulaması zorunluluğundan dolayı (örneğin elektronik pasaport uygulaması) elektronik kimlik kartı uygulamalarında uluslararası standartlara uyulmasını zorunlu hale gelmektedir. Bu türdeki uygulamalarda, ülkeler karşılıklı olarak birbirlerinin elektronik kimlik kartlarına güvenirler. Kimlik hırsızlığı, tüm dünyada önüne geçilmesi gereken önemli bir sorundur ve modern ulusal kimlik kartları, bu sorunun çözümüne katkı sağlamak üzere tasarlanmışlardır. Modern elektronik kimlik kartları, üzerinde bir yonga ve yonga içerisinde kişiye özel sertifikayı barındıran akıllı kartlar olarak tanımlanabilir. Bu akıllı kartlar, uluslararası geçerliliği bulunan birçok güvenlik testlerinden geçirilerek onaylanmış yonga ve bu yongalar üzerinde koşan akıllı kart işletim sistemi ile işletim sisteminin çalıştırdığı e-kimlik uygulamasını içerir.

2.1. Elektronik Kimlik Kartları (eID) için Kullanılan Yonga Donanımları

Yonga üreticisi büyük firmalar kimlik, iletişim ve ödeme sistemi uygulamaları için farklı ürünler geliştirmişlerdir. Ödeme sistemlerinde kullanılan ve EMV (**E**uropay, **M**asterCard, **V**isa) olarak adlandırılan akıllı kart yongaları VISA ve MASTERCARD kuruluşları tarfından sertifikalandırmaktadır.

Kimlik kartları ile ilgili yongalarda yapısal güvenlik önemli bir gereksinimdir. Bu yongaların güvenliğinin onaylanması için Ortak Kriterler (Common Criteria – CC) olarak adlandırılan kriterlerin sağlanması ve bu durumun bir laboratuvar tarafından geçerlenmesi gerekir. eID kartlarında kullanılacak yongaların donanımlarının CC EAL 5+ seviyesinde güvenlik sertifikasına sahip olması gerektiği konusunda ortak bir görüş oluşmuş durumdadır.

Elektronik kimlik kartlarında kullanılacak yonganın en az 48 Kbyte EEPROM, 6 Kbyte RAM bellek kapasitesine ve 12 MHz veya üzeri bir işlemci hızına sahip olması gerektiği pratikte varılan bir sonuçtur. Ayrıca, yonga üzerinde yardımcı bir işlemci olarak 3DES ve RSA şifre birimlerinin bulunması sayısal imza ve kimlik doğrulama işlemleri için gereklidir.

2.2. Elektronik Kimlik Kartları (eID) için Akıllı Kart İşletim Sistemleri

Elektronik kimlik kartları için tasarlanan işletim sistemlerinin, elektronik kimlik uygulamalarını çalıştıracak yapıda olması gerekir. Elektronik kimlik uygulamalarında sağlanması gereken standart, ISO 7816 (1-4), 8, 9 standardıdır. Bu standardı sağlayan kimlik kartları, uygulaması sonradan yüklenebilir olabileceği gibi "*native*" olarak adlandırılan bir yapıya sahip de olabilir. Son zamanlarda uygulaması sonradan yüklenebilen kartlar yerine native olarak tanımlanan kartlar çalışma hızı ve güvenlik gerekçeleri ile daha fazla tercih edilmektedir.

2.3. Elektronik Kimlik Kart (eID) Uygulamalarının Özellikleri

Elektronik kimlik kartı uygulamaları için bir standart bulunmamaktadır ve ülkeler kendi gereksinimlerine göre tanımlarlar. Ancak bazı ülkeler temassız kimlik kartları için ICAO'nun tanımlamış olduğu ICAO 9303 standartını kullanmaktadır. Ayrıca bazı ülkeler, özel gereksinimleri doğrultusunda bazı ek düzenlemeler yapmaktadırlar. Örneğin, Almanya biometrik verinin korunması için PACE güvenlik algoritmasını geliştirmiştir. Bu algortimayı uygulamalarında kullanmaktadır.

Özetle; kimlik uygulamaları aşağıdaki işlevleri gerçekleştiren bir çeşit elektronik kimlik doğrulama uygulaması olarak görülebilir:

- Karşılıklı asıllama işlevleri (Mutual authentication functions),
- Sayısal imza işlevleri,
- Biyometrik bilginin saklanması işlevi,
- Kişisel bilgilerin depolanması işlevi,
- E-devlet, elektronik oy kullanma vb. için gerekli işlevler.

2.4. Elektronik Kimlik Kartları (eID) için Uluslar Arası Standartlar

Ulusal kimlik kartlı uygulamalarında aşağıdaki standartlara uyulması önerilir:

- ISO/IEC 7816, ISO 7816 akıllı kart tabanlı elektronik kimlik kartları ile ilgili standart.
- ISO/ IEC 7810 eID kartların fiziksel standardı.
- ISO/ IEC 10373-3 eID kartların test yöntemleri standardı.
- ISO/ IEC 18013 part 1-3 sürücü belgesi standardı.
- ICAO Doc9303 standardı (bu standart daha çok seyahat belgesi standartı olarak yayımlanmasına karşın elektronik pasaport ve temassız elektronik kimlik kartları içinde kullanılabilen bir standarttır).

3. e-Pasaport Uygulaması

Günümüzde, ülke giriş/çıkışlarındaki denetim sağlamak amacıyla mühür ve ıslak imza içeren defter tipi klasik pasaportların kullanımı yaygın bir uygulamadır. Elektronik pasaport uygulamasında ise klasik pasaport defteri özelliklerine ek olarak elektronik bir yonga eklenmesi söz konusudur. Elektronik pasaport uygulaması, işlemlerin daha güvenli, daha hızlı ve kolayca gerçeklenmesini sağlayacaktır. Yonga içeren pasaportların ön yüzünde pasaportun elektronik olduğuna ilişkin olarak, Şekil–2'de gösterilen bir sembol bulunmaktadır.

Elektronik pasaport uygulamasında her ülke kendisine ait bir sertifikayı kart üzerindeki yongaya yükleyebilir ve diğer ülke gümrüklerinde elektronik pasaport okuyucu ile yonga içeren pasaport geçerlenebilir. Ayrıca yonga üzerindeki sertifika kullanılarak pasaport geçerlenebilir. Elektronik vize uygulaması hayata geçirilmişse, verilen vizeler doğrulanabilir.

Elektronik pasaport uygulamasına fiziksel şekle ve elektronik verilere ilişkin olarak "*ICAO - International Civil Aviation Organization*" kuruluşunun önerdiği standartlar kullanılmaktadır. Elektronik pasaportun yongası içerinde LDS (Logical Data Structure) olarak adlandırılan mantıksal veri yapısında tanımlanan veriler bulunmaktadır. LDS içerisinde EF.COM, EF.SOD ve EF.DGx olarak tanımlanan veri grupları bulunmaktadır. Herbir veri grubunda pasaport bilgileri ve pasaport verilen kişiye ait bilgiler gruplanarak tutulmaktadır. Örneğin DG1 olarak adlandırılan birinci grup veriler, kişiye ait ve makinaların okuyabileceği MRZ (Machine Readable Zone) bilgilerini içerir. DG2 veri grubunda ise kişinin yüzünün fotografı bulunur. Bu fotoğraf, defter üzerinde bulunan fotoğrafla aynıdır. Bu şekilde, fotoğrafın değiştirilip değiştirilmediği kolaylıkla tespit edilebileceği için görsel pasaportlara göre çok daha fazla güvenlik sağlanmaktadır. Elektronik pasaport yongası içerisinde bulunan dosyalardan EF.COM dosyası pasaport içerisindeki veri gruplarının yönetilmesini, EF.SOD dosyası ise pasif asıllama için gerekli güvenlik bilgileri olan SOD (*Security Object Data*) içerir.

3.1. Elektronik Pasaportlarda Güvenlik

Elektronik pasaportlarda güvenliğin sağlanması için çeşitli yöntemler kullanılmaktadır. Bu yöntemler Temel Erişim Denetimi (BAC), Genişletilmiş Erişim Denetimi (EAC), Pasif Asıllama (PA) yöntemi ve Etkin Asıllama (AA) yöntemidir.

3.1.1. Temel Erişim Denetimi (Basic Access Control - BAC)

Elektronik pasaportta bulunan yonga içerisindeki veriler yetkisiz kişiler tarafından pasaport görülmeden (yanından geçerken, '*skimming*') elektronik olarak okunabilir ya da yonga ile okuyucu arasındaki kriptosuz iletişim gizlice dinlenebilir (*eavesdropping*). "Yakından okuma" olarak adlandırılan yöntemler fiziksel olarak engellenebilse de gizlice dinleme (eavesdropping) engellenemez. Bu güvenlik tehditlerine karşı gizliliği korumak üzere Temel Erişim Denetimi yöntemini kullanılabilir. Temel erişim denetimi uygulanarak yanından geçerken okuma ve gizlice dinleme yöntemleri engellenebilir. BAC yönteminde, elektronik pasaport sahibinin pasaportunda bulunan yongadan kendisine ait bilgilerin güvenli olarak ve yetkili biri tarafından okunup okunmadığından haberi olur.

BAC yöntemi, pasaport okuyucu ile elektronik pasaport arasındaki iletişimin şifreli olarak gerçekleştirmesine dayanır. Bu yöntemde pasaport, sorgulayıcı sistemin yonganın MRZ bölgesindeki bilgilerden türetilmiş K_{ENC} ve K_{MAC} (Document Basic Access Keys) anahtarlarını bilip bilmediğini sorgular. Bu sorgulama, bir "*challange response*" protokolü yardımıyla, gerçekleştirilir ve sorgulayıcı sistemden beklenen verinin gelmemesi durumunda iletişim başlatılmaz. Sorgulayıcı sistemin başarılı şekilde doğrulanması durumunda, pasaport yongası, okuyucu ile arasında şifreli iletişimi başlatır. Bu şifreli iletişimde kripto anahtarı olarak, elde edilen K_{ENC} ve K_{MAC} anahtarları kullanılır.

3.1.2. Genişletilmiş Erişim Denetimi (Extended Access Control - EAC)

Genişletilmiş erişim denetimi, elektronik pasaportta yer alan yonga içerisindeki biyometrik verilere (parmak izi, iris motifi) yetkisiz erişimin engellenmesi için kullanılır. EAC uygulaması, BAC uygulamasına benzemektedir, ancak bu uygulamada Doküman Temel Erişim (*Document Basic Access*) Anahtarları (K_{ENC} ve K_{MAC}) yerine (*Document Extended Access*) Anahtarları kullanılır. Her bir yongada, kendine özel doküman erişim anahtarları ve sertifika bulunmaktadır. Bu anahtar MRZ'deki verilerden veya ulusal bir ana anahtardan elde edilmiş simetrik bir anahtar olabileceği gibi kart Doğrulama Sertifikası (*Card Verifiable Certificate - CVC*) kullanılarak üretilmiş asimetrik bir anahtar da olabilir. EAC uygulamasında, yonganın hesaplama ve şifreleme olanakları kullanılır. EAC yöntemi henüz pratik olarak hayata geçirilmemiştir. Çünkü ülkeler kendi açık anahtarlarının kullanımı ve dağıtımı için ortak bir yöntem oluşturamamışlardır.

3.1.3. Pasif Asıllama (Passive Authentication - PA)

Pasif asıllama yönteminde Güvenli Nesne Verisi'nin (*Security Object Data - SOD*) ve LDS'nin içeriklerinin değişip değişmediği kontrol edilir. Ancak bu yöntem ile pasaportta bulunan yonganın tamamen kopyalanıp kopyalanmadığı tespit edilemez.

Pasif asıllamada şu işlem adımları gerçekleştirilir:

- SOD bilgisi elektronik pasaport yongasından okunur.
- SOD'un içinden "*Document Signer - DS*" okunur (ya da o dokümana ait DS değeri sistem tarafından bilinmektedir).
- SOD'un sayısal imzası, KPu_{DS} ile doğrulanır. Böylece SOD'un, C_{DS}'de belirtilen ülke tarafından verilmiş ve değişmemiş olduğundan emin olunur. (C_{DS} değeri, SOD doğrulanması için kullanılmadan önce KPu_{CSCA} ile doğrulanır)
- Sorgulayıcı sistem LDS içerisinden ilgili veri gruplarını okur.
- Veri gruplarının özeti alınır ve SOD'daki özetle karşılaştırılır. Hesaplanan ve SOD'dan okunan özetlerin aynı olması durumunda verilerin asıl ve değişmemiş olduğu doğrulanmış olur.

3.1.4. Etkin Asıllama (Active Authentication - AA)

Etkin asıllama yöntemi, elektronik pasaport içerisinde bulunan yonganın tamamının kopyalanmasının engellenmesi amacıyla geliştirilmiş bir yöntemdir. Bu yöntemde elektronik yongada, yongaya özel etkin asıllama asimetrik anahtar çifti (KPr_{AA} ve KPu_{AA}) tutulur. KPu_{AA}'ya ait bilgilerin özeti de SOD'da tutulur ve pasaport sağlayıcının sayısal imzasıyla asıllanır. KPr_{AA} ise yonganın güvenli belleğinde tutulur.

Görünen (optik) MRZ'nin SOD'deki özeti alınmış MRZ ile asıllanması, yonga içerisindeki KPr_{AA} ve KPu_{AA} anahtarları kullanılarak yapılan "*challange-response*" ile birleştirilir. Böylece sorgulayıcı sistem, SOD'un gerçek bir elektronik pasaporta ait gerçek bir yongadan okunduğunu doğrulamış olur. Bu asıllama yönteminde yonganın hesaplama yetenekleri kullanılır.

Etkin asıllama şu işlem adımları ile gerçekleştirilir:

- Gözle veya optik olarak okunan MRZ verisi, Veri Grubu 1'deki (DG1) veriler ile karşılaştırılır. DG1 verilerinin asıllığı ve bütünlüğü pasif asıllama ile kanıtlanmış durumda olduğundan MRZ'nin de asıllığı ve bütünlüğü kanıtlanmış olur.
- Pasif asıllama ile DG15'in de asıllığı ve bütünlüğü kanıtlanmış olduğundan, KPu_{AA}'nın da asıllığı ve bütünlüğü kanıtlanmış olur.

SOD'un kopya olmadığından emin olmak için şu şekilde bir protokol uygulanır:

Şekil 2. *Türkiye Cumhuriyeti elektronik pasaportu.*

Sorgulayıcı sistem, rastgele bir sayı üreterek "*Internal Authenticate*" komutu verisi olarak pasaport yongasına yollar. Bu rastgele sayı KPr_{AA} anahtarı ile imzalanır ve sonuç sorgulayıcı sisteme geri yollanır. Sorgulayıcı sistem KPu_{AA} anahtarı ile gelen imzayı doğrular ve elektronik pasaport yongası bu şekilde asıllanmış olur.

4. Ödeme Sistemleri (EMV) Uygulamaları

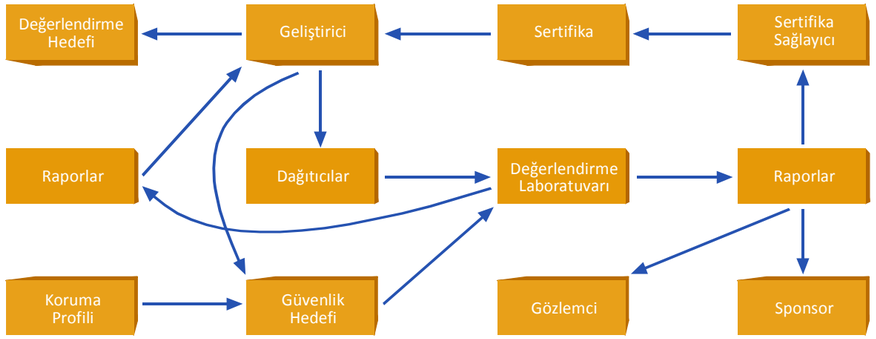
Akıllı kart teknolojisi, ilk kez ödeme sistemi uygulamalarında kullanılmıştır. Bu uygulamalar daha çok EMV (**E**uropay, **M**asterCard, **V**isa) uygulaması olarak adlandırılır ve akıllı kartların kredi kartı üzerinde kullanıma sunulduğu uygulamalardır. Bu uygulamalarda uluslarası bankacılık için kabul görmüş olan EMV standardı kullanılmaktadır. Ancak uygulamanın sertifikalandırılması işlemi Master Card, Visa gibi ödeme uygulamasını geliştiren kuruluş tarafından gerçekleştirilmektedir. Bu uygulamanın bulunduğu akıllı kart, ilgili kuruluşun logosu ile tanımlanır.

Ödeme sistemi uygulamaları ticari uygulamalardır ve bu uygulamalarda kamu kurumları için tasarlanmış akıllı kartların kullanılması, güvenlik açısından uygun değildir. Ticari uygulamalarda, kullanılan uygulamanın geçerliliği ve riskleri ticari kuruluşların sorumluluğundadır. Bu durumun tek istisnası, 5. konu başlığı altında anlatılan şehir kartı uygulaması olabilir. Çünkü şehir kartında asıl amaç hizmet sunmaktır ve sunulan bu hizmete bağlı olarak da ticari kazanç elde etmektir. Böylece elektronik pasaportta bulunan özel anahtar sadece o pasaporta özgü olduğundan yonga kopyalanmamış demektir.

5. Şehir Kartları Uygulaması

Şehir kartları olarak adlandırılan kartlar, üzerinde ilgili belediyenin belirleyeceği basit bir kimlik uygulaması ve EMV ödeme uygulaması olan kartlardır. Bu kartlar ile, belediye hizmetlerine ait ödemeler kolaylıkla yapılabilir. Ayrıca belediyeler, bulunduğu şehire ait şehir kartına sahip vatandaşlarına verdiği hizmetlerden ücret almayabilir veya alacağı ücrete indirimli tarife uygulayabilir.

Şehir kartları uygulamasındaki asıl amaç, belediye sınırları içerisinde yerleşik kişilerin belediyenin sağladığı ücretli hizmetlerden nakit para taşımadan yararlanabilmesidir. Belediyenin bu hizmeti, kartın üzerinde yüklü olan EMV uygulaması ile gerçekleştirilir. Böylece ulaşım, halk ekmek, doğal gaz, çevre temizlik vergisi v.b. hizmetlere ilişkin ödemelerin kolayca yapılabilmesi sağlanır. Ayrıca şehir kartına sahip olan kişi, parasal işlerini anlaşmalı bankaların ATM makinalarında da gerçekleştirebilir.



Şekil 3. *Değerlendirme rolleri.*

6. Ortak Kriterler (Common Criteria, CC) ve Akıllı Kart Güvenlik Sertifikasının Alınma Süreci

Akıllı kartlarda güvenlik önemli bir ihtiyaçtır. Akıllı kartların güvenli hizmet sağlayabilmesi için hem akıllı kart yongasının hem de yonga üzerinde bulunan işletim sistemi ve uygulamaların uyması gereken kurallar bulunmaktadır. Bu kurallar ilk olarak "TCSEC standard - Trusted Computing Security Evaluation Criteria" adıyla 1985 yılında ABD'de yayımlanmıştır. Bu standartta güvenlik, minimum koruma (D) seviyesi ile doğrulanmış tasarım (A1) seviyesi arasında derecelendirilmektedir. Avrupada güvenlik standartları ile ilgili çalışmalar 1990'larda başlamıştır. Bu yıllarda İngiltere, Almanya ve Fransa'nın öncülüğünde "ITSEC – Information Technology Security Evaluation Criteria" adı ile yeni bir güvenlik standartı oluşturulmuştur.

Ortak Kriterlerin ilk resmi sürümü 1996 yılında Avrupa, ABD ve Kanada tarafından onaylanmış ve 1998 yılında ikinci sürümü çıkarılmıştır. Ortak kriterler 1999 yılında ISO-15408 standartına dahil olmuştur. Günümüzde geçerli olan sürümler 2.3 sürümü ve 2008 yılında çıkarılan 3.1 sürümüdür. Ortak Kriterler ile ilgili dokümanlar, internette bulunan ortak kriter portalından ücretsiz olarak indirilebilmektedir.

Günümüzde Türkiye'nin de dahil olduğu birçok ülke, EAL 4 seviyesi ile EAL 7 seviyesi arasındaki güvenlik seviyelerini kabul edilebilir seviye olarak onaylamaktadırlar.

Ortak kriterlerde üç çeşit değerlendirme bulunmaktadır;

- Koruma Profili (Protection Profile-PP),
- Güvenlik Hedefi (Security Target-ST),
- Ürün veya Sistem değerlendirmesi.

Koruma Profili, belirli güvenlik hedeflerinin tanımlandığı ve yetkili otorite tarafından onaylanmış "güvenlik gereği paketleri" olarak yorumlanabilir. Akıllı kartların bir koruma profiline göre değerlendirilmesi zorunlu değildir. Buna karşın Güvenlik Hedefi değerlendirmesi zorunludur.

Ortak Kriterler güvenlik dereceleri, aşağıda belirtilen 7 seviyededir (*Common Criteria, CC*);

- EAL1 – İşlevsel olarak test edilmiş (functionally tested),
- EAL2 – Yapısal olarak test edilmiş (structurally tested),
- EAL3 – Yöntemsel olarak denetlenmiş, test edilmiş (methodically tested, checked),
- EAL4 – Yöntemsel olarak tasarlanmış, test edilmiş ve gözden geçirilmiş (methodically designed, tested and reviewed),
- EAL5 – Yarı resmi olarak tasarlanmış, test edilmiş (semiformally designed, tested),
- EAL6 – Yarı resmi olarak doğrulanmış, tasarlanmış ve test edilmiş (semiformally verified, designed and tested),
- EAL7 – Resmi olarak doğrulanmış ve test edilmiş tasarım (formally verified design and tested).

EAL1 en düşük güvenlik seviyesini, EAL7 ise en yüksek güvenlik seviyesini göstermektedir.

6.1. Akıllı Kartların Ortak Kriterler Değerlendirme Süreci

Akıllı kart ve benzeri şifreleme cihazlarının güvenlik seviyesi üzerinde fikir birliği sağlamak için birçok çalışma yapılmış ve CC Değerlendirmeleri kapsamında, uyulması gereken bazı kurallar tanımlanmıştır. Bu çalışmalar sonucunda CC kapsamında 7 güvenlik seviyesi oluşturulmuştur. CC testleri sonrasında, test edilen donanım veya yazılımlara sağladığı güvenlik seviyesine göre CC sertifikası verilerek ürünün ne kadar güvenli olduğu ifade edilmektedir.

Akıllı kart ürünlerinin CC güvenlik seviyesi, ortak kriterler test merkezlerinde belirlenmektedir. Bu merkezlerde akıllı

kart ürününe uygulanan testlerin sonucuna göre güvenlik seviyesini belirten bir CC sertifikası verilmektedir. CC sertifikasına sahip bir ürün, geliştirme süreci gereklerini ve güvenlik kıstaslarını sağlamış bir ürün olarak değerlendirilir.

Türkiye'de CC testleri, Türk Standartları Enstitüsü'nün (TSE) onay verdiği test laboratuvarlarında gerçekleştirmektedir. TÜBİTAK-BİLGEM bünyesinde, Ortak Kriterler Test Merkezi (OKTEM) olarak adlandırılan bir test merkezi bulunmaktadır. CC sertifikalandırma sürecinde, sürecin sağlıklı yürüyebilmesi amacıyla değişik birimler oluşturulmuştur. Bu birimler ve birimlerin ilişkileri Şekil – 3'deki şemada belirtilmiştir. Bu şemadaki birimlerin Türkiye'deki karşılıkları şu şekilde belirtilebilir:,

Sertifika sağlayıcı = TSE,

Değerlendirme laboratuvarı = OKTEM,

Geliştirici = TÜBİTAK-BİLGEM,

Değerlendirme hedefi = AKiS ürünü,

Sponsor ve Gözlemci = Ürünü kullanan veya kullanacak olan kişiler.

Elektronik Kimlik Dağıtım Sistemi (EKDS) projesi için "Sponsor" ve "Gözlemci" rollerinde Nüfüs Vatandaşlık İşleri müdürlüğü (NVI) bulunmaktadır.

Günümüzde güvenlik gereksiniminden dolayı akıllı kartlar için hem platform olarak adlandırılan donanım, hem de işletim sistemi ve üzerinde çalışan yazılımlar için güvenlik testleri uygulanarak CC sertifikası alınması bir zorunluluktur. Çeşitli akıllı kart uygulamaları için, sağlanması gereken en düşük güvenlik seviyeleri belirlenmiştir. Örneğin akıllı kart donanım platformu olarak, CC EAL 5+ onayı almış yüksek güvenliğe sahip yongaların (örneğin SLE66CLX800PE veya P5CD081 gibi tümdevrelerin) kullanılması ve üzerinde en az CC EAL 4+ güvenlik seviyesine sahip bir işletim sisteminin bulunması zorunludur. Türkiye Cumhuriyeti Ulusal Elektronik Kimlik Kartları için de bu seviyeler benimsenmiştir.

Önceki konu başlıklarında açıklanan uygulamalar için gerekli görülen güvenlik seviyeleri farklı olabilir. Örneğin ödeme sistemlerinde kullanılan donanımlar için CC EAL 5+ seviyesinde güvenlik gerekirken uygulama ve işletim sistemleri için EMV onayı yeterli görülmektedir. Çünkü ödeme sistemi ile ilgili riskler EMV üyesi kuruluşların sorumluluğundadır.

Derginin ilk sayısından bu yana "Akıllı Kartlar ve Uygulamaları" yazı dizisiyle karşınızda olduk. Bu sayı ile diziyi noktalıyoruz. İlginiz için teşekkür eder, ileriki sayılarda başka yazılarda görüşmek dileğiyle esenlikler dilerim.

KAYNAKÇA

[1] W. Rankl, W. Effing, *Smart Card Handbook*, Giesecke & Devrient Gmbh, Munich, Germany, 2003

[2] K. E. Mayes, K. Markantonakis, *Smart Cards, Tokens, and Applications*, University of London, UK, 2008

[3] S. Mangard, E. Oswald, T. Popp, *Power Analysis Attacks*, Graz University of Technology Graz, Austria, 2007

ELEKTRONİK SEÇİM

İLERİ DÜZEY KRİPTOGRAFİNİN YAPI TAŞLARI VE UYGULAMALARI

Fatih BİRİNCİ

Mehmet Sabır KİRAZ

Dergimizin önceki sayılarında, Kriptografi 1.0 olarak da adlandırılan kriptografinin temel yapı taşlarından bazılarını anlatmıştık. Kriptografi 1.0, simetrik-asimetrik şifreleme, imzalama ve bütünlük sağlama gibi günümüzde yaygın olarak kullanılan kriptografinin temel bileşenlerinden oluşmaktadır. Bunlar; gizlilik, kimlik doğrulama (asıllama) ve inkâr edememe gibi temel hizmetleri sağlamak için yeterlidir. Fakat, Kriptografi 1.0 bileşenleri, yeni yeni önem kazanmaya başlayan kişiye özel kalma ve anonimlik gibi yeni hizmetleri sağlamada yetersiz kalmaktadır. Bu hizmetler; elektronik seçim, elektronik para, şifreli metin arama ve elektronik açık artırma gibi pek çok yeni uygulamada gereklidir. Bu uygulamalarda yeni hizmetlerin sağlanması amacıyla Kriptografi 2.0 diye adlandırılan ileri düzey kriptografik yapıtaşları kullanılmaktadır. Yazımızda, bu yeni yapıtaşlarını ve uygulama alanlarını anlatmaya çalışacağız.

1. KRİPTOGRAFİ 2.0

Her telefon görüşmesi yaptığımızda, e-postalarımızı okuduğumuzda, kredi kartı kullandığımızda, arama motorlarında bir şeyler aradığımızda veya doktora gittiğimizde bize ait özel bilgiler bir yerlerdeki veri tabanlarına kaydedilir. Bu veritabanlarında saklanan bilgiler analiz edilerek alışveriş alışkanlıklarımız, gittiğimiz yerler, iletişim kurduğumuz kişiler ve sağlık sorunlarımız gibi mahrem bilgilere ulaşılabilir. Bazen bu bilgiler suçluların yakalanması gibi vakalarda yararlı olabilir. Fakat yanlış kişilerin eline geçmesi durumunda istenmeyen sonuçlara yol açabilir. Örneğin, ciddi bir hastalığın ilaçlarını aldığımızı öğrenen bir sigorta şirketi hakkımızdaki başka bilgileri de kullanarak bu hastalığa sahip olduğumuza kanaat getirip bizi sigortalamak istemeyebilir. Bankalar, kredi vermeye karar vermek için önceki borçlarımızı ödeyip ödemediğimizin yanında rızamız dışında başka özel bilgilerimizden de faydalanıyor olabilirler.

Bazı bilgilerin sadece bize özel kalması olarak tarif edilen kişiye özelliğin sınırlarını çizmek günümüzde hiç de kolay değildir. Özel bilgilerimizi bir taraftan saklamak isterken, bunları paylaşmak durumunda kalacağımız uygulama sayısı da giderek artmaktadır. Örneğin, 'Google latitude' servisini kullanarak nerede olduğumuzu arkadaşlarımızla paylaşmak ve yakında bulunan arkadaşlarımızı kahve içmeye davet etmek isteyebiliriz. Acil bir durumda bulunduğumuz yere ambulans gelmesi ile hayatımız kurtulabilir. Şu anda bulunduğumuz yer bilgisini paylaşmak isteyebilmemize karşın bu bilgilerin kaydının tutulması ile geçmişte bulunduğumuz yerlerin bilinmesini genellikle istemeyiz. Bu servisleri kullandığımız takdirde geçmiş bilgilerimizin kaydının tutulmadığından emin olabilir miyiz?

Bazı kişilerin paylaşmakta sakınca görmediği bilgileri diğer kişiler sır olarak tutmak isteyebilir. Buna, kime oy verdiğimiz bilgisini örnek olarak verebiliriz. Kişiye özel verilerin kayıt ve takibinde kişinin rızasının olması çok önemlidir. Örneğin, Google latitude servisinde, sistemden çıkabilir, yer bilgisini paylaşmak istemeyebilir veya başka bir yerde gibi görünebilirsiniz.

Teknolojinin gelişmesi ile beraber bazı bilgilerin sadece bize özel kalmasını sağlamak gittikçe zorlaşmaktadır. Kriptografi 2.0 temel anlamda kişiye özel bilgilerin gizli kalmasını sağlayarak belirli işlemleri yapabilmeyi hedeflemektedir. Bir sonraki bölümde bunu sağlamak için kullanılabilecek yapı taşlarını incelemeye çalışacağız.

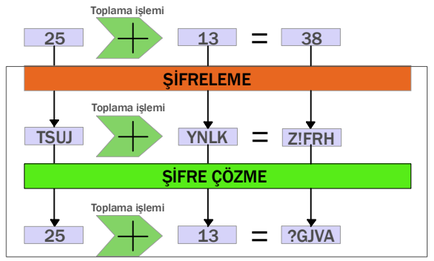
2. İLERİ DÜZEY KRİPTOGRAFİK YAPI TAŞLARI

2.1. Homomorfik Şifreleme

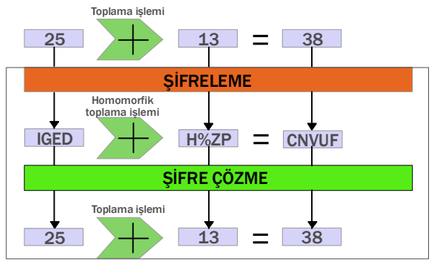
Önceki sayılarımızda bahsedildiği üzere, şifreleme algoritmalarını genel anlamda simetrik ve asimetrik şifreleme algoritmaları olarak ikiye ayırabiliriz. Kısaca özetlemek gerekirse, simetrik şifreleme algoritmalarında şifreleme ve şifre çözme anahtarları aynıdır. Asimetrik şifreleme algoritmalarında ise şifreleme (açık anahtar) ve şifre çözme anahtarları (gizli veya özel anahtar) birbirinden farklıdır. Açık anahtar herkes tarafından bilinmekte ve şifreleme için kullanılmaktadır, özel anahtar ise sadece şifreyi çözecek kişi tarafından bilinmekte ve şifre çözme için kullanılmaktadır. Dolayısıyla herkes şifreleme yapabilmekte fakat sadece özel anahtar sahibi şifresini çözebilmektedir. Açık anahtarın bilinmesine rağmen özel anahtarın bulunması, hesaplama zorluğundan dolayı pratikte mümkün değildir (Bknz. Kavramlar Sözlüğü).

Homomorfik şifreleme, asimetrik şifrelemenin özel bir durumudur ve sadece şifreli metinler kullanılarak açık metinler ile ilgili işlemler yapılmasını sağlar. *E* homomorfik şifreleme algoritması ile *E(x)* ve *E(y)* gibi iki şifreli metnin şifrelerini çözmeden *x* ve *y* açık metinlerin toplamlarının ya da çarpımlarının şifreli halini hesaplayabiliriz. Örneğin, *E(x).E(y)=E(xy)* olur, yani *E(x)* ve *E(y)* şifreli metinleri çözmeden *xy* metnin şifreli hali hesaplanır. Homomorfik asimetrik şifreleme algoritmaları e-seçim, e-ticaret ve dağıtık kripto gibi bir çok uygulamada kullanım alanı bulmaktadır.

Açık literatürde yayınlanan ilk asimetrik şifreleme algoritması RSA algoritmasıdır [1,2]. Temel RSA ile şifreleme işlemi, mesaj m ($\mathbb{Z}_n$'deki sayısal eşleniği) ve açık anahtar e'nin modüler üs işlemine tabi tutulması sonucu hesaplanır. Açık anahtar e ile modüler n'den (büyük asal bir sayı) oluşmakta ve herkes tarafından bilinmektedir. Dolayısıyla şifreleme işlemini herkes yapabilmektedir. Şifrenin çözülmesinde ise sadece alıcı tarafından bilinen gizli anahtar d kullanılmaktadır.



Şekil 1. *Homomorfik olmayan şifreleme.*



Şekil 2. *Homomorfik şifreleme.*

$n=pq$ ve $\emptyset=(p-1)(q-1)$
e: $1<e<\emptyset$ ve $OBEB(e,\emptyset)=1$ olacak şekilde rasgele[1]
d: $ed=1 \bmod \emptyset$ ve $1<d<\emptyset$
(e,n): açık anahtar
d: gizli anahtar
$E(m)=m^e \bmod n$ (Temel RSA ile şifreleme)
$D(m)=(E(m))^d \bmod n=m \bmod n$ (Şifre çözme)

Temel RSA kullanılarak yapılan şifreleme işlemi güvenli değildir. Çünkü RSA algoritmasının homomorfik özelliğinden dolayı şifreleme işleminden sonra mesaj herkes tarafından değiştirilebilmektedir.

$$E(m)\cdot t^e=(m\cdot t)^e \bmod n$$

(Değiştirilmiş şifreli mesaj)

Bu özellik klasik kriptografik sistemlerinde istenmeyen bir özelliktir. Nitekim temel RSA'daki bu güvenlik açığı mesaj dolgulama teknikleri ile giderilmiştir [2]. Bu yöntemlerin kullanımı ile bir nevi mesaj bütünlüğü sağlanmaya çalışılmaktadır. Bu yöntemlerde mesaj, dolgulama teknikleri kullanılarak kodlanır ve temel RSA ile şifrelenerek alıcısına gönderilir. Alıcı, mesajın şifresini çözdükten sonra mesajın beklenen formatta olup olmadığını kontrol eder. Eğer beklenen formatta ise mesajı kabul eder.

Buna karşın temel RSA'nın bu özelliğinin bazı uygulamalarda faydalı olabileceği de fark edilmiştir. Homomorfik şifreleme algoritmalarının en etkileyici yanı mesajın şifresini çözmeden mesaj üzerinde işlem yapılmasına olanak vermeleridir. RSA dışında, homomorfik özelliği için daha çok tercih edilen şifreleme sistemleri mevcuttur (ElGamal [1], Paillier [3] vb.).

Şifreleme algoritmaları iki tip homomorfik özellik göstermektedir.

1. *Çarpmaya göre homomorfik özellik*: Bu tip homomorfik özellik gösteren asimetrik şifreleme algoritmaları ile şifrelenmiş mesajlar birbirleri ile çarpılır ve sonuç deşifre edilirse açık mesajların çarpımı bulunacaktır. RSA, ElGamal ve Paillier asimetrik algoritmaları çarpmaya göre homomorfik özellik göstermektedir.

2. *Toplamaya göre homomorfik özellik*: Bu tip homomorfik özellik gösteren asimetrik şifreleme algoritmaları ile şifrelenmiş mesajlar birbirleri ile çarpılır ve sonuç deşifre edilirse açık mesajların toplamı bulunacaktır. ElGamal asimetrik şifreleme algoritması biraz değiştirilerek toplamaya göre homomorfik özellik kazandırılabilmektedir.

RSA ile ElGamal şifreleme algoritmalarının arasındaki farkları inceleyebiliriz. RSA ve ElGamal sistemeleri çarpmaya göre homomorfiktir. Fakat RSA'daki şifreli metinler belirleyicidir (deterministic). Yani aynı mesajın şifrelenmesi durumunda her zaman aynı şifreli metine ulaşılmaktadır. Bu yüzden RSA'nın homomorfik özelliği istenilen güvenlik seviyesine (seçilmiş açık metine karşı güvenlik) ulaşamamaktadır. Dolgulama teknikleri ile istenilen güvenliğe ulaşıldığı anda ise RSA, homomorfik özelliğini kaybetmektedir. Bu durumda şifreli metinler çarpıldığında, metinlerin çarpımının şifreli hali ortaya çıkmaz. ElGamal ise istenilen güvenlik seviyesine sahiptir. Bununla birlikte ElGamal sistemi ufak bir uyarlanmayla toplamaya göre de homomorfik hale dönüştürülebilmektedir. Bu sistemin rasgelelik özelliğine sahip olması ve istenilen diğer güvenlik kriterlerini sağlamasından dolayı araştırmacılar ElGamal sistemi üzerine yoğunlaşmışlardır.

2009 ortalarına kadar geliştirilen homomorfik şifreleme algoritmaları sadece çarpmaya ya da toplamaya göre homomorfik özellikler taşımaktaydı. 2009 yılında ise Craig Gentry IBM'deki ve MIT'deki doktora çalışmaları sırasında, hem çarpma hem de toplamaya göre homomorfik (tam homomorfik) özelliği bir arada sunan bir asimetrik şifreleme algoritması geliştirmiştir [4]. 1980 yıllarında ortaya atılan bu problemin çözümü, kriptografide son yıllarda yaşanan en önemli sıçrama olarak değerlendirilmektedir. Bu yolla kişilerin bilgileri saklı tutularak (iç tehdit olsa bile) güvenli bir şekilde hesaplama yapma yöntemleri geliştirilebilecektir.

