BİLGEM TEKNOLOJİ

Eylül 2021 / Sayı:12

TÜBİTAK BİLGEM Kurumsal Dergisi. Yılda 2 kez yayınlanır. Parayla satılamaz.

Beşinci Savaş Alanı: SİBER GÜVENLİK

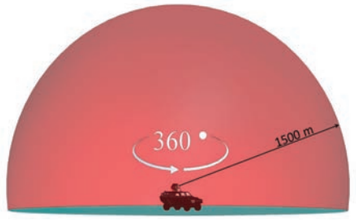
TÜBİTAK BİLGEM

Bu bir proje tanıtımıdır.

Araca Monte Lazer ARMOL

ARMOL, Her türlü hareketli platforma entegre edilebilen ve platform dışı sistemlerden tamamen bağımsız olarak çalışabilen yüksek güçlü lazer silahıdır.

- 5 kW'a kadar tek kipli lazer kaynağı
- Milli lazer ve hüzme yönlendirme sistemi
- Her mesafede hedefe otomatik lazer odaklama
- 360 derece her yöne küresel angaje olabilme
- Bekleme gerekmeksizin art arda uzun süreli atış imkanı
- Li-Ion bataryalı güç kaynağı sayesinde sessiz ve titreşimsiz operasyon
- Araç alternatörü, sistem jeneratörü ve harici kaynaktan şarj imkanı
- 4 eksenli stabilize sistem
- 4 eksenli hassas hedef takip sistemi
- Araç hareket halindeyken hedefe angaje olma
- Hedefe otomatik kitlenme ve otomatik takip
- Radar entegrasyon opsiyonu



360 Derece Kesintisiz Koruma Alanı

ARMOL Araç İçi

Drone İmha

EYP İmha

www.bilgem.tubitak.gov.tr

Başkandan

Merhaba

Siber güvenlik, siber saldırılara karşı alınan tedbirler bütünüdür. En genel anlamda siber güvenlik; bilgisayarların, ağların, programların ve verilerin yetkisiz erişimlere, saldırı ve sömürü amaçlı her türlü harekete karşı korunmasıdır. Siber alan, NATO tarafından kara, hava, deniz ve uzaydan sonra beşinci savaş alanı olarak ilan edilmiştir. Yakın dönemde Türk Silahlı Kuvvetleri bünyesinde Siber Savunma Komutanlığı kurulmuştur. Bilginin olduğu her alan önemli ve değerlidir. Biz ülkemizdeki her alanda yerli ve milli ürünlerin kullanılması gerektiğine inanıyoruz. Yabancı menşeli ürünlerin özellikle kamu ve askeri alanlarda kullanılması birer tehdit kaynağıdır. Bu yüzden siber güvenliğin yerli ve milli çözümlerle sağlanması kritik önem arz etmektedir.

Ülkemizde siber güvenlik alanındaki ilk yasal düzenleme Ekim 2012'de gerçekleştirildi. Bugüne kadar geçen sürede üç adet Siber güvenlik Stratejisi ve Eylem Planı hazırlandı. Geldiğimiz noktada siber uzay, devletler arasında yeni bir mücadele alanı olarak görülmekte ve devletlerin askeri kapasitelerini geliştirmek için bir fırsat olarak değerlendirilmektedir. Bu gelişmeler ve siber saldırı alanları, uluslararası sistemi daha da belirsiz ve tehlikeli hale getirmektedir. Türkiye'nin, siber güvenlik stratejisi geliştirme, siber savunma ve saldırı kapasitesine yatırım yapma ile ilgili çalışmalar yaptığı ve bu konuda ülkemizde bir farkındalık olduğu açıktır.

BİLGEM Siber Güvenlik Enstitüsü (SGE)

BİLGEM bünyesinde Siber Güvenlik Enstitüsü'nün temelleri 1997 yılında Ağ Güvenliği Grubu adı ile kapsamlı bir test laboratuvarının kurulması ile atıldı. Ağ Güvenliği Grubu, Türk Silahlı Kuvvetleri'nin ve kamu kurumlarının bilişim sistemleri güvenliği alanındaki ihtiyaçlarını karşılamak üzere pek çok proje gerçekleştirdi. Ülkemiz için önemli olan güvenlik mimarilerinin tasarımı, sistemlerin güvenli kurulumu, güvenlik testleri, risk analizi gibi alanlarda önemli tecrübeler kazanıldı. Türkiye'nin önde gelen bilişim sistemleri güvenliği merkezlerinden biri haline gelen Ağ Güvenliği Grubu daha sonra Bilişim Sistemleri Güvenliği Bölümü ve 2012 yılından itibaren de Siber güvenlik Enstitüsü (SGE) adını aldı.

BİLGEM Siber Güvenlik Enstitüsü olarak; siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürütmekte, ulusal siber güvenlik çalışmalarına rehberlik etmekte ve çözüme yönelik siber güvenlik projeleri gerçekleştirmekteyiz. Ayrıca eğitim, test ve danışmanlık faaliyetlerimiz de yoğun bir şekilde devam etmektedir. Yeni nesil siber güvenlik teknolojilerinin yerli ve milli, dünya pazarında yer alacak şekilde katma değeri yüksek ürün, hizmet ve teknolojiler geliştirilmesini sağlamak öncelikli hedeflerimiz arasında yer almaktadır.

Dergimizin bu sayısında siber güvenlikle ilgili kapsamlı bir dosya oluşturmaya çalıştık. Emeği geçen tüm çalışma arkadaşlarıma teşekkür ederim. Bir sonraki sayımızda buluşmak üzere, sağlıcakla kalın.

Dr. Ali Gözçin

İÇİNDEKİLER

Danışma Kurulu
Dr. Öğr. Üyesi Cüneyt Utku
Mustafa Kemal İşler
Cemil Sağıroğlu
Dr. Demet S. Armağan Şahinkaya
Erdal Bayram
Prof. Dr. Alikram Nuhbalaoğlu
Gürcan Okumuş
İsmail Doğan
Doç. Dr. Mesut Gökten
Dr. Mustafa Çetintaş
Dr. Orhan Muratoğlu

Yayın Kurulu
Dr. Aziz Ulvi Çalışkan
Bilal Kılıç
Erkan Yalçın
Dr. Hamza Özer
Dr. İzzet Karabay
Mehmet S.Ekinci
Tolga Mataracıoğlu

Sahibi (TÜBİTAK BİLGEM adına)
Dr. Ali Görçin

Genel Yayın Yönetmeni
Mehmet S.Ekinci

Yazı İşleri Müdürü (Sorumlu)
Dr. Aziz Ulvi Çalışkan

Sanat Yönetmeni
Ceren Olga Eke

Editörler
Dr. Ezgi Ayyıldız Demirci
Dr. Umut Uludağ
Dr. Levent Balamir Tavacıoğlu
Şerafettin Şentürk
Cenk Gökberk
Levent Hakkı Şenyürek
Dr. İbrahim Soner Karaca
Abdulbaki Zengin
Onur Özçelik
Abdullah Alpaydın
Bertuğ Kayhan
Ahmet Kezik
M. Burcu Hıdımoğlu

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

Telefon
(0262) 648 1000

Web
www.bilgem.tubitak.gov.tr

e-posta
bilgemteknoloji@tubitak.gov.tr

Baskı
Şan Ofset
Tel: (0212) 289 24 24

Baskı Tarihi
Eylül 2021
ISSN 2717-9273

Dergide yayınlanan yazı ve görsellere kaynak gösterilerek atıfta bulunulabilir. Dergide yayınlanan yazıların sorumluluğu yazarına aittir, TÜBİTAK BİLGEM sorumlu tutulamaz.
BİLGEM Teknoloji Dergisi,
Basın Ahlak Yasası'na uymayı taahhüt eder.

Proje Yönetimi ve Proje Yönetim Ofisi

Dr. Bülent Gümüş – Danışman / BİLGEM

"Proje; özgün bir ürün, hizmet veya sonuç yaratmak için yürütülen geçici bir girişim olarak tanımlanır."

Proje Yönetim Ofisi, PYO (Project Management Office, PMO) olarak adlandırılan organizasyonel birimler, çok sayıda proje yürüten firma ve kurumlarda, proje ve programların kuruluşun stratejilerine uygun olarak seçilmesi ve etkin bir şekilde yönetilmesinden sorumludur. PYO, proje ile ilgili yönetişim süreçlerini standartlaştıran, kaynak, metodoloji, araç ve tekniklerin paylaşılmasını kolaylaştıran bir yönetim yapısıdır. PYO, yetkin insanlar, süreçler ve araçların bir birleşimidir. İlgili birimlerin üstlendiği roller kuruluşun büyüklüğüne, yönetilen projelerin kapsamına bağlı olarak değişiklik gösterebilir.

Proje Yönetimi ve PYO konularının detaylarına girmeden önce, temel kavramların hızlıca üstünden geçmek iyi olur. İlgili kavramların tanımı için dünyaca kabul görmüş ve Proje Yönetim Enstitüsü (Project Management Institute, PMI) tarafından yayınlanan Proje Yönetim Bilgi Birikimi Kılavuzu'nu (Project Management Body of Knowledge, PMBOK, 2017) temel alacağız.

Portföy - Program - Proje

PMBOK'da Proje; "özgün bir ürün, hizmet veya sonuç yaratmak için yürütülen geçici bir girişim" olarak tanımlanır. Bu kısa tanımda, proje çıktısının "özgün" olduğu, çıktının ürün olabileceği gibi hizmet veya süreç gibi çözümler de olabileceği ve çıktıyı geliştirmek ve üretmek için başı ve sonu olan "geçici" faaliyet yürütüleceği ifade edilmiştir.