Tam homomorfik bir asimetrik şifreleme algoritması ile örneğin, sorgunuzu şifreleyerek arama motoruna gönderebileceksiniz. Arama motoru şifrenizi çözemeden istediğiniz işlemi yapacak ve sonucu size geri bildirecek, siz ise gönderilen cevabın şifresini çözerek sonucu bulabileceksiniz. Böylelikle arama motoruna ne aradığınızı söylemek zorunda kalmayacaksınız. Bu konudaki çalışmalar RSA algoritması kadar eskidir [5].

2.1.1. Homomorfik ElGamal Kripto Sistemi

G: n mertebesinde çarpma işlemine göre devirli bir grup (n elemanlı)
g: grubun üreteci
$h=g^a, a$: rasgele
a: gizli anahtar, $1 \le a \le n-2$
(n,g,h): açık anahtar

G grubu olarak büyük ve rasgele n asal sayısı için $\mathbb{Z}_n^*$ (Modüler n tamsayılardan oluşan çarpma işlemine göre devirli grup) kullanılabilmektedir. Bu durumda açık anahtar (n,g,h) olmaktadır. Gizli anahtarın ise $1 \le a \le n-2$ olması gerekmektedir.

Şifreleme

Şifreleme, geleneksel asimetrik şifrelemede olduğu gibi herkes tarafından yapılabilmektedir. Şöyle ki: Bora'nın m mesajını Ayşe'ye göndermek için şifrelemesi için aşağıdaki işlemleri yapması gerekmektedir.

1. Bora, Ayşe'nin açık anahtarını edinir. Ayşe'nin açık anahtarı genellikle herkese açık bir dizinde yer almaktadır.

[1] OBEB:Ortak Bölenlerin En Büyüğü.

Şifreleme

2. 0 ile $n-1$ sayısı arasında yer alacak şekilde mesajın sayısal değerini hesaplar. Gerekirse mesajı parçalara böler. Mesajın sayısal değerini $\overline{m}$ olarak adlandıralım.

3. $1 \leq r \leq n-2$ olacak şekilde rasgele bir sayı seçer.

4. $c_1=g^r$ ve kısa ömürlü anahtar olarak adlandırılan $s=h^r$ değerlerini hesaplar.

5. $c_2= \overline{m} \cdot s$ değerini hesaplar.

6. Ayşe'ye $E(m)=(c_1,c_2)=(g^r, \overline{m} \cdot h^r)$ şifreli mesajını gönderir.

Şifre Çözme

Ayşe kendisine gelen mesajın şifresini çözmek için aşağıdaki işlemleri yapmalıdır. Aşağıdaki işlemler modüler n'de yapılmaktadır.

1. Gizli anahtarını kullanarak kısa ömürlü anahtarı hesaplar: $s=c_1{}^a=g^{ar}$

2. $c_2 \cdot s^{-1}= \overline{m} \cdot h^r \cdot (g^{ar})^{-1}= \overline{m} \cdot g^{ar} \cdot (g^{ar})^{-1}= \overline{m}$

3. Ayşe, $\overline{m}$ sayısından m mesajını elde eder.

ElGamal şifreleme sisteminin güvenliği *Ayrık Logaritma Problemi*'ne dayalıdır. Bu problemde, g^a'dan a'nın bulunması modüler tabanda zordur (Bknz. Kavramlar Sözlüğü). ElGamal kripto sisteminde şifreli mesajların çarpımı, aşağıdaki formülden de anlaşılacağı gibi mesajların çarpımının şifrelenmiş hali ile sonuçlanmaktadır.

$$E(a) \cdot E(b)=(g^r, a \cdot h^r \ ) \cdot (g^s, b \cdot h^s)=(g^{r+s}, (a \cdot b) \cdot h^{r+s})=E(a \cdot b)$$

ElGamal algoritması küçük bir değişiklikle toplamaya göre homomorfik hale de getirilebilmektedir. E-seçim uygulamalarında genellikle toplamaya göre homomorfik şifreleme algoritmaları kullanılmaktadır. Örneğin bir referandumda birinci seçmenin oyunun $(g^{r_1}, g^{oy_1} \cdot h^{r_1})$, ikinci seçmenin oyunun ise $(g^{r_2}, g^{oy_2} \cdot h^{r_2})$ olduğunu düşünelim. Seçmenlerin oylarını açmadan oylarını toplamak istiyoruz. Bunun için kullanılmış oyları çarpmak yeterlidir. Çarpım sonucu $(g^{r_1+r_2}, g^{oy_1+oy_2} \cdot h^{r_1+r_2})$ olmaktadır.

ElGamal algoritmasını toplamaya göre homomorfik özellik gösterecek şekilde değiştirdik ve oyların şifreli hallerini topladık. Oyların toplamının şifreli halinden oyların toplamını nasıl hesaplayacağız ($g^{oyların\ toplamı}$) değerinden oyların toplamının hesaplanması)? Oyların toplamını hesaplamak için ayrık logaritma problemini çözemeyiz. Yukarıda bu problemin çözümünün zor olduğunu söylemiştik. Neyse ki oyların toplamını hesaplamanın bir yolu var; bunun için oyların toplamının belli bir değeri aşmayacağı gerçeği kullanılmaktadır. Bir sonraki bölümde anlatılacak olan Paillier Kripto Sisteminde mesaj kısıtlanması bulunmamaktadır.

Yukarıdaki örnekte dikkat edilmesi gereken bir başka nokta da, oyların şifresi çözülmeden toplandıkları için seçmenlerin birden fazla oy vermediğinin nasıl anlaşılacağıdır. Örneğin, bir referandum yapıldığını ve seçmenlerden evet/hayır oylarından birini kullanmaları istendiğini düşünelim. Seçmenlerin;

• Evet için $(g^r g^1 \cdot h^r)$,

• Hayır için $(g^r g^{-1} \cdot h^r)$ oylarından bir tanesini kullanmaları beklenmektedir.

Seçimin adil olması için seçmenlerin dürüst davrandığının, iki hayır $(g^r g^{-2} \cdot h^r)$ veya iki evet $(g^r g^2 \cdot h^r)$ şeklinde oy kullanmadıklarının anlaşılması gerekmektedir. Seçmenlerin dürüst davrandıklarını anlamak için ileride anlatılacak olan sıfır bilgi sızmalı kanıt protokolleri kullanılabilmektedir. Bu yolla kişilerin hiçbir bilgi sızdırılmadan sadece belirli işlemleri yapabilme kontrolü sağlanmış olur.

2.1.2. Homomorfik Paillier Kripto Sistemi

Paillier Kripto Sistemi 1999 yılında Pascal Paillier tarafından tasarlanmış olup yaygın olarak kullanılan rasgelelik özelliği olan bir asimetrik kripto sistemidir. Bu algoritmanın güvenliği n. artık sınıflarının hesaplanmasının zorluğuna dayanmaktadır.

Anahtar üretimi şu şekildedir:

1. k güvenlik parametresi olsun. k–bit uzunluğunda iki tane rasgele asal sayı p,q seçelim $OBEB(pq, (p-1), (q-1)) = 1$ olsun.

2. $N = pq$ ve $\lambda = OKEK(p-1, q-1)$ olsun[2].

3. $g \in \mathbb{Z}^*_{N^2}$ olsun.

4. N'nin g'nin derecesini bölebileceğini şu yöntemle teyit edelim:

$\mu=(L(g^\lambda \bmod N^2))^{-1} \bmod n$ öyle ki L fonksiyonu $L(u) = \frac{u-1}{N}$

Şifreleme

(λ, μ): gizli anahtar

(N,g): açık anahtar

1. $m<N$ şifrelenecek açık mesaj olsun.

2. Rasgele bir $r \in \mathbb{Z}^*_{N^2}$ seçilir.

3. Şifreli metin $c = g^m \, r^N \bmod N^2$ olarak hesaplanır.

Şifre Çözme

1. Şifreli metin $c \in \mathbb{Z}^*_{N^2}$,

2. Açık metin $m = L(c^{\lambda} \bmod N^2) \ \mu \bmod N$ şeklinde hesaplanır.

Paillier Kripto Sisteminin toplamaya göre homomorfik ElGamal kripto sisteminden farkı, mesaj uzunluğunda hiçbir kısıtlaması olmamasıdır.

[2] OKEK:Ortak Katların En Küçüğü.

2.2. Kör İmza

Kâğıt tabanlı dünyada yapmak istemediğimiz veya kullanım alanı bulamayan bazı uygulamalar elektronik dünyada işimize yarayabilmektedir. Örneğin, ne yazdığı okunamayan veya görülemeyen bir dokümanın altına imza atıldığını düşünün. "Sahtekârlık haberlerinde duyduğumuz böyle bir şeyi neden yapmak isteyelim ki?" veya "Ne işimize yarayacak?" gibi sorular aklınıza gelebilir. Kör imza olarak adlandırılan bu imza türü elektronik dünyada bazı şeylerin bize özel kalmasına yardımcı olur [6,7].

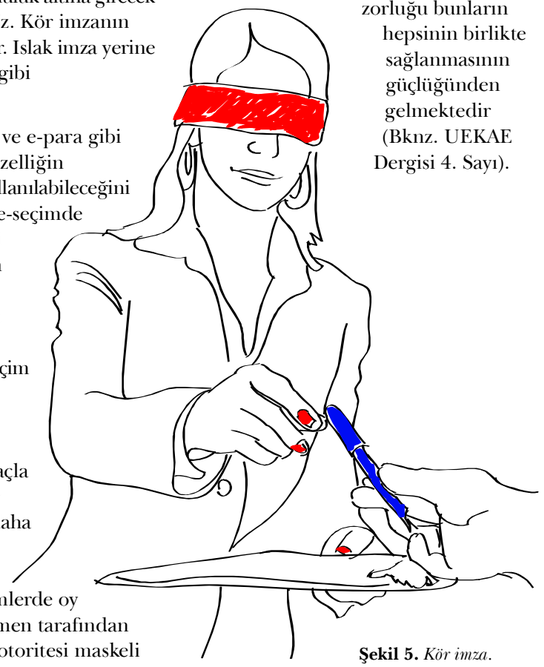
Şekil 3. *Kör imza.*

Kriptografi'ye, David Chaum tarafından 1982 yılında kazandırılan kör imza [7], imza atılacak metnin sahibi ile imzanın sahibinin farklı olduğu e-seçim ve e-para gibi protokollerde kişiye özelliğin sağlanması amacı ile kullanılmaktadır. Kâğıt tabanlı sistemlerle kör imza arasında benzetme yapabiliriz. İmzalanacak metin, üstüne karbon kâğıdı konularak bir zarfın içine konulur. Açılmaması için mühürlendikten sonra zarf, bir otoriteye gönderilir. Otorite zarfı imzalar fakat mühürlü olduğundan içine bakamaz. Mühürlü zarf açıldıktan sonra otorite tarafından imzalı metin elde edilecektir.

David Chaum'un tarif ettiği kör imzayı şu şekilde kısaca açıklayabiliriz. Bora'ya kör imza attırmak isteyen Ayşe, öncelikle imzalanacak metni, Bora'nın çözemeyeceği veya okuyamayacağı hale getirir. Bu işleme maskeleme adını veriyoruz. Bora, çözemediği veya okuyamadığı maskeli metne imzasını atar. Ayşe, maskeleme işlemin tersini Bora'nın gönderdiği dosyaya uygulayarak maskeyi kaldırır ve imzalı metni elde eder. Artık bu metnin imzası standart sayısal imzadan farksızdır ve Ayşe dilerse metnin üzerinde Bora'nın imzası olduğunu kanıtlayabilir.

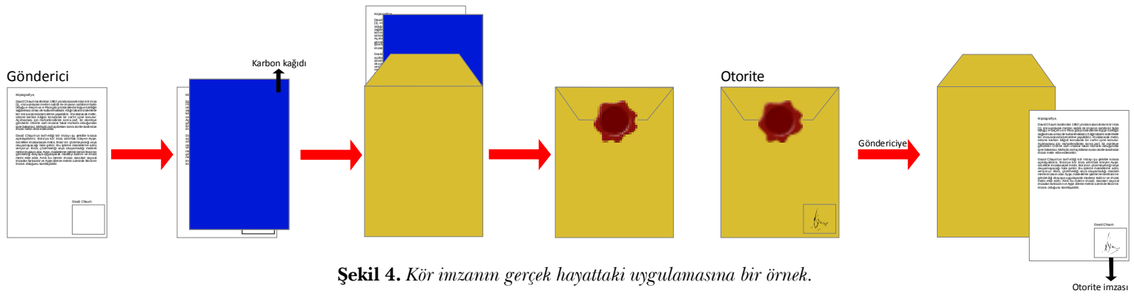
Bu yöntem ile Bora'ya her şey imzalatılabilir veya Bora görmediği bir şeyi imzalayarak yükümlülük altına girecek mi diye düşünebilirsiniz. Kör imzanın kullanım amacı farklıdır. Islak imza yerine geçen elektronik imza gibi kullanılmayacaktır.

Kör imzanın, e-seçim ve e-para gibi uygulamalarda kişiye özelliğin sağlanması amacıyla kullanılabileceğini belirtmiştik. Örneğin, e-seçimde kullanılan oyun geçerli sayılabilmesi için seçim otoritesi tarafından imzalanmış olması şart koşulabilir. Fakat oy pusulasını imzalarken seçim otoritesinin, seçmenin kime oy verdiğini de öğrenememesi gerekmektedir. Bu amaçla seçmen doldurduğu oy pusulasını maskeleyip daha sonra imzalayıp seçim otoritesine gönderir. Maskeli imzalı oy, seçimlerde oy vermeye yetkili bir seçmen tarafından gönderiliyor ise seçim otoritesi maskeli oya kör imza atar ve seçmene geri gönderir. Seçmen kendisine gelen mesajdaki maskeyi çıkararak otorite tarafından imzalı oyunu anonim olarak sayım merkezine gönderir.

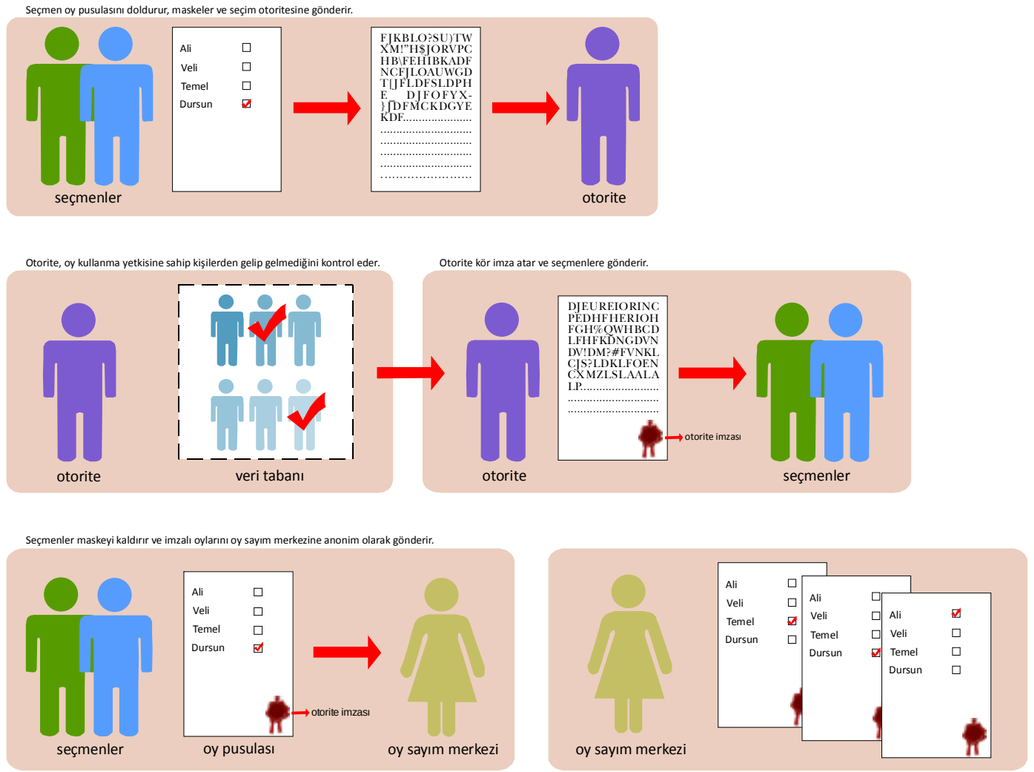


Şekil 5. *Kör imza.*

Yukarıdaki örnekler çoğaltılabilir. Anonimliğin sağlanmasına karşın bu protokolün güvenliği etkileyecek eksiklikleri mevcuttur. Güvenli ve güvenilir bir e-seçim sisteminde örneğin, seçmenin sayım merkezine anonim olarak bağlanması sağlanmalıdır, otorite imzalı pusulaların birden çok sayım merkezine gönderilmesi engellenmelidir ve sayım merkezinin seçim bitmeden oyları sayması engellenmelidir. e-seçim sistemlerinin zorluğu bunların hepsinin birlikte sağlanmasının güçlüğünden gelmektedir (Bknz. UEKAE Dergisi 4. Sayı).



Şekil 4. *Kör imzanın gerçek hayattaki uygulamasına bir örnek.*



Şekil 6. *E-seçim uygulaması.*

Kör imza, RSA, ElGamal ve DSA gibi yaygın olan asimetrik algoritmalarla gerçeklenebilmektedir. Temel RSA asimetrik şifreleme algoritması [1,2] kullanan kör imzalama yöntemleri hem çok basit hem de anlaşılırdır. Temel RSA imzası, mesaj m ($\mathbb{Z}_n$'deki sayısal eşleniğinin) ve gizli anahtar d'nin modüler üs işlemine tabi tutulması sonucu hesaplanır (Bknz. Bölüm 2.1 Homomorfik Şifreleme). İmzanın doğruluğunun hesaplanmasında kullanılacak açık anahtar e ve modüler n'den oluşmaktadır ve herkes tarafından bilinmektedir.

$$İmza = m^d mod\ N$$
(Temel RSA ile imzalama)

Temel RSA ile şifrelemenin güvenli olmadığı gibi bu algoritma kullanılarak atılan imzalar da güvenli değildir. Çünkü bu imzalama işleminden sonra mesaj değiştirilebilmektedir. Örneğin iki imzalı mesajın çarpımı yine geçerli bir imza olmaktadır.

$$\overline{İmza} = \bar{m}^d\ mod\ N$$
(Bir başka temel RSA ile imza)

$$İmza \cdot \overline{İmza} = (m.\bar{m})^d\ mod\ N$$
(Geçerli sahte imza)

İmzanın güvenliği için de mesaj dolgulama yöntemleri kullanılmaktadır [2].

Temel RSA'nın bu özelliği homomorfik şifrelemede olduğu gibi kör imzalarda da avantaja dönmektedir.

RSA ile Kör İmzalama

RSA'lı kör imzalarda mesajın maskelenmesi için rasgele sayılar kullanılır. Kullanılan rasgele sayının n ile aralarında asal olması gerekmektedir ($OBEB(r,n)=1$). Rasgele seçilen bir sayı ile n'in aralarında asal olma ihtimali çok yüksektir. Mesajın maskelenmesinde, $r^e\ mod\ n$ sayısı kullanılır. Bu değer aynı zamanda körlük faktörü olarak da adlandırılmaktadır. Mesaj, bu değerle çarpılarak maskelenir.

$r: rasgele, OBEB(r,n)=1 \qquad \bar{m} = m \cdot r^e\ mod\ n$ (maskeleme)

Maskelenmiş mesaj imzalanmak üzere otoriteye gönderilir. r rasgele olarak seçildiğinden ve $r \rightarrow r^e\ mod\ n$ dönüşümünün permütasyon olmasından dolayı $r^e\ mod\ n$ sayısı da rasgeledir. Mesaj, rasgele bir sayı ile çarpılarak maskelendiğinden hem otoriteye hem de hattı dinleyen saldırganlara mesaj hakkında bilgi sızdırılmamış olur. İmza otoritesi, maskeli mesaja temel RSA imzası atar ve sonucu mesaj sahibine gönderir.

Kör İmza

$$Kör\ İmza = \bar{m}^d mod\ n \qquad \text{(kör imza)}$$
$$\bar{m}^d mod\ n = (m \cdot r^e)^d\ mod\ n = m^d \cdot r^{ed}\ mod\ n \qquad \text{(kör imza)}$$
$$m^d \cdot r^{ed}\ mod\ n = m^d \cdot r\ mod\ n \qquad \text{(kör imza)}$$
$$(Kör\ İmza) \cdot r^{-1}\ mod\ n = m^d \cdot r \cdot r^{-1}\ mod\ n \qquad \text{(maske çözme)}$$
$$İmza = m^d mod\ n \qquad \text{(maske çözme)}$$

Mesaj sahibi rasgele sayıyı bildiği için kör imzadaki maskeyi çözerek imzalı mesajı elde edebilir. İmzalı mesaj incelendiğinde temel RSA ile atılan standart bir imzadan farklı olmadığı görülür.

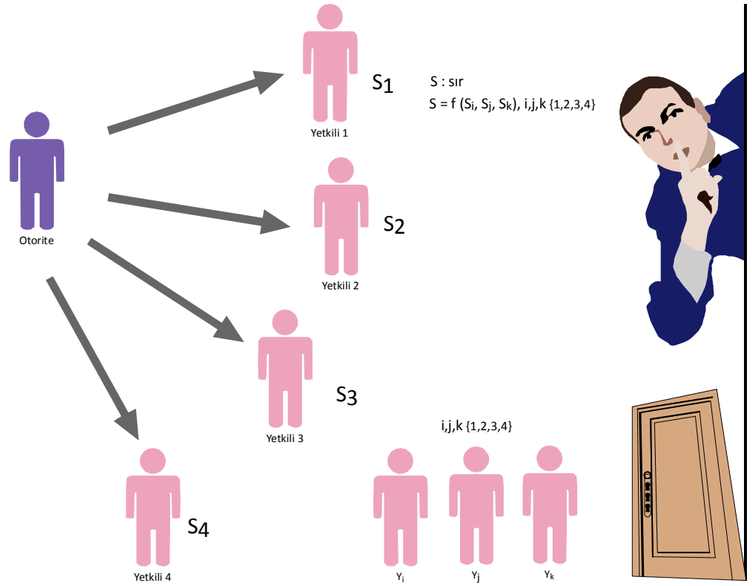
İmza işleminden sonra mesaj değiştirilebildiğinden dolayı RSA algoritmasının temel hali ile imzalama yapmanın güvensiz olduğunu belirtmiştik. Bunun engellenmesi ve sonuçta güvenli bir imza elde etmek için mesaj sahibi, standartlarda tanımlanan mesaj formatlarını ve dolgulama yöntemlerini kullanmalıdır. Mesaj sahibinin kötü niyetli olabileceği düşünüldüğünde imza kontrolü sırasında mesajın uygun formatta olup olmadığının kontrolü önem kazanmaktadır.

2.3. Sır Paylaşımı

Bazı uygulamalarda kripto anahtarının tek bir kişi tarafından bilinmesi sorun teşkil edebilmektedir. Örneğin seçim sistemlerinde şifreli oyların açılması için gerekli anahtarın tek bir kişinin sorumluluğuna verildiğini düşünelim. Bu kişinin anahtarının kullanılamaz hale gelmesi durumlarda seçim sonucunu hesaplamak (şifresini çözmek) mümkün olmayacaktır. Ayrıca, anahtara sahip olan bu kişi kötü niyetli olabilir ve seçim sonuçlarını olması gerekenden önce örneğin, seçim devam ederken çözmüş olabilir. Seçim sonuçlarının seçim devam ederken çözülmesinin sakıncalarını bir önceki yazımızda belirtmiştik (Bknz. UEKAE Dergisi 4. Sayı).

Aklımıza ilk gelen çözüm bu tip anahtarların yedeklenmesi veya aynı anahtardan birden fazla kişiye verilmesi gelebilir. Aynı anahtarın birden fazla kişi tarafından bilinmesi, anahtarın kaybedilme riskini azaltmakla birlikte seçim sonuçlarının zamanından önce çözülme ihtimalini de arttırmaktadır. Burada "Seçim sonucunun şifresini daha güvenilir bir şekilde çözmenin yolu var mı?" veya daha genel anlamda "Kripto anahtarını birden fazla kişi arasında paylaştırmak mümkün mü?" sorusu akla gelebilir. Bu konuda da kriptoloji yardımımıza koşmaktadır. Sır paylaşımı yöntemi ile kripto anahtarı bir grup yetkili arasında paylaştırılabilmektedir. Nükleer füzelerin ateşlenmesi gibi kritik işlemlerin onaylanmasında kullanılan sır paylaşımı, 1979 yılında Adi Shamir ve George Blakley tarafından (birbirlerinden bağımsız olarak) icat edilmiştir [8]. Bu yöntem ile anahtar birden fazla kişi arasında paylaştırılarak anahtarın kullanılamaması olasılığı azaltılırken grup içerisinden belli sayıda kişinin bir araya gelerek anahtarı oluşturabilmesi sağlanabilecektir. Örneğin yedi üyeden oluşan bir gruptan en az herhangi dört kişinin bir araya gelmesi ile anahtarın oluşturulması sağlanabilir. Böylelikle, kripto anahtarının kuraldışı olarak oluşturulma ve dolayısı ile yasadışı kullanılma olasılığı azaltılmış olur. Anahtarı oluşturmak için gerekli sayıdan az kişinin anahtar hakkında hiçbir fikir elde edememesi gerekmektedir. Matematiksel olarak yazarsak k sayısı şifreyi çözmek için birleşecek en az katılımcı, n ise toplam katılımcı sayısı olarak kabul edilirse bu sistemlere (k,n) - eşik sır paylaşım sistemleri denir $(1 \le k \le n)$.

Örneğimize geri dönersek yedi kişilik gruptan herhangi üç kişinin bir araya gelmesi ile asıl anahtar hakkında hiçbir bilgi öğrenilememelidir (yani, (4,7) - eşik sır paylaşımı). Bir başka ifade ile üç kişinin bir araya gelmesi ile elde edilecek bilgi, grup dışından birinin anahtar hakkındaki bilgisinden fazla olmamalıdır. Sır paylaşımına basit fakat güvensiz bir örnek verebiliriz; 128 bitlik bir kripto anahtarının dört kişi arasında paylaşılmak istendiğini düşünelim. Her bir kişiye 32 bit anahtar parçası ve bu parçanın sırasını gösteren bilginin dağıtılır. Tüm kişilerin bir araya gelmesi ile anahtarın elde edilebileceği açıktır. Fakat üç kişinin bir araya gelmesi ile anahtarın 96 bitlik kısmı tamamlanır. Geriye kalan 32 bitlik kısmın ise deneme ile bulunması çok zor değildir.



Şekil 7. *Sır paylaşımı.*

Sır paylaşımında kişilere dağıtılan parçaların uzunluğunun en az anahtarın uzunluğu kadar olması ve bunların rasgele olması gibi temel kurallar vardır.

Sır paylaşımında kişilere dağıtılan parçaların uzunluğunun en az anahtarın uzunluğu kadar olması ve bunların rasgele olması gibi temel kurallar vardır.

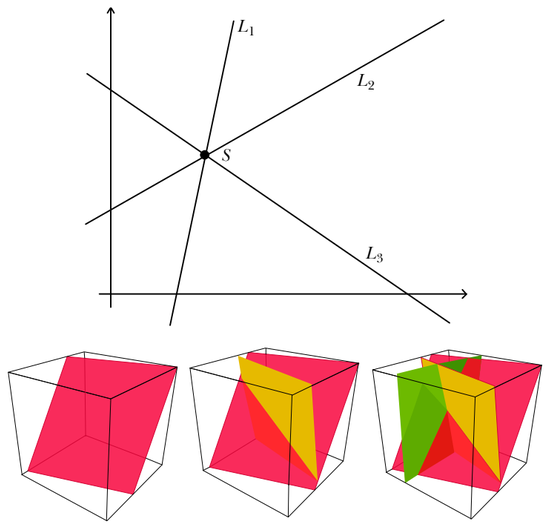
Bir başka örnek olarak yine 128 bitlik a anahtarının dört kişi arasında paylaştırılmak istendiğini düşünelim. Bu kez herkese rasgele 128 bitlik a_1, a_2, a_3, a_4 anahtarları verilmiş olsun. Asıl anahtar ise bunların hepsinin "dışlamalı ya da" (modüler 2) işlemiyle hesaplanmasıyla ($a=a_1 \oplus a_2 \oplus a_3 \oplus a_4$)bulunmaktadır. Önceki örnekten daha iyi olmakla birlikte bu yöntem ile grubun tamamının bir araya gelmesi gerekmektedir. Örneğin, a_1, a_2, a_3'ün bilinmesi ve a_4'ün bilinmemesi durumu hiçbirinin bilinmemesi durumuyla aynıdır.

Asimetrik şifrelemeyle sır paylaşımını sağlayan başka bir sistem de Asimetrik (t,n) - Eşik Homomorfik Kripto Sistemlerdir. Hem homomorfik, hem asimetrik hem de sır paylaşımını sağlayan en iyi örnekler için Eşik ElGamal ve Paillier kripto sistemleri verilebilir.

Bir sonraki bölümde basit ve anlaşılır iki sır paylaşımı yöntemi anlatılmaktadır.

2.3.1. Blakley Sır Paylaşımı

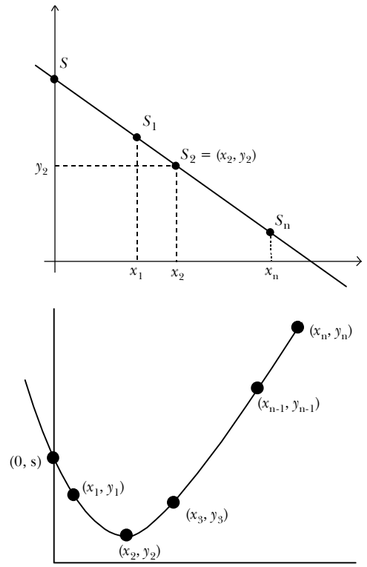
Blakley'in sır paylaşımı yönteminin anlaşılması için basit bir örnek verebiliriz. Gruptan herhangi üçünün bir araya gelerek anahtarı oluşturması istenildiğini düşünelim. Gruptaki üyelere rasgele paralel olmayan düzlemler verilir. Bu düzlemlerin bir özelliği daha vardır, hepsinin tek noktada kesişmesidir. İki düzlemin kesişmesi ile doğru, üçünün kesişmesi ile bir nokta (anahtar) elde edilir. Böylelikle herhangi üç kişinin bir araya gelmesi ile kesişim noktası yani anahtar oluşturabilir.



Şekil 8. *Blakley sır paylaşımı.*

2.3.2. Shamir Sır Paylaşımı

Shamir'in sır paylaşımı yöntemi, Blakley'in yönteminin özel bir halidir. Fakat hem daha kullanışlı hem de daha verimlidir. Shamir'in yönteminde polinomlar kullanılmaktadır ($p(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$). Üç kişinin bir araya gelerek anahtarı oluşturması isteniliyorsa grup üyelerine ikinci dereceden rasgele bir polinom üzerinde rasgele noktalar verilir. Hesaplanmak istenilen anahtarın polinomun y koordinatını kestiği nokta olduğunu düşünelim (yani $p(0)$). Herhangi üç kişi bir araya gelerek polinomu ve dolayısı ile anahtarı bulabilir. Kullanılan polinomun boyutu ile anahtarı oluşturmak için gerekli kişi sayısı arasında bir bağ vardır, kişi sayısının bir eksiğidir.



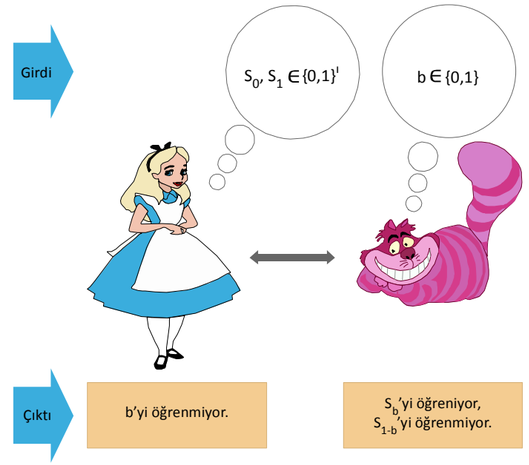
Şekil 9. *Shamir sır paylaşımı.*

Şimdiye kadar tarif edilen yöntemlerde grup üyelerinin dürüst olduklarını varsaydık. Grup üyelerinden biri veya birkaçının dürüst olmayabileceğinin de dikkate alınması gerekebilir. Elbette ki grupta eşik sayıda kişi anlaşarak anahtarı her zaman oluşturabilir. Bu durumu dikkate alarak geliştirilmiş sır paylaşımı protokolleri de vardır. Bu yöntemlerde, çok taraflı hesaplama ile birlikte sıfır bilgi protokolleri gibi ileri kripto protokolleri de kullanılmaktadır.

2.4. Habersiz Transfer

Sanal alışveriş merkezinden bir ürünün fiyatını öğrenmek istiyorsunuz fakat hangi ürün ile ilgilendiğinizin anlaşılmamasını istiyorsunuz. Ya da hangi bilgileri aldığınız anlaşılmayacak şekilde bir veritabanını sorgulamak istiyorsunuz. O zaman habersiz transfer protokollerini incelemenizi önerebiliriz.

Habersiz transfer protokolleri güvenli çok taraflı hesaplama protokollerinin temel yapılarından birisidir. Michael O. Rabin tarafından 1981 yılında yayınlanan teknik rapor ile literatüre girmiştir. Habersiz transfer çok güçlü bir yapıtaşıdır, tek başına kullanılarak her türlü çoklu hesaplama problemleri çözülebilir. Birçok güvenli çoklu hesaplama problemlerinde alt-protokol olarak da kullanılır.



Şekil 10. *Habersiz transfer.*

2.4.1. Rabin Habersiz Transferi [9,10]

Rabin'in protokolünde RSA algoritması kullanılmaktadır. Bu protokol ile Ayşe'nin gönderdiği mesajın şifresini Bora yüzde elli olasılıkla çözebilmektedir. Ayşe ise Bora'nın, mesajın şifresini çözüp çözemediğini bilememektedir. Bir başka deyişle Ayşe, Bora'nın mesajı çözdüğünü ancak yüzde elli olasılıkla bilmektedir.

Rabin Metodu

1. Ayşe, p ve q asal sayıları ile RSA modülü $n=pq$ ve ilgili e açık anahtarı üretir.
2. Ayşe, mesaj m'yi açık anahtarı kullanarak şifreler $m^e \bmod n$.
3. Ayşe "şifreli mesajı", n ve e'yi Bora'ya gönderir,
4. Bora, rasgele bir $x: 1<x<n$ sayısı bulur ve $x^2 \bmod n$'i hesaplar ve Ayşe'ye gönderir.
5. Ayşe, p ve q asal sayılarını bildiği için $x_1=\sqrt{x^2} \bmod n$'i hesaplayabilir. Karekök sonucu iki olasılık vardır, $x_1=x \bmod n$ veya $x_1=-x \bmod n$. Ayşe bunlardan birini rasgele seçip (yüzde elli olasılıkla) Bora'ya gönderir.
6. Bora, $d=OBEB(x-x_1, n)$'yi hesaplar.

Eğer $x_1=x \bmod n$ ise Bora hiçbir bilgi edinemeyecek ve mesajı çözemeyecektir. Aksi takdirde (yüzde elli olasılıkla) d asallardan birine eşit olacaktır ($d=p$ veya $d=q$). Yani yüzde elli olasılıkla Bora, asal sayıları bularak gizli anahtarı hesaplayabilecek ve dolayısı ile mesajı çözebilecektir. Ayşe ise gönderdiği sayının (x_1) Bora'nın tuttuğu sayıya (x) eşit olup olmadığını bilemeyeceğinden (yüzde elli olasılıkla bildiğinden) Bora'nın mesajı çözüp çözmediğini de bilemeyecektir (yüzde elli olasılıkla bilecektir).

Shimon Even, Oded Goldreich ve Abraham Lempel tarafından 1985 yılında duyurulan "2'de 1 habersiz transfer" protokolünde ise alıcı, göndericide bulunan iki mesajdan sadece birisi öğrenebilmekte fakat gönderici alıcının hangi mesajı öğrendiğini anlayamamaktadır. Ayşe a_0 ve a_1 mesajına sahip olsun, Bora da 0 veya 1 (b olarak adlandıralım) üretsin. Habersiz transfer çalıştırdıktan sonra Bora a_b mesajını elde edecek fakat a_{1-b} mesajı hakkında hiçbir bilgi sahibi olamayacaktır. Yani, alıcı mesajlardan ikisini birden öğrenemeyecektir. Ayşe ise Bora'nın hangi mesajı açabildiğini öğrenemeyecektir. Bu protokolün genelleştirilmiş hali "n'de 1 habersiz transfer protokolleri" de literatürde mevcuttur.

2.5. Taahhüt Şemaları

Bölüm 2.6'da anlatılacak olan sıfır bilgi sızmalı kanıt protokollerinin yapı taşlarındandır. Doğruluğu taahhüt edilmiş verilerin geçici olarak saklanması için kullanılmaktadır. İki aşamalıdır;

1. *Taahhüt aşaması*: Gönderen, örneğin Bora m mesajını bir kasaya koyar, kasayı kilitler ve Ayşe'ye gönderir.

2. *Kanıt (açığa çıkarma) aşaması*: Bora, kasadaki mesajın m mesajı olduğuna dair kanıtını ortaya koyarak Ayşe'yi ikna eder.

Bit, tamsayı ve dizi olmak üzere üç tip taahhüt şeması vardır. Taahhüt şemalarının iki özelliği sağlaması beklenmektedir. Bunlar;

Gizleme: Taahhüt aşamasından sonra kötü niyetli bir alıcı taahhüt edilen veri hakkında hiçbir şey öğrenememelidir. Yani, kasayı alan kişi anahtarı bilmediğinden asla açamamalıdır.

Bağlama: Kötü niyetli gönderici, kanıt aşamasında alıcıyı iki farklı veri konusunda ikna edememelidir. Yani, kasadaki m mesajını ondan farklı birm' mesajı şeklinde açamamalıdır.

2.5.1. Örnek bir Taahhüt Şeması

a. İlk aşamada; Bora, rasgele k anahtarı üretir ve $E_k(m)$'yi Ayşe'ye gönderir.

b. İkinci aşamada; Bora k anahtarını Ayşe'ye gönderir. Ayşe şifreyi çözerek mesajı elde eder.