Proje teriminin yanı sıra Program ve Portföy gibi terimler sıklıkla kullanılır. Bazen birbirinin yerine de kullanılan bu ifadeleri, anlam karmaşasını önlemek açısından açıklamak gerekmektedir. PMBOK'da Portföy; "stratejik hedeflere ulaşmak için bir grup olarak yönetilen projeler, programlar, yardımcı portföyler ve faaliyetler bütünü" olarak tanımlanır. Program ise; "tek tek yönetildiğinde sağlanamayan fayda ve kontrolü elde etmek için koordinasyon içerisinde yönetilen, bağlantılı projeler grubu" olarak tanımlanır. Programlar, portföyün içinde bir grup oluşturmakla birlikte portföyü destekleyen ve eşgüdümlü bir şekilde yönetilen alt programlardan, projelerden ya da diğer operasyonel işlerden oluşur.

Proje Yönetimi, paydaş ihtiyaç ve beklentilerinin karşılanması için proje faaliyetlerinin plan ve yönetiminde bilgi, beceri, araç ve tekniklerin uygulanmasıdır. Bu işten sorumlu olan ve proje ekibine liderlik yapan kişiye de Proje Yöneticisi denir.

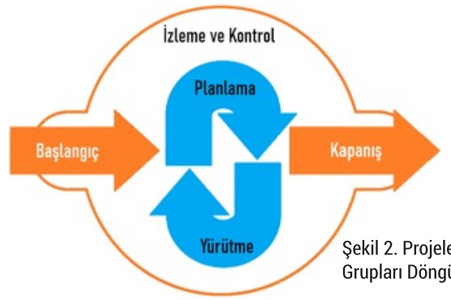
Diğer taraftan Portföy Yönetimi, portföy bileşenleri arasındaki çelişen talepleri dengeler, kaynakları kurumsal önceliklere ve kapasiteye dayalı olarak tahsis eder. Aynı zamanda stratejik hedeflerle uyumlu fayda sağlamak için yönetim ilkelerini ve uygulamaları da entegre eder.

En geniş kapsamlı olan Organizasyonel Proje Yönetimi kavramı ise kuruluşun stratejik hedeflerine ulaşmak amacıyla portföy, program ve proje yönetiminin bütünleşik yürütülmesini kapsar. Bu süreçte projelerle ilgili iki temel soru cevaplandırılır:

1. Doğru işleri yapıyor muyuz, doğru projeleri seçiyor muyuz?
   a. Kaynaklarımızı stratejik hedeflerimize en çok katkı yapacak girişimlere (program ve projelere) ayırdığımızdan emin miyiz?
   b. Kuruluşun sınırlı kaynaklarını ve değişime uyum gösterebilme kapasitesini hesaba katıyor muyuz?
2. İşleri doğru yapıyor muyuz, proje performansımız nasıl?
   a. Projelerin performansı planlanana uyuyor mu? En uygun maliyette yapılıyor mu? Projelerin bağımlılıklarını doğru yönetiyor muyuz?
   b. En önemlisi, bütün bu projelerden beklediğimiz değeri/faydayı elde ediyor muyuz?

Program ve proje yöneticilerinin önceliği daha çok "işin doğru yapılması"dır. Portföy Yöneticileri'nin odağı ise "doğru işin yapılması"dır. Portföy yönetimi doğru işin doğru zamanda ve ayrılan yeterli kaynakla birlikte uygulanmasını sağlar.

Proje yöneticilerinin, zaman ve bütçe planlamadan risk analizine, iletişim yönetiminden tedarik ve alt yüklenici yönetimine kadar 10 alanda bilgi ve tecrübe sahibi olması beklenmektedir. PMBOK proje yönetimi için 5 (beş) Süreç Grubu (Process Group), 49 (kırk dokuz) Süreç ve 10 (on) Bilgi Alanı (Knowledge Domain) tanımlar. Proje yönetişimi süreçlerinin her biri bir bilgi alanına ve bir süreç grubuna aittir.



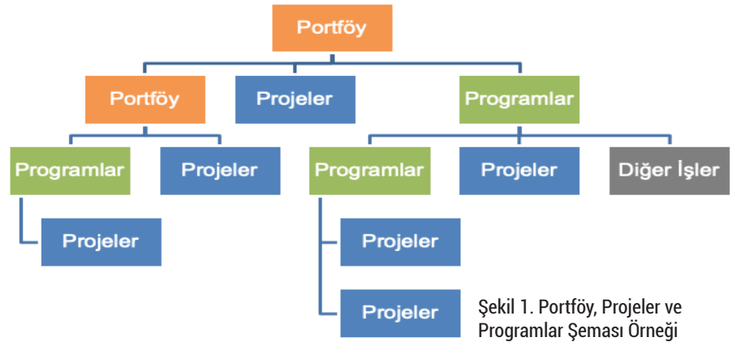
Şekil 2. Projeler Süreç Grupları Döngüsü

Proje süreç grupları, gerçekleştirilen görev ve aktivitelerin mantıksal sınıflandırılmasıdır.

1. Başlangıç: Projenin başlama izin ve onaylarının alınması, proje yöneticisinin atanması
2. Planlama: Proje hedeflerinin belirlenmesi, hedeflere ulaşmada alternatif yolların oluşturulması ve en uygununun seçilmesi
3. Yürütme: Oluşturulmuş olan planın insan kaynakları ve diğer kaynaklar koordine edilerek, hayata geçirilmesi
4. İzleme ve Kontrol: Yürüyen faaliyetleri düzenli olarak takip etme ve planlarla karşılaştırma, hedeflerden sapmayı önlemek için düzeltici faaliyetlerin uygulanması
5. Kapanış: Proje kabulünün resmileştirilmesi, projenin veya fazın kapanışı.

PMBOK'ta tanımlanan Bilgi Alanları aşağıdaki gibi sıralanmıştır.

- Entegrasyon Yönetimi
- Kapsam Yönetimi
- Zaman Çizelgesi Yönetimi
- Maliyet Yönetimi



Şekil 1. Portföy, Projeler ve Programlar Şeması Örneği

• Kalite Yönetimi
• Kaynak Yönetimi
• Risk Yönetimi
• İletişim Yönetimi
• Tedarik Yönetimi
• Paydaş Yönetimi.

Proje Yöneticisi

Birçok firma ve kurumda, proje planlama ve yönetimiyle ilgili bilgi, beceri ve yeteneklerin projelerde çalışırken kazanılmış olacağı düşünülür. Bu sebeple de tecrübeli mühendisler veya uzmanlar, "Proje Yöneticisi" olarak atanır. Ancak atanan kişi bu rol için hazır ve istekli değilse; proje yöneticisinde olması gereken karakteristik özelliklere ve bilgiye sahip değilse projeler başarısız olacaktır. Bununla birlikte proje yöneticisi olarak atanan kişinin de hem performansı hem de iş tatmini düşecektir. Böylelikle, kurum kötü bir yöneticiye sahip olacağı gibi iyi bir mühendisini de kaybetmiş olacaktır.

Proje Yöneticisinin sahip olması gereken beceriler şunlardır:
Teknik Beceriler: Zaman, kaynak, maliyet ve risklerin iyi planlanması ve yönetilmesi.
Stratejik: Strateji, misyon, vizyon, amaç ve hedefler, pazar ve rekabet unsurları doğrultusunda projelerin planlanıp yönetilmesi.
Liderlik Beceriler: Proje ekibine rehberlik, motive etme ve yönlendirme yapılabilmesi.

Proje Yönetim Ofisi (PYO)

Proje yönetimi ile ilgili bir mükemmeliyet merkezi olan PYO'nun birimin öncelikli görevlerini şöyle sıralayabiliriz:

Stratejik Planlama ve Yönetişim: Bu, PYO'nun en önemli işlevidir. Projeleri, önceden tanımlanmış kriterler kullanarak puanlama ve, potansiyel projelerin stratejik seçimi organizasyonun iş hedeflerine göre yapılabilir. PYO üst yönetime, sağlam bir iş senaryosu ve net bir maliyet/fayda oranı sağlayarak, şirketin stratejik hedefleriyle en iyi uyuşan aday projeleri seçmeleri için tavsiyede bulunur.

Proje yönetişimiyle ilgili olarak PYO, projelerin, programların veya portföylerin oluşturulması, yönetimi ve kontrolünü tanımlayan politikalar, düzenlemeler, süreçler ve prosedürleri belirler.

En İyi Uygulamalar ve Süreç: PYO, organizasyon içindeki en iyi uygulamaların ve süreçlerin belirlenmesini ve uygulamasını sağlar. PYO ayrıca, organizasyon genelinde tutarlı proje sonuçları için tutarlı proje yönetimi rehberi, yöntemleri, sistemleri, araçları ve ölçütlerini belirler. Bu, farklı birimlerde farklı projeler üzerinde çalışan proje yöneticileri arasında tutarlılığı sağlar.

	Projeler	Programlar	Portföyler
Kapsam	Projelerin tanımlanmış hedefleri vardır. Kapsam, proje yaşam döngüsü boyunca aşamalı olarak olgunlaşır.	Programlar daha geniş kapsamlıdır ve daha önemli faydalar sağlar.	Portföylerin organizasyonun stratejik hedeflerine göre değişen bir iş kapsamı vardır.
Değişim	Proje yöneticileri değişiklik beklentisi içindedirler ve değişikliği sürekli olarak yönetmeye ve kontrol etmeye yönelik süreçler yürütürler.	Program yöneticisi hem program içi hem de program dışı değişiklikler beklemeli ve bunları yönetmeye hazırlıklı olmalıdır.	Portföy yöneticileri, değişiklikleri sürekli olarak daha geniş bir çerçevede izler.
Yönetim	Proje yöneticileri, proje hedeflerine ulaşmak için proje ekibini ve proje çalışmalarını yönetirler.	Program yöneticileri, program personelini ve proje yöneticilerini yönetir ve genel bir vizyon ve liderlik desteği sağlar.	Portföy yöneticileri, portföy yönetimi personelini veya portföy için sorumlulukları olan personeli yönetebilir ya da koordine edebilir.
Başarı	Başarı, ürün ve proje kalitesi, takvim ve bütçeye uyum ve müşteri memnuniyeti derecesiyle ölçülür.	Başarı, programın başlangıçta belirlenen ihtiyaçları ve faydaları karşılama derecesine göre ölçülür.	Başarı, portföy bileşenlerinin toplam performansı ve portföyün gerçekleştirilmesine göre ölçülür.
İzleme	Proje yöneticileri, projenin hedefi olan ürünleri, hizmetleri ya da sonuçları üretme işini izler ve kontrol eder.	Program yöneticileri, programın genel hedeflerine, zaman çizelgelerine, bütçe hedeflerine ve programın faydalarına ulaşmasını sağlamak amacıyla program bileşenlerindeki ilerlemeyi izler.	Portföy yöneticileri, strateji değişikliklerini, kaynak dağılımını ve toplam performans sonuçlarını ve değer indikatörlerini izler.

Tablo 1. Proje, Program ve Portföy Yönetimi Karşılaştırması (PMBOK, 2017)

PYO	Rol ve Görevleri
Destekleyici (Supporting)	▸ Danışman rolündedir ▸ Bilgi havuzu olarak görev yapar. ▸ Standart şablonlar, en iyi uygulamalar, kılavuzlar oluşturur. ▸ Eğitimler düzenler, öğrenilmiş dersleri paylaşır. ▸ Projeler üzerinde kontrolü düşüktür.
Kontrolcü (Controlling)	▸ Destek sağlar. ▸ Proje yönetim metodolojilerini, araçlarını oluşturur ve benimsetir. ▸ Metodoloji ve araç uyumluluğunu denetler. ▸ Projeler üzerinde kontrolü orta düzeydir.
Yol Gösterici (Directing)	▸ Projeleri doğrudan yönetir. ▸ Projeler üzerinde kontrolü yüksektir.

Tablo 2. PYO Sorumlulukları

Ortak Dil, Kültür ve Zihniyet: PYO, çalışanları sektördeki farklı teknikler, metodolojiler ve en iyi uygulamalar hakkında bilgilendirerek ve eğiterek ortak bir proje kültürünün ve zihniyetinin yayılmasına yardımcı olur. Ayrıca, projeler için standart kilometre taşlarını, ölçütleri ve Anahtar Performans Göstergeleri (Key Performance Indicators, KPI)'ni tanımlayarak ortak bir proje dili kullanılmasına yardımcı olur. Bu şekilde, projelerin yönetimi tüm organizasyonda uyumlu ve verimli hale gelir.
Kaynak Yönetimi: PYO, zaman çizelgeleri, bütçeler, kaynak yükleri ve olasılık analizi bilgilerine dayalı öncelikleri yöneterek ve buna göre doğru zamanda doğru kaynakları sağlayarak kaynakları tüm projeler genelinde etkili bir şekilde yönetir ve tahsis eder. Ayrıca herhangi bir projede ihtiyaç duyulan rolleri ve sorumlulukları da tanımlar.
Eğitim: PYO genel olarak çalışanları ve özellikle proje yöneticilerini eğitir, onlara rehberlik eder ve koçluk yapar. Çalışanları proje yönetişimi konusunda güncel tutmak için proje yönetimi ile ilgili çalıştaylar ve eğitim programları düzenler.
Proje Çıktıları, Arşivleri ve Araç Setleri Oluşturma: PYO, projeleri yönetmek için şablonlar, araçlar ve yazılımlar sağlar. Daha iyi karar almak için proje performansına erken görünürlük ve, güvenilir verilerin toplanmasını sağlayan proje yönetim araçlarına yatırım yapar.

PYO ayrıca kurumsal hafızada önemli bir rol oynar. Proje tamamlandığında veya iptal edildiğinde, proje sırasında oluşturulan tüm proje belgelerini bir belge havuzunda arşivler. Bu, özellikle öğrenilen derslere ileride başvurmak için çok yararlıdır.

PYO Temel Bileşenleri ve Görevleri

İnsan
- Üst yönetim desteği ve geri bildirim.
- Proje yöneticileri için koçluk ve danışmanlık.
- Proje yöneticileri ve proje ekibi eğitimleri.

Süreç
- Proje seçme ve önceliklendirme süreci.
- Proje planlama ve yönetim süreci.
- Proje sonrası değerlendirme süreci.
- Proje yönetim kontrol süreçleri.

Araç
- Proje yönetim araçları ve bilgi sistemi.
- Şablonlar, kılavuzlar, kontrol listeleri.

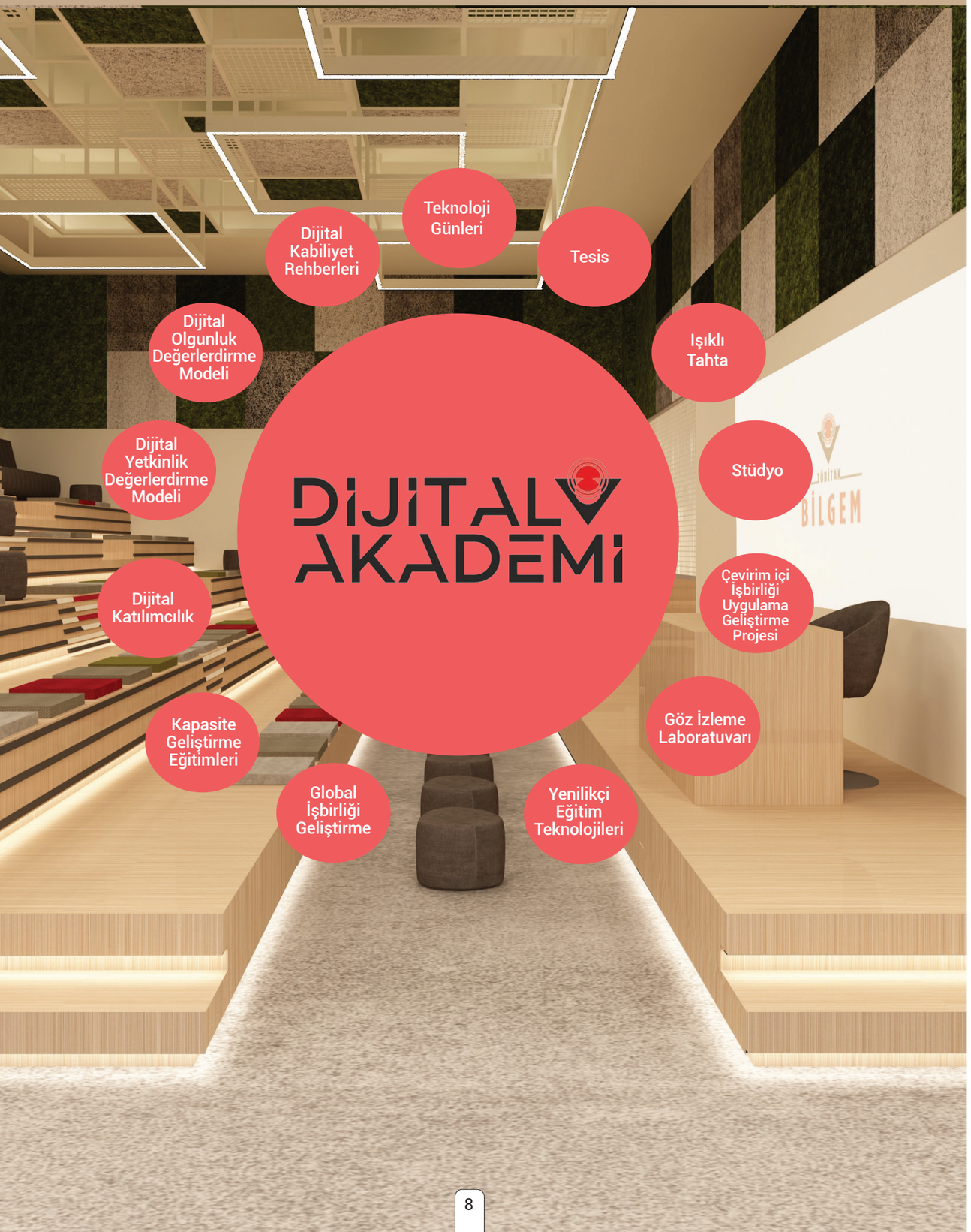
PYO'ların sorumlulukları, proje yönetimi destek fonksiyonları sağlamaktan doğrudan projelerin yönetimine kadar değişebilmektedir ve üç ana tür altında incelenebilir.

PYO proje bazlı çalışmalar yapan kuruluşların başarısında kritik öneme sahiptir. Bu birimin yokluğunda; etkin proje, program ve portföy yönetimi için yapılması gereken işler sahipsiz kalır, işlerin bir kısmı farklı aktörler ve birimler tarafından dağınık bir şekilde yapılır; bir kısmı ise hiç yapılmaz. PYO biriminin ve proje yönetim pratiklerinin başarılı bir şekilde kurulması ve işletilebilmesi için şartları şöyle sıralayabiliriz:

1. En başta üst yönetimin istemesi ve destek vermesi,
2. PYO biriminde çalışacak Proje yöneticilerinin deneyimli ve konusunda uzman kişiler olması,
3. Detaylı ama esnek bir Proje Yönetim sürecinin hazırlanması,
4. Proje yöneticilerinin projelerdeki etkililiğinin ve gücünün sağlanması,
5. Proje yönetiminin kurum içindeki kariyer yollarından biri olması,
6. Proje yönetimi için bilişim altyapısının kurulması,
7. Raporlama sisteminin ve eskalasyon mekanizmasının işlemesi,
8. Değişiklik yönetim sürecinin başarılı bir şekilde işletiliyor olması.