Bu örneğin gizleme ve bağlama özelliklerini yerine getirip getirmediğine bakalım. İlk aşamada mesaj rasgele bir anahtar ile şifrelendiğinden Ayşe ikinci aşamadan önce hesaplamaya dayalı zorluk nedeniyle mesaj hakkında bilgi edinemeyeceğinden gizleme özelliği sağlanmaktadır. Fakat ikinci aşamada Bora farklı bir anahtar gönderebileceğinden

(özellikle kısa mesajlarda) bağlama özelliği sağlanamayabilir. Bunun için mesajın değiştirilemeyeceğini bir şekilde garanti etmek gerekmektedir.

Bir Başka Örnek Taahhüt Şeması: $\mathcal{H}$, kriptografik özet algoritmasıdır.

a. İlk aşamada; Bora, rasgele r:k bit değeri üretir, r ve $\mathcal{H}(r,m)$'yi Ayşe'ye gönderir.

b. İkinci aşamada; Bora m mesajını Ayşe'ye gönderir.

Bu örneğin gizleme ve bağlama özelliklerini yerine getirip getirmediğine bakalım. Özet algoritmasının ön-görüntü dayanıklılığı (preimage resistance) özelliğinden dolayı mesaj özet değerinden elde edilemez. Özet algoritmasının çarpışmaya dayanıklılığı (collision resistance) özelliğinden dolayı ikinci aşamada başka bir mesaj verilmesi mümkün değildir. k parametresinin uzunluğuna bağlı olarak hem saklanma hem de bağlama özellikleri sağlanır. Fakat bu iki özellik de hesaplama zorluğuna dayalı olarak sağlanmaktadır. Daha iyisi yapılamaz mı?

2.5.2. Pedersen Taahhüt Şeması

Kurulum: Alıcı taraf (Ayşe) aşağıdaki işlemleri yapar.

a. G:n (büyük asal bir sayı) elemanlı çarpma işlemine göre devirli grup,örn. $\mathbb{Z}_n$.

b. g:grubun üreteci

c. $h=g^a$, a:rasgele

d. (G,n,g,h): açık anahtar

Taahhüt Aşaması: $\mathbb{Z}_n$'dan x elemanı taahhüt etmek için Bora, $\mathbb{Z}_n$'den rasgele bir r elemanı seçer, $c=g^x h^r \bmod n$'yi hesaplar ve Ayşe'ye gönderir.

Kanıt Aşaması: Bora, x ve r'yi Ayşe gönderir. Ayşe, $\bar{c}=g^x h^r \bmod n$'yi hesaplar ve kendisine gönderilen c ile karşılaştırır.

Pedersen Taahhüt Şeması'nın gizleme ve bağlama özelliklerini yerine getirip getirmediğine bakalım.

Gizleme: Her bir c taahhüdü için $\mathbb{Z}_n$'dan her bir x elemanı eşit olasılıkla seçilmiş olabilir. Yani her bir x için c taahhüdünü verecek bir r elemanı bulunabilir. Dolayısıyla bu şema, şartsız gizleme sağlar (Bknz. Kavramlar Sözlüğü).

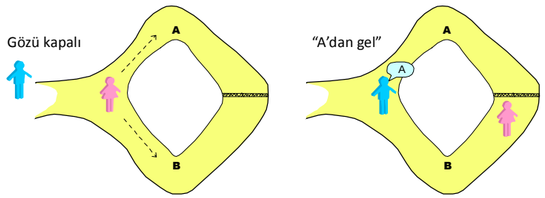
Bağlama: Bora'nın kanıt aşamasında, $\mathbb{Z}_n$'dan $\bar{x}\neq x$ olacak şekilde başka bir eleman gönderdiğini varsayalım. Bunun için Bora'nın $g^x h^r \bmod n = g^{\bar{x}} h^{\bar{r}} \bmod n$ olacak şekilde $\mathbb{Z}_n$'dan $\bar{x}$ ve $\bar{r}$ elemanlarını bulması gerekmektedir. Bunun için Bora'nın $a=\log_g h=(\bar{x}-x)(r-\bar{r})^{-1} \bmod n$ ayrık logaritma işlemini hesaplaması gerekmektedir ki bu işlemin hesaplama zorluğuna dayalı olarak zor bir problem olduğu bilinmektedir (Bknz. Kavramlar Sözlüğü).

2.6. Sıfır Bilgi Sızmalı Kanıt Protokolleri

Bir arkadaşınıza bir kapının anahtarının sizde olduğunu kanıtlamak istiyorsunuz. Kapıyı o kişinin önünde açarak anahtarının sizde olduğunu kanıtlayabilirsiniz. Peki, anahtarı o kişiye göstermeden sizde olduğuna inandırmak istiyorsanız ne yapabilirsiniz?

Siz ve o kişinin ortak tamamen güvendiği bir arkadaşınız olsun. Sadece o kişinin göreceği şekilde o anahtarla kapıyı açıp kilitleyip onu ikna edersiniz. O da diğer arkadaşa evet o anahtar bu kapıyı açıyor der ve inanır. Peki, ortak güvenilir bir kişi yoksa bu problemi nasıl çözebiliriz? Biraz daha zor bir problem olmakla birlikte çözümü vardır.

İki çıkışı olan bir mağara olduğunu düşünelim. Arkadaşınız bu iki çıkış arasındaki gizli bağlantıyı bildiğini iddia etmektedir. Gizli bağlantın yerini göstermeden sizi bildiğine ikna etmek istiyor. Arkadaşınız mağaranın içinde iken (hangi girişten girdiğini görmediniz) mağaranın önüne gelerek dilediğiniz bir çıkıştan çıkmasını istiyorsunuz. Arkadaşınız istenilen çıkışta belirdiği zaman gizli bağlantının yerini bildiğine ikna olacak mısınız? Arkadaşınızın mağaradan çıkmak için gizli bağlantıyı kullanmasına gerek kalmamış olabilir. Bunun olasılığı yüzde ellidir. Yani yüzde elli olasılıkla arkadaşınız gizli geçidin yerini biliyor olabilir. Bu durumda ikna olmuş sayılmazsınız. Bu işlemi on defa tekrarladığınızı ve her defasında arkadaşınızın istenilen yerden çıkmayı başardığını düşünelim. Gizli bağlantıyı bilmeden bunu yapma ihtimali çok düşüktür, binde bir civarındadır. Hala ikna olmadıysanız işleme devam edebilirsiniz [11].



Şekil 11. *Sıfır bilgi sızmalı mağara yolu.*

Sıfır bilgi sızmalı kanıt protokollerinin aşağıdaki özellikleri sağlaması beklenmektedir.

- *Eksiksizlik*: İddia doğru ise, dürüst davranan (kurallara uyan ve protokol adımlarını izleyen) doğrulayıcı protokolün sonunda ikna olacaktır.
- *Doğruluk*: İddia doğru değil ise, (ihmal edilebilir düzeyde hata payı ile) protokolün sonunda dürüst doğrulayıcı hiçbir şekilde ikna edilemeyecektir.
- *Sıfır Bilgi Sızması*: Protokolün başarı ile tamamlanması sonucu doğrulayıcı iddianın doğruluğu haricinde hiçbir ek bilgi öğrenemeyecektir.

İhmal edilebilir düzeyde hata içermelerinden dolayı sıfır bilgi sızmalı kanıt protokolleri matematikteki kanıt mekanizmalarından ayrılmaktadır. Yani, bu protokoller belirleyici olmamakla birlikte rasgelelik özelliği gösterirler.

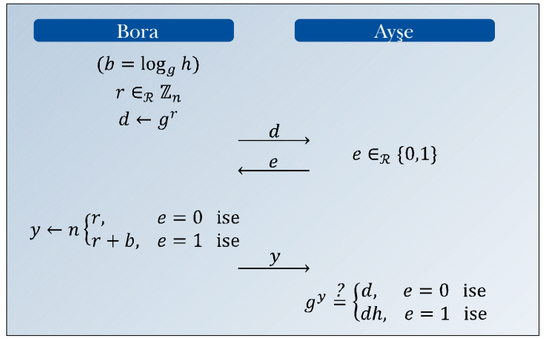
Ancak bu hata payı ihmal edilebilecek seviyelere kadar indirilebilmektedir. Bir uygulama alanına örnek olarak sıfır bilgi sızmalı kanıt protokolleri, dost düşman tanımlama sistemlerinde de kullanılabilmektedir.

Sıfır bilgi protokollerinin en etkileyici kullanım alanlarından bir tanesi, bu protokollerin kullanımıyla kişiye özellik/anonimlik sağlanırken dürüst davranıldığının da kanıtlanabilmesidir. Kullanıcı sıradan bir protokol adımlarını takip ederken yaptığı işlemlerin doğruluğunu sıfır bilgi yöntemi ile karşı tarafa kanıtlayabilir. Bu yolla protokollerin dürüst olmayan kişilere karşı güvenli hale getirilebilir. Örneğin seçmenden, referandumda kullandığı oyun evet/hayır/çekimser oylarından birisini içerdiğini, örneğin iki evet içermediğini kanıtlaması istenilebilir. Kâğıt tabanlı seçimlerde seçmenlerin kullandıkları oy zarfı bir oy içermektedir. Seçmen zarfın içine birden fazla oy pusulası koymuş olsa bile zarflar tek tek açıldığından bu durum anlaşılacaktır. Homomorfik tabanlı sistemlerde, kullanılan oy pusulaları açılmadan şifreli olarak toplandığından oy pusulasının evet/hayır/çekimser dışında oy içermediğinden emin olunması çok önemlidir. Aksi takdirde seçmenler görünürde bir oy gerçekte ise birden fazla oy kullanabilir. Sıfır bilgi protokolleri bunu rahatlıkla garanti edebilir.

Sıfır bilgi protokolleri modern kriptografiye 1985 yılında Shafi Goldwasser, Silvio Micali ve Charles Rackoff tarafından kazandırıldı [12, 13].

En basit ve yaygın olarak kullanılan kanıt protokollerinden birisi Schnorr protokolüdür. Schnorr protokolü, ayrık logaritma sonucunun bilindiğinin karşı tarafa ispatlanması olarak özetlenebilir.

2.6.1. Schnorr Protokolü



Kurulum: Sitem parametreleri aşağıdaki gibi hesaplanır.

a. G:n (büyük asal bir sayı) elemanlı çarpma işlemine göre devirli grup, örn. $\mathbb{Z}_n$.

b. g: grubun üreteci

c. $h=g^b$, b:rasgele

d. b:gizli anahtar

e. (n,g,h):açık anahtar

Protokol işleyişi: Bora, Ayşe'ye ayrık logaritma sonucunun bilindiğini ispatlayacaktır (yani, b'yi bildiğini göstermeden ispat edecektir.). Aşağıdaki protokolün t kere çalıştırılması ile Ayşe $(1/2)^t$ hata oranı ile ikna olacaktır.

Bora $\mathbb{Z}_n$'dan rasgele bir r seçer ve $d=g^r \bmod n$ değerini Ayşe'ye gönderir.

Ayşe, rasgele bir e bit (0 veya 1) seçer ve Bora'ya gönderir.

Bora, $y=r+eb \bmod n$ işlemini yapar ve y'yi Ayşe'ye gönderir.

Ayşe, $\bar{d}=g^y h^{-e} \bmod n$'yi hesaplar, $\bar{d}=d$ ise kabul eder.

Schnorr Protokolünün Güvenliği

Eksiksizlik: Protokol başarı ile sonuçlanırsa r ve b'yi bilmeyen birisinin y'yi hesaplama mümkün olmadığından (ayrık logaritma problemi), Bora'nın r değerini biliyor olması gerekir.

Doğruluk: Eğer Bora b'yi bilmiyorsa yapabileceği en iyi şey ilk adımda y'yi hesaplayabileceği bir d seçmektir. Ayşe e'yi (0 veya 1) rasgele seçtiğinden Bora'nın b'yi bilmeden doğru y hesaplama ihtimali (1/2)'dir. Protokol yeterince tekrarlanırsa Bora'nın b'yi bilmeden Ayşe'yi ikna etme ihtimali ihmal edilebilir düzeyde olacaktır.

Sıfır Bilgi Sızması: Protokolün işleyişi ile gizli parametren b'nin bulunmasına katkıda bulunacak ek bilgi açığa çıkmamaktadır.

Sıfır bilgi sızmalı kanıt protokolleri etkileşimli ve etkileşimsiz olabilmektedir. Schnorr protokolü etkileşimli bir sıfır bilgi sızmalı kanıt protokolüdür. Etkileşimsiz protokollerde kanıtlayıcı gerekli tüm bilgileri hazırlayıp doğrulayıcıya göndermektedir. Doğrulayıcı da gönderilen veriler üzerinden iddianın doğru olup olmadığını anlayabilmektedir. Etkileşimsiz protokollerde, Schnorr protokolünde olduğu doğrulayıcının o anda hazır olmasına ve iletişimde bulunmasına gerek yoktur.

Homomorfik şifreleme bölümünün sonunda verdiğimiz örnekte seçmenlerin dürüst davrandıklarını anlamak için sıfır bilgi sızmalı kanıt protokollerinin kullanılabileceğini belirtmiştik. Schnorr protokolü gibi sıfır bilgi sızmalı kanıt protokolleri, homomorfik tabanlı sistemlerde tarafların dürüst davrandığını anlamak için yaygın olarak kullanılmaktadır.

2.7. Karıştırıcı Sistemler

Karıştırıcı ağlar, kimin kime oy verdiği, kimin hangi siteleri gezdiği (onion routing, webmixes, vb.) veya kimin kime e-posta gönderdiği gibi kişi ile yaptığı iş arasında oluşabilecek ilişkilerinin yok edilmesini hedeflemektedir. Karıştırıcı ağlarda kullanıcı mesaj ilişkisinin yok edilmesi için rasgele permutasyon, asimetrik şifreleme ve tekrar şifreleme gibi değişik teknikler kullanılabilmektedir [14].

2.7.1. Tekrar Şifreleme Tekniği Kullanımıyla Karıştırma

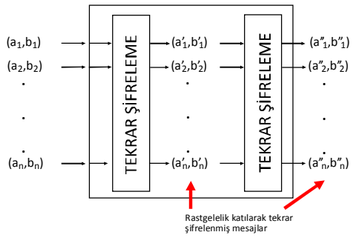
ElGamal gibi homomorfik şifreleyiciler kullanıldığı durumlarda, bu algoritmaların homomorfik özelliği kullanılarak kullanıcılar tarafından şifrelenen mesajlar sunucularda rasgelelik katılarak tekrar şifrelenebilir. Rasgele permutasyonların da kullanımı ile ağ üzerinde mesajları takip eden kişinin mesaj ile kullanıcı arasında ilişki kurmasının önüne geçilebilir.

ElGamal ile şifreleme işleminde mesajın değiştirilmeden tekrar şifrelenmesi için aşağıdaki işlemler yapılır.

Gönderici m, mesajı şifreleyerek $(a_1,b_1)=(g^{r_1},m\cdot h_1{}^{r_1})$ şifreli mesajı elde eder.

Birinci sunucu tekrar şifrelemek için rasgele s_1 üretir ve $(g^{s_1},1\cdot h_1{}^{s_1})$'yi hesaplar. Bunu kullanıcının gönderdiği (a_1,b_1) ile çarpar ve $(a_1',b_1')=(g^{r_1+s_1},m\cdot h_1{}^{r_1+s_1})$' elde eder.

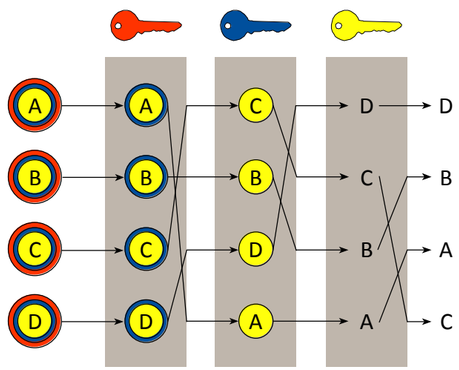
Diğer sunucularda benzer işlem yaparak takip edilebilirliği önlerler.



Şekil 12. *Tekrar şifreleme tekniği.*

2.7.2. Karıştırıcı Ağ Kullanımıyla Karıştırma

İlk kez 1981 yılında David Chaum tarafından ortaya atılmıştır [24]. Bir dizi vekil sunucu ve bu sunucular arasında şifreleme teknikleri kurulması önerilmektedir. İç içe geçmiş asimetrik şifreleme kullanımı ile trafik analizi önlenmeye çalışılmaktadır.



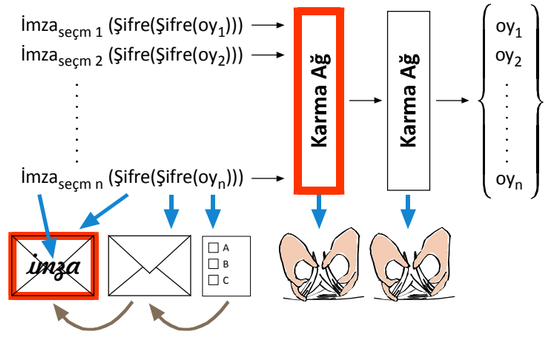
Şekil 13. *Basit bir şifre çözücü karıştırıcı ağ örneği.*

Dünyanın bazı ülkelerinde hala iki zarf usulü oy kullanılabilmektedir. Bu ülkelerde seçmenler oy pusulasını doldurur ve üzerinde hiçbir işaret olmayan bir zarfın içine koyarlar. Daha sonra bu zarfı, ikinci bir zarfın içine koyar, dıştaki zarfa kimliğini yazar, imzasını atar ve posta ile seçim otoritesine gönderirler. Seçim otoritesi kimliği doğrular dıştaki zarfı açar ve içteki zarfı oy sayma merkezine gönderir ve orada sandığa atılır ve karışır.

Örnek olarak benzer bir e-Seçim uygulaması düşünelim. Örneğimizde, seçmenler oy pusulalarını doldurur, oy sayıma otoritesinin imzası ile şifreler, kimlik doğrulama otoritesinin anahtarı ile bir daha şifreler ve elektronik imza atarlar. Daha sonra bu şifreli ve imzalı oyu seçim otoritesine gönderirler. Seçim otoritesi zarfı, kimlik doğrulama otoritesine gönderir. Kimlik doğrulanır, şifresi çözülür ve sorun yoksa sayım merkezine gönderilir. Sayım merkezi oyun şifresini çözer.

Elektronik sistemlerde, klasik sistemlere (zarf ve posta) göre daha dikkatli davranılması gerekebilir. Elektronik sistemle kimin hangi sırada oy verdiği daha net bir şekilde kaydedilebilir. Dolayısıyla seçim merkezine gelen şifreli ve çözülmüş oyları bilen birisi, bunların sırasından kimin kime oy verdiğini bulabilir.

Karıştırıcı ağlarda dürüst davranılmaması sonucu kullanıcı ile mesaj arasındaki ilişki yok olmayacaktır. Buna karşı önlem olarak çok sayıda sunucu kullanılabilir. Bu sunuculardan en az birinin dürüst davranması ve kullanıcı ile mesaj arasındaki ilişkileri yok etmesi yeterlidir.



Şekil 14. *Karıştırıcı ağlar ile e-seçim uygulaması.*

3. ÇOK TARAFLI GÜVENLİ HESAPLAMA

İki milyoner Ayşe ve Bora, servetlerinin miktarı hakkında hiçbir bilgi vermeden kimin daha zengin olduğunu öğrenmek istemektedirler. Andrew C. Yao, milyoner problemi olarak tanımladığı bu probleme 1982'deki makalesinde çözüm bulmaya çalışmıştır [15]. Daha sonra basitçe güvenli hesaplama olarak da adlandırılan bu konudaki çalışmalar başlamıştır. Örneğin iki taraflı güvenli hesaplamada Ayşe ve Bora, x ve y gizli verileri ile herkes tarafından bilinen bir fonksiyonun $f(x,y)$ sonucunu hesaplamak istemektedirler. Güvenli hesaplama, n kişinin katıldığı hesaplamalar olarak genellenebilmektedir [16].

Sıfır bilgi sızmalı kanıt problemleri ile de ilişkili olan güvenli hesaplama kavramı tarafların gizli bilgilerini birbirlerine vermeden hedefledikleri işlemleri yapmalarına olanak sağlaması açısından önemlidir. Habersiz transfer protokolleri de güvenli hesaplama sistemlerinin önemli bir yapı taşını oluşturmaktadır. Bir sonraki bölümde anlatılacak olan uygulamalar bu genelleştirilmiş yöntemlerle çözülebilmektedir. Güvenli çok taraflı hesaplamalar şu güvenlik ölçütlerini yerine getirmesi gerektirmektedir.

Doğruluk: $f(x,y)$ sonucu doğru hesaplamalıdır.

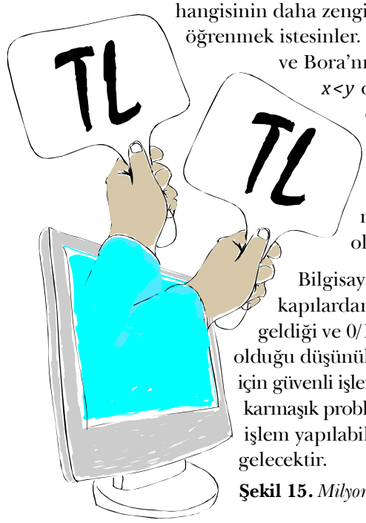
Mahremiyet: Hesaplama yapılırken kişilere ait özel bilgiler açığa çıkmamalıdır.

Adiliyet: İletişim bağlantısının kopması veya taraflardan birinin sahtekâr olması durumunda tarafların birinin diğer(ler)ine üstünlük sağlayamaması anlamına gelmektedir. Adiliyet başlı başına çözülmesi gereken bir problemdir. Bunun için taraflardan birinin bir bilgiyi öğrendiği anda diğerinin de öğrenebilmesi gerekmektedir. Örneğin, taraflardan biri diğerinden önce öğrendiğinde, kendisine gelmediğini, hata olduğunu veya bilmediğini iddia edebilir. Sahtekâr kişi iletişime devam etse bile hatalı bilgiler söyleyebilir. Bu durumda dürüst taraf gerçek sonucu öğrendiğini nasıl anlayabilir? İki taraflı hesaplamalarda adiliyet çok küçük hata payı ile sağlanabilirken üç ve daha fazla taraflı hesaplamalarda adiliyet doğrudan sağlanabilmektedir [17].

Bir sonraki bölümde yaygın olarak bilinen "Milyoner Problemi" ve "Aşk Problemi"ni inceleyeceğiz.

3.1. Milyoner Problemi

Ayşe ve Bora birbirlerine servetlerini söylemek istemeyip hangisinin daha zengin olduğunu öğrenmek istesinler. Ayşe'nin x milyonu ve Bora'nın y milyonu olsun. $x<y$ olup olmadığını öğrenmek istesinler. Bu problemin daha özel bir durumu ise $x\neq y$ olup sosyalist milyoner problemi olarak adlandırılır.



Bilgisayar sistemleri kapılardan (gate) meydana geldiği ve 0/1 girdi ve çıktılarının olduğu düşünülürse sadece bir kapı için güvenli işlem yapılabilmesi daha karmaşık problemler için de güvenli işlem yapılabilmesi anlamına gelecektir.

Şekil 15. *Milyoner problemi.*

3.2. Aşk Problemi

Ayşe ve Bora birbirlerine ilgi duyup duymadıklarını açığa vurmadan öğrenmek istemektedir. Fakat ilgi duyan kişiyi utandırmamak için ilgi duymayanın karşı tarafın duygusunu öğrenememesi istenmektedir. İki taraf birbirlerine ilgi duyduğu takdirde, bir taraf diğerinin duygularını öğrendiği anda diğerinin de aynı sonucu öğrenmesi gerekmektedir. Kolay görünmesine rağmen problemin çözümü kolayca akla gelmeyebilir. Tarafların yarı-dürüst davrandıklarını varsayarsak problemi aşağıdaki gibi çözebiliriz.

Protokollerdeki Davranış Modelleri

Protokol tasarlanırken aşağıdaki davranış modelleri altında incelenmektedirler.

1. *Dürüst model*: Bu modelde herkesin dürüst olduğu kabul edilir. Tarafların protokole harfiyen uydukları ve karşı tarafın verisini öğrenmeye çalışmadıkları varsayılır.

2. *Yarı-dürüst model*: Taraflar protokole harfiyen uyarlar, fakat karşı tarafın verisini öğrenmeye çalıştıkları varsayılır. Protokol çalışırken saldıran kişi sürekli iletişim bilgilerini daha sonra kullanmak üzere kaydeder.

3. *Dürüst olmayan model*: Tarafların protokolde adımlara uymayabilecekleri ve karşı tarafın verisini öğrenmeye çalışacakları varsayılır.

Bir problem için protokol tasarlanırken genellikle başlangıçta dürüst modelde tasarlanır ve ve sistemin güvenilirliği test edilir. Sonrasında yarı-dürüst modelde tasarlanır ve güvenliği analiz edilir. En sonunda da sıfır bilgi protokolleri eklenerek sistem dürüst olmayan modelde geliştirilir. Dürüst olmayabilecekleri düşünülen modellerde güvenliğin sağlanması için taraflardan dürüst davrandıklarını kanıtlamaları beklenir. Bunun için genellikle taahhüt şemalar ve sıfır bilgi sızmalı kanıt protokolleri kullanılmaktadır.

Kurulum: Ayşe ve Bora (2,2)- Eşik Sır Paylaşımlı ElGamal şifreleme kullanmaktadır ve h açık anahtardır.

1. x, Ayşe'nin y, Bora'nın gizli verileridir $x,y\in\{0,1\}$,

2. Ayşe, rasgele $r_A\in\mathbb{Z}_n$ ile $(a,b)=(g^{r_A},h^{r_A}g^x)$'yi hesaplayarak Bora'ya gönderir.

3. Bora, rasgele $r_B\in\mathbb{Z}_n$ ve y ile tekrar şifreleme yapar: $(c,d)=(g^{r_B}a^y,h^{r_B}b^y)$. (c,d) sonucunu Ayşe'ye gönderir.

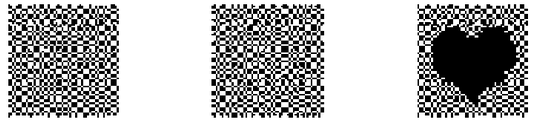
4. Ayşe ve Bora (c,d)'yi sır paylaşımı tekniğiyle birlikte çözerek xy sonucunu öğrenirler.

x	y	xy
0	0	0
0	1	0
1	0	0
1	1	1

Ayşe	Bora	?
Hayır	Hayır	0
Hayır	Evet	0
Evet	Hayır	0
Evet	Evet	♥

Dürüst olmayan model kullanıldığı durumlarda sıfır bilgi protokolleri kullanılarak tarafların doğru söyledikleri garanti edilebilmektedir. Adiliyet içinse tarafların protokol adımları süresince kendi paylarını parça parça diğer tarafa açıklaması gibi (örneğin bit bit) teknikler kullanılabilmektedir. Fakat iki taraflı hesaplamanın doğası gereği tam adiliyet sağlanamamaktadır [18].

Aşk probleminin çözümü için resim paylaşımı gibi başka teknikler de kullanılabilmektedir.



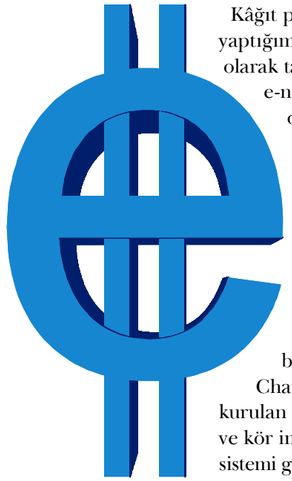
Şekil 16. *Aşk problemine grafikli çözüm.*

4. GÜNCEL UYGULAMA ALANLARI

Yazımızın başında temel kriptografinin özellikle kişiye özelliğin sağlanması konusunda yetersiz kaldığını belirtmiştik. Aşağıda kısaca bahsedeceğimiz uygulamalarda Kriptoloji 1.0'in yanında ileri düzey kriptografik algoritma ve protokoller de kullanılmaktadır.

4.1. E-nakit

E-nakit, e-para, sayısal (sanal) para/nakit olarak da adlandırılabilmektedir. Elektronik olarak kullanılabilen para anlamındadır. Genellikle e-ticaret ile karıştırılmaktadır. e-ticaret ile bankada bulunan paranızı veya kredi kartınızı kullanarak internet veya telefon ile alışveriş yapmanızı sağlayan sistemler kastedilmektedir. E-nakit ise kağıt paranın yerine geçen elektronik para anlamında kullanılmaktadır.



Şekil 17. *E-nakit.*

Kâğıt para kullandığımız zaman yaptığımız alışverişler elektronik olarak takip edilememektedir. Peki, e-nakit ile de kâğıt parada olduğu gibi anonim alışveriş yapılabilir mi? Ya da sahte para üretiminin önüne geçilebilir mi?

E-nakit konusunda literatürde çeşitli çözüm önerileri sunulmuştur. Fakat günümüzde bunlar yaygın kullanım imkanı bulamamıştır. Örneğin, David Chaum tarafından 1990 yılında kurulan DigiCash şirketi, dijital imza ve kör imza kullanımı ile e-nakit sistemi geliştirmiştir. DigiCash, e-nakit konusunda yeterince pazar oluşmaması sonucunda 1998 yılında kapanmıştır.

4.2. E-müzayede

Değişik tipte müzayede çeşitleri vardır. Bunlardan bazıları aşağıda listelenmiştir.

1. *İngiliz*: Düşük seviyeden başlar ve gittikçe artar. En yüksek fiyatı veren kazanır. eBay, Sotheby's gibi siteler bu çeşit müzayede yapmaktadır.

2. *Felemenk*: Yüksek fiyattan başlar ve müzayedeci tarafından düşürülür. İlk teklif veren kazanır.

3. *Duble Müzayede*: Alıcı ve satıcı tarafından teklif verilir. Müzayedeci sonuca karar verir (örn. NYSE, NASDAQ, CBOT).

4. *Vickrey*: En yüksek teklif veren kazanır fakat ikinci yüksek teklifteki fiyat uygulanır.

5. *Kapalı Zarf Usulü*: Kapalı olarak teklif verilir. En yüksek teklifi veren kazanır (örn. eBay).

Şekil 18. *E-müzayede.*

Açık artırmada bazı tarafların bir araya gelerek diğerlerini kandırması, müzayedeci ve satıcının (başka ad altında) fiyat yükseltmesi, malın gönderilmemesi veya sahte emanetçi gibi problemler vardır. E-müzayedelerdeki sistemlerindeki bazı güvenlik hedefleri aşağıda listelenmiştir.

- Alıcı, satıcı ve müzayedecinin sahtekârlık yapmasının önlenmesi,
- Alıcı ve satıcıların anonimliklerinin sağlanması,
- Teklif bilgisinin kişi bilgisinden ayrılması,
- Kapalı zarf usulü müzayedelerde sonucun hesaplanmasına kadar tekliflerin gizlenmesi,
- İhaleye fesat karıştırılmaması açısından ihaleyi yapan kurumun teklifleri zamanından önce açamaması,
- Tekliflerin değişmediğinin garanti edilmesi,
- İhale sonrası kazanan tarafın teklifini inkâr edememesi,
- Kaybeden tarafların kimliğinin ve/veya tekliflerinin gizlenmesi.

Güvenlik hedeflerinin sağlanması için açık literatürde yayınlanmış bazı müzayede metotları mevcuttur. Bu sistemlerde Kriptoloji 1.0'nin yanında, kişilerin tekliflerinin gizlenmesi amacı ile homomorfik şifreleme gibi ileri kriptografik teknikler de kullanılabilmektedir. Elkind ve Lipmaa, Vickrey'in e-müzayede için önerdikleri sistemde homomorfik şifreleme ve sıfır bilgi sızmalı kanıt protokolleri kullanılmaktadır [19].

Farklılıkları olmakla birlikte e-ihale sistemleri de e-müzayede sistemlerine benzetilebilir. Danimarka'daki şeker pancarı üreticileri güvenli e-ihaleyi, adil bir pazar fiyatı üzerinden ürünlerini satabilmek için kullanmaktadırlar. Bu sistemde, teklifler gönderilmeden önce şifrelenir. Sistem tekliflerle işlem yapacağı zaman güvenli çok taraflı hesaplama tekniklerini kullanarak şifreli teklifler üzerinden sonucu hesaplar [25].

4.3. E-kontrat İmzalama (E-noter)

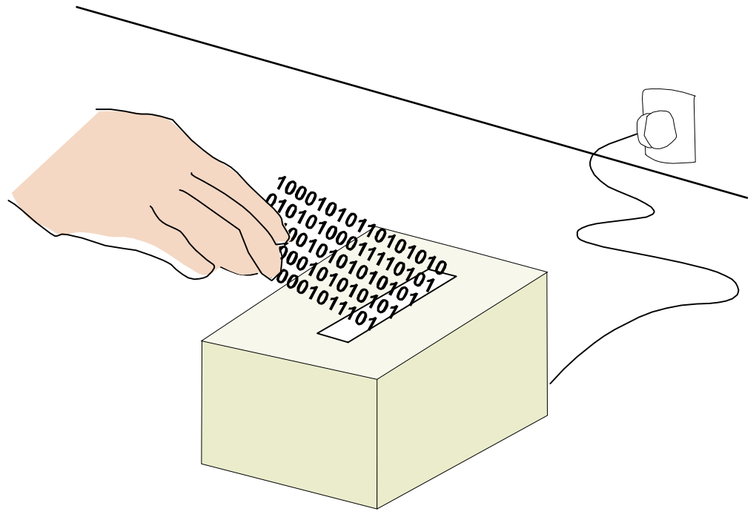
İstanbul'da bir ev almak istiyorsunuz fakat almak istediğiniz evin sahibi yurt dışında ve uzunca bir süre dönmeyecek. Satın alma işlemleri için satış sözleşmesinin imzalanması gerektiğinden sizin notere gitmeniz, yurt dışında bulunan ev sahibinin de bir Türk Konsolosluğuna giderek noter işlemlerini halletmesi gibi zaman alıcı ve yorucu işlemlerin yerine getirilmesi gerekmektedir. E-noter kavramı ile satış sözleşmesi çevrim içi, adil ve elektronik olarak imzalanabilir. Bu yolla başta zaman ve özgürlük olmak üzere birçok şeyden tasarruf edilebilir. Yukarıda anlatılan ileri kriptoloji yapıtaşları ile güvenli protokoller tasarlanarak verimli çözümler sunulabilir.

4.4 E-seçim

UEKAE Dergisi 4. sayısında konu edilen e-seçim sistemlerinde anonimlik gibi sağlaması gereken birçok özellik vardır. Kriptografinin en zor uygulama alanlarından birisi olan internet üzerinden yapılacak seçimler için Kriptografi 1.0 yetersiz kalmaktadır. Bunun için, homomorfik şifreleme, kör imza, sır paylaşımı, karıştırıcı ağlar ve sıfır bilgi sızmalı kanıt protokolleri ileri düzey kriptografik yapı taşlarını kullanan birçok sistem önerilmiştir. Sonraki yazımızda dünyadaki internet tabanlı e-seçim uygulamalarını ve bu sistemlerdeki ileri kriptoloji yapıtaşlarının kullanımını daha detaylı inceleyeceğiz.

4.5 İz Bırakmadan Bilgiye Erişim ve Anonim Arama

Arama motorları veya açık veritabanları güncel bilgi edinmek için vazgeçilmez kaynaklardandır. Fakat bunlar, aynı zamanda mahremiyet için de büyük tehdit oluşturmaktadırlar. Meraklı bir veri tabanı operatörü yapılan işlerden, IP adresimizden veya yer bilgimizden bir şekilde kim olduğumuz konusunda fikir edinebilir. Diğer taraftan kapalı veritabanlarını kullanarak analizler yapılabilir veya sadece belirli bilgilere ulaşılması istenebilir. Örneğin, THY'nin bir uçağı başka bir ülkeye uçacak olsun. Bu ülkenin istihbarat birimleri uçaktakilerin terörist listesinde (gizli bir liste) yer alıp almadığını anlamak istemektedir. Çözüm olarak THY, uçakla gidecek bütün yolcuların bilgilerini onlara verebilir. Ancak bu yolla tüm yolcuların bilgileri verildiğinden bu bilgilerin başka amaçla kullanılıp kullanılmayacağı bilinemez. Bu problem de Kriptografi 2.0 yapıtaşları kullanılarak çözülebilir. Aynen arama motorlarında şifreli metnin aranması gibi şifreli terörist listesi şifreli yolcu listesi ile karşılaştırılarak sadece teröristlerin bulunduğu bir şifreli sonuç öğrenebilir. Bu yolla diğer yolcularının bilgileri saklı kalabilir.



Şekil 19. *Gezici Sistem Çantası ile şehir merkezinden uzak köylerde kimlik kartı başvurunun gerçekleştirilmesi.*

Başka bir örnek olarak A ve B şirketleri (örneğin bankaların) kendilerine ait müşterilerinin bilgilerini veritabanlarında saklıyor olsunlar. A ve B şirketleri bu verileri kullanarak ortak bazı analizler yapmak istemektedir. Ancak şirketler müşterilerine ait bilgilerin diğer şirketin eline geçmesini de istememektedirler. Bu tür problemlere de Kriptografi 2.0 yapıtaşları çözümler sunmuştur.

Genel olarak anonimliği sağlayarak bilgiye erişimi iki yönden ele alabiliriz. Birincisi kimliğimizin, ikincisi ise aradığımız bilginin gizlenmesidir.

Kimliğimizin saklanması için anonim ağlar kullanılabilmektedir. Bunun için yazımızda anlatılan karıştırıcı ağlar kullanılabilmektedir. Bu yöntemlerde vekil sunucular ve kriptografi kullanımıyla kullanıcı/verisi arasındaki ilişki yok edilmeye çalışılmaktadır. Aradığımız bilgi ile kimliğimiz arasındaki ilişkinin gizlenmesi pek çok açıdan önemlidir. Bu problem literatürde ilk kez 1996 yılında Chor, Goldreich, Kushilevitz ve Sudan tarafından dile getirilmiştir [23]. Basit fakat verimli olmayan yol kullanıcının veritabanındaki tüm verileri almasıdır. Böylelikle kullanıcının veritabanındaki hangi bilgi ile ilgilendiği anlaşılamayacaktır. Ancak bu şekilde şartsız güvenlik özelliği sağlanabilir. Literatürde hesaplama zorluğuna dayalı ve daha pratik kişiye özellik sağlayan arama metotları mevcuttur.