Kaynakça

▸ The Standard for Portfolio Management – Fourth Edition (2017).
▸ Proje Yönetimi Bilgi Birikimi Kılavuzu (PMBOK® Kılavuzu) 6. Baskı & Çevik Uygulama Kılavuzu
▸ Wright, D. (2012). Developing your PMO roadmap. Paper presented at PMI® Global Congress 2012—North America, Vancouver, British Columbia, Canada. Newtown Square, PA: Project Management Institute. (https://www.pmi.org/learning/library/developing-pmo-roadmap-framework-assessment-6060)
▸ 5 Major roles a Project Management Office plays within a company, https://www.planisware.com/hub/blog/5-major-roles-project-management-office-plays-within-company
▸ Breaking the PMO sound barrier, https://www.pmi.org/learning/library/establishing-successful-pmo-applying-new-framework-6062



BİLGEM DİJİTAL AKADEMİ

Fatih Tekmen - Araştırmacı, Rümeysa Çakmak - Araştırmacı, Tuğçe Yılmaz - Uzman Yardımcısı,
Sevinç Karakaş- Uzman, Nuriye Ünlü - Ens. Md. Yrd. / BİLGEM YTE

"BİLGEM YTE bünyesinde bulunan Dijital Akademi ile eğitim ve rehberlik sunumuna yönelik altyapılar hazırlanacak, kurum içi ve d-Devlet ekosistem paydaşlarımıza yönelik olarak kapasite kazandırma çalışmaları yürütülecektir."

Küresel dijital eğilimleri ve gelişmeleri takip etmek, ekosistem paydaşları ile iş birliğinde yeni teknoloji ve yenilikçi yaklaşımlara ilişkin kapasite geliştirmek TÜBİTAK BİLGEM'in stratejik amaçları arasında önemli bir yere sahiptir. Bu doğrultuda TÜBİTAK BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü(YTE), ekosistem etkileşiminin sürekli ve etkin bir şekilde sağlanmasına yönelik olarak, 2016 yılından bu yana Dijital Olgunluk Değerlendirme Modeli'ni yürütüyor. Dijital Yetkinlik Değerlendirme Modeli ile Dijital Kabiliyet Rehberliği çalışmaları tek bir çatı altına alındı ve Dijital Akademi hizmeti tüm ekosistemin kullanımına sunuldu.

Dijital Akademi'de bugüne kadar hayata geçirilen modeller büyük önem taşıyor.

Birinci aşama: 2016 yılında başlatılan iç destekli Dijital Olgunluk Değerlendirme Modeli ve Rehberlik (DIJITAL-OMR) Projesi, Dijital Devlet (d-Devlet) alanında ülkemiz koşulları ile kamu kurumlarının ihtiyaçları göz önünde bulundurarak uluslararası çalışmalar çerçevesinde kurumsal dijital kabiliyetlerinin bütüncül bir yapı üzerinden değerlendirilmesini sağlıyor. Dijital Olgunluk Değerlendirme Modeli'nin geliştirilmesi ve bu Model ile uyumlu Rehberlerin hazırlanmasıyla birlikte dijital kurumsal kapasitenin artırılmasına yönelik hizmet sunuluyor.

Proje kapsamında d-Devlet çalışmalarında sistemli ve bütüncül bakış açısı getirilerek kamu kurumlarının dijital yetkinliklerinin geliştirilmesi ve yürüttükleri proje ve faaliyetlerinin etkililik, etkinlik ve bilgi güvenliği niteliklerinin artırılmasıyla dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi sağlanıyor.

İkinci aşama: Dijital Olgunluk Değerlendirme Modeli ile uyumlu olarak 2017 yılında Türkiye'ye özgü Dijital Yetkinlik Değerlendirme Modeli geliştirilmiş ve Model ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönlerinin belirlenmesi ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanıyor.

Dijital Olgunluk Değerlendirme Modeli ve Rehberlik Projesi kapsamında hazırlanan tüm rehberlerin www.dijitalakademi.gov.tr platformu ile kullanıcılara açık erişimi sağlanıyor. Rehberlerin kullanımının yaygınlaşması amacıyla eğitim programları,

toplantılar ve çalıştaylar düzenlenerek etkin mekanizmaların hayata geçirilmesi hedefleniyor.

Üçüncü aşama: Mayıs 2019 yılında TÜBİTAK BİLGEM'in iç destekli projesi olarak başlayan Dijital Akademi çalışmaları Dijital Olgunluk Değerlendirme Modeli ve Rehberlik Projesi kapsamında yayımlanan rehberlerin eğitimleri ve PostgreSQL Geliştirici Eğitimleri ile başladı. 2017 yılında İşletim ve Bakım Rehberi Eğitimleri ile başlayan eğitimler 2018 yılında Veri Merkezi Rehberi Eğitimleri ve PostgreSQL Geliştirici Eğitimleri ile hız kazandı.

Tüm bu aşamalarda 2017 yılında başlayan dijital kapasite geliştirme eğitimlerine 125 kamu kurum ve kuruluşu, özel sektör firmaları, üniversiteler ile sivil toplum kuruluşlarından temsilciler katıldı. Gerçekleşen 53 eğitimde %91,3 genel memnuniyet ortalaması ile 951 bilişim uzmanına 694 saat eğitim verildi. 2020 yılı içerisindeyse 17 eğitimde 405 bilişim uzmanına %91,6 genel memnuniyet ortalaması ile eğitim sunuldu. 2021 yılında da Dijital Akademi eğitimleri ve rehberlik hizmetleri ile d-Devlet ekosisteminde görev alan bilişim uzmanlarının yetkinliklerinin artırılması hedefleniyor.

Dijital Akademi Çatısının Oluşumu

Dijital Akademi ile yeni teknolojiler ve yenilikçi yaklaşımlar kullanılarak yetkinlik bazlı dijital kapasite kazanımına yönelik altyapılar hazırlanarak kurum içi ve d-devlet ekosistem paydaşlarımıza söz konusu altyapılar üzerinden kapasite kazandırma çalışmaları yürütülecektir. d-Devlet ekosistemi kapasite kazandırma çalışmalarında kullanılmak üzere duyulan fiziksel mekan ihtiyacının karşılanması amacıyla TÜBİTAK Çukurambar Ek Bina'nın giriş katında tahsis edilen alan Dijital Akademi tesisine dönüştürülecektir.

Dijital Akademi ile sunulacak dijital kapasite kazandırma çalışmalarına ilişkin Rehberlik Kataloğu oluşturulmuş olup TÜBİTAK BİLGEM dahil olmak üzere tüm ekosistem paydaşlarının sahip olduğu yetkinlik ve tecrübelerin aktarımı sağlanacaktır. Kamu bilişim uzmanlarının yetkinliklerini arttıracak, yeteneklerini geliştirecek rehberlik programları verilecektir.

Kamu bilişim uzmanlarının eğitim ihtiyaçlarını gerek uzaktan gerek geleneksel yollarla karşılamak ve kamunun dijital dönüşümüne eğitimlerle ve işbirlikleriyle destek sağlamak misyonuyla bu konuda çözümler geliştirilmektedir. Günümüz ihtiyaçları ve gelişmeleri doğrultusunda, uzaktan eğitim sistemi ile eğitim ihtiyaçlarına her zaman her yerde cevap verebilmek hedefleniyor. Uzaktan eğitim altyapısı ile zamandan ve mekândan bağımsız olarak ihtiyaç duyulan eğitimlerin kişinin kendi hızında alması amaçlanıyor.

Öğrenme Yönetim Sistemi (LMS)

Eğitimlerin uzaktan gerçekleşebilmesi için Öğrenme Yönetim Sistemi (LMS) kurulmuştur. 2020 yaz stajyer eğitim programı ve enstitü oryantasyon programı bu sistem üzerinden gerçekleştirildi. Ayrıca, düzenlenen rehberlik hizmetleri eğitimleri de bu sistem üzerinden verildi.

Kamu bilişim uzmanlarına çeşitli öğrenim içeriklerini bir arada sunan uzaktan eğitim platformu "Dijital Akademi Öğrenme Yönetim Sistemi" ile farklı modüller seçerek öğrenime başlama veya tercihlerine göre doğrudan bir kurs seçerek baştan sona tamamlama imkânları sunulması hedefleniyor. Eğitmen ve eğitime katılacaklar için kolay kullanım sağlayan Türkiye'de de birçok kurum ve kuruluş tarafından kullanılan Moodle ile çevirim içi kurslar oluşturuluyor.

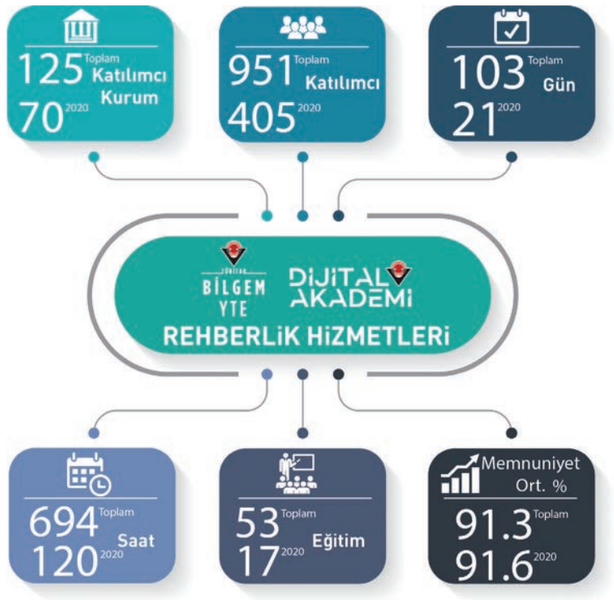
Moodle, bir Uzaktan Eğitim platformunda ihtiyaç duyulabilecek çevrimiçi canlı ders, webinar, interaktif eğitim videoları, ödev, anket, sertifika, forum gibi etkinliklerin çoğunu fazlasıyla yerine getirebilecek özelliklere de sahip olacaktır.

Çoklu-ortam kaynakları (Youtube videoları, LMS ile uyumlu Adobe programları ile üretilen materyaller vb.) Moodle üzerinde kolaylıkla yönetilebilecektir.

Yüz Yüze Eğitim

Dijital Akademi Etkinlik Alanı için ihtiyaçlar belirlenmiş ve tesis tasarlanmıştır. İhale süreci devam eden alan için 100 kişi kapasiteli bir amfi oluşturulacaktır. Çeşitli etkinliklerin, seminerlerin, konferansların ve meet-up'ların düzenlenebileceği tesis ile daha geniş katılımlar sağlanması hedeflenmektedir.

Amfi alanına ek olarak sınıf eğitimleri için bir adet eğitim sınıfı bulunuyor. 20 kişi kapasiteli uygulamalı eğitimler de verilebilen bu eğitim sınıfı, katılımcıların arasındaki etkileşimi arttırabilmek için U düzeninde tasarlandı.



Yanı sıra, çevrimiçi derslere yönelik video çekim için stüdyo kuruldu. Eğitim videoları çekimi için Işıklı Tahta (lightboard) kullanılıyor. Böylelikle izleyici hem eğitmeni görebilirken hem de yazılanları rahatça takip edebiliyor. Bu stüdyoda yapılan çekimler ile video içerikler de oluşturulabilmekte. Eğitim videoları sadece dijital kaynaklar kullanılarak ve ekran çekimleri ile de hazırlanabiliyor.

2021 yılında da "Dijital Akademi Eğitimleri ve Rehberlik Hizmetleri" ile d-Devlet ekosisteminde görev alan kurumların olgunluk gelişimleri ve bilişim uzmanlarının yetkinliklerinin artırılması hedefleniyor.

Beşinci Savaş Alanı: SİBER GÜVENLİK

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020-2023

> Hayatın her alanında varolan siber güvenliğe, belirli bir disiplinle yaklaşılması artık bir zorunluluktur.

Erkut Beydağlı - Başuzman Araştırmacı / BİLGEM SGE

Siber güvenlik kavramının farklı tanımlamaları olmakla birlikte basit ve kapsayıcı tanımı, Bilişim Teknolojileri Bileşenlerini kapsayan siber uzayda her noktaya uygulanan güvenlik disiplini olarak ifade edilebilir. 2011'de başlayan ve 2050'de bitmesi öngörülen Endüstri 4.0, Bilişim Teknolojileri ile tüm yaşamsal mekanizmaları bir araya getirmeyi hedefleyen bir devrim olduğundan, bu devrimin güvenlik adaptasyonu olarak siber güvenlik disiplininin yaşam disiplinimize entegre olması beklenir. Örneğin, eve aldığımız veya bahçemizi izleyen bir kamera, IoT (Nesnelerin İnterneti) dünyasının bir bileşeni olmaktadır.

Disiplinine uygun olarak hareket edilmediğinde, güvenlik (security) ve mahremiyet (privacy) problemleri oluşacaktır. Ulusal çapta düşünüldüğünde; kurum ve kuruluşlar arası veri paylaşımının güvenli biçimde sağlanması, kaynağı ve hedefi yurt içi olan veri trafiğinin yurt içinde kalması stratejik hedefleri gündeme gelmektedir. Kurumsal, sektörel ve ulusal bazda siber olaylara hazırlık seviyelerinin risk temelli analizler ve planlamalara dayalı yaklaşımlarla artırılması hedeflenmelidir.

Dijital dünyada güvenliği sağlayabilmek için dünya devletleri siber güvenlik stratejileri hazırlamakta, yayınlamakta ve ilgili kurumlarını görevlendirilerek gerçekleştirme ve denetimi sağlanmaktadır. Ülkemiz, bu konuda üzerine düşen görevi yerine getirmektedir. Ülkemizin bu konuda Ulaştırma ve Altyapı Bakanlığı koordinasyonunda yapılan çalışmaları sonucunda sırasıyla yayınlanan stratejileri aşağıda listelenmiştir:

- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2016-2019
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023

Ulusal Siber Güvenlik Stratejisi ve Eylem Planları, birbirinin devamı şeklinde bütünselliği sağlayacak yaklaşımla ilerlemekte ve hayatımıza giren yeni teknolojilere yönelik güvenliği sağlama amaçlı olarak stratejileri ve eylem planlarını içermektedir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023 ile belirlenen toplam 8 (sekiz) adet stratejik amaç ve bu stratejik amaçların anlaşılabilmesine, başarılı olarak gerçekleşebilmesine katkı oluşturabileceği düşünülen açıklamalar/değerlendirmeler aşağıda listelenmiştir:

> Kritik altyapıların siber güvenliği (IT-Bilgi Teknolojileri ve OT-Operasyonel Teknolojiler güvenliği kapsamlı), hayati derecede önem taşımaktadır.

Kritik Altyapıların Korunması ve Mukavemetin Artırılması

Kritik altyapılar denildiğinde öncelikli olarak; Enerji, Elektronik Haberleşme, Ulaştırma ve Su Yönetimi akla gelmekle birlikte genel olarak kritik altyapıların kapsamını sorun oluştuğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran tüm bilişim altyapıları olarak ifade edebiliriz.

Kritik altyapılar büyük ölçekte endüstriyel kontrol sistemlerini içermektedir. Endüstriyel Kontrol Sistemleri (Industrial Control Systems, ICS); Denetleyici Kontrol ve Veri Toplama Sistemleri (Supervisory Control and Data Acquisitions, SCADA), Dağıtılmış Kontrol Sistemleri (Distributed Control Systems, DCS) ve Programlanabilir Mantık Denetleyicileri (Programmable Logic Controllers, PLC) gibi diğer daha küçük kontrol sistemi yapılandırmaları dahil olmak üzere çeşitli kontrol sistemlerini kapsayan genel bir terimdir.

Kritik altyapılara gerçekleştirilebilecek bir siber saldırı çok ciddi derecede zararlar ortaya çıkarabileceğinden, siber saldırganlar için bu durum ciddi bir saldırı motivasyonu oluşturmaktadır. Bu saldırı

ları engellemeye yönelik olarak kritik altyapıların IEC 62443 Standardı kapsamında sertifikalandırılması değerlendirilmelidir. Bilişim sistemleri için özelleşmiş olan ISO/IEC 27001 standardının Endüstriyel Otomasyon ve Kontrol Sistemleri için karşılığı IEC 62443 olarak ifade edilebilir. Kritik altyapı sektörlerinde düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi stratejiktir.

Kritik altyapılarda en önemli hususlardan bir tanesi iş sürekliliği olduğundan, kritik altyapılarımızın siber güvenliğinin 7/24 konsepti ile korunması ve sürekli ayakta tutulacak şekilde yedeklilik yaklaşımıyla işletilmeleri gerekmektedir.

Ulusal Kapasitenin Geliştirilmesi

Siber güvenlik alanında en önemli konulardan bir tanesi de yetişmiş nitelikli insan gücü ve siber güvenlik farkındalığıdır. Bu kapsamda örnek olarak; Savunma Sanayi Başkanlığı (SSB) himayesinde kurulan SiberKüme (Türkiye Siber Güvenlik Kümelenmesi, www.siberkume.org.tr) tarafından, yetişmiş insan gücü sağlamaya ve siber güvenlik farkındalığına yönelik çalışmalar artarak devam etmektedir. Özellikle üniversitelerde, siber güvenlik lisans ve yüksek lisans programları başlatılmakta ve kamu kurumları tarafından siber güvenlik yaz okulları, tatbikatları ve yarışmaları düzenlenmektedir. Kurumlarda Siber Olaylara Müdahale Ekipleri (SOME) oluşturulması ve güçlendirilmesi de bu stratejik amaç doğrultusunda planlanmaktadır. SOME'nin yetkinlik seviyelerinin ölçülmesi/izlenmesi ve ekip üyeleri yetkinliklerinin artırılması stratejiktir. Ayrıca toplum genelinde siber güvenlik farkındalığını artırıcı etkinliklerin her kesime (aileler, çocuklar, öğrenciler, gençler, kadınlar, yaşlılar ve engelliler) ulaşılması öncelikli hedefler arasında yer almaktadır.

Siber güvenliğin sağlanması kapsamında birey olarak güvenlik farkındalığı son derece önemli olup, özellikle insan unsuruna yönelik sosyal mühendislik saldırıları konusunda dikkatli olunması her zaman hatırlanmalıdır.

Organik Siber Güvenlik Ağı

Siber saldırılara [zararlı yazılımlar (fidye yazılımları, virüs, solucan, truva atı vb.) oltalama saldırıları, gelişmiş kalıcı tehditler, sıfırıncı gün saldırıları, vb.] ilişkin işbirliği ve anlık bilgi paylaşımının sağlanabileceği bir platformun etkinliğinin artırılması önemlidir. Burada özellikle Ulusal Siber Olaylara Müdahale Merkezi (BTK USOM) koordinasyonunda, siber güvenlik alanında çalışan veya siber güvenliğe ilgi duyan her kesimden insanın bilgi ve tecrübe paylaşımına katılmasına imkan ve yön verecek organik siber güvenlik ağının etkinleştirilmesi hedeflenmektedir. Özellikle kurumlarda bulunan SOME ve üniversitelerde oluşturulabilecek siber güvenlik kulüplerinin bu platforma katkısının son derece yüksek olacağı değerlendirilmektedir.