IBM'deki araştırmacıların keşfettikleri tam homomorfik asimetrik şifreleme algoritması, anonim aramaya başka bir anlam katmıştır. Bu teknik ile aramalarımız şifreli olarak arama motoruna gönderilecektir. Arama motoru şifreyi çözemeyecek fakat şifreleme algoritmasının homomorfik özelliğinden dolayı tüm işlemleri bu veri üzerinden yapabilecektir. Arama sonucu, sadece sizin açabileceğiniz şekilde şifreli olarak size gelecektir.

Tamamen anonim bir internet ortamı da istenmeyen bir şeydir. Özellikle devletler internetten işlenen suçları takip edebilmek için bazı bilgileri kaydetmektedir.

5. KAVRAMLAR SÖZLÜĞÜ

Şartsız Güvenlik (Information Theoretic Security): Sınırsız hesaplama gücüne sahip bir saldırgan tarafından bile kırılamayan kripto sistemleri için kullanılmaktadır [20]. Saldırganın sistemi kırmak için yeterince bilgiye sahip olmamasından dolayı bilgi kuramına dayalı güvenlik olarak da adlandırılmaktadır.

Şartsız güvenli kripto sistemleri çok uzun anahtar materyalinin üretimini ve dağıtımını gerektirdiği için pratikte kullanımları zordur. 1917 yılında Gilbert Vernam tarafından bulunan ve ismi ile anılan şifreleme sistemi de şartsız güvenli bir şifreleme sistemidir [21]. Vernam şifresinde mesajlar, mesaj uzunluğu kadar anahtar ile "dışlamalı ya da" (xor) yapılarak şifrelenmektedir. Anahtarlar rasgele üretilmeli ve her anahtar sadece bir kez kullanılmalıdır. Rus ajanlarının da bu sistemi kullandığı fakat aynı anahtarı birden fazla kullanmalarından dolayı şifrenin Amerikalılar tarafından çözüldüğü açık literatürde yer almaktadır [22].

Gelecekte sonsuz hesaplama yapan kuantum bilgisayarların çıkması bile bu güvenliğe sahip sistemlerin güvenliğine zarar veremeyecektir.

Hesaplama Zorluğuna Dayalı Güvenlik (Computational Security): Saldırganın sınırlı hesaplama gücüne sahip olduğu ve bu gücü kullanarak kripto sistemini makul bir sürede kıramayacağı varsayımı altında güvenli olan kripto sistemleri için kullanılmaktadır (çarpanlarına ayırma problemi, ayrık logaritma problemi vb.). RSA, ElGamal ve AES gibi birçok kripto algoritması hesaplama zorluğuna dayalı olarak güvenlidir. Anahtar üretim ve dağıtımının daha kolay olmasından dolayı bu tür kripto sistemleri tercih edilmektedirler. Sınırsız hesaplama yapan sistemlerin varlığı ile beraber bu sistemlerin güvenliği ortadan kalkacaktır.

KAYNAKÇA

[1] Handbook of Applied Cryptography.

http://www.cacr.math.uwaterloo.ca/hac/

[2] PKCS #1: RSA Cryptography Standard.

http://www.rsa.com/rsalabs/node.asp?id=2125

[3] Paillier cryptosystem.

http://en.wikipedia.org/wiki/Paillier_cryptosystem

[4] C.Gentry, S.Halevi, V.Vaikuntanathan Fully Homomorphic Encryption over the Integers. To appear at

EUROCRYPT'10. Craig Gentry. Fully homomorphic encryption using ideal lattices. STOC 2009: 169-178

http://domino.research.ibm.com/comm/research_projects.nsf/pages/security.homoenc.html

[5] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms," in Foundations of Secure Computation,pp. 169–177, Academic Press, 1978.

[6] http://en.wikipedia.org/wiki/Blind_signature

[7] David Chaum, Blind signatures for untraceable payments, Advances in Cryptology - Crypto '82, Springer-Verlag (1983), 199-203.

[8] Blakley, G. R. (1979). "Safeguarding cryptographic keys". Proceedings of the National Computer Conference 48: 313–317.

Shamir, Adi (1979). "How to share a secret". Communications of the ACM 22 (11): 612–613.

http://www.cs.tau.ac.il/~bchor/Shamir.html

http://www.rsa.com/rsalabs/node.asp?id=2259

[9] Michael O. Rabin: How to exchange Secrets with Oblivious Transfer, Technical Report TR-81 Harvard University: Aiken Computation Lab (1981).

[10] S. Even, O. Goldreich, and A. Lempel, "A Randomized Protocol for Signing Contracts", Communications of the ACM, Volume 28, Issue 6, pg. 637-647, 1985.

[11] Quisquater, J.J., L. Guillou, T. Berson, "How to Explain Zero-Knowledge Protocols to Your Children", Advances in Cryptology - CRYPTO '99, Lecture Notes in Computer Science 435, pp. 628-631, 1990.

[12] S. Goldwasser, S. Micali and C. Rackoff: The Knowledge Complexity of Interactive Proof Systems, SIAM J.Computing, Vol. 18, pp. 186-208, 1989. http://crypto.cs.mcgill.ca/~crepeau/COMP647/2007/TOPIC02/GMR89.pdf

[13] Identification with Zero Knowledge Protocols, SANS Institute InfoSec Reading Room.

[14] htt://en.wikipedia.org/wiki/Mix_network

[15] Andrew Chi-Chih Yao: Protocols for Secure Computations (Extended Abstract) FOCS 1982.

[16] Mehmet S. Kiraz. Secure and Fair Two-Party Computation. PhD Thesis, http://alexandria.tue.nl/extra2/200811317.pdf. Technical University of Eimdhoven, 2008.

[17] R. Cleve. Limits on the security of coin flips when half the processors are faulty. In STOC '86: Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing, pages 364-369. ACM Press, 1986.

[18] D. Boneh and M. Naor. Timed commitments. In Advances in Cryptology– Crypto 2000, volume 1880 of Lecture Notes in Computer Science, pages 236 254. Springer-Verlag, 2000.

[19] E. Elkind and H. Lipmaa. Interleaving Cryptography and Mechanism Design: The Case of Online Auctions. Financial Cryptography 2004.

[20] Unconditional Security, http://web.mit.edu/6.857/OldStuff/Fall98/www/lectures/unconditional.ps

Information Theoretic Security http://en.wikipedia.org/wiki/Information_theoretic_security

[21] Vernam, Gilbert S. Secret Signaling System. U.S. Patent 1,310,719. (Issued July 22, 1919).

[22] NSA. The VENONA Project. http://www.nsa.gov/about/_files/cryptologic_heritage/publications/coldwar/venona_story.pdf

[23] Benny Chor, Eyal Kushilevitz, Oded Goldreich, Madhu Sudan: Private Information Retrieval. J. ACM 45(6): 965-981 (1998)

[24] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 4(2), February 1981.

[25] Ivan Damgård Tomas Toft Trading Sugar Beet Quotas - Secure Multiparty Computation in Practice. 2008.

KURUMSAL YÖNETİM

Stratejik Yönetim

Suha ERSİN

Stratejik Yönetim uygulayabilmek için etkin “Kurumsal Yönetim”e sahip olunmalıdır. Bu nedenle, derginin Kurumsal Yönetim bölümlerinde bu sayıya kadar yayımlanmış olan yazılarda belirttiğimiz hususların, sağlanması ve uygulanması öncelikle düşünülmelidir.

TANIMLAR

Strateji Tanımı

Strateji : Hedefe varmak için izlenecek yol (sevkülçeyş)

Latince : stratum : yol, çizgi, nehir yatağı

Yunanca : stratos (ordu) + ago (yönetmek)

{yunanlı general "Strategos"a atıf (savunma taktikleri ile ünlü)}

Stratejik Plan

Kurum ve kuruluşların; kalkınma planları, programlar, ilgili mevzuat ve benimsedikleri temel ilkeler çerçevesinde geleceğe ilişkin misyon ve vizyonlarını oluşturmak, stratejik amaçlar ve ölçülebilir hedefler saptamak, performanslarını önceden belirlenmiş olan göstergeler doğrultusunda ölçmek ve bu sürecin izleme ve değerlendirmesini yapmak amacıyla katılımcı yöntemlerle hazırladıkları plan dokümanıdır. Gelecek 5 (beş) yıl için hazırlanır.

Performans Programı

"Kurum ve kuruluşların bir mali yılda stratejik planı doğrultusunda yürütmesi gereken faaliyetleri, bu faaliyetlerin kaynak ihtiyacını, performans hedef ve göstergelerini içeren, idare bütçesi ve idare faaliyet raporunun hazırlanmasına esas teşkil eden programdır." Gelecek 1 (bir) yıl için hazırlanır.

Faaliyet Raporu

"Stratejik plan ve performans programları uyarınca yürütülen faaliyetleri, belirlenmiş performans göstergelerine göre hedef ve gerçekleşme durumu ile meydana gelen sapmaların nedenlerini açıklayan, kurum ve kuruluş hakkındaki genel ve mali bilgileri içeren rapordur." Geçmiş 1 (bir) yıl için hazırlanır.

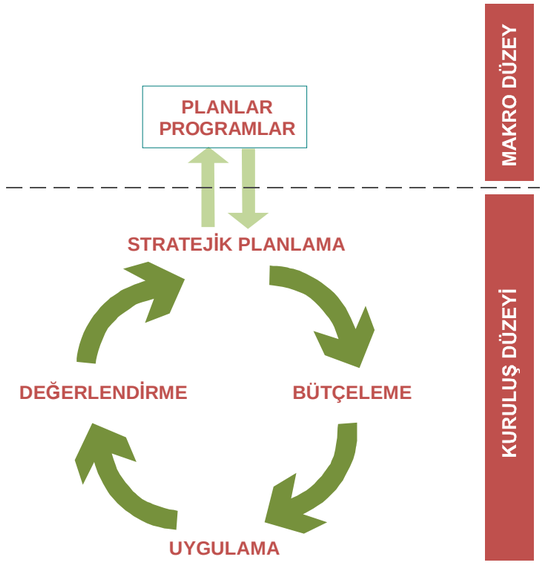
Performans Değerlendirmesi

"Kurum ve kuruluşların belirlediği stratejik amaç ve hedeflere ulaşmak için izlediği yolun, performans hedeflerine ulaşmak üzere kullanılan yöntemlerin, yürütülen faaliyet ve projeler ile bunların sonucunda elde edilen çıktı ve sonuçların değerlendirilmesidir." Bir başka ifadeyle, "Neredeyiz ?. Ne Durumdayız ?." sorularının cevaplarını bulmak amacıyla yapılan çalışmalardır.

Değerlendirme Yöntemleri: Anket, Görüşme, Toplantı, Gözlem, Durum Analizi (Bkz. ÖGE-3. PERFORMANS ÖLÇME, İZLEME VE DEĞERLENDİRME Bölümü), Denetim Sonuçları

STRATEJİK PLANLAMA İLE MAKRO PLANLAMA İLİŞKİSİ

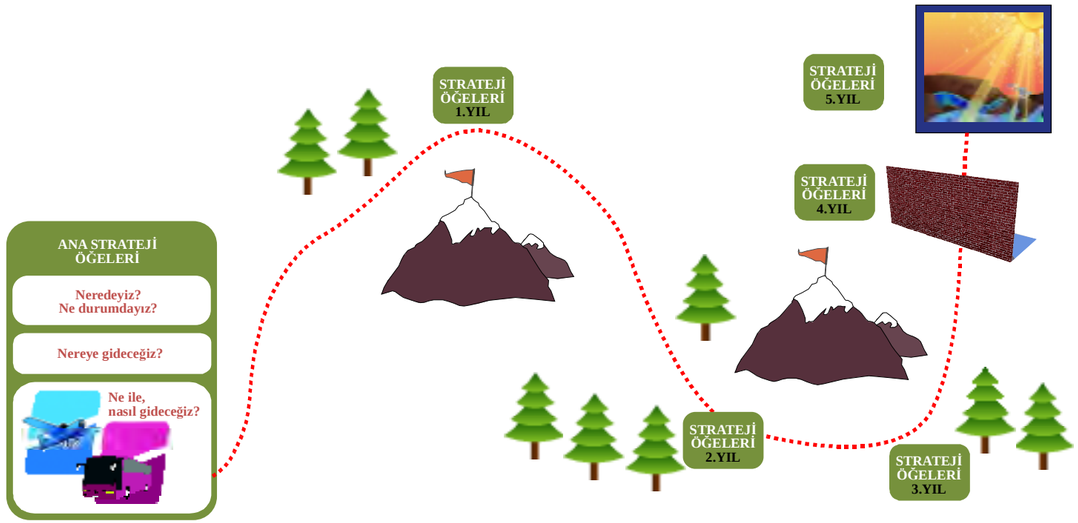
Burada "Makro Planlama (Düzey)" ile anlatılmak istenen, Hükümet Politikaları, Kalkınma Plan ve Programları, Orta Vadeli Program ve Orta Vadeli Mali Plan, AB politika ve programları, Sektörel üst kurumların programları, strateji oluşturan diğer kuruluşlarının programları, vb., stratejik planlama faaliyetleri ile doğrudan ilişkili olan kurum/kuruluş düzeyinin üzerindeki veya dış çevresindeki çalışmalardır.



Makro düzey yani kurum dışı çevreler; Politik, Ekonomik, Sosyal, Teknolojik ve Sektörel olarak, hem ülke temelinde ve hem de dünya genelinde sınıflanır.

Ülke ve dünyadaki genel eğilimler, itici güçler, değişimler dikkate alınmalı ve kuruluş düzeyine indirgenmelidir (Bkz. ÖGE-1. GZFT, PESTS ANALİZİ Bölümü).

STRATEJİK YÖNETİM ÖGELERİ İLE STRATEJİK PLANLAMA



STRATEJİK YÖNETİM ÖGELERİ		
>> Plan ve Programlar >> Paydaş Analizi >> GZFT (SWOT) Analizi >> PESTS (Çevre) Analizi	DURUM ANALİZİ	*Başarımızı Nasıl Takip Eder ve Değerlendiririz?* **Neredeyiz? Ne Durumdayız?**
>> Raporlama >> Karşılaştırma, Kıyaslama	İZLEME	
>> Geri Besleme >> Ölçme Yöntemlerinin Belirlenmesi >> Kurumsal Performans Göstergeleri >> İlerleme ve Sonuçların Değerlendirilmesi (Fark Analizi)	KURUMSAL PERFORMANS ÖLÇME VE DEĞERLENDİRME	
>> Kuruluşun Varoluş Gerekçesi >> Temel İlkeler	MİSYON VE İLKELER	*Nereye Ulaşmak İstiyoruz?* **Nereye Gideceğiz?**
>> Arzu Edilen Gelecek, Ülkü	VİZYON (ÜLKÜ)	
>> Ulaşılmak İstenen Amaçlar >> Açık, Somut ve Ölçülebilir Hedefler	STRATEJİK AMAÇLAR VE HEDEFLER	
>> Amaç ve Hedeflere Ulaşma Yöntemleri (Ürün, Teknoloji, Pazar vb. Stratejiler)	STRATEJİLER (ALT STRATEJİK AMAÇLAR)	*Gitmek İstediğimiz Yere Nasıl Gideceğiz?* **Ne ile Gideceğiz? Nasıl Gideceğiz?**
>> Ayrıntılı İş Planları >> Maliyetlendirme >> Performans Programı >> Bütçeleme	FAALİYETLER, PROJELER VEYA EYLEMLER	

Öncelikle kurumun vizyon, misyon, temel değerleri (ilkeleri) ile stratejik amaç ve hedefleri belirlenir. Bu amaçla geniş bir katılımın sağlandığı bir veya iki haftalık kesintisiz çalışmalar yapmak en verimli olanıdır. Bu çalışmalara başlarken, kurumun mevcut organizasyon ve süreç yapısı ile kurumsal performans değerleri hakkında katılımcıların bilgilendirilmesi, daha hızlı ve anlamlı sonuçlar elde etmek için faydalı olacaktır. Vizyon doğrultusunda hedeflenen "Kurum Kültürü"nün oluşturulması amacıyla, öncelikle kurum kültürünü belirleyici çalışmalar yapılmalı, ortaya çıkan verilerden yararlanarak gerekli dönüşüm faaliyetleri yürürlüğe konulmalıdır.

Bu çalışmalara üst yönetimin doğrudan katılması verilen önemin ifadesi olarak gereklidir. Diğer taraftan, kurumun/birimin stratejik amaç ve hedefleri, çalışanların performans değerlendirmelerine kadar indirgenerek bütünlük sağlanmalı, performans hedefleri ile ilgili ödüllendirme yapılmalıdır.

İlgili Stratejik Yönetim dokümanlarının (Stratejik Plan, Performans Programı ve Faaliyet Raporu) hazırlanması amacıyla Stratejik Yönetim Ögelerinin belirlenmesi çalışmaları, sorumlu Stratejik Yönetim/Planlama birimi eş güdümünde yapılır. Bu çalışmalar her yıl tekrarlanan bir şekilde sürdürülür. Faaliyetlerin zamanlaması ilgili dokümanların yılın ilk yarısı içinde tamamlanacağı varsayılarak planlanır.

Tablo 1. Ana ve alt strateji ögeleri.

ANA VE ALT STRATEJİ ÖGELERİ
Neredeyiz? Ne Durumdayız?
DURUM ANALİZİ, İZLEME, PERFORMANS ÖLÇME VE DEĞERLENDİRME
>> Öge-1 : GZFT (SWOT), PESTS (Çevre) Analizleri >> Öge-2 : Faaliyet Alanları, Ürün ve Hizmetler >> Öge-3 : Performans Ölçme, İzleme ve Değerlendirme
Nereye Gideceğiz?
MİSYON VE İLKELER, VİZYON, AMAÇ VE HEDEFLER
>> Öge-4 : Birim Stratejik Amaçları >> Öge-5 : Birim Stratejik Hedefleri >> Öge-6 : Birim Performans Ölçüleri >> Öge-7 : Süreç Performans Ölçüleri
Ne ile Gideceğiz? Nasıl Gideceğiz?
STRATEJİLER, FAALİYETLER, PROJELER VEYA EYLEMLER
>> Öge-8 : Birim Eylemleri (Projeler, Faaliyetler) >> Öge-9 : Birim Eylemleri için Kaynak İhtiyacı

Stratejik Yönetim Ögelerinin kurum içinde geniş bir katılım ile belirlenmesi, çalışanların yönetime katılması suretiyle kuruma bağlılıklarını arttıracağı için, dikey organizasyon temelinde de alt kurullar (üst ve alt "Strateji Geliştirme Kurul"ları) kurulması ve/veya her seviyeden çalışan ile toplantılar yapılması uygun olur.

Stratejik Yönetim/Planlama Birimi, ilgili alt Birimlerden temin ettiği Stratejik Yönetim Ögelerini (alt strateji ögeleri olarak) birleştirir ve ortaya çıkan Stratejik Plan dokümanını onaylanmak üzere üst yönetime (üst yönetici ve/veya yönetim kurulu) sunar. Üst yönetimin onayladığı Stratejik Plan dokümanı yayımlanarak (gerekiyorsa üst makama gönderilerek) uygulama başlatılır.

Ana ve alt strateji ögeleri Tablo.1'de gösterilmiştir.

ALT STRATEJİ ÖGELERİ

ÖGE-1. GZFT, PESTS ANALİZİ

• Stratejik Yönetim anlayışı doğrultusunda uygulanan GZFT (Güçlü, Zayıf Yanlar, Fırsat ve Tehditler Analizi- SWOT) analizi; kurumun zayıf ve güçlü yönleriyle, karşı karşıya bulunduğu fırsatların ve tehditlerin detaylı olarak irdelenmesine yardımcı olan araçlardan biridir.

• Kurumsal risk yönetimi kapsamında yürütülen faaliyetlerin ve/veya uygulama araçlarının çıktılarından da yararlanılır.

• Kurum çevre analizinde (Politik, Ekonomik, Sosyal, Teknolojik ve Sektörel Çevre Analizi- PESTS), rakiplerinin durumunu, sektörün durumunu ve makro çevrede oluşan değişimleri inceler.

• Çevre analizi yapılırken çevresel faktörlerin kuruluş için ne gibi fırsatlar ve tehditler ortaya koyduğu incelenir. Çevre analizinde; dünyadaki genel eğilimler, Türkiye'de kurumun faaliyet gösterdiği ortamdaki değişimler, kalkınma planları ve programlar, hükümet programları ve varsa istikrar programları ile diğer kuruluşların ve kesimlerin durumu ve özellikle kuruluşun hizmet ettiği hedef kitlenin beklentileri dikkate alınır.

• Çevre analizinde, öncelikle Türkiye ve dünyadaki temel eğilimler, her bir çevre kapsamında belirlenir. Sonra bu temel eğilimler, gerçekleşme ihtimali ve etki ağırlıkları dikkate alınarak değerlendirilir.

ÖGE-2. FAALİYET ALANLARI, ÜRÜN VE HİZMETLER

• Kurumun hizmet verdiği faaliyet alanları dikkate alınır.

• Kuruluş amacı ve misyonu ile bağlantılı olmalıdır.

• Kurumun müşterilerine sunduğu ürün ve hizmetleri gösterir.

• Faaliyet alanları kapsamında ürünler ve müşteriler arasındaki ilişkilerde tanımlanır.

ÖGE-3. PERFORMANS ÖLÇME, İZLEME VE DEĞERLENDİRME

• Performans ölçümü, performans ölçüleri (göstergeleri) kullanılarak kurumun uygulama (iş) sonuçlarının ölçülmesidir. Bu amaçla; "Kurumsal Performans Bilgi Sistemi" oluşturulmalı, performans göstergelerine ait verilerin girişi, güncellemesi ve analizi bu sistem ile bütünleşik bir şekilde yapılmalıdır.

• Performans ölçümü ve değerlendirmesi; misyon, vizyon, stratejik amaç ve hedeflerle ilişkili olarak belirlenmiş olan performans ölçülerine ait gerçekleşen sonuçların, izlenmesi ve hedeflere göre kıyaslamasının yapılmasıdır.

• Performans değerlendirmesi kapsamında yapılan kıyaslama, "Fark Analizi" olarak da düşünülebilir. Fark Analizi her bir Kurumsal performans göstergesi (ölçüsü) bazında yapılır ve gelecek yıllardaki hedeflerin belirlenmesinde önemli yer tutar. Performans göstergelerindeki sapmalar (Fark Analizi) üst yönetim tarafından yakından izlenmeli ve gerekli önlemler zamanında alınmalıdır.

• Kurumsal Performans ölçülerinin izleme sıklığı bir yıl olarak tanımlanmış olmasına rağmen, Bilgi Sistemleri alt yapısının sağladığı olanaklar çerçevesinde daha kısa sürelerle de yapılabilir.

ÖGE-4. BİRİM STRATEJİK AMAÇLARI

• Belirli bir zaman diliminde Birimin ulaşmayı hedeflediği sonuçlardır.

• Açık ve net olarak ifade edilmiş stratejik amaçlar etkilidir.

• Stratejik amaçlar, Kurum ve birim faaliyetlerini, etkinliğini daha ileri götürecek nitelikte olmalı ve aynı zamanda ulaşılabilir bir özellik taşımalıdır.

• Birimin stratejik amaçları, gerçekleştiğinde Birim için mevcut duruma göre fark yaratacak ve bir şeyleri değiştirecek nitelikte tanımlanmalıdır. Birimin diğer amaçlarından daha anlamlı ve önemli olmalıdır.

• Vizyona giderken geçilecek istasyonları ifade eden sözler olabilir.

• Stratejik amaçlar kolaylıkla anlaşılır, genel ifadeler olmalıdır. Çok detaylı olmamalı, teknik bilgiler içermesinden mümkün olduğunca kaçınılmalıdır.

• Gerçekleşen bir önceki yılın faaliyet ve performans bilgilerinden yararlanılmalı ve gerekiyorsa güncellenmelidir.

ÖGE-5. BİRİM STRATEJİK HEDEFLERİ

• Stratejik hedef, stratejik amaçların gerçekleştirilebilmesi için ortaya konan ölçülebilir somut ve orta vadeli alt amaçlardır.

• Stratejik hedefler; stratejik amaçlarda belirtilen genel hedefleri değerlendirmede kullanılacak nicel performans göstergelerini tanımlayabilmek için belirlenecek ayrıntılı alt amaçlardır.

• Bir stratejik amaca yönelik birden fazla hedef belirlenebilir. Önemli olan amaca ulaşmayı sağlayacak hedeflerin tam ve doğru olması, anlamsız hedeflere yer verilmemesidir.

• Stratejik hedef sonuçları, Birimin çıktılarına dönük ve belirli bir süre sonunda ulaşılacak değerlerdir.

• Miktar, maliyet, kalite, zaman, verimlilik ve etkinlik boyutları göz önünde tutulmalıdır.

• Gerçekleşen bir önceki yılın faaliyet ve performans bilgilerinden yararlanılmalı ve gerekiyorsa güncellenmelidir.

ÖGE-6. BİRİM PERFORMANS ÖLÇÜLERİ (GÖSTERGELERİ)

• Birim performans ölçüleri (göstergeleri), Birim stratejik hedeflerinin performanslarını gösteren nicel değerlerdir.

• Birimin stratejik amaç ve hedefleriyle ilişkili olarak belirlenir.

• Birim Performans ölçüleri; Miktar, maliyet, kalite, zaman, verimlilik ve etkinlik ölçütleri temelinde belirlenir.

• Amaca ulaşmayı sağlayacak performans göstergeleri tam ve doğru olmalı, anlamsız performans göstergeleri yenilenmelidir.

• Birim/süreç bazındaki performans göstergeleri ile proje kapsamındaki dokümanlarda belirtilen proje göstergeleri arasında tutarlılık olmalıdır.

• Gerçekleşen bir önceki yılın faaliyet ve performans bilgilerinden yararlanılmalı ve gerekiyorsa güncellenmelidir.

ÖGE-7. SÜREÇ PERFORMANS ÖLÇÜLERİ (GÖSTERGELERİ)

• Süreç performans ölçüleri (göstergeleri), Birimin alt süreçlerine ait stratejik hedeflerin performanslarını gösteren nicel değerlerdir.

• Birimin stratejik amaç ve hedefleriyle ilişkili olarak belirlenir.

• Süreç Performans ölçüleri; Miktar, maliyet, kalite, zaman, verimlilik ve etkinlik ölçütleri temelinde belirlenir.

• Amaca ulaşmayı sağlayacak performans göstergeleri tam ve doğru olmalı, anlamsız

performans göstergeleri yenilenmelidir.

• Birim/süreç bazındaki performans göstergeleri ile proje kapsamındaki dokümanlarda belirtilen proje göstergeleri arasında tutarlılık olmalıdır.

• Gerçekleşen bir önceki yılın faaliyet ve performans bilgilerinden yararlanılmalı ve gerekiyorsa güncellenmelidir.

ÖGE-8. BİRİM EYLEMLERİ (PROJELERİ, FAALİYETLERİ)

• Stratejik amaçların hedeflere uygun şekilde gerçekleşebilmesi için uygulanması gereken faaliyetler veya projelerdir.

• Faaliyetler veya projeler, Stratejik amaç ve hedefler ile performans ölçülerine "Nasıl" ulaşılacağını gösterir.

• Faaliyet veya projeler oluşturulurken başka faaliyet ve projelerle çakışmamasına, yetki ve sorumlulukların açık olarak belirlenmesine dikkat edilmelidir. Bu kapsamda performans yönetimi ve hesap verebilirlik açısından faaliyet ve proje sorumlularının belirlenmesi gereklidir.

• Her stratejik amaca yönelik faaliyetlerin ortaya konması ve buna göre sınıflandırılması sağlanmalıdır. Böylece her bir stratejik amaca yönelik hedefler ve alt faaliyetleri açıklanmış olacaktır.

• Stratejik amaçlar ve projeler arasında tutarlılık sağlanmalıdır.

ÖGE-9. BİRİM EYLEMLERİ İÇİN KAYNAK İHTİYACI

• Kaynak ihtiyacının belirlenmesi faaliyet ve proje maliyetlerinin tespiti ile başlar. Bir performans hedefine ilişkin faaliyet ve proje maliyetlerinin toplamı performans hedefinin maliyetini, bir stratejik amaç ve hedefe ilişkin performans hedeflerinin maliyetlerinin toplamı ise ilgili amaç ve hedefe ulaşmanın maliyetini gösterir.

• Faaliyetlerin maliyet yapısının analizi, planların oluşturulmasına, süreçlerin kontrolüne ve stratejik kararların alınmasına yardımcı olur. Bu analizin sağlıklı bir şekilde yapılabilmesi için, faaliyetlerin hangi tür maliyetleri ortaya

çıkardığı, bu maliyetlerin özellikleri, faaliyet düzeyiyle ilişkileri, iş süreçleriyle etkileşimi, girdi fiyatlarının yapısı, alternatif girdilerin varlığı gibi hususların değerlendirilmesi gerekir.

• Faaliyetler analiz edilirken alternatif maliyetler de göz önünde bulundurmalıdır. Ayrıca, maliyet yapısının analizinde, iş süreç analizleri yapılarak faaliyetlerin, en hızlı şekilde ve en düşük maliyetle yapılması sağlanmalıdır.

• Gerçekleşen bir önceki yılın faaliyet ve performans bilgilerinden yararlanılmalıdır.

• Sorumlu birim ve proje yöneticileri tarafından talep edilen kaynak ihtiyaçları ile onlara sunulan bütçe değerleri arasında uyumsuzluk olmamalıdır. Üst yönetim planlama doğruluğunu sağlamak amacıyla, planlama ve gerçekleşme arasındaki farkları izlemeli, birim/proje yöneticilerinin performans değerlendirmelerinde kullanmalıdır.

• Birim/proje yöneticileri tarafından tüm kaynak harcamalarını (üretim ve tüketim (cari) kavramı çerçevesinde; işgücü, genel gider, malzeme harcamaları) kapsayacak şekilde planlanmalıdır.

KAMU KURUMLARINI BAĞLAYICI YASAL GEREKÇELER

5018 Sayılı Kanun Madde 9 : STRATEJİK PLANLAMA VE PERFORMANS ESASLI BÜTÇELEME

• Kamu idareleri; kalkınma planları, programlar, ilgili mevzuat ve benimsedikleri temel ilkeler çerçevesinde geleceğe ilişkin misyon ve vizyonlarını oluşturmak, stratejik amaçlar ve ölçülebilir hedefler saptamak, performanslarını önceden belirlenmiş olan göstergeler doğrultusunda ölçmek ve bu sürecin izleme ve değerlendirmesini yapmak amacıyla katılımcı yöntemlerle stratejik plan hazırlarlar.

• Kamu idareleri, kamu hizmetlerinin istenilen düzeyde ve kalitede sunulabilmesi için bütçeleri ile program ve proje bazında kaynak tahsislerini; stratejik planlarına, yıllık amaç ve hedefleri ile performans göstergelerine dayandırmak zorundadırlar.

• Stratejik plan hazırlamakla yükümlü olacak kamu idarelerinin ve stratejik planlama sürecine ilişkin takvimin tespitine, stratejik planların kalkınma planı ve programlarla ilişkilendirilmesine yönelik usul ve esasların belirlenmesine Devlet Planlama Teşkilatı Müsteşarlığı yetkilidir.

• Kamu idareleri bütçelerini, stratejik planlarında yer alan misyon, vizyon, stratejik amaç ve hedeflerle uyumlu ve performans esasına dayalı olarak hazırlarlar. Kamu idarelerinin bütçelerinin stratejik planlarda belirlenen performans göstergelerine uygunluğu ve idarelerin bu çerçevede yürütecekleri faaliyetler ile performans esaslı bütçelemeye ilişkin diğer hususları belirlemeye Maliye Bakanlığı yetkilidir.

• Maliye Bakanlığı, Devlet Planlama Teşkilatı Müsteşarlığı ve ilgili kamu idaresi tarafından birlikte tespit edilecek olan performans göstergeleri, kuruluşların bütçelerinde yer alır. Performans denetimleri bu göstergeler çerçevesinde gerçekleştirilir.

5018 Sayılı Kanun Madde 41 : FAALİYET RAPORLARI

• Üst yöneticiler ve bütçeyle ödenek tahsis edilen harcama yetkilileri tarafından idari sorumlulukları çerçevesinde her yıl faaliyet raporları düzenlenir. Bu raporlar, stratejik planlama ve performans programları uyarınca yürütülen faaliyetleri, belirlenmiş performans göstergelerine göre hedef ve gerçekleşme durumu ile meydana gelen sapmaların nedenlerini açıklayacak şekilde hazırlanır.

26 Mayıs 2006 Tarihli Yönetmelik:KAMU İDARELERİNDE STRATEJİK PLANLAMAYA İLİŞKİN USUL VE ESASLAR HAKKINDA YÖNETMELİK

• **Genel İlkeler**

Madde 5 –

(1) Stratejik planlama sürecinde;

b) Çalışmalar, strateji geliştirme biriminin koordinatörlüğünde tüm birimlerin katılım ve katkılarıyla yürütülür.

c) Stratejik planların doğrudan doğruya kamu idarelerince ve idarelerin kendi çalışanları tarafından hazırlanması zorunludur.

• **Stratejik planların süresi, güncelleştirilmesi ve yenilenmesi**

Madde 7 –

(1) Stratejik planlar beş yıllık dönemi kapsar.

(2) Stratejik planlar en az iki yıl uygulandıktan sonra stratejik planın kalan süresi için güncelleştirilebilir. Güncelleştirme, stratejik planın misyon, vizyon ve amaçları değiştirilmeden, hedeflerde yapılan nicel değişikliklerdir.

• **Plan ve programlarla ilişki**

Madde 12 –

(1) Kamu idarelerinin stratejik planları, kalkınma planı, orta vadeli program ve faaliyet alanı ile ilgili diğer ulusal, bölgesel ve sektörel plan ve programlara uygun olarak hazırlanır.

(2) Kamu idareleri, stratejik planlarını hazırlarken orta vadeli programda yer alan amaç, politikalar ve makro büyüklükler ile orta vadeli malî planda belirlenen teklif tavanlarını dikkate alarak yıllar itibarıyla amaç ve hedefler bazında kaynak dağılım tahmininde bulunur.

• **Performans programı**

Madde 16 –

(1) Performans programları, stratejik planların yıllık uygulama dilimlerini oluşturur. Kamu idareleri performans programlarını stratejik planlarına uygun olarak Maliye Bakanlığınca belirlenen usul ve esaslar çerçevesinde hazırlar.

(2) Bütçeler performans programına uygun olarak hazırlanır.

DEĞERLENDİRME

Sonuç olarak: Kurum ve kuruluşların üst yöneticileri; doğru yöne gittiklerini bilmek ve hedeflerine zamanında ulaşabilmek amacıyla, stratejik yönetim ögelerine önem vermeli ve çok yakından izlemelidir.

Ayrıca :

• Üst yönetim tarafından **önem**i anlaşılmalı,

• Üst ve alt "Strateji Geliştirme Kurul"ları oluşturularak, **geniş katılım** sağlanmalı,

• Kurumsal Performans **Bilgi Sistemi** oluşturulmalı,

• Amaca ulaşmayı sağlayacak performans göstergeleri **tam ve doğru olma**lı,

• Stratejik amaçlar ve projeler arasında **tutarlılık** sağlanmalı,

• Birim/süreç bazındaki performans göstergeleri ile proje göstergeleri arasında **tutarlılık** olmalı,

• Anlamsız performans göstergeleri **yenilenme**li,

• Performans göstergelerindeki sapmalar (Fark Analizi) izlenmeli ve gerekli **önlemler alınmalı**,

• Belirlenen kaynak ihtiyaçları ile bütçe değerleri arasında **uyumsuzluk olmama**lı,

• Kurumun/birimin stratejik amaç ve hedefleri, çalışanların **performans değerlendirmeleri**nde yer almalı,

• Vizyon doğrultusunda hedeflenen "**Kurum Kültürü**" oluşturulmalı,

• Performans hedefleriyle ilişkili **ödül sistemi** kurulmalı,

• Stratejik Yönetim uygulayabilmek için etkin "**Kurumsal Yönetim**"e sahip olunmalıdır.

Bir geminin kaptan köşkündeki göstergeler tam ve doğru değil ise hedeflenen limana zamanında ulaşması zordur.

Radar Antenleri – V: Faz Dizili Antenler – Besleme, Uygulama ve Gelişim Yönü

Bahattin TÜRETKEN, Koray SÜRMELİ, Aziz U. ÇALIŞKAN

Özet - *Bu çalışmada faz dizili antenlerin besleme yapılarından, verici/alıcı birimlerinden, SiGe ve* LDMOS *teknolojilerinden, son teknoloji uygulamalarından ve faz dizili antenlerin gelişim yönünden bahsedilecektir.*

Anahtar Sözcükler - *Aktif diziler, verici/alıcı birimleri, dizi besleme yapıları, faz dizili antenler, faz kaydırıcılar, pasif diziler, radar.*

1 GİRİŞ

Faz dizili antenlerin elektriksel mimarisi, fiziksel yapıları, dizi anten kuramı, doğrusal dizi yapıları, elektronik hüzme tarama/yönlendirme, düzlemsel diziler, özdirenç ve kuplaj ve ızgara kulakçıklar ile ilgili incelemeler bir önceki sayımızda "Radar Antenleri – IV: Faz Dizili Anten Kuramına Genel Bakış" adlı makale ile ayrıntılı olarak anlatılmış ve örnek uygulamalar verilmişti [1], [2]. Bu çalışmada ise, besleme yapıları, verici/alıcı birimleri, SiGe/GaN teknolojileri ve teknolojik gidişattan bahsedilecektir.

Faz dizili antenler; besleme devreleri, verici/alıcı birimleri ve bu birimleri kontrol eden merkezi kontrol biriminden oluşmaktadır.

2 BESLEME DEVRELERİ

Besleme devreleri, anten elemanlarının genlik ve faz değerlerini oluşturmak için kullanılan yapılardır. Bu yapılar ile beslenen dizi elemanları sayesinde istenilen hüzme yapısı oluşturulmaktadır.

Bir dizi içerisindeki anten elemanları çeşitli yöntemlerle beslenebilir. Bu yöntemler sınırlı (*constrained*) ve serbest (*unconstrained*) olmak üzere iki temel grupta toplanırlar [3], [4].

Sınırlı besleme durumunda mikrodalga enerjisi anten elemanlarına iletim hatları ve güç bölücüler aracılığıyla dağıtılır. Bu besleme yapısı ile hem doğrusal hem de düzlemsel diziler beslenebilir. Serbest beslemede ise enerji geometrik ve fiziksel optik ilkeleri kullanılarak bir iletim ortamı veya serbest uzay içerisinden dağıtılır.