Yeni Nesil Teknolojilerin Güvenliği

Yeni nesil teknolojilerin (örneğin bulut bilişim, nesnelerin interneti, 5G) hayatımıza girmesi veya yakın zamanda girecek olması ile birlikte bunların getireceği konfor ile birlikte güvenli kullanımları için önlemler alınması da son derece önemli olacaktır. Bu önlemlerin etkinliğinin artırılabilmesi için de yapay zeka teknolojisinin kullanılabilmesi bu stratejik hedef kapsamında gündeme gelmektedir. Otonom/yarı-otonom olarak inceleme sağlayacak algoritmaların yapay zeka teknolojisi ile kullanılması, olası siber güvenlik saldırılarının gerçek zamanlı tespitini ve alınabilecek önlemlerin tetiklenebilmesini sağlayacaktır.

Siber Suçlarla Mücadele

Bu alanda özellikle siber suçların (bilgisayar ve internete özgü suçlar) azaltılabilmesine yönelik olarak gerekli güvenlik önlemlerini içeren bilişim altyapılarının standardizasyonu, saldırganların tespit edilebilmesi ve caydırıcılığı sağlayacak etkinlikte yasal yaptırımların gündemde olması önemlidir. Siber suçlarda hedef insan, mal varlığı veya işletilen sistem olabilmektedir. Özellikle maddi çıkar elde etmeye yönelik saldırılarda talep edilen maddi tutarın anonim veya takip edilemeyen bir şekilde transfer edilebilmesi, saldırganların bu alana yönelik yoğun bir şekilde saldırı mesaisi harcamasına sebep olmaktadır. Uluslararası saldırgan motivasyonunun da yüksek olduğu bu alanda saldırı engelleme ve olası saldırı durumunda saldırgan tespiti için ilgili kolluk kuvvetleri arasında uluslararası işbirliklerinin tesis edilebilmesi için çalışmalar yapılması önemlidir.

Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi

Yerli ve Milli Siber Güvenlik Çözümleri, test ve sertifikasyonun gündeme alındığı bu stratejik amacın gerçekleştirilebilmesi için ilgili kuruluşlar (kamu-akademi-özel sektör) yoğun bir çaba içerisindedir. Burada işbirliği ve birlikte çalışma son derece önemlidir. Bu stratejik amaç doğrultusunda, uluslararası pazarda da ülkemizde geliştirilmiş siber güvenlik çözümlerinin rekabet edebilmesi hedeflenmektedir.

SiberKüme üye kuruluşlar tarafından siber güvenlik çözümlerinin geliştirildiği, ilgili siber güvenlik test kuruluşları (TÜBİTAK, TR-TEST, özel laboratuvarlar) tarafından test edildiği ve sertifikasyon kapsamında da Türk Standartları Enstitüsü (TSE), TR-TEST tarafından gerekli belgelendirmelerin yapıldığı ulusal bir mekanizmanın bu stratejik hedef kapsamında ortaya çıkarılması ve geliştirilmesi önemlidir. Test ve sertifikasyon altyapısının, ülkemizde kullanılan yabancı siber güvenlik çözümlerine de aynı disiplinin uygulaması hedeflenmektedir.

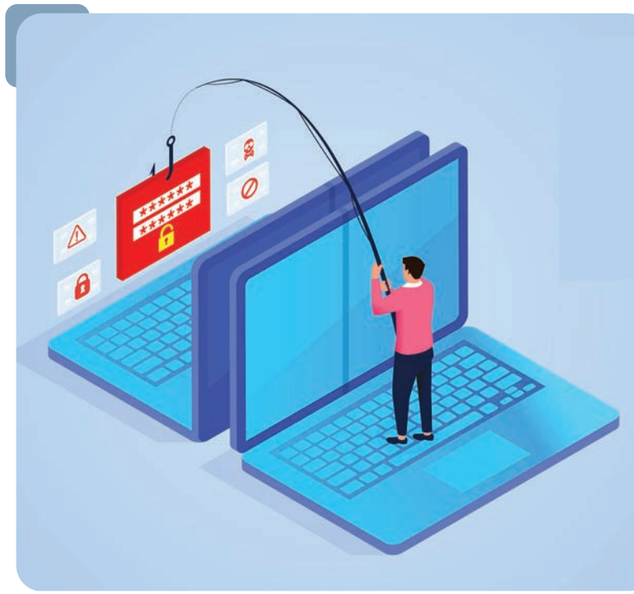
Siber Güvenliğin Milli Güvenliğe Entegrasyonu

Siber olaylara müdahalenin olay öncesi, esnası ve sonrasını kapsayan bir bütün olmasından hareketle; proaktif siber savunma anlayışının geliştirilmeye devam edilmesi son derece önemlidir. Bu stratejik amaç doğrultusunda iç ve dış siber güvenlik tehditlerinden korunabilmek için milli güvenlik politikalarımızda siber güvenlik ile ilişkili önlemlerin de yer alması sağlanacaktır. Bu kapsamda; Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CB DDO), Savunma Sanayi Başkanlığı, Siber Savunma Komutanlığı, BTK USOM ve TÜBİTAK kurumlarının koordinasyonunun son derece önemli olduğu değerlendirilmektedir.

Uluslararası İş Birliğinin Geliştirilmesi

Siber saldırılar, fiziksel mekan bağımsız saldırılardır. Saldırgan, bulunduğu fiziksel mekandan bağımsız olarak istediği fiziksel noktaya sınır ötesinden saldırı gerçekleştirebilir. Bu sebeple saldırı analizi, saldırgan tespiti kapsamında ve saldırılara karşı birlikte önlem alabilmek için uluslararası işbirlikleri ve uluslararası organik savunma platformlarının oluşturulması gerekmektedir. Bu stratejik amaç doğrultusunda uluslararası siber güvenlik tatbikatları düzenlenmesi, mevcut işbirliklerinin geliştirilmesi, siber saldırı engelleme ve saldırgan tespitine hizmet edecek yeni işbirliklerinin oluşturulması sağlanacaktır.

Yukarıda belirtilen stratejik amaçların gerçekleştirilmesine yönelik olarak ülkemizde ilgili uzman kurum ve kuruluşlar (Kamu, Özel Sektör, Akademi ve STK'lar) 2020-2023 dönem aralığı için 40 (kırk) adet eylem ve 75 (yetmiş beş) adet uygulama adımı kapsamında görevlendirilmiş olup, ilgili görevlerin gerçekleştirilmesi Ulaştırma ve Altyapı Bakanlığı koordinasyonunda periyodik olarak denetlenmektedir.



BİLGEM Siber Güvenlik Enstitüsü Koordinatörü Ayşe İnanç:

Bilginin olduğu her alan önemli ve değerlidir.

Ayşe İnanç

Lisans ve Yüksek Lisans eğitimini Berlin Frei Ünversitesi, Bilgisayar Mühendisliği Bölümü'nde tamamladı. 2010 yılında başladığı Belbim A.Ş'de 'Akıllı Yolcu Bilgilendirme ve Ödeme Sistemleri' başta olmak üzere çeşitli projelerde görev aldı. 2016 yılında TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü'nde çalışmaya başladı.

Uzmanlık alanları arasında Yazılım güvenliği ve kriptoloji, Mikroservis mimarisi ve teknolojileri, bulut teknolojileri yer almaktadır. Kasım 2020'den beri BİLGEM SGE Koordinatörü olarak görev yapmaktadır.

Fotoğraflar - Kerem Bora Özbayrak - Uzman Yardımcısı / BİLGEM IGBY

Siber güvenlik; bilgisayarların, ağların, programların ve verilerin yetkisiz erişimlere, saldırı ve sömürü amaçlı her türlü harekete karşı korunmasıdır.

BİLGEM SGE Enstitü Koordinatörü Sayın Ayşe İnanç ile bir röportaj gerçekleştirdik. Ayşe Hocamız, siber güvenliğin ne olduğu, günümüzdeki yeri ve önemi, Kurum ve ülke olarak neler yaptığımızı, daha neler yapmamız gerektiği ile ilgili aydınlatıcı bilgiler verdi…

Siber güvenlik nedir? Ne anlamalıyız?

Siber güvenlik, siber saldırılara karşı alınan tedbirler bütünüdür. En genel anlamda siber güvenlik; bilgisayarların, ağların, programların ve verilerin yetkisiz erişimlere, saldırı ve sömürü amaçlı her türlü harekete karşı korunmasıdır. Bu kapsamda baktığımızda 5 temel alan öne çıkmaktadır: Uygulama güvenliği, ağ güvenliği, bilgi güvenliği, veri kurtarma ve siber güvenlik eğitimleri.

Uygulama güvenliği alanında, bilişim kapsamındaki tüm cihazlar ve uygulamalar için kullanılan tasarım – geliştirme – devreye alma - güncelleme ve bakım süreçleri olarak adlandırabileceğimiz yaşam döngüsü boyunca ve sonrasında, kullanıcı bazlı zafiyetleri de içine alan geniş bir güvenlik perspektifi ile koruma aklımıza gelmelidir.

Ağ güvenliği; ağın güvenliği ve bütünlüğünün sağlanmasına yönelik tedbirler içerir. Ağın maruz kalabileceği tehditlerin modellenmesi ve savunma mekanizmasının geliştirilmesi, ağ güvenliğini sağlamaya yönelik en temel hedeflerdir.