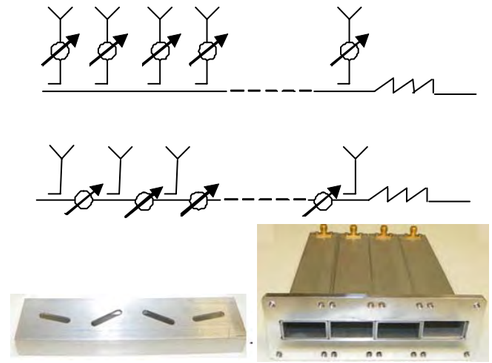
Sınırlı besleme; ağ besleme, çoklu hüzme (*multibeam*) ve mercekler olmak üzere üç büyük gruba ayrılır.

2.1 Ağ Besleme

Ağ besleme (*network feed*) seri ve paralel besleme olmak üzere iki sınıfa ayrılır. Her iki grupta da besleme yapıları hem bir "kalem hüzme" hem de tek darbe (*monopulse*) toplam ve fark ışıma diyagramları sağlayacak biçimde tasarlanır.

2.1.1 Seri Besleme

Seri besleme art arda bağlanmış jonksiyonlardan oluşur. Öyle ki, birinci çıkış ucuna (*port*) gelen enerji bir jonksiyondan, ikinci çıkış ucuna gelen enerji iki jonksiyondan ve benzer biçimde, son çıkış ucuna gelen enerji tüm jonksiyonlardan geçer. Şekil 1'de örnek besleme yapıları gösterilmiştir.



Şekil 1. *Seri besleme.*

Hüzmeyi yönlendirmek için fazörler ışıma elemanlarını besleyen her bir dala yerleştirilir. Genlik besleme yapısı jonksiyonlarda bağlaştırıcıların (*coupler*) uygun şekilde tasarlanmasıyla elde edilir.

Seri besleme yapılarının üretimi ve montajı kolaydır. Ayrıca, seri besleme yapıları çok düşük kayba ve mükemmel

güç bölme özelliğine sahiptir. Her bir bağlaştırıcının ayrı ayrı tasarlanması ve yönelme açısının frekansa bağlılığı, bu besleme yapısının dezavantajlarını oluşturur.

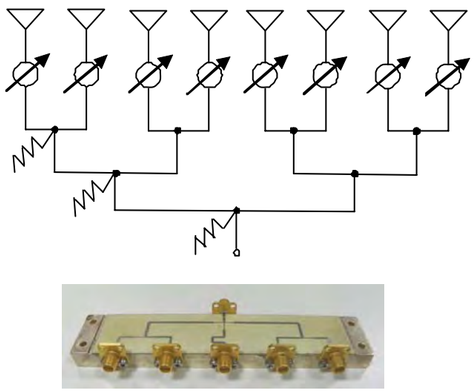
Tek darbe toplam ve fark ışıma diyagramları dizinin ortasından beslenmesiyle elde edilebilir. Toplam ve fark ışıma diyagramlarını elde edebilmek için iki ayrı besleme hattı kullanılır. Bu hatlar bir ağ içerisinde birleştirilir [5]. Genlik dağılımlarının bağımsız olarak kontrol edilebilmesi mümkündür. Seri besleme yapısının bant genişliği yol uzunluklarını eşit yaparak artırılabilir. Ancak bant genişliği fazörler ve bağlaştırıcılar tarafından sınırlandırılmış ise, bu yöntem çok az yarar sağlar. Yol farkı olmadığında hüzme yönlendirme hesaplamalarını yapmak daha kolaydır.

2.1.2 Paralel Besleme

Paralel besleme yapısında giriş ucundan her bir elemana kadar tekrarlı jonksiyonlar kullanılır. Böylece giriş ucundan her bir elemana kadar olan elektriksel yol uzunlukları birbirine eşit olur. Örnek bir besleme yapısı Şekil 2'de gösterilmiştir. Genellikle paralel besleme, çift sayıda elemana sahip dizilerde kullanılır ve eleman sayısının bir eksiği kadar da jonksiyona gerek duyulur.

Paralel bir beslemede, eş genlikli bir besleme dağılımı için bütün güç bölücülerin aynı olması gerekmektedir. Aksi halde, eşit olmayan güç bölücülere gerek vardır.

Pasif faz dizili antenlerde besleme ağlarının düşük kayıplı olması istendiğinden, genellikle dalga kılavuzları kullanılır. Aktif faz dizili antenlerde ise, besleme ağındaki bir miktar kayıp kabul edilebilir ve şerit hatlı yapılar kullanılır. Böylece dizinin ağırlığı, maliyeti ve kalınlığı azaltılabilir.



Şekil 2. *Paralel besleme.*

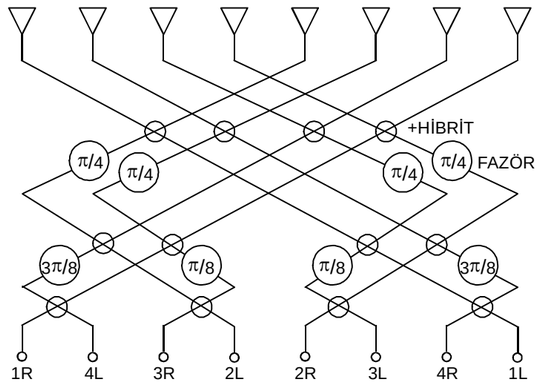
Paralel besleme yapısında, dizinin merkezine göre simetrik olarak yerleştirilen bir eleman çiftinden alınan işaretler, toplam ve fark işaretleri oluşturabilmek amacıyla sihirli T (*magic T*) içerisinde birleştirilirler. Dizi açıklığı boyunca bütün eleman çiftlerinden alınan toplam işaretler, daha sonra bir güç birleştirici ağ içerisinde birleştirilerek toplam ışıma diyagramı elde edilir. Toplam ışıma diyagramı için istenilen genlik dağılımı güç birleştirme ağı içerisinde işaretlerin uygun şekilde ağırlıklandırılması ile elde edilir. Bütün eleman çiftlerinden alınan fark işaretleri, ayrı bir güç birleştirici ağ içinde birleştirilerek fark ışıma diyagramı elde edilir. Hem toplam hem de fark ışıma diyagramları için düşük yan kulakçık düzeyleri elde edebilmek amacıyla, iki birleştirme ağı içerisindeki genlik dağılımlarının farklı oluşturulması gerekir. Böylece toplam ve fark ışıma diyagramlarının bağımsız olarak kontrol edilebilmesi mümkün olabilmektedir.

2.2 Çoklu Hüzme Besleme

Faz dizili antenler için bir diğer sınırlı besleme yapısı, çoklu hüzme biçimlendirme devrelerinden oluşur. Bu tür besleme devreleri ile geniş bir bölgeyi kapsayan eş zamanlı çoklu hüzmeler oluşturulabilir. Her bir hüzme eşit kazanca ve şekle sahiptir.

2.2.1 *Butler* Matrisi

Butler matrisi yaygın bir biçimde kullanılan çoklu hüzme besleme ağ yapısıdır. Hüzme uçlarının sayısı eleman uçlarının sayısına eşittir. Bağlantı iletim hatları birbirlerine 90° melezler (*hybrid*) kullanılarak bağlanırlar. Sabit faz birimleri her bir hüzme için uygun fazı sağlar. Eğer faz birimleri eşdeğer zaman geciktirme birimleri ile



Şekil 3. *Butler matrisi.*

değiştirilirse bant genişliği azalır (Şekil 3).

Hüzme giriş uçlarının herhangi birinden sürülen işaret bütün ışıma elemanlarını eş genlikle besler. Işıma elemanlarının faz farkları ise $180^{\circ}/N$ değerinin tek katı olacak biçimde değişir. Burada N ışıma elemanlarının toplam sayısıdır. Eş genlikli besleme dağılımı olduğu için oluşan dizi ışıma diyagramları $\sin(Nx)/\sin(x)$ biçimindedir. Her bir hüzmenin tepe noktası diğer hüzmelerin sıfır noktalarına yerleştirilir. Bu hüzmeler birbirlerine dik olduğu için hüzmeler arasında çapraz kuplaj kaybı yoktur. Frekans değiştiğinde hüzmelerin hüzme genişlikleri değişmezken konumları değişir.

2.3 Mercekler

2.3.1 *Rotman* Mercekleri

Rotman mercekleri paralel levha dalga kılavuzları, şerit hat veya mikroşerit gibi iki boyutlu dalga kılavuzlama ortamından oluşur [6]. Hüzme uçları konkav bir yay üzerine, eleman uçları ise bu yayın karşısında yer alan başka bir konkav yay üzerine yerleştirilirler. Genellikle hüzme uçlarının sayısı ile eleman uçlarının sayısı eşit değildir. *Rotman* merceklerinde hüzme pozisyonları geometri ile sabit tutulur. Frekans değiştikçe hüzmeler daralır veya genişler.

2.3.2 *Bootlace* Mercekleri

Bootlace mercekleri optik olarak kaynak işaretini dağıtma yoluyla dizi elemanlarının beslenmesini sağlar. İletim tipi ve yansıma tipi olamak üzere iki çeşit *Bootlace* mercek yapısı vardır. Mercek sistemi diğer besleme ağı yapılarına göre daha basittir. Ancak genlik kontrolü sağlamazlar. Ayrıca, besleme sistemini oluşturabilmek için fiziksel olarak büyük bir alana gereksinim duyulur.

3 VERİCİ/ALICI BİRİMLERİ

3.1 Faz Kaydırıcılar

Faz kaydırıcılar (*phase shifters*), elektronik olarak hüzme tarama yapılan dizi antenlerde en önemli bileşenlerden biridir. Hüzmeyi belirli bir açıya yönlendirebilmek için elemanlar arasında belirli bir faz farkına ihtiyaç duyulur. Bir 6 bit faz kaydırıcı $2^6 = 64$ adet $5{,}625^{\circ}$'lik faz artımına sahiptir. 64 adet farklı faz artımı, farksal faz artımları 5,625°, 11,25°, 22,5°, 45°, 90° ve 180° olan altı tane faz kaydırıcının uygun olanlarının art arda bağlanmasıyla elde edilir. Daha sonra istenilen faz kaymasını sağlamak için faz kaydırıcıların uygun bitleri anahtarlanır. Sayısal fazörler özel bilgisayarlarla kontrol edilebildiklerinden, elektronik taramalı diziler için daha uygundur.

Bir faz kaydırıcı için kritik parametreler RF kaybı, faz kayması ile birlikte olan genlik değişimi, anahtarlama süreleri ve faz kaymasını gerçekleştirebilmek için gerek duyulan güç miktarıdır. Aynı zamanda faz kaydırıcının ağırlık ve boyutu ile kontrol devreleri de önemli parametrelerdir.

Pasif faz dizili antenlerde kullanılmak üzere elektronik olarak kontrol edilen ferrit faz kaydırıcılar ve diyotlu faz kaydırıcılar geliştirilmiştir. Diyotlu faz kaydırıcılar hızlı anahtarlama süreleri, düşük ağırlık ve düşük maliyet gibi avantajlara sahiptir. Ancak araya girme kaybı (*insertion loss*) değerleri yüksektir. Daha yavaş anahtarlama sürelerinin sorun oluşturmadığı ve düşük araya girme kaybı istenildiği durumlarda ferrit faz kaydırıcılar kullanılır.

3.2 Ferrit Faz Kaydırıcılar

Genel olarak dört farklı ferrit faz kaydırıcı yapısı mevcuttur [7]–[11]. Bunlar değişken manyetik geçirgenlik katsayısına sahip olan ferrit faz kaydırıcılar, halka (*toroidal*) ferrit faz kaydırıcılar, çift mod (*dual-mode*) ferrit faz kaydırıcılar ve döner alan ferrit faz kaydırıcılardır. Değişken manyetik geçirgenlik katsayısına sahip olan ferrit faz kaydırıcılarda bir ferrit parça bir dalga kılavuzunun merkezine yerleştirilir ve bir sarmal bobin ile boyuna olarak manyetize edilir. İlerleyen RF dalgasının faz kayma miktarı, sarmal bobin içerisinden geçirilen akım miktarı ile kontrol edilen manyetik alanın genliğine bağlıdır. Değişken manyetik geçirgenlik katsayısına sahip olan ferrit faz kaydırıcılar genellikle değişken ve karşılıdır (resiprok), fakat manyetik bobinin yüksek endüktansı nedeniyle düşük anahtarlama hızlarına sahiptirler.

Karşılı olmayan halka faz kaydırıcılar sabit kontrollü akım yapısını kullanmazlar. Halka faz kaydırıcılar bir dalga kılavuzunun merkezine yerleştirilmiş ferromanyetik bir halkadan oluşurlar ve bir kare histerezis halka ile ferritin manyetizasyonu üzerinde çalışırlar. Farksal faz kayması manyetizasyonun bir doğrultudan diğerine anahtarlanmasıyla elde edilir. Halkanın manyetizasyonunu değiştirmek için halkanın merkezinden bir kontrol teli geçer. Halka manyetizasyonu ikinci duruma geçiren bir anahtarlama darbesi gelene kadar enerji harcamadan belirli bir durumda kalır.

Çift mod karşılı ferrit faz kaydırıcılar karşılı faz kaydırıcılarının avantajlarını ve karşılı olmayan faz kaydırıcılarının da verimliliğini sağlar. İstenilen faz kaymasını sağlamak için çift mod ferrit faz kaydırıcısının merkezinde yer alan değişken ferrit eksenel olarak manyetize edilir. Bu merkezi bölümün sonunda karşılı olmayan dairesel kutuplama fonksiyonunu elde edebilmek amacıyla, sabit bir "dört kutuplu" (*quadrapole*) alan ile enine manyetize edilmiş, kısa, çeyrek dalga boyunda ferrit bölümler kullanılır. Çalışma durumunda giriş çeyrek dalga

plakası doğrusal polarizasyonlu dalgayı dairesel polarizasyonlu dalgaya dönüştürür. Bu dalga uygulanan alanın doğrultusuna ve genliğine bağlı olan kendi içsel fazı ile ferrit yüklü bölge içerisinden ilerler. Çıkıştaki çeyrek dalga plakası dairesel polarizasyonlu dalgayı tekrar doğrusal polarizasyonlu dalgaya çevirir. Karşılı bir aygıtta, karşılı olmayan bu etkilerin birleşimi sayesinde manyetizasyonun doğrultusunun tersine çevrilmesine gerek duyulmaz. Anahtarlama sürelerini küçültmek için enine manyetik (*transverse magnetic*) dört kutuplu alan ile kontrol edilen değişken ferrit bölümlerinin yer aldığı alternatif tasarımlar da mevcuttur.

Döner alan ferrit faz kaydırıcılar karşılıdır. Bu faz kaydırıcı yapısı, sırasıyla, dikdörtgen dalga kılavuzundan dairesel dalga kılavuzuna dönüştürücü, doğrusal polarizasyondan dairesel polarizasyona dönüşüm gerçekleştiren bir kutuplayıcı (*polariser*), enine manyetize edilmiş bir ferrit parça, dairesel polarizasyondan doğrusal polarizasyona dönüşüm gerçekleştiren bir başka kutuplayıcı ve dairesel dalga kılavuzundan dikdörtgen dalga kılavuzuna dönüştürücüden oluşmaktadır. Merkezdeki ferrit dairesel dalga kılavuzunun içerisini tamamen doldurur ve enine dört kutuplu bir alan ile sürülür. Bu alan çerçeve içerisine yerleştirilen sinüs ve kosinüs sarmalları ile üretilir. Her sarmal ferrit parça içerisinde enine dört kutuplu manyetik alan üretir. Sarmallar birbirine geçirilir. Öyle ki, iki sarmal içerisindeki akımları ayarlamak suretiyle dört-kutup alanın ana eksenleri herhangi bir açıya döndürülebilir. Faz kaymasının miktarı, manyetize edilmiş olan ferrit parçanın ana ekseninin etkin açısı ile orantılıdır.

3.3 Elektronik Faz Kaydırıcılar

Genel olarak dört farklı elektronik faz kaydırıcı yapısı mevcuttur [12], [13]. Bunlar anahtarlamalı hat faz kaydırıcılar, hat yansımalı faz kaydırıcılar, yüklemeli hat faz kaydırıcılar ve yüksek ya da alçak geçiren faz kaydırıcılardır.

Faz yapısını elektronik olarak anahtarlayabilmek için bu devreler içerisinde *pin* diyotlar, alan etkili transistörler (*FET*) veya mikroelektromekanik anahtarlar (*MEMS*) kullanılır. Anahtarlamalı hat faz kaydırıcılar ve hat yansımalı faz kaydırıcılar, farklı uzunluktaki iki iletim hattından birini seçmek için anahtarlar kullanırlar. Yüklemeli hat faz kaydırıcılarda ise, faz hızını artırmak için devre içerisinde yer alan endüktörler, faz hızını azaltmak için de devre içindeki kondansatörler anahtarlanır. Bu yapıda reaktans bileşenlerinin birbirlerini sıfırlamaması için çeyrek dalga hat kullanılır. Yüksek/alçak geçiren faz kaydırıcılarda, T devresi içerisindeki uygun elemanlar seçilerek anahtarlar ya alçak geçiren devre ya da yüksek geçiren devre durumuna getirilir. Devre alçak geçiren durumunda faz gecikmesi sağlarken, yüksek geçiren durumunda da faz ilerlemesi sağlar.

MEMS faz kaydırıcılarda eleman başına ışıyan güç miktarı nispeten daha düşük olduğundan pasif faz dizili antenler için bir alternatif sunarlar. *MEMS* faz kaydırıcılar küçük boyutları, düşük ağırlıkları, düşük araya girme kayıpları ve düşük güç tüketme gibi özellikleri nedeniyle yüzey etkin (*space-based*) dizi anten uygulamalarında kullanılırlar.

1990'lı yıllarda verici/alıcı birimleri için tek parça mikrodalga tümdevre ('*Monolithic Microwave Integrated Circuit*', *MMIC*) faz kaydırıcılar geliştirilmiştir. Bu tip faz kaydırıcılar küçük boyutlara, yüksek anahtarlama hızlarına, düşük güç tüketim düzeylerine ve düşük maliyet özelliklerine sahip olup, bir verici/alıcı biriminin düşük güç tarafında alçak geçiren süzgeçten sonra kullanılır.

4 SiGe VE *LDMOS* TEKNOLOJİLERİ

GaAs teknolojisi, yüksek taşıyıcı hareketliliğine sahip olduğundan yüksek frekans uygulamalarında sıkça kullanılmaktadır. Yüksek gerilime dayanma özelliği, düşük ısıl direnci ve ışınıma (radyasyona) karşı yüksek bağışıklığı bu teknolojinin askeri uygulamalarda da yaygın olarak kullanılmasını sağlamıştır. Bununla beraber, GaAs teknolojisinin üretim süreçlerindeki düşük verim problemine çözüm bulunamaması, bu teknoloji ile üretilen bileşenlerin (komponentlerin) maliyetlerinin yüksek olmasına neden olmaktadır. Faz dizili antenlerde çok sayıda verici/alıcı birimi kullanıldığından, bileşenlerin toplam maliyete katkısı yüksektir. Sadece maliyeti düşürmek için değil, GaAs teknolojiyle gelinen noktada kalmayıp, daha hafif ve hava soğutmalı anten tasarımının yapılabilmesi için de alternatif teknolojiler geliştirmek, günümüzde üzerinde çalışılan konulardandır.

Yüksek frekans uygulamalarında (cep telefonu, *WLAN* gibi) *LDMOS* (*Laterally Diffused MOS*) ve SiGe *HBT* (*Heterojunction Bipolar Transistor*) *BiCMOS* teknolojileri geniş olarak kullanılmaktadır. Benzer olarak, faz dizili antenlerin verici/alıcı birimlerinde de silisyum (Si) teknolojisinin kullanılması gündemdedir. Askeri uygulamalarda Si teknolojisinin kullanılmaya başlamasıyla, yakın gelecekte bu sistemlerin hem fiyatlarının düşmesi hem de güvenilirliğinin yükselmesi beklenmektedir.

Enstitümüzde sistem veya cihaz tasarımına genel olarak bileşen düzeyinden başlanmaktadır. Kripto cihazları için milli algoritma içeren uygulamaya özgü tümdevrelerin ('*Application-Specific IC*', *ASIC*) enstitümüzde üretilmesi gibi, faz dizili antenlerde kullanılan *MMIC*'lerin de enstitümüzde gerçeklenmesi planlanmıştır. Bu amaçla DPT'nin desteklediği altyapı projeleri ile enstitümüzün Yarıiletken

Teknolojileri Araştırma Labortuvarının (YİTAL) cihaz parkı; S bandında güç kuvvetlendiricisi gerçeklemek için *LDMOS* teknolojisini ve X bandında çalışabilecek *MMIC* üretimi için de 0,25 μm SiGeC *BiCMOS* teknolojisini geliştirecek biçimde güncellenmiştir. Aşağıda bu teknolojiler kısaca tanıtılacaktır:

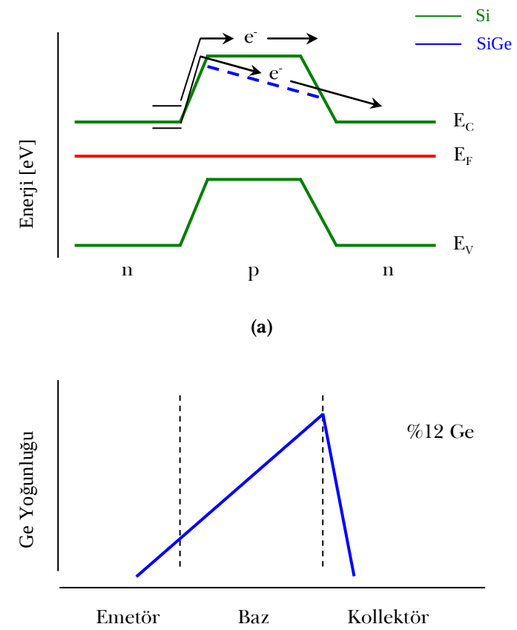
a) *LDMOS* Teknolojisi

Bu teknolojiyle üretilen RF güç transistörleri; yüksek gerilimde çalışma olanağı, kaynak kontağının doğrudan toprağa bağlanması, güvenilirliğinin yüksek ve alternatiflerine göre (*pHEMT*, GaN) düşük maliyetli olması nedenleriyle cep telefonlarının baz istasyonlarında ağırlıklı olarak kullanılmaktadır. Benzer olarak, S bandı faz dizili radarların güç katında da *LDMOS* transistörleri kullanılmaya başlanmıştır.

Standart *MOS* transistörlerden farklı olarak, *LDMOS* yapısında transistörün etkin kanal genişliği fiziksel kanal boyundan daha kısadır. Bu özellik transistörün kanal bölgesindeki katkı profilinin kaynak bölgesinden savak bölgesine doğru sert bir eğimde olması sağlanarak elde edilir. Böylelikle bu yapının daha yüksek frekansta çalışması sağlanmıştır. Transistörün yüksek gerilimde çalışma özelliği ise, kanal bölgesini takiben savak bölgesinin az katkılı - yüksek dirençli - olmasıyla elde edilir. Yüksek dirençli savak bölgesinin uzunluğu artırılarak *LDMOS* transistörünün çalışma gerilimi yükseltilir. Savak bölgesindeki bu ek direnç, transistörün akımının sınırlanması üzerinde negatif etki oluşturmaz, fakat transistörün güç verimini düşürmesi (*Power Added Efficiency*) açısından önem taşımaktadır. *LDMOS*'un çalışma gerilimi savak direnci yükseltilerek elde edildiğinden, transistörün belverme gerilimi çalışma isterlerini ancak karşılayacak değerde seçilmelidir. *LDMOS* yapısı RF güç uygulamaları için ayrık bileşen olarak kullanılmasına ek olarak *MMIC*'lerde de kullanılmaktadır. 2010 yılı içinde 6 GHz *WLAN* uygulamaları için 1 W çıkış güçünü % 40 savak verimi ile sağlayan *LDMOS*, SiGe *BiCMOS* süreci içinde gerçeklenmiştir [14].

b) SiGe Teknolojisi

Bu teknolojinin getirdiği temel yenilik bipolar transistörün baz bölgesine Germanyum (Ge) katkısıdır. Bipolar transistörün emetör bölgesinden baz bölgesine giren taşıyıcılar (npn yapısı için elektronlar) bu bölgede artık bir azınlık taşıyıcısıdır ve kollektör bölgesine ulaşıncaya kadar difüzyonla hareket ederler. Taşıyıcıların baz bölgesinde aldıkları mesafe ne kadar kısa ise ya da taşıyıcılar bu bölgede ne kadar hızlı hareket ederlerse, transistör o kadar hızlı çalışacaktır. Bipolar transistörlerin kesim frekansının yükseltilmesi için, 1990'lı yılların başında *IBM* firması, silisyuma Ge eklenmesiyle Si kristalinin enerji bant aralığının değiştirilebildiğini göstermiştir. Ge atomlarının yoğunluğunun emetör jonksiyonundan başlayarak kollektör jonksiyonuna kadar dereceli olarak artırılması halinde baz bölgesi içinde yasak bandın enerji düzeyi dereceli olarak düşmektedir. Bu durum baz bölgesi içinde sözde bir elektriksel alan oluşmasına neden olmakta ve taşıyıcıların hareketliliğini yükseltmektir. Oluşan bu elekriksel alan 30-40 kV/cm mertebesindedir. Bu mertebede bir elektriksel alan yaratmak için silisyuma atomca % 12 mertebesinde Ge katkılanması gerekmektedir. Ge katkısıyla bipolar transistörün baz bölgesindeki enerji bandının değişimi Şekil 4'te gösterilmiştir.



Şekil 4. *SiGe karma jonksiyonlu bipolar transistörün a) enerji bant diyagramı, b) baz bölgesine yapılan Ge katkı profili.*

Karma jonksiyonlu (*heterojunction*) bipolar transistörlerin baz bölgelerinin oluşturulmasında bölgesel epitaksiyel film depolama tekniği kullanılmaktadır. Si pul yüzeyinde bölgesel olarak depolanan SiGe filmleri, süreç tamamlandığında bipolar transistörlerin baz bölgelerini oluşturmakta, böylece, standart *CMOS* sürecinin yanında, bipolar düzenler için gerekli baz ve emetör bölgeleri eklenerek, aynı kırmık üzerinde hem *NMOS* ve *PMOS* hem de bipolar yapılar üretilebilmektedir. Si kristaline Ge katkılanmasıyla yasak bant aralığının değiştirilmesi ve bipolar transistörün performansının yükselmesine ek olarak,

bu yapının *CMOS* üretim adımları ile beraber üretilebilir olması da önemli bir gelişmedir. Si kristaline Ge katkısıyla yüksek performanslı *MMIC* üretimi gerçekleştirilebilmektedir.

Standart *CMOS* ve SiGe *HBT* teknolojilerinde en küçük boyuta göre kesim frekansının değişimi Lawrence tarafından ayrıntılı olarak incelenmiştir [15].

5 UYGULAMALAR VE GELİŞİM YÖNÜ

Şimdiye kadar bir çok faz dizili anten uygulamasında pasif faz dizili antenler kullanılmıştı. Çünkü aktif faz dizili antenler henüz olgunlaşmamışlardı ve çok pahalı yapılardı. GaAs *MMIC* teknolojisinin gelmesiyle aktif faz dizili anten konusu üzerinde daha geniş çalışmalar gerçekleştirildi. *MMIC* teknolojisinin otomotik modül montaj teknikleriyle birlikte kullanılması aktif faz dizili antenlerin maliyetini önemli ölçüde azaltmış ve böylece aktif faz dizili antenler tercih edilmeye başlanmıştır.

5.1 Pasif Faz Dizili Antenler

a) *AN/SPY-1* Radarı

S bandı *AN/SPY-1* anteni pasif melez bir faz dizili anten yapısıdır. Dizi yüzeyinin temel yapı blokları her biri 32 ışıma elemanından oluşan dizi modülleri ile sonlandırılmıştır. İki dizi modülü bir alıcı alt dizi yapısını meydana getirmektedir [16]. Ana dizi fonksiyonları için 68 adet dizi modülü mevcuttur. Yardımcı fonksiyonlar için 2 adet dizi modülü kullanılmaktır. Dörder tane dizi modülü bir verici alt dizi yapısını meydana getirmektedir. Verici alt kesimleri içerisinde 32 adet yüksek güçlü, yürüyen dalga tüp kuvvetlendiricisi yer almaktadır.

Her bir dizi modülü üzerinde 32:1 güç bölücü ile entegre edilmiş 32 tane faz kaydırıcı ve sekiz tane de faz kaydırıcı sürücü kartı bulunmaktadır. Bu modüller üçgen ızgara biçiminde yerleştirilmiş 32 adet huni *(horn)* antene monte edilmiştir.

Faz kaydırma fonksiyonunu gerçekleştirebilmek için karşılı olmayan halka ferrit faz kaydırıcılar kullanılmıştır. Düşük maliyet sağlayabilmek için yüklemeli melez jonksiyon yapısı kullanan ağlar yerine reaktif bölücü ağ yapısı kullanılmıştır. Alıcı hüzme biçimlendirme ağı ağırlığı azaltılmış dalga kılavuzu kullanmaktadır.

b) B-1 Radarı

Bu dizide paralel dalga kılavuzu besleme yapısı kullanılmaktadır. Faz kontrol modülleri dizinin her bir elemanı için karşılı olmayan halka ferrit faz kaydırıcılar içermektedir. Işıma elemanı olarak dielektrik yüklü dairesel dalga kılavuzları kullanılmıştır.

c) *ASARS*[1] *ESA*[2]

Bu dizi anten yapısı yapay açıklık radarı içerisinde keşif amaçlı kullanılmaktadır. Paralel besleme yapısındaki bu anten X bandında çalışmakta ve ışıma elemanı olarak 2400 adet açık sonlandırmalı dikdörtgen dalga kılavuzundan oluşmaktadır. Dizinin her bir sütununda analog kontrollü döner alan ferrit faz kaydırıcılar bulunmaktadır.

5.2 Aktif Faz Dizili Antenler

Bu tür antenler aşağıdaki radar sistemlerinde kullanılmaktadır:

a) *AMSAR*[3]

Tasarlanan aktif anten X bandında çalışan ve 60 cm çap içerisine yerleştirilmiş 1000 adet verici/alıcı biriminden oluşan bir dizi yapısıdır. Verici/alıcı birimleri *MMIC* teknolojisi kullanılarak gerçekleştirilmiştir [17]. Bu dizi anten tuğla mimarisinde tasarlanmıştır. Verici/alıcı birimleri dizi yüzeyine dik olacak biçimde, doğrusal, düşey bir soğuk plaka üzerine monte edilmiştir. Birimler paralel güç ayırıcılarına bağlanmıştır. Alt diziler yığın (*stacked*) şeklinde yerleştirilerek tüm diziyi oluştururlar. Her bir verici/alıcı birimi çift polarizasyonlu bir ışıma elemanına bağlanır. Işıma elemanları ise üçgen bir ızgara yapısında yerleştirilmiştir.

b) F-22 Radarı

F-22 radarı tuğla mimarisi ile tasarlanmış ayrık verici/alıcı birimlerinden oluşan ve X bandında çalışan bir aktif faz dizili anten uygulamasıdır. Ayrık verici/alıcı birimleri verici/alıcı fonksiyonları arasında yüksek yalıtım sağlamaktadır. Ayrıca üretim maliyetlerini de azaltmaktadır.

c) F-15 C

Bu anten F-15 savaş uçaklarının burun kısmına yerleştirilmektedir. Tuğla mimarisi ile tasarlanmış olan bu dizi anten F-15 uçaklarının dünyanın aktif elektronik taramalı dizi (‘*Active Electronically Scanned Array*’, *AESA*) teknolojisini kullanan ilk savaş jetleri olmasını sağlamıştır.

d) *GBR*[4]

X bandında çalışan ve yüksek irtifa alan savunmasında kullanılan bu radar 9,2 m²'lik yüzey alanına sahip olup, bu dizi anten içerisinde ışıma elemanı olarak 25344 tane dielektrik yüklü dairesel dalga kılavuzu kullanılmıştır [18]. Her bir eleman yüksek güç verici/alıcı birimi tarafından beslenmektedir. Dizi her biri 352 eleman içeren 72 alt diziden oluşmaktadır. Her bir alt dizi 11 adet verici/alıcı

[1] *Advanced Synthetic Aperture Radar System*
[2] *European Space Agency*
[3] *Airborne Multirole Solid-State Active Array Radar*
[4] *Ground Based Radar*

eleman tümleşkesi (‘*T/R Element Assembly*’, *TREA*), alt dizi modülü (*SAM*) ve bir ‘*AC/DC*’ dönüştürücüden oluşmaktadır. Bir *TREA* 32 adet ışıma elemanı, 32 adet verici/alıcı birimi, sekiz adet ‘*DC/DC*’ dönüştürücü, dört adet hüzme biçimlendirme kontrol birimi ve *RAM* biriminden oluşur. Her bir *SAM* bir alt diziyi sürmek için kullanılır ve alt dizi düzeyinde hüzme tarama kontrol devre kartı, her bir verici/alıcı kanalı için zaman geciktirme birimleri, düşük gürültülü kuvvetlendiriciler (*LNA*), kuvvetlendiriciler ve anahtarlar içerir. *TREA* dizinin içerisine ön taraftan, *SAM* ise arka taraftan eklenir.

5.3 *IRIDIUM*

IRIDIUM küresel kişisel haberleşme sistemi, L bandında çalışan üç adet aktif faz dizili anten paneli içermektedir [19]. Her bir faz dizisi paneli, eş zamanlı ve sabit 16 hüzme oluşturmaktadır. Toplamda elde edilen 48 hüzme kullanıcıları kapsamakta ve böylece kullanıcılar haberleşme ağı yoluyla, uydu sistemi ile haberleşebilmektedir.

Her bir dizi paneli 100'ün üzerinde yama anten içermektedir ve her bir anten bir verici/alıcı birimi ile beslenmektedir. Hüzme biçimlendirici yapısı sekiz adet 16×16 *Butler* matrisinden oluşmaktadır.

5.4 *CTS* Dizileri

CTS (*Continuous Transverse Stab*) dizi yapısı uygun tasarlanmış, iki boyutlu elektronik tarama yapabilme yeteneğine sahip, düşük ağırlıklı ve düşük maliyetli, yürüyen dalgalı düzlemsel dizidir.

CTS elemanları düşük *Q* değerlerine sahiptir. Bu nedenle, yarık veya yama antenlere göre bant genişliği, polarizasyon saflığı ve tarama kapasitesi parametreleri açısından önemli avantajlara sahiptir.

CTS dizisinde H düzlemi taraması, diziyi besleyen doğrusal verici/alıcı birimi aracılığıyla, dizinin paralel plaka bölgesi içindeki yürüyen dalganın fazı değiştirilerek sağlanır. E düzleminde tarama ise paralel tabaka bölgesi içerisinde etkin yayılma sabitinin değişimi kontrol edilerek sağlanır. H ve E düzlemi tarama teknikleri, birlikte iki boyutlu elektronik tarama sağlarlar.

5.5 *APAR*[5]

Çok fonksiyonlu aktif faz dizili gemi radarı *APAR* Thales (Hollanda) firması tarafından geliştirilmiştir. X bandında çalışan bu radarın 4 ana yüzü mevcut olup, her yüzünde 3424 *T/R* modülü bulunmaktadır. Hacim arama mesafesi 150 km, ufuk arama mesafesi 75 km olup, aynı anda 200 hava hedefini, 150 su üstü hedefini, angajman, arama ve takip yapabilmektedir. Bunun yanında, füzeye yol gösterme (*missile guidance*), su üstü top ateşi (*gunfire support*) desteği de sağlamaktadır.

[5] *Active Phased Array Radar*

5.6 Sayısal Hüzme Biçimlendirme

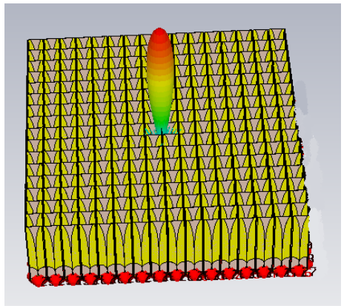
Aktif faz dizili antenler programlanabilir fonksiyonellik ile tamamen sayısal olan çok fonksiyonlu dizilerdir. Sayısal hüzme biçimlendirme yapısında sadece yüksek güç ve düşük gürültülü kuvvetlendirici birimleri analogtur. Hüzme biçimlendirmenin yanında tüm genlik ve faz kaydırma fonksiyonları da sayısal olarak gerçekleştirilir. Gönderilen dalga şekilleri doğrudan sayısal sentezciler tarafından üretilir. Alınan işaretler çok hızlı analog sayısal dönüştürücüler ile yakalanır. Çok büyük dizilerde hüzme tarama için doğru zaman gecikmeleri sayısal olarak gerçekleştirilebilir. Açıkça görüldüğü üzere, bu mimari çok hızlı veri işleme gerektirmektedir.

5.7 Akıllı Antenler

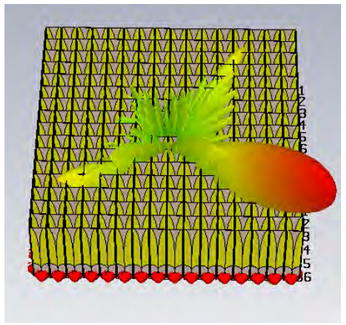
Akıllı (*smart*) antenler, en genel tanımıyla, sayısal işaret işleme kapasitesine sahip; hüzme biçimlendirme, hüzme tarama, sıfır noktası oluşturma, hüzme yönlendirme gibi işlevleri gerçekleştiren anten sistemleridir. Üç ana elemandan oluşur: anten birimi, RF birimi ve *DSP* algoritmaları. Son yıllarda kablosuz haberleşme sistemlerinin oldukça yaygın kullanılmasıyla bazı gereksinimler ortaya çıkmış ve bu gereksinimlerin karşılanması da bir takım problemleri beraberinde getirmiştir. Bu problemler; kapasite, menzil, yüksek veri aktarım oranı, hareketlilik (*mobility*), spektral verim ve biyolojik etkilerin sınırlandırılması olarak özetlenebilir. Bu problemlerin üstesinden gelmenin yolu Akıllı Anten Sistemlerinin (AAS) kullanılmasıdır. AAS ile hüzme istenilen kullanıcıya yönlendirildiği gibi, istenilmeyen etkilerin (girişim) azaltılması amacıyla, ilgilenilmeyen bölge yönünde anten kazancını en küçük kılıp, ışıma diyagramının sıfır noktalarının buralara denk düşmesi sağlanabilir. Aynı zamanda bu sistemler, çoklu yol (*multipath*) işaretlerini en aza indirmek veya işaret/gürültü oranını geliştirebilmek için gerçek zamanda anten hüzmelerini uyarlayabilirler.

Akıllı anten sistemlerin üç çeşidi vardır: anahtarlamalı, faz dizili ve uyarlamalı (aktif) faz dizili. Anahtarlamalı hüzme yapısında sabit bir hüzme, anahtarlar yardımıyla dizinin uygun elemanlarının kaydırılarak beslenmesi yoluyla istenilen noktaya döndürülebilir. Basit bir yapısı olup, düşük çözünürlük gerektiren uygulamalarda kullanılabilir. Akıllı anten yapısı ile hüzme biçimlendirme ve yönlendirme örneği Şekil 5'te gösterilmiştir.

Faz dizili yapı pasif bir yapı olup, faz kaydırıcılarla tek bir hüzmenin döndürülmesi işlemidir. Bu yapı anahtarlamalı



(a)



(b)

Şekil 5. *Akıllı anten yapısıyla hüzme yönlendirme: a) eş faz beslemeli, b) elektronik olarak yönlendirilmiş.*

hüzme yapısından biraz daha karmaşık olup, hüzme biçimlendirme yapamaması en büyük dezavantajıdır.

Uyarlamalı (*adaptive*) diziler ise aktif yapılardır. Daha karmaşık ve pahalıdır. Yüksek çözünürlük gerektiren uygulamalarda kullanımları kaçınılmazdır. Bu yapılar ile hüzmeye verilmesi gereken şekil çeşitli algoritmalarla belirlenir (*MF* (*Matched Filter*), *MVDR* (*Minimum Variance Distortionless Response*), *MUSIC* (*Multiple Signal Classification*), *ESPRIT*, *CLOSEST*, *Hung-Turner Projection* vb.) İstenilen hüzme şekli, sayısı, yan kulakçık düzeyi, sıfır noktaları ve yönü gibi parametreler sayısal hüzme biçimlendirme algoritmaları (*SMI* (*Sample Matrix Inverse*), *LMS* (*Least Mean Square*), *RMS* (*Recursive Least Square*), *CMA* (*Constant Modulus Algorithm*), *APA* (*Affine-Projection Algorithm*), *QNA* (*Quasi-Newton Algorithm*)) ile anten elemanlarının faz ve genlik değerleri ayarlanarak elde edilir.

6 SONUÇ

MMIC yapıların sıklıkla kullanılmaya başlaması, mikrodalga elemanlarının tümleştirilmelerindeki teknolojik ilerleme ve otomotik montajlama sistemlerinin gelişimi, radar ve haberleşme uygulamaları için aktif faz dizili antenlerin tercih edilmesini kolaylaştırmıştır.

Nanoteknoloji geliştikçe sayısal hüzme biçimlendirme yapıları analog yapıların yerini alacaktır.

TEŞEKKÜR

Bu yazının gözden geçirilmesi sırasında gösterdiği büyük titizlik nedeniyle Sayın Dr. Levent Balamir Tavacıoğlu'na teşekkür ederiz.

KAYNAKÇA

[1] B. Türetken ve K. Sürmeli, "Radar antenleri - IV: faz dizili anten kuramına genel bakış", *UEKAE Dergisi*, sa. 4, sf. 118–125, Eylül-Aralık 2010.

[2] B. Türetken ve K. Sürmeli, "Aktif faz dizili anten tasarımına sayısal modelleme tekniğiyle yeniden bakış", *V. URSI-Türkiye'2010 Bilimsel Kongresi ve Ulusal Genel Kurul Toplantısı*, Güzelyurt, KKTC, Ağu. 2010, sf. 452–455.

[3] D. Parker and D. C. Zimmermann, "Phased arrays—part II: implementations, applications and future trends," *IEEE Trans. Microwave Theory Tech.*, vol. 50, no. 3, pp. 688–698, Mar. 2002.

[4] E. L. Holzman and A. K. Agrawal, "A comparison of active phased array, corporate beamforming architectures," *IEEE Intl. Phased Array Syst. Technol. Symp. Dig.*, Boston, Massachusetts, Oct. 1996, pp. 429–434.

[5] A. R. Lopez, "Monopulse networks for series feeding an array antenna," *IEEE Trans. Antennas Propag.*, vol. 16, no. 4, pp. 436–440, July 1968.

[6] W. Rotman, "Wide-angle scanning with microwave double-layer pillboxes," *IRE Trans. Antennas Propag.*, vol. 6, no. 1, pp. 96–105, Jan. 1958.

[7] L. R. Whicker, "Future directions for microwave ferrite components," *IEEE MTT-S Intl. Microwave Symp. Dig.*, Orlando, Florida, Apr.-May 1979, pp. 367–369.

[8] L. R. Whicker, "Review of ferrite phase shifter technology," *IEEE G-MTT Intl. Microwave Symp. Dig.*, Boulder, Colorado, June 1973, pp. 95–97.

[9] C. R. Boyd, Jr. "A dual-mode latching, reciprocal ferrite phase shifter," *IEEE G-MTT Inlt. Microwave Symp. Dig.*, Newport Beach, California, May 1970, pp. 337–340.

[10] R. G. Roberts, "An X-band reciprocal latching Faraday rotator phase shifter," *IEEE G-MTT Intl. Microwave Symp. Dig.*, Newport Beach, California, May 1970, pp. 341–345.

[11] W. E. Hord, C. R. Boyd, Jr. and D. Diaz, "A new type of fast switching dual-mode ferrite phase shifter," *IEEE MTT-S Intl. Microwave Symp. Dig.*, Las Vegas, Nevada, June 1987, vol. 2, pp. 985–988.

[12] J. F. White, "Diode phase shifters for array antennas," *IEEE Trans. Microwave Theory Tech.*, vol. 22, no. 6, pp. 658–674, June 1974.

[13] M. E. Davis, "Integrated diode phase-shifter elements for an X-band phased-array antenna," *IEEE Trans. Microwave Theory Tech.*, vol. 23, no. 12, Dec. 1975, pp. 1080–1084.

[14] D. Gruner *et al.*, "A 1 W Si-LDMOS power amplifier with 40 % drain efficiency for 6 GHz WLAN applications," *IEEE MTT-S Intl. Microwave Symp. Dig.*, Anaheim, California, May 2010, pp. 517–520.

[15] L. E Larson, "SiGe HBT BiCMOS technology as an enabler for next generation communications systems," *Proc. 12th Gallium Arsenide Applications Symp. (GAAS® 2004)*, Amsterdam, Oct. 2004, pp. 251–254.

[16] W. T. Patton, "Compact, constrained feed array for AN/SPY-1," in *Practical Phased Array Antenna Systems*, E. Brookner (ed.), Norwood, MA: Artech House, 1991, lec. 8, pp. 8.1–8.35.

[17] G. J. Albarel, G. S. Tanner and M. Uhlmann, "AMSAR antenna architecture and predicted performance," *IEEE Intl. Phased Array Syst. Technol. Symp. Dig.*, Boston, Massachusetts, Oct. 1996, pp. 450–453.

[18] M. Sarcione *et al.*, "The design, development and testing of the THAAD (theater high altitude area defense) solid state phased array (formerly ground based radar)," *IEEE Intl. Phased Array Syst. Technol. Symp. Dig.*, Boston, Massachusetts, Oct. 1996, pp. 260–265.

[19] J. J. Schuss *et al.*, "The IRIDIUM® main mission antenna concept," *IEEE Intl. Phased Array Syst. Technol. Symp. Dig.*, Boston, Massachusetts, Oct. 1996, pp. 411–415.

Mikrodalga Radarda K-Dağılımlı Kargaşa

Yıldırım BAHADIRLAR

Özet - *Bu çalışmada, mikrodalga radarda deniz kargaşasını modellemek üzere kullanılacak faz uyumlu (*coherent*) kargaşa modeli üzerinde durulmuş, kargaşa işaretinde karmaşık özilinti (*complex autocorrelation*) niteliğini de özellik olarak bulundurabilen bir modelleme yaklaşımı sunulmuştur. Kargaşa modeli K-dağılımı olasılık yoğunluk fonksiyonuna sahip ayrık serilerin oluşturulmasında kullanılmıştır. Modelin etkinliği istatistiksel sınama işlemleri gerçekleştirilerek gösterilmiştir. Modelde bulunan doğrusal dönüşüm için özbağlanımlı ('autoregressive', AR) süzgeç kullanılarak özilinti fonksiyonuna sahip kargaşa işaretleri elde edilmiştir.*

Anahtar Sözcükler - *Mikrodalga radar, deniz kargaşası (*sea clutter*), K-dağılımı, özbağlanımlı (*autoregressive*) model.*

1 GİRİŞ

Mikrodalga (MD) radarlarda donanımdan kaynaklanan gürültünün yanında, deniz yüzeyinden saçılan elektromanyetik (EM) dalgaların oluşturduğu, yağmur yoğunluğu nedeniyle ve karadan yansıma sonucunda oluşan üç ana kargaşa (*clutter*) kaynağı bulunur. Bu çalışmada deniz kargaşa modellemesi için benzetimlerde ve alıcı karakteristiklerinin çıkarılmasında yararlanılabilecek Rayleigh dışı dağılımlardan K-dağılımı ele alınacak, bu dağılım için gerçekleştirilen benzetim sonuçları verilecektir.

Deniz dalgaları kılcal (*capillary*) dalgalar ve yerçekimi dalgaları (*gravity waves*) olmak üzere iki temel gruba ayrılmaktadır. Kılcal dalgalar 2-3 cm ya da daha düşük dalga boyuna sahip olup, ağırlıklı olarak suyun yüzey gerilimi nedeniyle sönümlenen dalgalardır. Yerçekimi dalgaları ise daha büyük dalga boyuna sahiptir ve ağırlıklı olarak, yerçekimi etkisiyle sönümlenmektedir [1]. Yerçekimi dalgalarının özelliklerine ilişkin iki durumdan söz edilir: 1) rüzgâr nedeniyle dalgaların yükseldiği deniz durumu (*sea state*), 2) dalgaların rüzgâr etkisi ortadan kalktığında oluşan açılma (*swell*) durumu. Açılma durumunda dalgalar uzun ve alçak frekanslı sinüs dalgaları gibidir. MD radarlarda frekans aralığı dikkate alındığında, deniz dalgalarının yerçekimi dalgaları üzerine binen çok sayıda kılcal dalganın bileşiminden oluştuğu düşünülebilir. Düşük sıyırma (*grazing*) açısı ile çalışan bir MD radarı için deniz kargaşası, basitçe, kılcal dalgalar nedeniyle oluşan rezonans saçılımı ya da *Bragg* saçılımı olarak düşünülebilir. Ancak, bu basitleştirilmiş modelde düşük sıyırma açılarındaki gölgeleme ve kırınım etkileri dikkate alınmamış olur.

Deniz yüzeyinin bazı bölümleri için, kırılan dalgaların tepe noktaları nedeniyle oluşan ve yatay ve dikey polarizasyonda da eşit enerjiye sahip işaretler oluşturan "hızlı saçıcılar" diye adlandırılabilecek saçıcı etkiler de bulunmaktadır [2]. Bu etkilerin tümü göz önüne alındığında deniz kargaşası net olarak doğrusal olmayan (*nonlinear*) bir fiziksel süreç olarak kabul edilir ve bir rastlantısal (*stochastic*) süreç olarak modellenir.

Deniz yüzeyinde büyük bir alanı aydınlatan radarlardan alınan zarf işaretinin, Rayleigh olasılık yoğunluk fonksiyonuna ('*Probability Density Function*', *PDF*) genellikle uyduğu gözlenmiştir [3]. Bu, denizden yansıyan işaretin çok sayıda bağımsız saçıcıdan gelerek dik bileşenler (*I-Q*) verisini oluşturduğu anlamına gelir ve merkezi sınır kuramı (*central limit theorem*) gereğince, genlik verisinin Rayleigh dağılımına yakınsadığı düşünülür. Ancak, yüksek çözünürlüklü, düşük sıyırma açısında çalışan modern radarlarda, özellikle yatay polarizasyonda alınan işaretlerde Rayleigh dağılımından büyük sapmalar gözlenir. A-skop[1] ekranında düşük çözünürlüklü radarlardan alınan "gürültü biçimli" işaretlerin aksine, ani sıçramalara sahip (*spiky*) ve hedef benzeri işaretler görülür [3]. Sıçramalı özelliğe sahip bu işaretler, aydınlatılan görece küçük alandaki deniz yüzeyinin durağan olmayan hareketinden ya da aydınlatılan alandaki az sayıdaki saçıcının merkezi sınır kuramı gereğince bir Gauss dağılımlı yansıma oluşturamayacağı gerçeğinden kaynaklanır [3]–[4]. Ölçümlerden elde edilen deneysel olasılık yoğunluk fonksiyonları uzun kuyruklu ve standart sapma/ortalama oranları yüksek özellikler göstermektedir. Ölçümler sonucunda, yüksek çözünürlüklü ve alçak sıyırma açısında çalışan radarlardan alınan işaretlerin Rayleigh dışı olasılık yoğunluk fonksiyonlarına sahip uzun kuyruklu dağılımlar olduğu saptanmıştır [3], [5]–[8].

Teknik yazındaki kargaşa modelleme çalışmalarında Rayleigh dışı üç tür dağılım önerilmektedir: deniz ve kara kargaşası için Log-normal ve Weibull dağılımları, radar işaretlerine ek olarak pürüzlü (*rough*) yüzeylerden ve türbülans ortamlarından saçılan alanların da olasılık dağılımını temsil etmek üzere K-dağılımı [6]–[11].

Radarda kargaşa modelleme çalışmaları iki açıdan önem taşımaktadır: Birincisi, çözümleme aşamasında radar donanımındaki algılayıcı katlarının başarımını daha yüksek doğrulukla kestirmek mümkün olmaktadır. İkincisi ise, tasarım aşamasında en iyi (optimum) ya da en iyi altı (*sub-optimum*) başarıma sahip alıcıların geliştirilmesine olanak tanımaktadır. Ayrıca, radar simülatörü gibi uygulamalarda belirli örüntüye sahip kargaşa işaretlerinin yordamsal (*algorithmic*) işlemler aracılığıyla üretilmesini sağlar.

Radarda algılama işlemlerinin başarım tayini ve sistemi en iyi kılma (optimizasyon) çalışmaları kapsamında kargaşa modellemesi yapılırken, kargaşa işaretinin zamanda ve uzamda ilintisi (*temporal and spatial correlation*) de dikkate alınır. Algılama ve hedef izleme süreçlerinin başarımı kargaşa işaretinin olasılık yoğunluk fonksiyonu yanında, işaretin darbeden darbeye ilinti katsayısına ve bir menzil hücresi ile diğer bir hücre arasındaki ilintiye de sıkı sıkıya bağlıdır [12]–[14].

2 K-DAĞILIMLI KARGAŞA

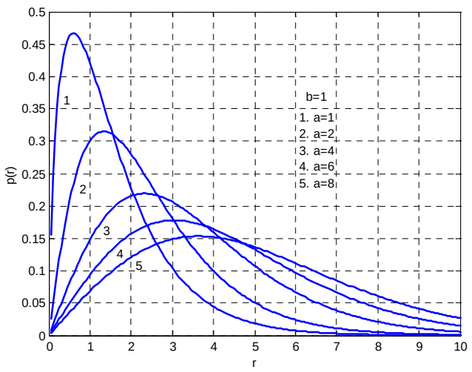
K-dağılımı bileşik yapılı bir olasılık dağılımı olduğundan, denizden yansıyan kargaşa işaretinin hem genliğini hem de ilintili bir yapıda olma durumunu temsil edebilmektedir. Dağılım farklı ilinti uzaklıklarına veya zamanlarına sahip iki bileşenin çarpımı biçiminde yorumlanabilir. Birinci bileşen, kökünü Gama dağılımından alan ve kargaşa işaretinin ortalama düzeyini temsil eden bileşendir. İkinci bileşen ise Rayleigh dağılımına sahip ve yerel kırpışmayı (*speckle*) temsil eden bileşendir. Deniz yüzeyindeki belirli bir hücre için verilen ortalama deniz dalga yüksekliği geri yansıyan işaretin ortalama gücüne etki eder ve saniye düzeyinde yavaş değişimler gösterir. Diğer taraftan, rüzgârdan sürekli etkilenen kılcal dalgalar milisaniye düzeyinde kısa ilintili Rayleigh dağılımına sahip bileşeni oluştururlar. Bu bileşik yapı nedeniyle K-dağılımı deniz kargaşası için iyi bir modeldir ve kargaşa genliğinin istatistiğini yüksek doğrulukla modelleyebilir [7].

K-dağılıma sahip r rastlantı değişkeninin Olasılık Yoğunluk Fonksiyonu (OYF) (1) eşitliğindeki gibi verilebilir:

$$p(r)=\frac{2b}{\Gamma(\alpha)}\left(\frac{br}{2}\right)^{\alpha}K_{\alpha-1}(br),\qquad 0\le r\le\infty \tag{1}$$

Burada, α değişkeni dağılımın biçim parametresini, b değişkeni ise ölçek parametresini temsil eder. $K_{\alpha-1}(.)$, $(\alpha-1)$ inci dereceden değiştirilmiş Bessel fonksiyonudur. Şekil 1'de $b=1$ olmak üzere farklı biçim parametrelerine ilişkin K-dağılımı OYF'leri verilmiştir.

Yüksek biçim parametresi (α) değerleri ile büyük standart sapmalı ve yüksek kipsel (*modal*) değerli dağılım fonksiyonları elde edilirken, düşük α değerlerinde küçük standart sapmalı, ancak yine uzun kuyruğa sahip dağılım fonksiyonları elde edilebilmektedir. Uzun kuyruk, sıçrama

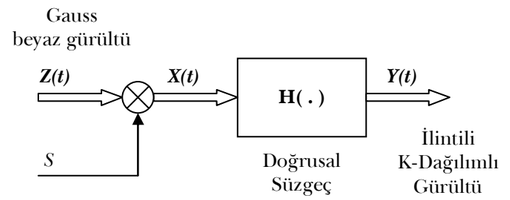


Şekil 1. *Değişen biçim parametresi α'ya bağlı K-dağılımı olasılık yoğunluk fonksiyonları (b=1).*

nitelikli işaretlerin varlığının bir göstergesi olarak Rayleigh dışı dağılım olma niteliğini işaret etmektedir.

2.1 Dışyapılı Model

Dışyapılı (*exogenous*) model, OYF ile ilinti fonksiyonunun bağımsız bir biçimde denetiminin yapılmasını sağlayan bir modeldir. *SIRP*'lar da (*Spherically Invariant Random Process*) bu model ailesine giren rastlantı süreçleridir [11], [15]–[16]. Şekil 2'de bir dışyapılı model verilmektedir.



Şekil 2. *Karmaşık Gauss dışı ilintili süreçler için dışyapılı model.*

SIRV (*Spherically Invariant Random Vector*), bir birinci dereceden karakteristik OYF, bir kovaryans matrisi ve bir ortalama vektörü ile OYF'si tek (*unique*) olarak tanımlanabilen (gerçel ya da karmaşık sayılı) bir rastlantısal vektördür. *SIRP* ise, kendisinden örnekleme yoluyla elde edilen tüm vektörlerin birer *SIRV* olacağı bir rastlantı sürecidir [15]–[18].

Temsil kuramı (*representation theorem*) *SIRV*'nin istatistiksel özelliklerini Gauss OYF'sine bağlayan bir kuramdır ve şu biçimde verilebilir: Eğer bir rastlantı süreci *SIRV* ise, öyle bir negatif olmayan S değişkeni bulunur ki, bu rastlantı vektörünün bu değişken ile koşullanmış OYF'si bir

[1] Eski tip analog radarlarda kullanılan, hedefin menzilini gösteren ekran.

çok değişkenli (*multivariate*) Gauss dağılımıdır [15]–[17]. Aşağıda, bu kuramı temel alan K-dağılımlı kargaşa modeli ele alınacaktır.

2.2 K-Dağılımlı Özilintili Kargaşa Modeli

Deniz kargaşası modelleme çalışmalarında, kargaşa işaretinin olasılık yoğunluk ve özilinti fonksiyonlarını birbirinden bağımsız olarak denetlemek gerektiği görülmektedir. Bu amaç doğrultusunda, ilintisiz kargaşa işareti

$$\mathbf{X} = \mathbf{Z}S \tag{2}$$

olarak tanımlanmış olsun. Burada, $\mathbf{X} = \left[X_1,\ X_2,\ ...,\ X_N\right]^T$ bir *SIRV*, $\mathbf{Z} = \left[Z_1,\ Z_2,\ ...,\ Z_N\right]^T$ kovaryans matrisi $\mathbf{M}$, ortalaması sıfır olan bir Gauss rastlantı vektörü ve S, OYF'si $f_S(s)$ olan, negatif olmayan bir rastlantı değişkenidir. Buradaki çözümlemede $\mathbf{Z}$ ve S istatistiksel olarak birbirinden bağımsız varsayılmaktadır. Bu durumda $\mathbf{X}$'in S değişkeni ile koşullanmış koşullu olasılık yoğunluk fonksiyonu (3) eşitliğindeki gibi verilebilir:

$$f_{\mathbf{X}/S}(\mathbf{x}/s) = (2\pi)^{-N/2}\left|\mathbf{M}\right|^{-1/2} s^{-N} exp(-\frac{q}{2s^2}) \tag{3}$$

Buradaki q, $\mathbf{x}^T\mathbf{M}^{-1}\mathbf{x}$ ile verilen karesel ifadeyi ve $|\mathbf{M}|$ de kovaryans matrisi $\mathbf{M}$'nin determinantını temsil eder. $\mathbf{X}$'in OYF'si ise (4) eşitliği ile verilir:

$$f_{\mathbf{X}}(\mathbf{x}) = (2\pi)^{-N/2}\left|\mathbf{M}\right|^{-1/2} h_N(q) \tag{4}$$

Burada $h_N(q)$ (5) eşitliğindeki gibidir:

$$h_N(q) = \int_0^\infty s^{-N} exp(-\frac{q}{2s^2}) f_S(s) ds \tag{5}$$

$f_S(s)$ yukarıda belirtildiği gibi S'nin OYF'sidir ve bu rastlantı değişkeninin karakteristik OYF'si olarak tanımlanır [15]–[16]. Buradan, bir *SIRV*'nin OYF'sinin bir kovaryans matrisi ve bir birinci dereceden karakteristik OYF ile tamamıyla belirlenebildiği görülmektedir. Buna ek olarak, *SIRV* negatif olmayan karesel bir ifadenin fonksiyonudur. Ancak, buradaki ifade Gauss durumundaki basit üstel ifadeden daha karmaşıktır. Dolayısıyla *SIRP*, bilinen Gauss rastlantı sürecinin genel hali olarak karşımıza çıkar [16].

SIRV $\mathbf{X}$'in kovaryans matrisi $\Sigma = \mathbf{M}E\left\{S^2\right\}$ ile verilir ve burada $E\left\{S^2\right\}$, S rastlantı değişkeninin karesel ortalama değeridir. Buradan, S'nin karesel ortalama değeriyle normalleştirilen *SIRV* kovaryans matrisinin Gauss rastlantı vektörünün kovaryans matrisi olduğu görülür. $E\left\{S^2\right\} = 1$ alarak *SIRV* kovaryans matrisi Gauss kovaryans matrisi ile eşit yapılabilir. Buradan görüldüğü gibi, istenen bir Gauss dışı *SIRV* olasılık yoğunluk fonksiyonu uygun bir $f_S(s)$ fonksiyonu seçilerek elde edilebilir, diğer taraftan özilinti fonksiyonu Gauss sürecinin özilinti fonksiyonuna eşit yapılabilir [15]–[16]. Rangaswamy, Weiner ve Öztürk K-dağılımı ve bazı dağılımlar için karakteristik olasılık yoğunluk fonksiyonlarını kapalı form eşitlikler halinde vermiştir [16], [17].

2.3 Faz Uyumlu K-Dağılımlı Kargaşa Üretim Yordamı

Bu bölümde K-dağılımlı kargaşa işareti üretmek için gerekli işlem basamakları ele alınacaktır. Faz uyumlu bir gösterimde N dik bileşenden oluşan bir rastlantı vektörü üretmek ile $2N$ gerçel elemandan oluşan bir vektör üretmek birbirine denk işlemlerdir. Bu durumda, eş fazlı ve dik fazlı bileşenlerinin ortak varyansı

$$\sigma^2 = \frac{1}{2}E\left[X^2\right] \tag{6}$$

ile verilir.

Öncelikle, $2N$ elemanlı gerçel vektör

$$\mathbf{Y} = \left[Y_{c1}\quad Y_{s1}\quad \ldots\quad Y_{cN}\quad Y_{sN}\right] \tag{7}$$

ile tanımlansın. Burada, c ve s, sırasıyla, eş fazlı ve dik fazlı bileşenleri göstermektedir. K-dağılımlı bir zarf işaretinin olasılık yoğunluk fonksiyonu (1) eşitliğinde daha önce verildiği gibidir ve $2N$ bileşene ilişkin ilgili *SIRV* olasılık yoğunluk fonksiyonu da (8) eşitliğinde verildiği gibi olur [16]:

$$f_{\mathbf{Y}}(\mathbf{y}) = (2\pi)^{-N}\left|\mathbf{M}\right|^{-1/2} h_{2N}(q)$$
$$h_{2N}(q) = \frac{b^{2N}}{\Gamma(\alpha)}\frac{\left(\sqrt[b]{q}\right)^{\alpha-N}}{2^{\alpha-1}} K_{N-\alpha}\left(\sqrt[b]{q}\right) \tag{8}$$

K-dağılımlı *SIRV*'nin karakteristik OYF'si genelleştirilmiş χ olasılık yoğunluk fonksiyonu olup kapalı biçimde yazılabilmektedir. $f_S(s)$ karakteristik fonksiyonuna ve birim ortalama karesel değere (*unit mean square value*) sahip S değişkenini üretmek için (9) eşitliği ile verilen ilgili χ olasılık yoğunluk fonksiyonu kullanılabilir [16].

$$f_V(\upsilon) = \frac{2b}{\Gamma(\alpha)2^\alpha}(b\upsilon)^{2\alpha-1} exp\left(-\frac{b^2\upsilon^2}{2}\right)u(\upsilon) \tag{9}$$

Burada, b ölçek, α biçim parametresidir ve $u(\upsilon)$ birim basamak fonksiyonunu temsil eder. Bu dağılımda V rastlantı değişkeninin ortalama karesel değeri $a^2 = 2\alpha/b^2$ ile verilir. Buradan ortalama karesel değeri 1'e eşit olan S rastlantı değişkeni $S = V/a$ eşitliği ile elde edilebilir.

Yukarıda verilen tanımlama ve açıklamalar ışığında faz uyumlu, ilintili ve K-dağılıma sahip bir *SIRV* üretmek için gerekli işlem basamakları şöyle sıralanabilir:

1°) Sıfır ortalamalı ve birim kovaryans matrisli bir Z Gauss rastlantı vektörü elde et.

2°) Olasılık yoğunluk fonksiyonu $f_V(\upsilon)$ olan bir V rastlantı değişkeni üret ve bu değişkenin ortalama karesel değerini a^2 olarak tanımla.

3°) S değişkenini elde etmek için V değişkenini a ile normalleştir: $S = V/a$.

4°) $\mathbf{X} = \mathbf{Z}S$ çarpımını elde et. Bu aşamada sıfır ortalamalı ve birim kovaryans matrisli, beyaz gürültü özellikli bir *SIRV* elde edilmiş olur.

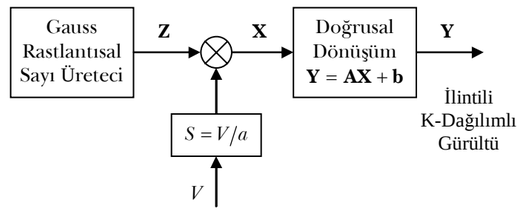
5°) Son olarak, istenen ortalama değerli ve istenen kovaryans matrisli *SIRV* $\mathbf{Y}$ vektörünü elde etmek için $\mathbf{Y} = \mathbf{A}\mathbf{X} + \mathbf{b}$ doğrusal dönüşümü uygulanır. (Gauss rastlantı vektörlerinin bir çok özelliği *SIRV*'lere de uygulanabilir. Benzetim amaçları açısından en önemli özellik doğrusal dönüşüm altında kapalılık özelliğidir (*closure property*) ve şu biçimde ifade edilebilir: Eğer $\mathbf{X}$ karakteristik olasılık yoğunluğu $f_S(s)$ olan bir *SIRV* ise $\mathbf{Y} = \mathbf{A}\mathbf{X} + \mathbf{b}$ eşitliği ile verilen $\mathbf{Y}$ aynı karakteristik olasılık yoğunluğuna sahip bir *SIRV*'dir. Burada, $\mathbf{A}$ matrisi $\mathbf{A}\mathbf{A}^T = \mathbf{\Sigma}$'yı veren doğrusal dönüşüm matrisi, $\mathbf{b}$ de $\mathbf{X}$ ile aynı boyutta, bilinen bir vektördür [16]. Bu özellik, özilintili kargaşa işaretlerinin oluşturulmasında doğrusal dönüşümün doğrudan kullanılabileceğini gösterir.)

İşlem basamakları biçiminde verilen K-dağılımlı kargaşa işareti üretim modeli Şekil 3'te ayrıca gösterilmiştir.

Olasılık yoğunluk fonksiyonu bir χ dağılımı ile verilen yukarıda (2°) basamağındaki V rastlantı değişkenini üretmek üzere Gama dağılımı üreteçlerinden yararlanılabilir.

2.4 Biçim Parametresi Ampirik Modeli

Ward ve arkadaşları büyük miktarda ölçülmüş veriye dayanarak K-dağılımının biçim parametresini kestirmek üzere ampirik bir bağıntı önermiştir [5], [19]. Veri tabanı içinde belirli bir dağılma gösteren sonuçlar basit bir fonksiyonel ifadeye indirgenmektedir. Bu yolla önerilen ampirik model (10) eşitliğindeki gibi verilebilmektedir:



Şekil 3. *Karakteristik OYF'si bilinen K-dağılımlı kargaşa işareti üretim modeli.*

$$\log(\alpha) = \frac{2}{3}\log(\psi) + \frac{5}{8}\log(l) + \xi - \kappa \tag{10}$$

Burada, α biçim parametresinin kestirilen değerini, l çapraz menzil çözünürlüğünü ($100\text{ m} < l < 800\text{ m}$), ψ derece cinsinden sıyırma açısını ($0{,}1^\circ < \psi < 10^\circ$) ifade etmektedir. ξ ise, denizin kabarma yönüne bağlılığı gösteren bir değişkendir ve aşağıdaki gibi tanımlanmaktadır:

- Kabarma yönünden yukarı ya da aşağı yönler için:

$$\xi = -\frac{1}{3}$$

- Kabarma yönüne yön için:

$$\xi = +\frac{1}{3}$$

- Kabarma olmadığı durumda ya da ara yönler için:

$$\xi = 0$$

κ polarizasyon etkisini tanımlamaktadır; $\kappa = 1$ dikey, $\kappa = 1{,}7$ yatay polarizasyon için verilmektedir.

İlginç olabilecek biçimde, deniz durumu değişmelerine, rüzgârın radar bakış açısına göreli geliş açısına ve rüzgar hızına istatistiksel olarak anlamlı olabilecek düzeyde bir bağlılık gözlenmemiştir. Ayrıca, yukarıdaki parametrelerin her biri ayrı ayrı biçim parametresindeki değişimlere uydurulduğu için parametreler arasındaki karmaşık ara-bağlılıklar ampirik modele katılamamıştır. Ampirik modelin oluşturulmasında kullanılan verilerin tümü 4 m menzil çözünürlüğüne sahip radar ile alınmış verilerdir. Bu nedenle modelde menzil çözünürlüğüne bağlılık bulunmamaktadır. Ancak, K-dağılımı biçim parametresini değiştirerek menzil çözünürlüğündeki kötüleşme durumunu sentezlemek olanaklıdır. Buradaki ampirik modelden biçim parametresi elde edilerek benzetim çalışmalarında kullanıldığında uzamda farklılıklar gösteren değişik kargaşa tiplerinin belirli bir çözünürlülük düzeyindeki eğilimleri elde edilmiştir [19].

2.5 Biçim Parametresinin Değişimi

Bir kıyı gözetleme radarının konuşlandırılabileceği en yüksek rakım 1200 m alındığında sıyırma açısının değeri önceki bölümde biçim parametresini kestirmek için verilen ampirik modelin geçerli olduğu $\psi_{\max} < 10^\circ$ üst sınırını sağlamalıdır. Bu koşul altında radarın önündeki kör bölge yaklaşık 6,8 km olmaktadır. Ampirik modelin geçerli olduğu alt sınır ise $0.1^\circ < \psi$ 'dir. Deniz seviyesinden 50m yüksekliğe yerleştirilmiş bir radar alt sınır koşulu sağlandığında yaklaşık 28,6 km menzili görebilecektir. Bu durumlar göz önüne alındığında ampirik modelin geçerli olduğu tüm sıyırma açısı aralığı kullanılmış olmaktadır. İki sınır durum ve radar 1200 m yüksekliğe yerleştirildiğinde $l < 800\text{ m}$ için gözleyebileceği menzil $R = 45{,}8$ km değeri dikkate alınarak,

gerekli parametreleri aşağıda verilen bir radar için K-dağılımı biçim parametresi α değerleri hesaplanmış ve Tablo 1'de verilmiştir:

- Yatay demet genişliği: $\theta_a = 1^\circ$,
- Menzil çözünürlüğü: $\rho = 3$ m,
- Denizde kabarma yok ya da ara yönlerde kabarma durumu: $\xi = 0$

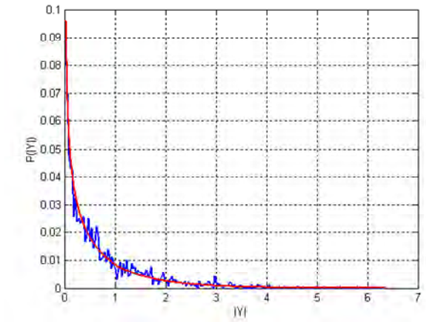
Tablodaki biçim parametresine ilişkin değerler incelendiğinde $\alpha = 0,21$ ile $\alpha = 9,20$ değerleri arasında kalındığı gözlenmektedir. Alt sınır değeri, Gama üretici sınırlılığı nedeniyle ancak $\alpha \cong 0,25$ alınabilmiştir. Bu çalışmanın amacına uygun olarak $\alpha = 1,71$ ve $\alpha = 9,20$ değerleri için faz uyumlu K-dağılımlı örnek serileri üretilerek gözlem ve sınamalar yapılmıştır.

Tablo 1. K-Dağılımı Biçim Parametresinin Üç Durumdaki Değeri

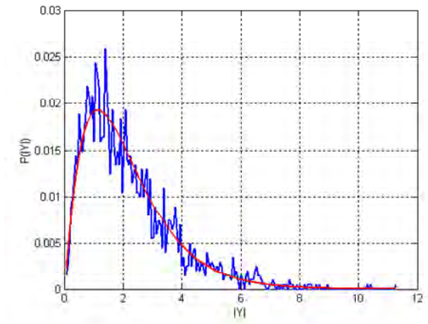
Sıyırma Açısı ψ [°]	**Menzil** R [m]	**Çapraz Menzil** l [m]	**Biçim Parametresi** α	
			Yatay Pol.	Düşey Pol.
~10°	6805	119	1,84	9,20
~0,1°	28645	500	0,21	1,05
~1,5°	45858	800	1,71	8,55

Biçim parametresine ilişkin yukarıda seçilen üç değer kullanılarak 2048 örneklik faz uyumlu K-dağılımlı ilintili kargaşa işaretleri üretilerek bunların istatistiksel sınama işlemleri Kolmogorov-Smirnov istatistiksel uygunluk testi yapılarak gerçekleştirilmiştir. İşaretler üretilirken SIRV vektörlerinin boyutu, kırpışma bileşeninin bir özelliği olan özilinti fonksiyonunun sönümlenmesine izin verecek ve darbe tümleştirme sayısına uygun olacak biçimde $N = 16$ olarak seçilmiştir. Özilinti fonksiyonu [20]'de tanımlandığı gibi alınmıştır. İstatistiksel sınama sonuçlarından her üç durumda da kargaşa işaretlerinin mutlak değerinin K-dağılımlı olasılık yoğunluk fonksiyonuna sahip olduğu görülmüştür. Şekil 4'te aynı işaretlerden elde edilen örnek OYF'ler (*sample PDF*) ile biçim parametresi kullanılarak elde edilen analitik olasılık yoğunluk fonksiyonuları üst üste çizdirilmiş olarak görülmektedir.

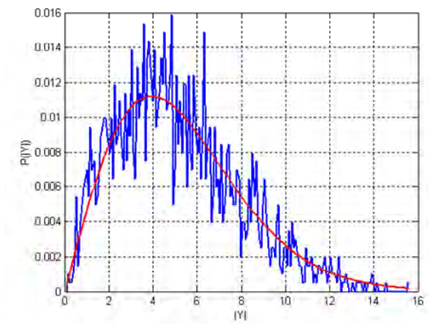
K-dağılımlı kargaşa modeli çıkışındaki işaretlerde kırpışma bileşenini ve onu modüle eden Gama bileşenini gözlemlemek üzere üretilen faz uyumlu zaman serilerinin mutlak değerleri Şekil 5'te biçim parametrelerine göre çizdirilmiştir. Biçim parametresinin küçük değerlerinde Gama bileşeninin etkisi işaretlerde gruplaşma/topaklaşma



(a)



(b)



(c)

Şekil 4. *Örnek OYF'ler ve biçim parametresi ile elde edilen analitik K-dağılımı OYF'leri (örnek sayısı = 2048):*
a) $\alpha = 0,251$, b) $\alpha = 1,71$, c) $\alpha = 9,20$.

biçiminde kendisini göstermekte, biçim parametre değeri büyüdükçe belirli bir ortalama değere sahip Rayleigh dağılımlı serilere benzemektedir. Şekil 5(d)'de *SIRV* vektörünün eleman sayısı $N = 64$'e çıkarıldığında uzun dönemli ilintiyi temsil eden Gama bileşeninin etkisinin daha

belirgin bir topaklaşma biçiminde elde edildiği görülmektedir. Dağılımın Gauss dışı ve kuyruklu bir dağılım olması nedeniyle işaretlerde sıçrama niteliği ayrıca gözlenmekte, biçim parametresi büyüdükçe bu etki azalmaktadır.