Bilgi güvenliği hedefleri; yetkisiz erişimleri önlemek, veri güvenliğini sağlamak olarak özetlenebilir. Bu kapsamda uygulamalar geliştirilmekte, standartlar oluşturulmakta, eğitimler gerçekleştirilmektedir. DLP, ISO 27001 çalışmaları, siber güvenlik eğitimleri, kriptografi çalışmaları örnek olarak verilebilir.

Veri kurtarma; hem risk analizi çerçevesinde veri kayıplarına karşı geliştirilecek kurtarma stratejilerini, hem de dijital verilerin incelenmesi kapsamındaki veri kurtarma çalışmalarını içerir. İlkinde amaç, kurumsal faaliyetlerin bir kesintiye uğramaksızın devam etmesini sağlamak, diğerinde ise adli soruşturmalar kapsamında dijital adli analiz çalışmalarını gerçekleştirmektir.

Siber güvenlik operasyonları adımlarını da şöyle sıralayabiliriz:

- Tehdit belirleme, risk analizi
- Bilgi/Veri koruma yöntemleri geliştirme
- Saldırı ve yetkisiz erişimleri tespit etme
- Saldırı ve yetkisiz erişimleri engelleme ve cevap verme
- Bilgi/Veri kurtarma ve bilgi güvenliğini yeniden tesis etme
- Cihaz / Yazılım / Sistem denetleme ve sıkılaştırma

Siber dünya: Beşinci savaş alanı

Siber güvenliğin sağlanmasında milli ve yerli çözümlerin önemli ve kritik olduğu alanlar hakkında bilgi verebilir misiniz?

Bilginin olduğu her alan önemli ve değerlidir. Bu kap-

samda ülkemizde her alandaki bilgiyi korumak sorumluluğumuzdadır. Siber dünya, NATO tarafından kara, hava, deniz ve uzaydan sonra beşinci savaş alanı olarak ilan edilmiştir. Sanal bir ortamda gerçekleşiyor olmasından dolayı henüz farkındalık seviyesi alt düzeydedir, fakat yaratmış olduğu fiziksel zararlarla ne kadar tehlikeli olduğunu kanıtlamıştır. Bundan dolayı tüm alanlarda yerli ve milli ürünlerle çözüm sunulamaması, her alanda büyük bir zafiyete yol açmakta ve dışarıya bağımlılığımızı artırmaktadır.

Kritik veri; kurum, sistem, ürün ve birey bazında ayrı ayrı değerlendirilmelidir. Kritikliğin seviyesine, en basit değerlendirme yöntemi olarak, veri kaybı durumunun ülkemize, kurumlara, bireylere olan etkisi ölçüsünde karar verebiliriz. Örneğin en kritik veriler kuşkusuz askeri kurumlarda yer almaktadır. Dışişleri Bakanlığı verileri de uluslararası alanda ülkemiz için kritiklik düzeyi en yüksek seviyededir. Sistem bazında baktığımızda elektrik şebekesini kontrol eden SCADA sistemleri, bir hastanedeki hasta verileri, bir petrokimya endüstrisindeki güvenlik kontrolleri ya da evlerimizde kullandığınız bilgisayarlardaki verilerimiz gibi daha özele ve detaya inildikçe aslında her alanda kritik verilerin olduğunu görmekteyiz.

Biz ülkemizdeki her alanda yerli ve milli ürünlerin kullanılması gerektiğine inanıyoruz. Yabancı menşeli ürünlerin özellikle kamu ve askeri alanlarda kullanılması birer tehdit kaynağıdır. Bu yüzden siber güvenliğin yerli ve milli çözümlerle sağlanması kritik önem arz etmektedir.

Alandaki ulusal gelişmeler

Siber güvenlik çözümlerinde ülkemizdeki mevcut durum ve gelişimi gerekli alanlarla ilgili görüşleriniz nelerdir? Ülke olarak bu alanda neredeyiz, neler yapıyoruz?
Ülkemizde siber güvenlik alanındaki yasal düzenleme ilk olarak Ekim 2012'de Bakanlar Kurulu tarafından alınan "Ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar" ile gerçekleştirilmiş oldu. Bugüne kadar geçen sürede üç adet Siber güvenlik Stratejisi ve Eylem Planı hazırlandı. Türk Silahlı Kuvvetleri bünyesinde Siber Savunma Komutanlığı kuruldu.

Ülkemiz için kritik altyapılar belirlendi. Kurumsal ve sektörel SOME'ler için rehber dokümanlar hazırlandı. Kişisel Verileri Koruma Kanunu (KVKK) kabul edildi ve ikincil düzenlemeler gerçekleştirildi. "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği" çıkarıldı.

2018 yılında Savunma Sanayii Başkanlığı himayesinde Türkiye Siber Güvenlik Kümelenmesi oluşturuldu. Türkiye Siber Güvenlik Kümelenmesi hedeflerini, "Türkiye'deki siber güvenlik firmalarının sayısını artırmak, üyelerinin teknik, idari ve finansal açılardan gelişimine destek olmak, Siber Güvenlik ekosisteminin standartlarını geliştirmek, üyelerinin ürün ve hizmetlerinin markalaşmasına yardımcı olmak, üyelerinin ulusal ve global pazarda rekabet gücünü artırmak, Siber Güvenlik alanındaki insan kaynağı sayısını artırmak, niteliklerini geliştirmek ve toplumda siber güvenlik bilincini geliştirmek" olarak açıklamıştır.

En son Ulaştırma Bakanlığı tarafından Aralık 2020'de "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)" yayınlandı. BİLGEM SGE olarak hem eylem planında belirtilen alanlarda hem de 11. Kalkınma Planı'nda belirtilen hedeflere uygun olarak kurumsal hedeflerimizi belirliyor ve çalışmalarımızı bu hedeflere uygun alanlarda yoğunlaştırmaya çalışıyoruz.

Geldiğimiz noktada siber uzay, devletler arasında yeni bir mücadele alanı olarak görülmekte ve devletlerin askeri kapasitelerini geliştirmek için bir fırsat olarak değerlendirilmektedir. Bu gelişmeler ve siber saldırı alanları, uluslararası sistemi daha da belirsiz ve tehlikeli hale getirmektedir. Bu sebeple Türkiye'nin, siber güvenlik stratejisi geliştirme, siber savunma ve saldırı kapasitesine yatırım yapma konusunda çalışmalar yaptığı ve bu konuda ülkemizde bir farkındalık olduğu açıktır. Ulusal Siber Güvenlik Stratejisi ve Eylem Planları hazırlanmış ve siber güvenlik özelinde kurumsal yapılanmalar oluşturulmuştur.

BİLGEM Siber Güvenlik Enstitüsü (SGE)

BİLGEM siber güvenlik alanında neler yapmaktadır, ne tür hizmetler vermektedir? Kurumu bu açıdan ulusal ve uluslararası ölçekte değerlendirebilir misiniz?
SGE'nin temelleri 1997 yılında Ağ Güvenliği Grubu adı ile kapsamlı bir test laboratuvarının kurulması ile atıldı. Ağ Güvenliği Grubu, Türk Silahlı Kuvvetleri'nin ve kamu kurumlarının bilişim sistemleri güvenliği alanındaki ihtiyaçlarını karşılamak üzere pek çok proje gerçekleştirdi. Ülkemiz için önemli olan güvenlik mimarilerinin tasarımı, sistemlerin güvenli kurulumu, güvenlik testleri, risk analizi gibi alanlarda önemli tecrübeler kazanıldı.

> **Siber dünya, NATO tarafından kara, hava, deniz ve uzaydan sonra beşinci savaş alanı olarak ilan edilmiştir.**

2005 yılında Ulusal Bilgi Sistemleri Güvenlik Programı tanımlandı. Bu programın en önemli hedeflerinden biri ülkemizin siber güvenliğinin sağlanması idi. Bu kapsamda TÜBİTAK BİLGEM bünyesinde Türkiye Bilgisayar Olaylarına Müdahale ekibi (TR-BOME) kuruldu. TR-BOME kritik kamu kurumlarında BOME yapılanmasının kurulabilmesi için gerekli eğitim ve koordinasyon faaliyetlerini yürüttü. 2013 yılında BTK bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM) kuruluncaya kadar da bu faaliyetlere devam edildi.

Türkiye'nin önde gelen bilişim sistemleri güvenliği merkezlerinden biri haline gelen Ağ Güvenliği Grubu daha sonra Bilişim Sistemleri Güvenliği Bölümü ve 2012 yılından itibaren de Siber Güvenlik Enstitüsü (SGE) adını aldı.

Siber Güvenlik Enstitüsü olarak; siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürütmekte, ulusal siber güvenlik çalışmalarına rehberlik etmekte ve çözüme yönelik siber güvenlik projeleri gerçekleştirmekteyiz. Ayrıca eğitim, test ve danışmanlık faaliyetlerimiz de yoğun bir şekilde devam etmektedir.

Çeşitli alanlarda ulusal çapta Ar-Ge çalışmalarımız devam etmektedir. Bunlar;
√ Bulut Bilişim ve Veri Mahremiyeti alanındaki çalışmalar,
√ Uç nokta ve bilgi güvenliği alanındaki çalışmalar,
√ Kritik altyapılara yönelik saldırı ve savunma çalışmaları,
√ Merkezi saldırı tespit sistemi,
√ Balküpü / tuzak sistemleri,
√ Uygulamalı siber güvenlik eğitimleri için sanal eğitim altyapısı platformu çalışmaları,
√ Dijital adli analiz çalışmaları olarak özetlenebilir.