2.6 Temel Algılayıcı Yardımıyla Bir Karşılaştırma

Basit bir algılayıcı, bir zarf algılayıcı ve belirli bir sabit değere ayarlanmış genlik eşiği ile kurulabilir. Bu algılayıcının radarın her bakış açısında gönderilen bir darbeye/dalga şekline karşılık menzil boyunca algılama yaptığı ve başarımının bir çok bakış açısı üzerinden ölçüldüğü varsayılabilir. Aynı zamanda, kargaşa zarf işaretinin olasılık modeli için en genel biçimde Rayleigh dağılımı varsayımı yapılabilir. Bu durumda, yanlış alarm olasılığı (*Probability of False Alarm*) P_{FA} (11) eşitliğinde görüldüğü gibi ifade edilir:

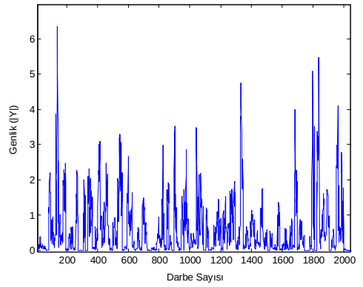
$$\mathrm{P_{FA}} = \int_{E_T}^{\infty} \frac{r}{\sigma_K^2} \exp\left(\frac{r^2}{2\sigma_K^2}\right) dr \qquad (11)$$

Burada, E_T genlik eşiğini, σ_K^2 kargaşa zarf işaretinin varyansını temsil etmektedir. (12) eşitliği kullanılarak E_T genlik eşiği yanlış alarm olasılığı ve kargaşa işaretinin varyansına bağlı olarak aşağıdaki gibi verilebilir:

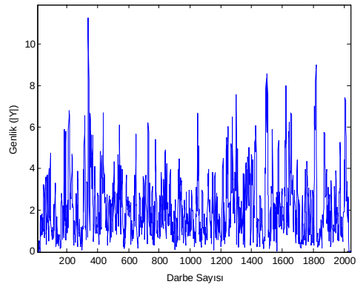
$$E_T = \sqrt{2\sigma_K^2 \ln\left(1/\mathrm{P_{FA}}\right)} \qquad (12)$$

Olasılık yoğunluk fonksiyonu Rayleigh dağılımından ayrı olan bir kargaşa zarf işareti E_T eşiğini kullanan algılayıcıya uygulandığında kargaşa işaretinin varyansı tam olarak kestirilse dahi model uyuşmazlığı nedeniyle yanlış alarm olasılığının tutması beklenemez. Ancak, elde edilen P_{FA} değerleri dağılımlar arasında basitçe bağıl bir karşılaştırma yapılmasını sağlayabilir. Tablo 2'de K-dağılımı için iki biçim parametre değeri seçilerek, özilintili ve özilintisiz kargaşa işaretleri için kestirilen yanlış alarm olasılıkları verilmiştir. Özilintili durum için ilgili bir ilinti elde etmek üzere 12 nci dereceden özbağlanımlı (*AR*) süzgeç kullanılmıştır.

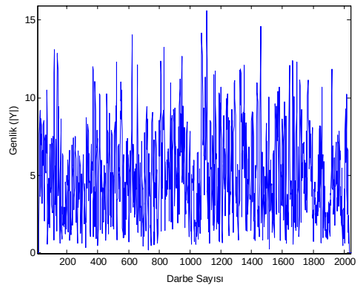
Tablo 2'den görüldüğü gibi Rayleigh dağılımına göre seçilen sabit eşikleme ile başka bir dağılıma sahip kargaşa işareti eşiklendiği zaman P_{FA} değerleri önemli ölçüde değişmektedir. Özellikle küçük P_{FA} değerleri hedeflendiği durumda yanlış alarm oranı beklenen değerinden önemli ölçekte sapmaktadır. Büyük P_{FA} değerinde biçim parametresine bağlı sapma önemli ölçüde gerçekleşmezken, küçük P_{FA} değeri hedeflendiğinde ve biçim parametresinin küçük değerlerine gidildiği durumda sapma oranı artmaktadır. İlintili olma özelliği de benzer biçimde etki etmekte; küçük P_{FA} hedeflendiğinde ve küçük biçim parametresi söz konusu olduğunda ilintili olma niteliği P_{FA} değerini daha büyük miktarda arttırmaktadır. Bu sonuçlar



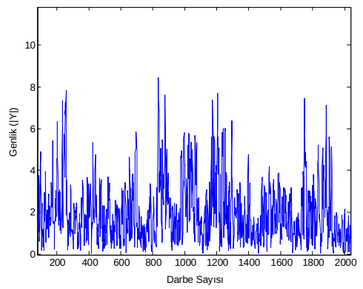
(a)



(b)



(c)



(d)

Şekil 5. *K-dağılımlı kargaşa modeli çıkışında biçim parametresine göre elde edilen genlik (mutlak değer) işaretleri:*
a) $\alpha = 0,251$, $N = 16$, b) $\alpha = 1,71$, $N = 16$
c) $\alpha = 9,20$, $N = 16$, d) $\alpha = 1,71$, $N = 64$.

uzun kuyruklu dağılımlar ve özilintili işaretlerden beklenen özelliklerle uyuşmaktadır.

Tablo 2. P_{FA}**'nın K-Dağılımı ve Özelliklerine Bağlı Değişimi**

P_{FA}	Örnek Sayısı	Rayleigh Dağılımı için $\hat{P}_{FA}$	K-Dağılımı için $\hat{P}_{FA}$			
			$\alpha = 2$		$\alpha = 5$	
			İlintili	İlintisiz	İlintili	İlintisiz
10^{-3}	10^{5}	$1{,}1\times10^{-3}$	$2{,}7\times10^{-3}$	$2{,}8\times10^{-3}$	$2{,}5\times10^{-3}$	$2{,}2\times10^{-3}$
10^{-5}	10^{6}	$1{,}1\times10^{-5}$	36×10^{-5}	29×10^{-5}	$14{,}9\times10^{-3}$	$15{,}5\times10^{-5}$

3 SONUÇ

Mikrodalga radar işaretlerinde deniz kargaşasını modellemeye dönük bu çalışmada, dışyapılı (*exogenous*) kargaşa modeli kullanarak faz uyumlu ve ilintili deniz kargaşa işaretlerinin üretilmesi konusu ele alınmıştır. İşaretlerdeki yavaş değişen bileşenin (Gama bileşeni) dışyapılı modelde bulunması nedeniyle K-dağılımı yordamı yüksek çözünürlülüklü radar ile ölçülen işaretlerin özelliklerine daha yakın kargaşa işaretlerinin üretilebilmesini sağlamaktadır.

Dışyapılı modelde özilinti fonksiyonu doğrusallık dışı bir dönüşümden geçirilmediği için istenen ilinti fonksiyonlarını gerçekleştirmek üzere yüksek dereceli özbağlanımlı süzgeçler elde etmek olanaklıdır. K-dağılımlı kargaşa için verilen ampirik model ile sıyırma açısına, menzil çözünürlüğüne, denizin kabarma yönüne ve polarizasyona göre biçim parametresini hesaplamak, daha sonra K-dağılımı serileri elde ederek bunları alıcı karakteristiklerinin çıkarılmasında ve benzetimlerde kullanmak mümkündür.

TEŞEKKÜR

Bu yazının gözden geçirilmesi sırasındaki katkıları ve titizliği nedeniyle Sayın Dr. Levent Balamir Tavacıoğlu'na ve Sayın Sencer Melih Deniz'e teşekkür ederim.

KAYNAKÇA

[1] S. Haykin and S. Puthusserypady, *Chaotic Dynamics of Sea Clutter*. John Wiley & Sons, 1999, pp. 7–12.

[2] V. U. Zavorotny and A. G. Voronovich, "Two-scale model and ocean radar Doppler spectra at moderate- and low-grazing angles," *IEEE Trans. Antennas Propag.*, vol. 46, no. 1, pp. 84–92, Jan. 1998.

[3] E. Jakeman and P. N. Pusey, "A model for non-Rayleigh sea echo," *IEEE Trans. Antennas Propag.*, vol. 24, no. 6, pp. 806–814, Nov. 1976.

[4] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 2nd ed., Singapore: McGraw-Hill, 1984.

[5] K. D. Ward, C. J. Baker and S. Watts, "Maritime surveillance radar — part 1: radar scattering from the ocean surface," *IEE Proc. Radar Signal Process.*, vol. 137, no. 2, pp 51–62, Apr. 1990.

[6] Y. Ishikawa, M. Sekine, T. Musha, "Observation of K-Distributed sea clutter via an X-Band radar," *Electron. Commn. Japan (Part I: Commun.)*, vol. 77, no. 11, pp. 72–82, Nov. 1994.

[7] A. Farina, F. Gini, M. V. Greco and L. Verrazzani, "High resolution sea clutter data: statistical analysis of recorded live data," *IEE Proc. Radar, Sonar Navig.*, vol. 144, no. 3, pp. 121–130, June 1997.

[8] D. C. Schleher, *MTI Radar*, Dedham. MA: Artech House, 1978, pp. 37–73.

[9] F. T. Ulaby and M. C. Dobson, *Handbook of Radar Scattering Statistics for Terrain*, Dedham, MA: Artech House, 1989.

[10] L. J. Marier, Jr., "Correlated K-Distributed clutter generation for radar detection and track," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 31, no. 2, pp. 568–580, Apr. 1995.

[11] E. Conte, M. Longo and M. Lops, "Modeling and simulation of non-Rayleigh radar clutter," *IEE Proc. Radar Signal Process.*, vol. 138, no. 2, pp. 121–130, Apr. 1991.

[12] R. L. Fante, "Probability of detecting a fluctuating target immersed in both noise and clutter," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 13, no. 6, pp. 711–716, Nov. 1977.

[13] A. Farina, A. Russo, F. Scannapieco and S. Barbarossa, "Theory of radar detection in coherent Weibull clutter," *IEE Proc. Commun., Radar Signal Process.*, vol. 134, no. 2, pp. 174–190, Apr. 1987.

[14] S. Watts, "Cell-averaging CFAR gain in spatially correlated K-distributed clutter," *IEE Proc. Radar, Sonar Navig.*, vol. 143, no. 5, pp. 321–327, Oct. 1996.

[15] M. Rangaswamy, D. D. Weiner and A. Öztürk, "Simulation of correlated non-Gaussian interference for radar signal detection," *Proc. 25th Asilomar Conf. Signals, Systems and Computers*, Pasific Grove, California, Nov. 1991, vol. 1, pp. 148–152.

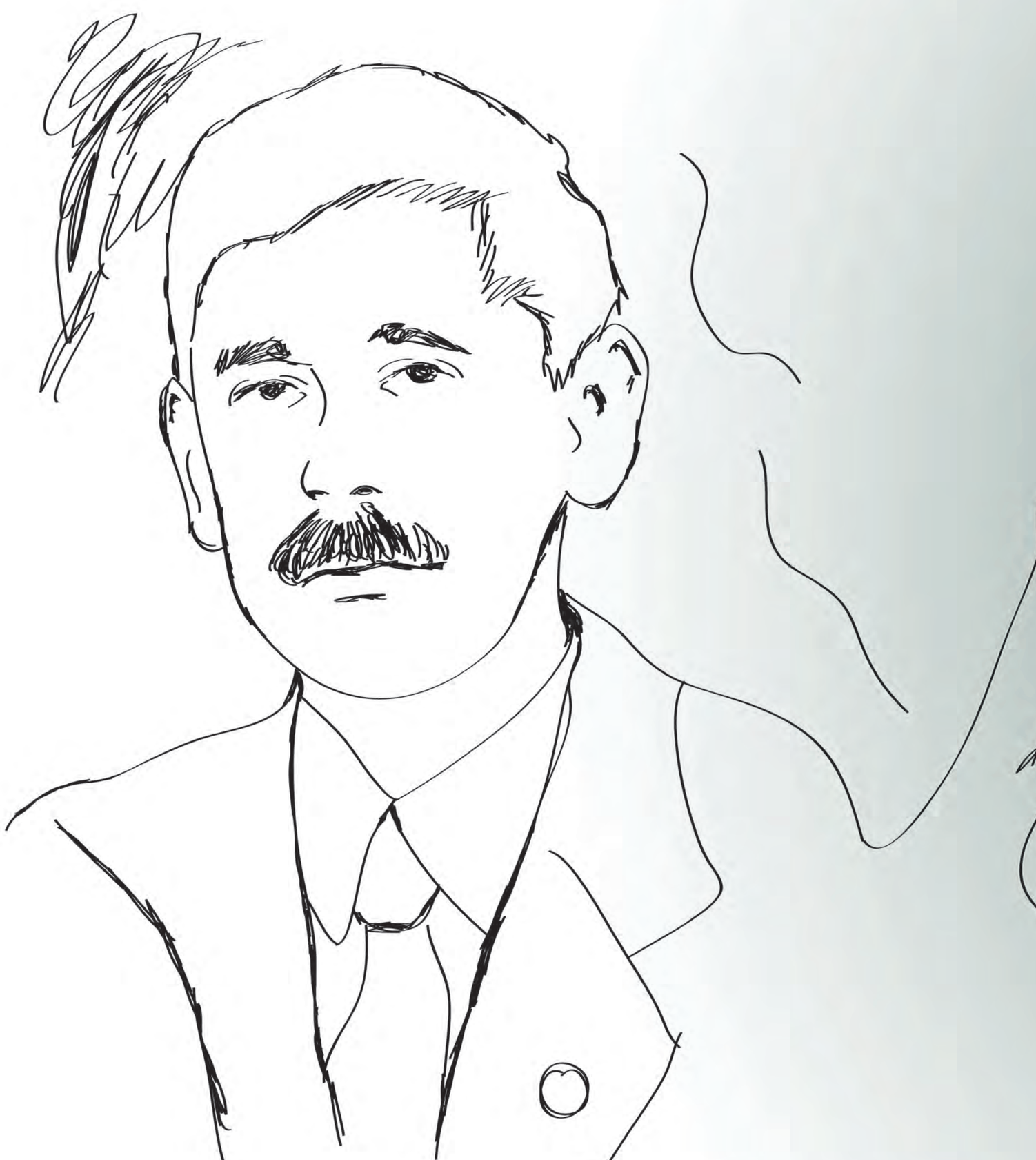
[16] M. Rangaswamy, D. D. Weiner and A. Öztürk, "Computer generation of correlated non-Gaussian radar clutter," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 31, no. 1, pp. 106–116, Jan. 1995.

[17] M. Rangaswamy, D. D. Weiner and A. Öztürk, "Non-Gaussian random vector identification using spherically invariant random processes," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 29, no. 1, pp. 111–124, Jan. 1993.

[18] E. Conte and M. Longo, "Characterisation of radar clutter as a spherically invariant random process," *IEE Proc. Commun., Radar Signal Process.*, vol. 134, no. 2, pp. 191–197, Apr. 1987.

[19] S. Watts and K.D. Ward ,"Spatial correlation in K-distributed sea clutter," *IEE Proc. Commun., Radar Signal Process.*, vol. 134, no. 6, pp. 526–532, Oct. 1987.

[20] Y. Bahadırlar, "Mikrodalga Radarda Kargaşa ve Gürültü Modelleme", *TÜBİTAK BİLGEM BTE Arşivi - Teknik Rapor*, UU-ADP MWRS 205, Sürüm-2, 2003.



Mustafa AKTEKİN

Başarı Öyküsü / Çağrı KOÇ

1950 yılının 12 Mayıs'ında başlayan bir yaşam öyküsü, 2004 yılının temmuz ayında, beklenmedik bir biçimde son buldu.

Yerli yersiz gündeme gelen, belki de kasıtlı olarak getirilen bir trafik kazası, onu ve iki kişiyi daha, sevenlerinden erken ayırdı. Oysa her birinin hayalleri, planları, umutları vardı. Yaşanamadan kalan hayaller, planlar... Herhalde bu nedenle başsağlığı ziyaretimizde, Mustafa Bey'in eşi bize şu öğüdü vermişti: "*Sakın yaşamınızı ertelemeyin.*"

AKADEMİK YAŞAMI

Mustafa Aktekin'in mühendislik yaşamı 1972 yılında, İstanbul Teknik Üniversitesi Elektrik Fakültesi'nden yüksek mühendis diploması alarak mezun oldu. 1973 yılının Ocak ayında Karadeniz Teknik Üniversitesi'nde asistan olarak göreve başladı. Burada, mühendislik fakültesine bağlı Elektronik ve Haberleşme Mühendisliği Bölümü'nün kuruluş çalışmalarında görev aldı. Henüz çok yeni olan bölümün laboratuvarlarını kurmayı kendine görev edindi.

Bu dönemi, Prof. Dr. Atilla Ataman'dan dinliyoruz:

"Almanya'da doktora çalışmamı tamamlayıp 1973 yılının Ekim ayında Karadeniz Teknik Üniversitesi'ne geldiğimde Mustafa oradaydı. O sırada her şey yeni kuruluyordu; sadece makine-elektrik fakültesi vardı. Sonradan YÖK ile birlikte, mühendislik fakültesi kuruldu; altındaki bölümlerden biri de elektrik-elektronik mühendisliği b ölümü oldu. O dönemde İTÜ'den hocalar görevli olarak gelir giderlerdi. Mustafa, bu hocalardan Sn. Oruç Bilgiç ve Sn. Turgut Menalioğlu ile birlikte, çok güzel çalışmalar yapmış, laboratuvarların kurulmasında ve deney föylerinin hazırlanmasında çalışmıştı.

Karadeniz Teknik Üniversitesi'nde ders verirken.

Güzel de bir arkadaşlıkları vardı; onların Trabzon'da kaldıkları akşamlar birlikte Boztepe'ye giderler, yemek yer, sohbet ederlerdi. O zaman Trabzon'da bir Özgür Otel vardı. İTÜ'den gelen hocalar orada kalırlardı; biz de giderdik. Mustafa, özellikle Ord.Prof.Dr.Bedri Karafakioğlu'nun geldiği günleri hiç kaçırmaz, mutlaka o sohbet toplantılarına katılırdı...

O dönemde 850.000 USD civarında bir geliri olan bir United Nations Development Programme (UNDP) projemiz vardı. Bu proje kapsamında yurtdışına eleman gönderebiliyorduk; makina-teçhizat alabiliyorduk; yurtdışından danışman getirtebiliyorduk. Biz uzun pazarlıklarla proje makamını yurtdışından danışman istemediğimize ikna etmiş, o kalemdeki kaynağı da diğer ikisine aktartmıştık. Mustafa da bu proje kapsamında doktora yapmak üzere yurt dışına gitmişti."

Karadeniz Teknik Üniversitesi'nde.

Mustafa Aktekin, 1976 yılında doktora yapmak üzere İngiltere'ye, Sussex Üniversitesi'ne gitti. Gitmeden hemen önce, 1976 yılının Şubat'ında, kendi deyişiyle "birlikte yaşlanmak için" eşi Sema Hanım ile evlendi. 1980 yılında "Bandwidth Compression in a Digital Packet Switching Communication Link" konulu doktora tezini başarıyla tamamladı ve zorunlu hizmetini yapmak üzere, Trabzon'a, yine Karadeniz Teknik Üniversitesi'ne döndü.

Prof. Dr. Atilla Ataman, bu konuda şunları söylüyor:

"Aslında bizim onun için düşündüğümüz doktora çalışması yarıiletken teknolojileri ile ilgiliydi ama Mustafa bambaşka bir konuyu tercih etmişti. Ama seçtiği konu da, yaptıkları da büyük bir kazançtı ülke için. Biraz içine kapalı, ketum bir yapısı

TELETAŞ'ta, Erhan Yücel'le beraber.

vardı ama son derece iyi bir mühendisti. Zaman zaman karşısındakine aktarmakta zorlansa da aklındaki kurgu her zaman çok temiz ve çok doğru olurdu. Pırıl pırıl, nitelikli ve hassas bir insandı. Dedikodudan ve politikadan uzak dururdu. Kendi işiyle ilgilenmeyi tercih ederdi."

Mustafa Aktekin, Karadeniz Teknik Üniversitesi'nde asistan, doktor asistan ve yardımcı doçent olarak geçirdiği zaman diliminde, laboratuvarların kurulmasına ek olarak, lisans ve lisans üstü programlarda dersler ve tezler verilmesi gibi çalışmalar yürüttü.

Mustafa Aktekin, 1985 yılında doçentlik sınavını başarıyla vererek Doçent ünvanını taşımaya hak kazandı.

TEORİ İLE PRATİĞİN BULUŞMASI

1985 yılı, önemli bir yıl. Çünkü oluşturduğu bilgi birikimini, pratiğe dökmeye karar verip İstanbul'a, bir zamanların zirvedeki şirketi, TELETAŞ[1]'a geldi. Burada yerli sayısal santrallar ve uçbirimleri tasarlayan birimlerin başına geçerek aynı anda 3 proje grubuna önderlik etti. Bu gruplardan ilki telefon grubu. Belçika'daki Alcatel Bell'den getirilen telefonların yerine geçecek ürünlerin tasarımlarının yapıldığı grup. İkincisi modem tasarım grubu. Sonuncusu ise, santral grubu. Yani uzun süre şirketin büyük ortağı olan Alcatel Bell'den gizli yürütülen milli sayısal telefon santralı projesinin tasarım ekibi. Bu ekibin geliştirdiği santrallar, üretilip PTT ile yapılan sözleşme gereği sahaya kurulduklarında, Türkiye, bütün dünyadaki 9. santral ailesinin sahibi olmuştu.

TELETAŞ'ta, Canan Mörü Ceylan ile.

Bolu'da Levent Santrali'ni PTT'ye tanıtırken.

Bizim Sn. Aktekin ile yollarımızın kesiştiği yıl 1987. Santral grubu. Bugün BİLGEM ve UEKAE kadrosunda çalışmakta olan bazı arkadaşlarla birlikte, TELETAŞ'a sıfır kilometre mühendis olarak girmiştik. Okulda öğrendiklerimizin gerçek yaşamdaki yerini, mühendislik mantığını, hatta iş yaşamının kurallarını ondan öğrendik. Yeri geldi biz onu çileden çıkardık, yeri geldi verdiği kısa takvimlerle o bizi kızdırdı. Ama gerçek şu ki, işlerin hızlı bitmesi için herkesi zorlarken hedefi hem projeyi tamamlamak hem de akademik geçmişinin etkisiyle bizleri bir adım ileri götürmekti.

Bu açılardan bakıldığında çalışma ortamımız gerçek bir okul gibiydi. Yerli bir santralı ortaya çıkarmayı ve kullanılır hale getirmeyi aklımıza koymuştuk. Kanımıza işleyen başarma hırsı ve zevki o dönemde öğrendiklerimizdi. TÜBİTAK'a geldiğimizde yaptıklarımızı yapma gücünü veren veren de aynı duygulardı. O günlerdi bizler için kırılma noktası. O dönemde öğrendiklerimiz ve birlikte yaptıklarımızdı sonrasında bize ülkemiz için teknolojik bağımsızlığı kazanma hedefini koymamızı sağlayan. O günlerdi, yabancı yapar, biz yapamayız kanısının silindiği günler... Mustafa Aktekin'in bütün bunlarda çok ciddi payı vardı; yurt dışına gidenleri eleştirir, bilgi birikiminin ülkemizde kalmasına büyük önem verirdi; "Yabancılar yapıyorsa biz de yaparız" derdi her zaman. Zaman içinde içimize işledi hepsi...

[1] TELETAŞ Telekomünikasyon Endüstri ve Ticaret A.Ş. : 1993 yılında yapılan olağanüstü (!) özelleştirme sonrasında, zaman içinde eriye eriye ALCATEL LUCENT TELETAŞ haline gelen, birçok yerde adı dahi anılmayan, ulusal ürün tasarım ve üretiminin temellerinin atıldığı şirket.


Doğayı ve doğada vakit geçirmeyi çok severdi.

Biz, yani şu anda BİLGEM ve UEKAE'de çalışmaya devam eden bir grup mühendis, 1994 yılına kadar Mustafa Aktekin ile birlikte çalıştık. 1993-1994 yılları, biraz önce sözünü ettiğimiz özelleştirme ve sonrasındaki huzursuzluk dönemiydi. Bu dönemi, ne yapacağımızı düşünerek, seçenekleri değerlendirerek, kendi aramızda toplanarak geçirmiştik. Sonunda, bizden önceki ekibi izleyerek, UEKAE Müdürü Sn. Alparslan Babaoğlu'nun deyişiyle, "kapısında Türk bayrağı dalgalanan" TÜBİTAK'ta karar kılmıştık.

O dönemde Mustafa Aktekin, bizlerle aynı sıkıntıları yaşamakla ve bütün toplantılarımıza katılmakla birlikte, bizim gibi gemileri yakıp TÜBİTAK'a gelmemişti.

Bu noktada, ailesine, çocuklarına olan düşkünlüğünden söz etmek gerek. İşe ilk başladığım, iş dünyasının ciddi ve ağırbaşlı olması gerektiğini düşündüğüm yıllarda, Mustafa Aktekin'in bilgisayar parolalarını çocuklarının adlarından türettiğini öğrenmiş ve çok şaşırmıştım! Bu belki onun uzaktaki ideal mühendis kavramından, "insan ve iyi mühendis" kavramına geçişti benim için... Daha yakın, daha insancıl, daha bizden biri... Bundan sonra başlamıştı grupça hep birlikte gittiğimiz tiyatrolar, konserler, gün içinde kutladığımız doğum günleri...

Sohbet anlarında hareketsiz duramayışı, konuşurken ya da beklerken sürekli iki yana sallanması da, hiç yitirmediği çocuk ruhunun, coşkusunun ve enerjisinin bir dışavurumu olarak hala anılarımızda. İki kızı ve bir oğlu olan Mustafa Aktekin, yıllar sonra dünyaya gelen küçük oğluna mekanik oyuncaklar yapacak kadar yaratıcılığını ve çocuk ruhunu canlı tutmuştu.


Oğlu Mert'le.

Mustafa Aktekin, 1995 yılının Ağustos ayından 1998 sonuna kadar olan dönemi SİMKO[2]'da geçirdi. Burada, şirketin Özel Şebekeler Bölümü'nde proje müdürü olarak görev yaptı. Bir PBX[3]'in üst düzey tasarımından ön üretimine kadar olan sürecin yönetiminden sorumlu müdür olarak görev yaptığı SİMKO'dan, Yıldız Teknik Üniversitesi kampüsündeki KOSGEB'de kurduğu kendi şirketine geçti: MAKS Elektronik Sistemler Geliştirme Sanayi ve Ticaret Ltd. Şti.

Kendi patronu olma süreci, 2000 yılının Haziran ayına kadar sürdü. Buradaki temel ilgi alanını da yine sayısal santrallar ve işaretleşme sistemleri oluşturdu. Değişik projelerde çalıştıktan sonra, o dönemde TÜBİTAK'a doğrudan bağlı olarak çalışan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'ne proje yöneticisi olarak geldi. Ne diyelim, 1994'ten 2000'e kadar dayanmıştı; kadere karşı gelinmiyor; burada buluşuyoruz...

2000 yılında başlayan TÜBİTAK yaşamı süresince kendisiyle birlikte çalışan ekip ile konuşuyoruz şimdi de:

Ekibin Mustafa Aktekin ile tanışıklığı 2000 yılında MAKS'a yaptıkları ziyaret ile başlıyor. Oradaki çalışmalar ve TÜBİTAK'taki projeler hakkında bir

2 SIEMENS-SİMKO Ticaret ve Sanayi A.Ş.
3 PBX : Private Branch Exchange


Kızları Burcu ve Yaprak, oğlu Mert ve eşi Sema Hanım'la birlikte.

görüşme yapıyorlar öncelikle. Karşılıklı olarak bir uyumun sağlanacağına inanılmış olacak ki, bu görüşme bir proje ekibi bünyesinde birlikte çalışma ile sürüyor. Ekip arkadaşları Sn. Can Çevikbaş ve Sn. Celal Mızrak, bu çalışmayı şöyle anlatıyorlar: "Hem de ne çalışmak, gece gündüz uğraştığımız olurdu. Projede zaman kısıtı vardı ve bu baskıyı çok yoğun yaşıyorduk. Sadece çalışırdık; başka hiçbir şeye zaman yoktu. Birlikte yaptığımız en sosyal etkinlik, yine proje için Ankara'ya yaptığımız yolculuklardı. Gün boyu çalışıp, gece de devam edip ertesi sabah 05:00'da Ankara'ya gitmek üzere yola çıktığımız çok olmuştu." Böyle bir yoğunluğun yaşandığı bir çalışma ortamında insanları bir arada tutan ne olabilir? İş ahlakı? Göreve bağlılık? Adanmışlık? Sanırız hepsi...

Ekibin bir diğer üyesi Sn. Sevil Yücel, mühendislik yaşamına Mustafa Aktekin'in yanında başlayanlardan. İş hayatında kendisi için koyduğu hedef, "onun gibi bir mühendis olmak". Kendisine kulak veriyoruz: "Teknik bilgisi ve yetkinliği öyle bir düzeydeydi ki, ne yapacağını bilemeyen insanlara ve yavaşlığa tahammülü yoktu. Bir işin yapılmasını beklemek yerine o işi kendisi yapmayı seçebilirdi. Bu yüzden onu bazen kablo çekerken bile görebilirdiniz."

TELETAŞ'tan beri onu tanıyan ve birlikte çalıştığı son yöneticisi olan Sn. Önder Yetiş, kendisini "harikulade bir sistem mühendisi" olarak tanımlıyor. "Hayal eder, tasarlar, ortaya koyardı" diyor. Onun gibi birinin kolay kolay yetişmeyeceğini vurguluyor ve sürekli birşeylerle meşgul olan aklının, ne zaman ne tasarlayacağının belli olmadığını söylüyor. Gerçekten de Mustafa Aktekin'in bilimsel merakı ve araştırmacı kişiliği, onun sadece elektronik ile ya da sadece mühendislikle sınırlı kalmayıp başka alanlarla da ilgilenmesine yol açmıştı zaman içinde. Öylesine değişik alanlarla ilgilenirdi ki, kendisiyle örneğin Mısır piramitlerini konuşabilirdiniz. Bir dişçiyle ya da tıp doktoruyla da ciddi tartışmalara girebilirdi.

En temel özelliği herşeyi, ama herşeyi sorgulamasıydı. Gözlemciydi ve yaptığı gözlemleri günlük yaşamda kullanırdı. Olayların değişik açılarını bulmayı sever, hiçbir şeyi söylendiği ya da anlatıldığı biçimiyle kabullenmezdi. Kolay ikna olmazdı; mutlaka mantıklı açıklamalar beklerdi. Denge ve tutarlılık beklerdi. Yenilikleri, yeni teknolojileri yakından izler, onları tasarımlarında kullanırdı. Çevresindekilere, cocuklarına, öğrencilerine, hep bakış açılarını genişletmeleri gerektiğini söyler, isterlerse hayatta herşeyi yapabileceklerini anlatırdı. Durmazdı; duranı da sevmezdi. Ununu eleyip eleğini asmış insanlar ve bu felsefe, öfkelendirirdi onu. Bütün bu yaklaşımlar, onunla birlikte çalışan insanların kişiliğine işlerdi bir şekilde...

SON SÖZ

Onu aramızdan alan o t emmuz gecesinin ve sabahının anıları hafızalarımızda hala tazeliğini koruyor. Beklenmedik biçimde, veda bile edemeden ondan ayrılmak zorunda kaldık ama bilgisiyle, insanlığıyla, ilkeleriyle birçoğumuzun yaşamında derin izler bıraktı. Onu tanımak ve onunla çalışmış olmak büyük bir şanstı bizler için. Onun projelerinden, diğer bir deyişle onun okulundan yetişen birçok mühendis, birçok başarılı projeye imza attı; atıyor; durmayacaklar da üstelik; devam edecekler. İnsanlar onları hatırlayan olmadığında, unutulduklarında ölürler. Öyleyse Mustafa Aktekin'in öldüğünü söylemek mümkün mü?

Sevgiyle ve özlemle anıyoruz kendisini... Unutmadık...

Aktekin ailesine katkılarından dolayı teşekkür ederiz.

TÜRK MUTFAĞI

zülal cingil

Dünyanın sayılı mutfaklarından biri olan Türk mutfağı, ülkemizin geleneksel mutfağıdır. Türk mutfağında asıl olan karın doyurmak değil, ağız tadı ile yemek yemektir. Yöreden yöreye farklılaşan ürünleriyle Osmanlı mutfağının mirasçısı olan Türk mutfağı, Balkan ve Ortadoğu mutfaklarını etkilemiş, aynı zamanda bu mutfaklardan da etkilenmiştir.

Arkaplan: Cevizli kabak tatlısı.

Türk mutfak kültürünü incelerken, Türklerin 10. ve 11. yüzyıllara kadar dayanan, Orta Asya geçmişinden günümüze uzanan tarihsel süreçle karşılaşırız. Göçebe yaşamdan Anadolu'ya gelip, yerleşik düzene geçildikten sonra mutfak kültüründe de değişimler yaşanmıştır. Bugün tanımladığımız Türk mutfağı; Anadolu'da Selçuklu, Bizans, İran-Abbasi ve Osmanlı mutfaklarının etkisiyle yüzyıllar boyunca değişerek, zenginleşmiş ve olgunlaşmıştır.

Türkler, Orta Asya'dan konserve türündeki yiyeceklerden yoğurt, pastırma, bulgur ve tarhanayı Anadolu'ya getirmişlerdir. Bu yiyecekler tamamen Türk buluşudur ve Türklerin göçebelik, hayvancılık, tarıma dayalı sosyo-ekonomik yapılarının gereği olarak ortaya çıkmış kültür ürünleridir.

15. yüzyılda İstanbul'un fethi ile başlayan ve 19. yüzyıl sonlarına kadar devam eden süreç içinde Osmanlı Sarayı mutfak kültürü gelişmiştir. Bu gelenekte kuzu ve koyun etiyle hazırlanan kebap, yahni, külbastı ve köfteler, pirinç pilavının çeşitleri, tahıl ve baklagilleri içeren et suyu ile pişirilmiş çorbalar, yaş ve kuru meyveler ile hazırlanmış hoşaf, şerbet, şurup, reçel ile çevirmeler, börek çeşitleri, etli dolmalar, zeytinyağlılar, tavuk ve balık yemekleri, helva çeşitleri, baklava, güllaç, kadayıf ve sütlü tatlıları görürüz. Türk mutfağı pekmez, yoğurt, bulgur gibi kendine özgü sağlıklı yiyecek türlerini de ortaya çıkarmıştır.

Yemekler her zaman tuzsuz tereyağı ile pişirilmektedir. Baharat kullanımı oldukça yaygındır. Osmanlı Saray mutfağında kullanımı yaygın olan kuru ve yaş meyvelerin baharat olarak et ve pilavlarda kullanımı 19. yüzyıl mutfak geleneğinde azalmıştır.

Et çeşiti olarak mevsiminde kuzu diğer zamanlarda ise koyun eti kullanılmaktadır. Tavuk, güvercin, keklik, kaz, bıldırcın, ördek ve 18. yüzyıldan itibaren hindi saray mutfak geleneğinde zengin sofralara sunulan ayrıcalıklı tatlar olarak yerini almıştır. Balık da Osmanlı Saray mutfağında sultan ve çevresinin severek tükettiği lezzetlerin içinde yer almaktadır.

Tencere yemekleri geçmişte koruk, limon suyu, nar ekşisi ve tabii ki soğanın yanı sıra çeşitli baharatlar ile tatlandırılırdı. Saray mutfaklarında sıradan halkın tükettiği bulgur yerine pirinç; bal, pekmez yerine şeker; esmer ekmek ve yufka yerine beyaz mayalı ekmek çeşitleri tüketilirdi. Domates, fasulye, patates, hindi, kakao, mısır, bazı kabak çeşitleri 18. ve 19. yüzyıllarda Osmanlı mutfağına girmiştir. Türk mutfağında çok kullanılan domates ve domates salçası kullanımı 20. yüzyıl başlarında başlayan bir yeniliktir.

19. yüzyılda batıya açılan Osmanlı Sarayı, mutfak kültüründe de Avrupa'dan etkilenmiştir. Önceleri sofra adabında yenilikler benimsenmeye başlamış, sini yerine masa, minder yerine sandalye, ortak kullanılan tabak yerine bireysel tabak ve beraberinde çatal, bıçak ve su takımları saray ve konaklarda yer almaya başlamış. Yemek odaları Sultan Abdülhamit döneminde yaygınlaşmaya başlamıştır. 1850'lerden sonra Avrupa kültürü Osmanlı mutfağını etkilemeye başlamıştır. Osmanlı Sarayı'nda başka bir yenilik de 19. yüzyıl sonuna ait mönülerde Fransız yemekleri ile Türk yemeklerinin bir arada sunulmaya başlanmasıdır. Eş zamanlı olarak Osmanlı yemek kitaplarında rozbif, biftek, omlet, alafranga gevrek, pate, garnitür, sos gibi Avrupa kökenli yemek tarifleri yayınlanmıştır. Alafranga tatlar zaman içinde Türk mutfak geleneğine eklemlenmiş, çoğu zaman yeni bir biçimde yorumlanarak yemek tarifleri arasında bugün alıştığımız lezzet kalıpları içinde yer almıştır.

Son 50-60 yıl klasik Türk mutfak geleneğinin yapısının değişimi üzerinde çok etkili olmuştur. Sanayi toplumunun gereklilikleri ve getirdikleri, beslenme biliminin ortaya çıkışı ve gelişimi tüm dünyada olduğu gibi klasik Osmanlı-Türk mutfak geleneğini de etkilemiştir. Örneğin geçmişte tercih edilen tereyağ yerini önce margarine daha sonraları zeytinyağı ve diğer sıvı yağlara terk etmiş; küçümsenen dana eti, kuzu ve koyun etinin yerini almış; zenginliğin göstergesi beyaz ekmek yerini doğal köy ekmeklerine bırakmıştır.

Çorba özellikle kış aylarında Türk mutfağının vazgeçilmez bir parçasıdır. Yemek, her zaman sofraların baştacı olan çorbalarla başlar. Mercimek çorbası, ezogelin çorbası, düğün çorbası, yayla çorbası ve tarhana çorbası en çok tercih edilen çorbalardır. Etler, sebzeler ve baklagiller ile et suyu, un, yoğurt ve şehriye çorbaların ana malzemeleridir.

Türk mutfağındaki et yemekleri kebaplar, köfteler ve sulu et yemekleri türündeki yemeklerdir.

Türk mutfağında etler başlıca 4 değişik yöntemle hazırlanır:

- Odun veya kömür ateşi üzerinde ızgara yöntemi,
- Kızartma yöntemi,
- Fırın yöntemi,
- Tencere yöntemi.

Türk mutfağı sebze yemekleri açısından çok büyük bir çeşitliliğe sahiptir. Dolmalar ve sarmalar, etli sebze yemekleri, kızartma sebzeler ve zeytinyağlıların sayısız çeşitleri mevcuttur.

Türk mutfağında önemli bir yeri olan hamur işlerinin başında evlerde veya fırınlarda pişirilen buğdaydan, çavdar unundan, mısırdan, kepekten yapılan ekmek gelmektedir. Başlıca ekmek tipleri arasında şunları sıralayabiliriz: Yufka, sac ekmeği, mayalı tepsi ekmeği, tandır ekmeği, taş fırın ekmeği, ekşili ekmek, ebeleme, mısır ekmeği, bazlama.

Arkaplan: Çavdar ekmeği.

Arkaplan: Şafak çorbası.

Lahmacun, gözleme, kete, katmer, pide, mantı, erişte ve börekler Türk mutfağının en sevilen hamur işleri arasındadır. Lahmacun ve pideler fırınlama yöntemiyle; çok sayıda çeşidi olan börekler ise fırınlama veya kızartma yöntemiyle hazırlanırlar. Kıyma, peynir, patates ve ıspanak en yaygın börek içleri arasındadır. Bazen tek yemek olarak sunulan böreğe ayran eşlik eder. Hazırlaması oldukça zahmetli olan su böreği açılan yufkanın suda haşlanmasından sonra kullanılmasını gerektiren bir börek türüdür. Tava böreklerinin en güzel örneği içine peynir konulan sigara böreğidir.

Pilav ve makarnalar da hamur işleri sınıfına katıldığında çok geniş bir çeşitlilik ortaya çıkar. Et yemekleri ile baklagillere eşlik eden pilav türleri yalnız pirinç değil, bulgurla ve kuskuslu da yapılır. Sade, domatesli, bademli, fıstıklı, şehriyeli, üzümlü, bezelyeli, patlıcanlı, tavuklu türleri vardır. Düğünlerde ise zerdeyle birlikte ikram edilir. Ev makarnası olarak da bilinen erişte Türk mutfağına ait bir lezzettir.

Türk mutfağının kendine has içecekleri mevcuttur. Yoğurdun sulandırılmasıyla yapılan ayran tamamen Türk mutfağına özgü bir içecektir. Boza, şalgam suyu ve şerbet de Türk mutfağının soğuk içecekleri arasındadır.

Sıcak içecekler arasında Türk kahvesi ve Türk çayı özel bir yere sahiptir. Türk kahvesi kabaca çekilmiş kahvenin cezve denilen uzun saplı kaplar içinde pişirilmesiyle hazırlanır. Dünya çapında ün kazanmış olan Türk kahvesi fincan adı verilen küçük bardaklar içinde servis edilir. Türk çayı günümüzde tercih edilme açısından kahvenin tahtına oturmuş sıcak bir içecektir. İki parça çaydanlık veya semaver kullanılarak toz çaydan hazırlanır. İnce belli çay bardaklarında servis edilir. Türk çayı da hazırlanma yöntemi nedeniyle dünya çapında ün kazanmıştır.

Arkaplan: Ispanaklı börek.

Türk mutfağı tatlılar açısından çok zengin bir mutfaktır. Türk tatlıları çok geniş bir çeşitlilik gösterirler. Baklava, kadayıf, lokma gibi hamurlu tatlılar; muhallebi, keşkül, kazandibi gibi sütlü tatlılar; hoşaf ve kompostolar; revani, helva, aşure ve kabak tatlısı gibi farklı lezzetlerle geniş bir yelpazeye sahiptir.

Baklava, Türk mutfağının dünyaca tanınmış tatlıları arasındadır. Çok ince açılmış yufka arasına kaymak, ceviz veya antep fıstığı konarak pişirildikten sonra şerbetle tatlandırılarak hazırlanır. Tel kadayıf ise çok ince teller halinde satılan hamurla hazırlanır ve ceviz gibi içlerle doldurularak fırında kızartıldıktan sonra şerbetle tatlandırılır.

Sütlü tatlılar sütün şekerle kaynatıldıktan sonra nişasta, pirinç veya pirinç unu ile katılaştırılması yoluyla hazırlanırlar. Kazandibi ise muhallebi gibi hazırlandıktan sonra elde edilen tatlının bir tepside kızartılarak karamelleştirilmesi sonucu elde edilen ilginç bir Türk tatlısıdır. Tavuk göğsü de sütlü bir tatlıdır, ayrıca içine tavuk etinin göğüs kısmı didiklenmektedir. Keşkül, ziyafet sofralarında tercih edilir; güllaç ise ramazan sofralarının baş tatlısıdır.

Arkaplan: Baklava.

İrmik helvası, revani gibi bazı tatlıların yapımında irmik kullanılır. Helva, tören tatlısıdır ve komşulara dağıtılır. Temel malzemeleri un ya da irmik, yağ, şeker ve süttür. Aşure; buğday, kuru üzüm, incir, kayısı, fasulye ve nohut gibi birçok bitkisel malzemeler kullanılarak hazırlanan bir tatlıdır. Genellikle Muharrem ayının onu ile yirmisi arasında yapılır. Rivayete göre Nuh Tufanı'nın bitiminde, gemideki yolculara, kilerde kalan son yiyecekler bir araya getirilerek yapılmıştır. Kurtuluşun kutlandığı son yemekte yenilen aşure kırk çeşit malzeme içerir. Kabak tatlısı balkabağının şekerle pişirilmesi yoluyla hazırlanır. Sonbahar ve kış aylarında tercih edilen Türk mutfağına ait bir tatlıdır.

Pekmez, şıra, pestil, muska, bulama, sucuk, şurup, şerbet gibi üzüm kaynaklı ürünlerin hemen her yöremizde yaygın olduğu göze çarpmaktadır.

Yöreden yöreye farklılaşan lezzetleri barındıran yeme-içme biçimleri, özel gün, kutlama ve törenlerde ayrı bir anlam hatta kutsallık taşır. Türk mutfağı, çeşit zenginliği ve damak tadına uygunluk yönünden olduğu kadar birçok yemek ve yiyecek türü ile sağlıklı ve dengeli beslenmeye ve vejeteryan mutfağına kaynaklık edebilecek örnekleri barındırmaktadır.

Karadeniz, Güneydoğu Anadolu, Akdeniz, Batı Anadolu, İç ve Doğu Anadolu mutfakları kendilerine ait zengin yemek hazinelerine sahiptirler.

Arkaplan: İrmik helvası.

Karadeniz Mutfağı

Karadeniz Bölgesi'nde kıyı şeridi ile dağların diğer tarafında kalan karasal coğrafya mutfağı farklılık gösterir. Karadeniz'de tarım için elverişli düzlük alanların olmayışı ve zor iklim şartları Karadeniz insanı için farklı bir mutfak kültürü yaratır.

Hamsi, mısır unu ve karalahana, fasulye Karadeniz illerinde beslenmenin temelini oluşturur. Minci denilen çökelek benzeri peynir, hemen her öğün yenir. Daha çok Vakfıkebir ilçesinde üretilen Trabzon yağı yurt çapında ünlüdür. Mısır ekmeği, peynirli, mincili, kıymalı, sucuklu, yumurtalı, kabaklı ve yağlı pideler, hamsili ekmek, cumur pidesi, en ünlü yöresel lezzetlerdendir.

Sabah kahvaltıları kimi yörelerde tirma denilen un çorbası ve yağda kızartılan ekmek parçalarıyla yapılır. Genellikle öğle yemeğinde yenilen kuymak, yörenin en sevilen yemekleri arasındadır. Kuymak yapmak için mısır ununa su katılır ve bulamaç kıvamına gelinceye değin kaynatılır. İçine isteğe göre dilimlenmiş peynir, minci, süt, haşlanmış ısırgan otu konularak pişirilir.

Kuskusu andıran çimdik makarnası da oldukça yaygın bir yemektir. Mısır, sütlü kabak, karalahana, balık çorbası da akşam yemekleri arasındadır. Karalahana yığması da yörenin ilginç yemeklerindendir. Şeker fasulyeden yapılan kuru fasulyenin tadına doyum olmaz.

Hamsiden yapılan buğulama, pilav, dolma, haşlama, tava, güveç, ızgara, tuzlama, çorba yöre mutfağının vazgeçilmez yemeklerindendir. Hamsi kayganası, hamsi kuşu ile turşu ve turşu kavurması özellikle kış aylarında tercih edilir. Yörede tomara denen yabani bir bitkiden salata ve turşu yapılır.

Taş fırınlarda, odun ateşinde pişen Trabzon ya da Vakfıkebir ekmeğiyle, Akçaabat köftesinin tadına doyum olmaz. Köftenin lezzetinin sırrı, usta ellerde yapılması olduğu kadar, Karadeniz'in doğal ortamında yetişen kekik kokulu etlerindendir.

Yazın sıcak günlerinde içilen ayranlı mısır çorbaları, serinletici olduğu kadar, bir o kadar da doyurucu, aynı zamanda da diyet yemeğidir. Karadenizlilerin sarımsaklı yoğurtla yedikleri, mısır unuyla yapılan, patlıcan tavaları ise çok lezzetlidir.

Muhlama, pastırmalı ekmek, bandırma, içyağlı çörek, çekme helva, anakız çorbası, anakız pilavı, biryan, tirit, üryani eriği hoşafı, pelverde, kızılcık ekşisi, yarma mısır çorbası, süt çorbası, koliva çorbası, kendime çorbası, bulgur çorbası, karalahana çorbası, çayır lahanası çorbası, lihciya çorbası, kuru fasulye çorbası, pazı ve taze soğan kayganası, karbar yaprağı kayganası, zimilange yaprağı kayganası, kuzukulağı kayganası, fasulye turşusu kayganası, güllüce-pazı yaprağı kayganası, taze patates yaprağı kayganası, hoşmeri, kazkaldıran, sırhan kuymağı, manat, su kabağı kızartması, kara kabak yemeği, kabak dolması, yağda yumurta, yoğurt doğraması, patates yemeği, cımur, guguvak yemeği, zimilange yemeği, karbar yaprağı yemeği, taze fasulye kavurması, kalkanoğlu pilavı, fındık dolması Karadeniz mutfağı örneklerindendir.

Karadeniz tatlılarından bahsedecek olursak, içine fındık koyarak, oklavanın üzerinde hamurun büzülmesiyle şekil verilen burma tatlısı, yufkaların arasına muhallebi koyularak hazırlanan Laz böreği, Hamsiköy sütlacı ve pekmezle yapılan bir çeşit aşure olan termoni en gözde olanlarıdır. Kavut, un helvası, beton helva, pepçura ve zugal da bu yörenin tatlılarıdır.

Yabani bitkilerden hamuçera (dağ çileği), lifor (böğürtlen), mora (ahududu), ahlat (yabanarmudu), karayemiş (kirazı andırır, daha az tatlıdır), çakal eriği (ekşi dağ eriği) en sevilen meyvelerdir.

Arkaplan: Zeytinyağlı taze fasulye.

Güneydoğu Anadolu Mutfağı

Güneydoğu Anadolu mutfağında buğday ve bulgur en çok kullanılan malzemelerdir. Bunun yanında nohut, mercimek, pirinç gibi bakliyat da yaygın olarak kullanılır. Süt ürünleri ve kırmızı et, bölgenin diğer önemli mutfak malzemeleridir. Kırmızı et olarak daha çok koyun eti tercih edilir. Bu besin ürünleri değişik baharatlar, acılı ve salçalı malzemelerle karıştırılarak çok çeşitli yemekler yapılır. Bölge mutfağı; kebap türleri, çiğ köfte, içli köfte, mercimek köftesi ve lahmacunla simgeleşmiştir. Etli-bulgurlu köfteler, çorbalar, etli-sebzeli yemekler bölge mutfağının zengin yemek çeşitlerini oluşturur. Yoğurdun pişirilerek et, sebze ve tahılla karıştırılmasıyla yapılan yemek çeşitlerine rastlanır. Kebaplık etler, baharatlar ve acılı-ekşili karışımlarla terbiye edilir ve daha çok kömür ateşinde pişirilir. Kebaplarda kıyma ve kuşbaşı et kullanılır. Kebaplar, sebzeli, meyveli ve sade olarak da pişirilebilir. Bölge mutfağında et, sebze ve meyvelerle karıştırılarak yahni ve dolmalarda da bolca kullanılır. Bu yöremize ait belli başlı kebap türleri şunlardır: Kemeli tike kebabı, yenidünya kebabı, patlıcan kebabı, yoğurtlu kebap, büryan, haşhaş kebabı, soğanlı kebap, domatesli kebap, alinazik. Belli başlı etli yemekler ise meftune, kelle paça, incik haşlaması, paşa köftesi, frenk tavası ve soğan tavasıdır.

Güneydoğu Anadolu Bölgesi'nin mutfağında buğday ve buğday ürünleri çok önemli bir yer tutar. Pilavlar bölge mutfağının vazgeçilmez yemeklerini oluştururlar. Bölgede pişirilen pilavlardan bazıları duvaklı pilav, şehriyeli pilav, mercimekli pilav, ciğerli pilav, meyhane pilavı, firik pilavı, mığrıbi pilavıdır.

Çorbalar sade suyla olduğu gibi, sütlü, ayranlı ve et sulu olarak da pişirilir. Lebeniye, alaca çorba, ezogelin çorbası, dövmeli alaca çorba, yoğurtlu çorba, börek çorbası, keme çorbası, şiveydiz çorbası, püsürük çorbası, uyduruk, muni çorbası, yuvalama çorbası, beyran çorbası, tarhana çorbası bölgede pişirilen belli başlı çorba türleridir.

Şanlıurfa'nın ünlü kırmızı pul biberi isot, yemeklerde çok kullanılır. Yemeklere tat ve koku vermesi için filfel, nane, rihen, kekik, zahter, kızbara kullanılır. Domates ve biber salçasının da yöre mutfağında önemli yeri vardır.

Güneydoğu Anadolu'nun üzüm yetişen bölgelerinde üzümden yapılan pekmez ile çeşitli tatlılar üretilmektedir. Üzüm suyuna elma, ayva ve kış kabağı gibi meyveler katılarak reçel yapılır. Ayrıca üzüm suyundan pestil ve sucuk gibi tatlılar da üretilir. Bölgede en yaygın yapılan tatlı türü baklavadır. Özel günlerde tatlı olarak lokma ve helva yaygın olarak tüketilir. Bölge mutfağında sütlü tatlılar da geniş bir yer tutar. Tene helvası, top helvası, nişe bulamacı, şıllık, şöbiyet, bülbül yuvası, dolama, fıstık ezmesi, fıstıklı kadayıf, burma kadayıf, nuriye, zingil, revani, halbur hurma, küncülü akıt, şekerli leblebi, Mardin badem şekeri yörenin tatlı çeşitlerini oluşturur.

Mırra, yöreye has bir kahve çeşididir. Meyan kökünden elde edilen meyan şerbeti ise serinletici bir yaz içeceğidir.

Arkaplan: Hünkarbeğendi.

Akdeniz Mutfağı

Beslenme ve sağlık arasındaki yakın ilişkinin somut kanıtlara dönüştüğü son yüzyılda "sağlıklı mutfak", "doğal mutfak", "ekolojik besin" kavramları beslenme biçimlerini dönüştürmeye başlamıştır. Bu yönelimin beslenme sistemi "Akdeniz tipi beslenme biçimi" dir. Etle otun tencere yemeğinde buluşması Akdeniz etkisi ile gelişen Türk mutfağı örneğidir.

Akdeniz mutfağı, buğday, zeytinyağı, sebze-meyve, su ürünleri, süt türevleri, baharata dayandırılmaktadır. Fasulye, nohut, mercimek, bezelye, susam, lahana, karnabahar, maydanoz, kuşkonmaz, soğan, sarımsak, pırasa, pancar, pazı, bamya, patlıcan, salatalık gibi sebzeler ile turunçgiller Akdeniz çevresinde yaygındır. Et, genellikle kıyma olarak köfte yapımında ve kebaplarda kullanılır. Arabaşı, sütlü çorba, humus, kısır, keşkek ve künefe özel gün yiyecekleridir. Yoğurtlu kebap, Arap kebabı, patlıcan kebabı, ezme kebabı, seyis lahmacunu, fırında buğulama pirzola, dil şiş kebabı, bakla ezmesi, halevet, tepsi kebabı, kağıt kebabı, yalancı köfte Hatay mutfağına ait yemek çeşitlerindendir.

Buğday ununda hazırlanan ekmek türleri, unlu ve hamurlu yiyeceklerde çeşit fazlalığı dikkat çekmektedir. Bulgur, kuskus, yarma, firik gibi buğday ürünlerinin mutfağımızdaki kullanımı tüm bölgelerimizde, özellikle Akdeniz'de yaygındır.

Akdeniz beslenme sisteminin diğer bir karakteristik yönünü su ve deniz ürünleri oluşturur. Hatay'ın Samandağ, Hassa ve İskenderun ilçelerinde balık türleri kızartma, buğulama ve ızgara yöntemlerinin dışındaki yöntemlerle de pişirilir. Bu kesimlerde iri balıkların etleri et tokmakları ile dövülüp, bulgurla yoğrulur ve sini köftesi yapılır. Balık ve halka soğan kat kat döşenip, sumak ekşisi, biber ve zeytinyağı eklenerek balık ekşilisi adı verilen yemek yapılır.

Akdeniz mutfağının bir başka özelliğini oluşturan baharatlar geçmiş dönemlerde Akdeniz havzasına Suriye yolu ile Yakın ve Orta Doğu bölgelerinden geliyordu. Türk mutfağının genel yapısında baharat çeşitleri sayıca az olmakla birlikte, Doğu Akdeniz ve Güney bölgelerimizde çeşidin ve kullanım oranının fazlalaştığını görmekteyiz. Akdeniz mutfağında sütlaç tarçınla, yöresel farklılık taşıyan kabak tatlısı ıtır çiçeği ile, turunç reçeli defne yaprağı ile tavuk eti karabiber, çamfıstığı ve sinabbar denilen taze baharatlarla; sebzeli börekler reyhan çiçeği, narpız veya nane ile tatlandırılmaktadır.

Yoğurdun pişirilmesi tekniğine dayanan farklı bir uygulama Hatay ilimizde görülür. Keçi sütünden mayalanan yoğurt, tahta küreklerle sürekli karıştırılıp tuz katılarak iyice pişirilir. Çökelek kıvamına gelen tuzlu yoğurt uygun kalıplara basılır. Sebze ve buğday ürünlerinden hazırlanan yemeklerde, çorbalarda soğuk su ile eritilerek kullanılır. Kahvaltıda bol zeytinyağı ile ezilerek, çayla birlikte tüketimi de yaygındır.

Arkaplan: Humus.

Batı Anadolu Mutfağı

Batı Anadolu'da yeşil yapraklı bitkilerden yapılan yemekler yaygındır. İstanbul ve Ege yöresinde sütlü tatlılar tercih edilir. Ege ve Marmara'da su ürünlerinden balık tüketilir.

Ege yöresinde başta börülce, pırasa, kereviz, patlıcan olmak üzere sebzeler diğer yörelerden daha çok kullanılır. Arapsaçı, baldıran, bambul, dağ marulu, deniz börülcesi, ebegümeci, gelincik, hardal, hindiba, ısırgan, kara hardal, turp, kazayağı, köremen, kuş yüreği, deli kenker, uslu kenker, keçikörmeni, iğnelik, tilkişen, sarmaşık, dallama, acıot, kuzukulağı, labada gibi otlar da bolca tüketilir. Ege yemek kültürünün temelini zeytinyağı oluşturur. Etli yemekler, sebzeler, pilav, dolmalar, tamamen zeytinyağlı olarak pişirilir. Salata ve haşlanmış otlar üzerine zeytinyağı ve limon konulur. Kahvaltıda genellikle zeytin ve zeytinyağı bulunur. Kekik, nane gibi otlarla tatlandırılan zeytinyağı, ekmek ve tulum peyniri ile tüketilir. Kalp ve damar hastalıklarına karşın en iyi çare zeytinyağıdır. Keşkek, patlıcan böreği, mercimekli bükme, katmer, çeşitli yahniler, gözleme, özel gün yemeklerinin başında yer alır.

Marmara ve Trakya yöresinde buğday ürünleri, pirinç, koyun eti, yoğurt ve peynir en çok kullanılan ürünlerdir. Yağ türü olarak ayçiçeği, zeytinyağı ve tereyağı kullanılır. Bursa döneri, iskender çok tanınmıştır. Tekirdağ köftesi, İnegöl köftesi çok meşhurdur. Özel günlerde koyun etinden yapılan yemekler pişirilir. Elbasan tava bu yemeklerin en ünlüsüdür. Gaziler helvası, peynir helvası da Trakya'da sık yapılan tatlılardandır. Silivri'nin yoğurdu, Edirne'nin peyniri, ciğer tavası ve yaprak ciğeri, İstanbul'un kazandibi ve tavuk göğsü çok ünlüdür.

Arkaplan: Zeytinyağlı yaprak sarması.

İç ve Doğu Anadolu Mutfağı

İç ve Doğu Anadolu'da tahıl ve hamur işleri, fırınlı, pirinçli yemekler yaygındır. Zeytinyağı Doğu Anadolu'da popüler değildir.

İç Anadolu yöresi yiyecek kültüründe, buğday ürünleri un ve bulgur başta gelir. Koyun eti, yoğurt, patates ve sebzeler (kabak, şalgam, patlıcan, taze fasulye) önemli yer tutar. Baharda kendiliğinden yetişen bitkilerden madımak, livik, evelik, ebegömeci, gelinparmağı, ısırgan, kuşkuş, tellice ile yapılan yemeklerin de ayrı lezzetleri vardır. Özel günlerde kuzu tandır, bulgur pilavı, nohutlu yahni, su böreği, mantı, un helvası, sütlaç yapılır. Gözleme, börek, pide en sevilen hamur işi yiyeceklerdir. Kayseri mantısı, Konya'nın etli ekmeği çok meşhurdur.

İç Anadolu mutfağının önemli yemekleri: Peskütan çorbası, keş çorbası, pancar çorbası, kesme çorbası, toyga çorbası, tarhana çorbası, urumeli, katıklı çorba, ayran çorbası, kavurma herlesi, mercimek herlesi, mercimek çorbası, bulgur çorbası, düğülcek çorbası, pirinç çorbası, şehriye çorbası, patates çorbası, şalgam çorbası, madımak çorbası, kelecoş, sübüra, ekmekaşı, pehli, aşlak kavurması, babikko, sebzeli et, soğanlı et, tas kebabı, sac kebabı, soğanlı yahni, etli kuru fasulye, karın yahnisi, kıyma mıhlaması, patates mıhlaması, ıspanak mıhlaması, pancar mıhlaması, turşu mıhlaması, etli sarma, etli dolmalar, şalgam dolması, karın dolması, mumbar dolması, karın tavası, kabak tavası, çirli et, üzümlü et, sulu köfte/bulgurlu köfte, tadlama, mirik köftesi, alatlı pilavı, mercimekli bulgur pilavı, bezirgan pilavı, düğün pilavı, yumurta eriştesi pilavı, kavurma eriştesi pilavı, madımak pilavı, şalgam pilave, evelik pilavı, köylü böreği, tel böreği, yarımca börek, dible, bişi, sübüra, lıngel, pirohi, hurma, karaş, kelle tatlısı.

Doğu Anadolu yöresinde buğdaydan yapılan un, yarma ve bulgur kullanımı önemlidir. Yoğurt ve peynir, süt ürünleri arasında en çok tüketilenlerdir. Hayvansal yağ çok kullanılır. Özel günlerde et ile pişirilen kuru baklagiller, yahniler, yoğurtlu çorbalar, kete, pişi ve kadayıf ikram edilir.

Doğu Anadolu mutfağının önemli yemekleri: İçli köfte, Harput çorbası, Harput köftesi, patila, sırın, gındik, ışkınlı yumurta, dilim dolma, pirpirim, söğürtme, güven, tirit, kavurma, ayranlı çorba, yayla çorbası, yoğurtlu bulgur, sarımsaklı fasulye, gıldirikli köfte, sarma, süslü fıdoş.

Kültürümüzün bir parçası olan Türk Mutfağının tarihsel gelişimi ve yörelere göre gösterdiği farklılıklara çok kısa olarak değindiğimiz satırları okurken umarım keyif almışınızdır. Doğrusu böyle bir mutfağa sahip olmak gurur verici ve özel...

Arkaplan: Patates böreği.

SİFRESAYAR

Umut ULUDAĞ

soru7

Bilgisayar ağı yöneticileri, sistemde gerekli güvenliği sağlayabilmek için, kullanıcıların seçtiği erişim şifrelerinin uzunluğu, yapısı, ve değiştirilme sıklığı ile ilgili kurallar düzenlerler. Örneğin, aşağıdaki kuralları göz önüne alalım:

1) Şifreler 8 karakter olacaktır.

2) Şifredeki her bir karakter, şu kümeden rastgele seçilecektir (karakterler tekrarlı olabilir)
K = {a, b, c, ç, d, …, v, y, z, A, B, C, Ç, D, …, V, Y, Z, 0, 1, 2, …, 9}
(Türkçe alfabedeki büyük-küçük harfler ve rakamlar)

3) Şifreler tüm kullanıcılar tarafından her hafta değiştirilecektir.

Türkiye'nin nüfusunu 73 milyon (ve sabit) kabul edersek, yukarıdaki kurallara uyan şifreler (örneğin: aabbCC12, 12345678, 5BcVtH02, Gü456Lşl…), tüm Türkiye nüfusuna, hiçbir şifreyi tekrar kullanmaya gerek kalmadan, en fazla kaç asır yeter? (1 yılı tam 52 hafta olarak alınız.)

soru8

İletişim dillerindeki harflerin istatistiksel dağılımları kriptoanalize yardımcı olabilecek unsurlardandır. Aşağıda verilen paragrafta:

(i) Hangi dört harf toplamda % 40' tan fazla bir orana sahiptir?

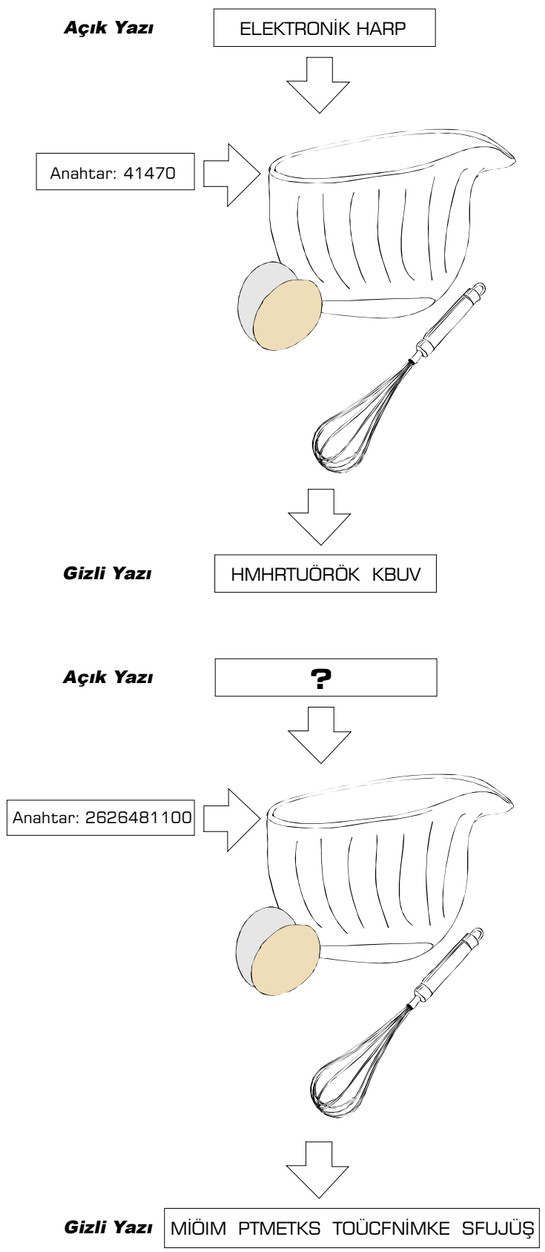
(ii) Alfabemizdeki hangi harfler, paragrafta hiç bulunmamaktadır?

(iii) Paragrafta en az bir örneği bulunan harflerin kümesinde, en az sıklıkla bulunan beş harf hangileridir?

ELEKTRONİK İMZA, İMZANIN ATILDIĞI BELGENİN İÇERİĞİ DE KULLANILARAK OLUŞTURULUR. BU NEDENLE, HER DOKÜMANIN ALTINDAKİ ELEKTRONİK İMZA BİRBİRİNDEN FARKLIDIR. BÖYLECE E-İMZA VERİ BÜTÜNLÜĞÜNÜ DE SAĞLAMIŞ OLUR. BELGE İÇERİĞİ DEĞİŞTİRİLDİĞİNDE İMZA ARTIK GEÇERSİZ OLACAKTIR. HALBUKİ, ELLE ATILAN ISLAK İMZA TÜM BELGELERE AYNI ŞEKİLDE ATILIR VE FİZİKSEL OLARAK TAKLİDİ KOLAYDIR. DOLAYISIYLA, ISLAK İMZA ATILMIŞ BİR BELGEYİ DEĞİŞTİRSENİZ BİLE İMZA GEÇERLİLİĞİNİ KORUMAKTADIR.

(Alıntı: UEKAE Dergisi, Sayı: 1, Sayfa: 52, "Elektronik İmza")

soru9



soru10

2, 3, 5, 7, 11, 23, 29, 41, 43, 47, 61, 67, 83, 89, 101, 113, 131, ?

soru11

RSA gibi asimetrik şifreleme sistemleri çok büyük asal sayılara ihtiyaç duymaktadır (bkz. UEKAE Dergisi, Sayı: 1, Sayfa: 32-41, "Günümüzde Kriptoloji"). Bu sayıların bulunması için, verilen bir sayının asal olup olmadığını çok yüksek bir doğrulukla (ama kesinlik olmaksızın) belirleyen testler (örneğin Miller-Rabin testi) geliştirilmiştir.

Wilson teoremi diye anılan aşağıdaki teorem bir sayının asal olup olmadığını kesinlikle (yani, hata olasılığı 0 olarak) bulabilmektedir:

p sayısının asal olması için gerek ve yeter şart:

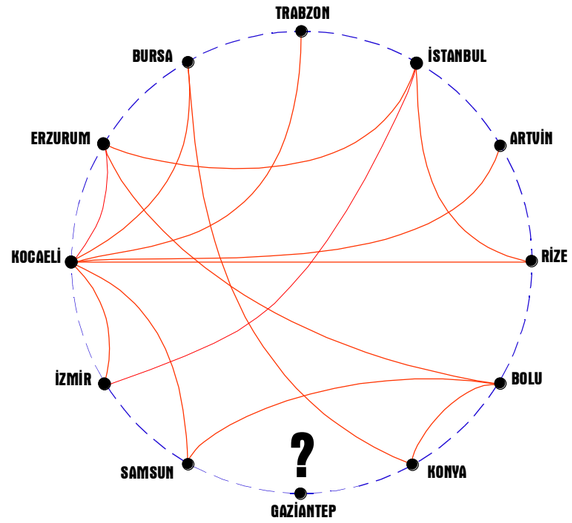
$$(p\text{-}1)! = \text{-}1 \pmod{p}$$

(i) Bu teoremin ilk 5 asal sayı için doğru olduğunu gösteriniz.

(ii) Bu teoremi pratikte yukarıda bahsedilen testlerden biri olarak neden kullanamayacağımızı açıklayınız.

soru12

Aşağıdaki şemaya göre, GAZİANTEP ilimiz, hangi illerle bağlanmalıdır?



Şifresayar bölümündeki 6 sorudan en az 3 tanesini doğru cevaplayıp, çözümlerini iletişim bilgileriyle birlikte odullusoru@uekae.tubitak.gov.tr e-posta adresine, "BİLGEM Dergisi: Şifresayar" konu bilgisi ile 30 Nisan 2011 tarihine kadar gönderenler arasından kura ile belirlenecek 5 kişiye TÜBİTAK Popüler Bilim Kitapları arasından seçilen kitaplar hediye edilecektir. Soruların cevapları derginin bir sonraki sayısında yayınlacaktır. Ödüllü diğer sorulara www.bilgem.tubitak.gov.tr adresindeki "Ödüllü Kriptoloji Soruları" bölümünden ulaşabilirsiniz.

SİFRESAYAR

Umut ULUDAĞ

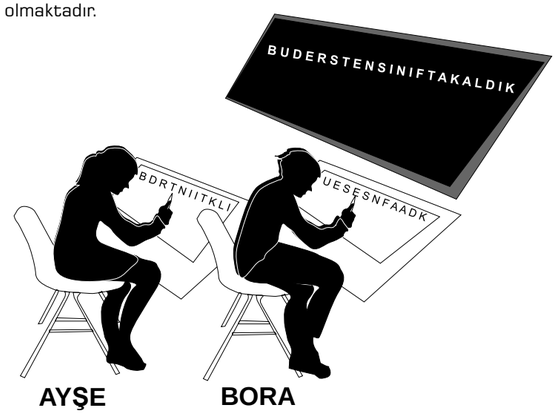
cevap 1

VERİNİNGEÇTİĞİHEMENHERYERDEKRİPTOLOJİKTEKNİKLER UYGULANMAKTAÇOKDEĞİŞİKHİZMETLERSAĞLANMAKTADIR

(Alıntı: UEKAE Dergisi, Sayı: 1, Sayfa: 41, "Günümüzde Kriptoloji")

Dörtlünün elemanları, bilgideki harfleri, bilgiyi paylaştıracakları kişilerin isimlerinin alfabetik sırasına göre (Ayşe – Bora sırası gibi), art arda paylaşmakta, bu işlemi tüm bilgi harfleri dağıtılana kadar sürdürmektedir. Bu durumda, soruda, Ayşe – Bora – Erol – Güven sırasına göre harfler paylaşılmıştır, ve paylaşılan bilgi, 4 ayrı paylaşım bilgisini yukarıdaki kurala göre birleştirmekle bulunan:

"VERİNİNGEÇTİĞİHEMENHERYERDEKRİPTOLOJİKTEKNİKLE RUYGULANMAKTAÇOKDEĞİŞİKHİZMETLERSAĞLANMAKTADIR" olmaktadır.

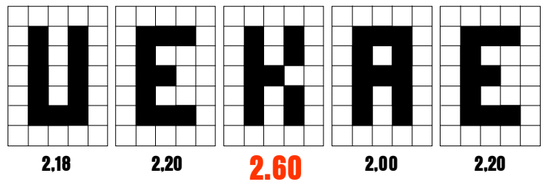


cevap 2

2, 3, 5, 7, 2, 4, 8, 10, 5, 11, 4, 10, 5, 7, 11

Sıralı asal sayıların rakamları toplamı verilmiştir. Sıradaki 15. asal olan 47 nin rakamları toplamı 11 olduğundan, cevap 11 dir.

cevap 3



Sorudaki ikili (binary) imgelerin altlarına, siyah renkli karakterlerin (Çevre / Alan) oranları yazılmıştır.

Karakter "U": Çevre = 24 birim, alan = 11 birim, oran = 2,18
Karakter "E": Çevre = 22 birim, alan = 10 birim, oran = 2,20
Karakter "A": Çevre = 24 birim, alan = 12 birim, oran = 2,00

Sorulan "K" imgesi için, çevre = 26 birim, alan = 10 birim olduğundan, cevap 2,60 olarak bulunur.

cevap 4

Açık Yazı	Gizli Yazı
İŞTE ŞİFRE	ĞVÜL ĞTHLÜ
KAMU SERTİFİKASYON MERKEZİ	YÖÇN PRBUÇNLHLVTĞU LCĞNTĞÖ

Açık yazıdan gizli yazıya ulaşırken,

(i) önce Sezar şifresi kullanılarak, her harf, 3 birim ötelenmiştir:

İŞTE ŞİFRE ⟶ LÜVĞ ÜLHTĞ

(ii) daha sonra, ayrık kelimeler, ters yüz edilmiştir: yani son harf, 1. harf; sondan bir önceki harf, 2. harf ... yapılmıştır:

LÜVĞ ÜLHTĞ ⟶ ĞVÜL ĞTHLÜ

Sorudaki gizli yazı önce ters yüz edilirse:

YÖÇN PRBUÇNLHLVTĞU LCĞNTĞÖ ⟶
NÇÖY UĞTVLHLNÇUBRP ÖĞTNĞCL

bulunur. Son olarak, yukarıdaki her harf, 3 gerisindeki ile değiştirilirse:

KAMU SERTİFİKASYON MERKEZİ
açık yazısına erişilir.

cevap 5

(ii) nin olasılığı daha büyüktür.

(i) deki olayın olasılığını hesaplayalım: Melahat'in doğruluğunu denemesi gerekebilecek toplam anahtar sayısı, 2^{128}dir.

Saniyede 1.000.000.000 anahtar denemesiyle, 365 gün (= 365x24x60x60 saniye = 31.536.000 saniye) boyunca deneyebileceği toplam anahtar sayısı ise yaklaşık $3{,}15\cdot 10^{16}$dır. Bu durumda, Melahat'in başarılı olma olasılığı

$$\frac{2^{128}}{3{,}15\cdot 10^{16}} \approx 1{,}08\cdot 10^{22}$$ 'de 1 olmaktadır.

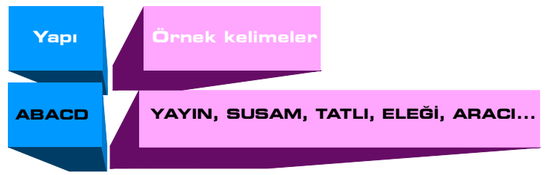
(ii) deki olayın olasılığını hesaplayalım: Herhangi bir haftada, sayısal lotonun sonucu, C(49,6) adet 6 numara içeren kombinasyonlar kümesinden rastgele yaratılan bir tanesidir. Can her hafta sadece 1 kolon oynadığından, 1. haftada büyük ikramiyeyi kazanma olasılığı

$C(49,6) = 13.983.816$ 'da 1 dir. Arka arkaya gelen haftalarda kazanma olasılıkları bağımsız olaylar olduklarından, 3 haftanın 3'ü boyunca, her hafta 1 kolon oynayarak, hep büyük ikramiyeyi kazanma olasılığı:

$(13.983.816)^3 \approx 0{,}27\cdot 10^{22}$ 'de 1 olmaktadır.

Bu durumda, Can'ın lotoda bu şekilde başarılı olma olasılığı, Melahat'in anahtar bulmada başarılı olma olasılığından yaklaşık 4 kat fazla olmaktadır.

cevap 6



E-kimlikler geliyor

Nüfus cüzdanlarının yerine geçecek Türkiye Cumhuriyeti Kimlik Kartı (e-kimlik) için bu yıl yaygınlaştırma çalışmalarına başladık.
Pilot uygulamada 220.000 kimlik kartı dağıttık.
127 kamu uygulamasını tek çatıda toplayan e-devlete erişim güvenliğini en üst düzeye çıkardık.
Yakında her cebe giriyoruz.

www.bilgem.tubitak.gov.tr

TÜBİTAK
BİLGEM