Ar-Ge çalışmaları dışında siber güvenlik hizmetleri olarak adlandırdığımız endüstriyel hizmet projelerimiz bulunmaktadır. Bu kapsamda, başta ülkemizin stratejik öneme sahip kurumları ve önemli sektör kuruluşları için standart güvenlik savunmalarını aşan tehdit ve saldırılara karşı, siber güvenlik testleri ve denetimleri gerçekleştirilmektedir.

Enstitümüzde ayrıca siber güvenlik alanında ülkemizde nitelikli iş gücünün artırılmasına yönelik sızma testi eğitimleri ve siber güvenlik ile ilgili teorik ve uygulamalı eğitimler verilmektedir. Siber güvenlik alanında danışmanlık hizmetleri ile birlikte rehber ve kılavuz hazırlama çalışmaları da yürütmekteyiz.

Siber Güvenlik Enstitüsü olarak, siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürütmekte, ulusal siber güvenlik çalışmalarına rehberlik etmekte ve çözüme yönelik siber güvenlik projeleri gerçekleştirmekteyiz.

Uluslararası işbirlikleri kapsamında NATO Siber Savunma Mükemmeliyet Merkezi'nde bir temsilci bulundurmaktayız. Bu sayede uluslararası alanda yapılan çalışmaları yerinde takip etmekte ve düzenlenen tatbikatlara katılım sağlamaktayız. Bu kapsamda yine NATO desteği ile farklı ülkelerde siber güvenlik eğitimleri gerçekleştiriyoruz. Bugüne kadar Azerbaycan, Ürdün ve Tunus'ta toplam 4 eğitim gerçekleştirdik. 2021 yılı içinde yine Azerbaycan'da bir eğitim gerçekleştirmeyi planlıyoruz. Söz konusu eğitimlerin katılımcıları arasında ilgili ülkelerin askeri ve farklı kamu kurumlarından seçilen personelleri yer almaktadır. Bu kişilere ülkemizde geliştirilen yerli ürünlerden bahsetme ve bir pazar payı oluşturma şansı da bulmaktayız.

SGE'nin yakın, orta ve uzun vadeli hedefleri nelerdir?
Siber Güvenlik, farklı alanların bir arada incelenmesi ve doğru şekilde yönetilmesi gereken bir alandır. Teknik konular yanında yasal, politik, askeri gibi farklı alanların da devreye girdiği bir alan olduğundan, strateji ve hedeflerin ulusal ve uluslararası çerçevede belirlenmesi gerekmektedir. SGE olarak, kurumsal hedeflerimizi hem Ulusal Siber Güvenlik Stratejisi ve Eylem Planında belirtilen maddelere göre hem de siber güvenlik alanında araştırma ve geliştirmeye yönelik yaptığımız çalışmalara göre belirlemekteyiz.

Yakın vadeli hedeflerimiz arasında, siber güvenlik alanında yetişmiş insan gücüne olan ihtiyaçtan dolayı kamu kurumları, üniversiteler, özel sektör ve eğitim kurumları ile eylem planı kapsamında çalışmaların planlanması ve hayata geçirilmesi yer almaktadır. Eğitim vermenin yanında öğrenciler için düzenlenen siber güvenlik kamplarında etkin rol almak, eğlenerek öğrenmeyi sağlayan ve güvenlik bakış açısını kazandıran faaliyetlerden olan CTF (Capture The Flag) yarışmaları gerçekleştirmek hedeflerimiz arasındadır.

Siber güvenlik alanında yerli ve milli teknolojilerin geliştirilmesi ve uluslararası boyutta ticari çalışmalar yürütmek, yakın zamanlı hedeflerimiz arasındadır. Ürünleşme aşamasındaki projelerimizle, siber güvenlik alanında yeni teknolojilere yerli imkanlarla sahip olunmasına katkıda bulunmayı, ülkemizde gerçek anlamda güvenliğin sağlanması ve güvenlik gibi bir alanda dışa bağımlılığın azaltılmasını hedeflemekteyiz.

Orta vadeli hedeflerimiz arasında kritik altyapılar ile ilgili çalışmalar bulunmaktadır. Öncelikli olarak enerji sistemleri için uygulanabilecek bir model geliştirmeyi, bunun diğer kritik altyapılar için de uyarlanabilir bir yapı olmasını ve bu önemdeki sistemlere savunma yetenekleri kazandırmayı amaçlamaktayız.

BİLGEM Siber Güvenlik Enstitüsü'nün yakın, orta ve uzun vadeli hedefleri arasında, yeni nesil siber güvenlik teknolojilerinin yerli ve milli, dünya pazarında yer alacak şekilde katma değeri yüksek ürün, hizmet ve teknolojiler geliştirilmesini sağlamak yer almaktadır. Alanda, ulusal ve uluslararası seviyede, kamu, sanayi ve akademi işbirliği ile çalışmalar yapmak ve koordinasyon sağlamak hedeflerimiz arasında yer almaktadır.

SGE'de ihtiyaç duyduğunuz çalışan profili hakkında bilgi verebilir misiniz?
SGE'de farklı uzmanlık alanlarına olan ihtiyaç sebebiyle çalışan profilimiz de farklılık göstermektedir. Yürütmüş olduğumuz sızma testi, güvenlik denetlemeleri ve siber güvenlik çözümlerine yönelik çalışmalarımız kapsamında; uluslararası alanda kabul görmüş güvenlik metodolojilerine hâkim, ağ ve topoloji bilgisi olan, sistem güvenlik açıklarını tespit edip çözüm geliştirebilen çalışanların yanı sıra temel siber güvenlik prensiplerine hâkim, kriptografi ve güvenli yazılım geliştirme süreçleri hakkında tecrübeli çalışanlar yer almaktadır.

Hızla gelişen ve değişen teknolojiyi düşündüğümüzde değişimleri çok yakından takip etmek ve ortaya çıkabilecek tüm riskleri tespit etmek, yorumlamak ve çözüm üretmek gerekmektedir. SGE çalışanları hem bu gelişmeleri takip etmekte hem de eğitimler vermektedir.

TÜBİTAK BİLGEM

Bu bir proje tanıtımıdır.

Yerlisinyal
Demiryolu Sinyalizasyon Sistemleri

YERLİSİNYAL Projeleri, ülkemizdeki demiryolu hatlarında var olan sinyalizasyon eksikliğini gidermeyi ve bu alandaki büyük dışa bağımlılığı ortadan kaldırmayı amaçlamaktadır. Bu kapsamda sinyalsiz demiryolu hatları, emniyetli ve yerli ürünlerle donatılmaktadır.

Geliştirilen YERLİSİNYAL anklaşman sistemleri ve trafik kontrol merkezleri, Türkiye'nin çeşitli bölgelerinde toplam 850 km.lik demiryolu hat kesiminde devreye alınmaktadır. 1500 km.lik hat kesimi için ise projelendirme çalışmaları devam etmektedir.

Ürünler-Konvansiyonel Demiryolu Hatları İçin
- Hatboyu Sinyalizasyon Sistemleri
- Anklaşman Sistemleri (SIL4)
- Saha Ekipmanı Sürme Üniteleri (SIL4)
- Trafik Kontrol Merkezleri
- Bölgesel, Yerel Kumanda Masaları

Özellikler
- Uluslararası standartlara uygunluk
- Yüksek emniyet seviyesi ve işlevsellik
- Düşük ilk yatırım maliyeti
- Düşük bakım ve işletme giderleri
- Kritik tüm bileşenleri yerli
- Açık arayüzlere sahip

U-D-3-P · Yerli Sinyal 09 · Yerli Sinyal 03 · Yerli Sinyal 06 · Yerli Sinyal 44 · Yerli Sinyal 01 · Yerli Sinyal 34 · ETCS L1 Yerli Sinyal

www.bilgem.tubitak.gov.tr

Siber Güvenlikte Trend Konular ve Çalışmalar

Mahmut Can Sözeri / TURKCELL Siber Güvenlik Direktörlüğü

> **Artık bir zararlı, sadece ilgili bulaşa maruz kalan bilgisayarı değil, bulunduğu ev ve işyeri ağındaki diğer bilgisayarları, mahalleyi, şehri, ülkeyi, kıtayı derken tüm dünyayı etkilemeye başladı.**

Siber güvenlik kavramı denilince ya da bu kavram ile ilişkili en temel konular gündemde iken, akıllara bundan yaklaşık 20 yıl kadar önce virüs bulaşması geliyordu. Bilgisayarınıza bir virüs bulaşır, bilgisayarınız çalışmaz hale gelirdi ya da dosyalarda bozulmalar olurdu. Bu durumu zamanla CD/DVD'ler ile USB Bellek'ler (halk arasında Flash Bellek'ler) takip etti. CD/DVD ve USB Belleklerin kullanılmaya başlanmasıyla beraber, bu bellek kaynaklarından da virüs bulaşmaları söz konusu oldu. Özellikle iş yerlerinde ve okullarda İnternet altyapılarının ve kullanımlarının yaygınlaşmasıyla artık bir bilgisayardaki bir virüs, USB Bellek, CD/DVD, harici Hard Disk gibi herhangi bir harici aygıta ihtiyaç duymadan diğer bilgisayarlara aynı ağ üzerinden bulaşmaya başladı.

Devamında evlerimizde de İnternet kullanımı yaygınlaştı ve İnternetten indirilen dosyalar aracılığıyla ev ağındaki bilgisayarlara virüs bulaşması söz konusu oldu. Kavramlar değişti, gelişti, yaygınlaştı, virüs kelimesi tek başına siber tehditleri anlatmak için yeterli gelmedi. Trojen'ler, fidye yazılımları, truva atları, casus (spyware) yazılımları, keylogger (klavye hareketleri kayıt eden) yazılımlar, solucanlar gibi akademik dünyada ve siber güvenlik alanında çalışanlar tarafından zaten bilinen ve tanımlanan virüs çeşitlerinin bilinirliği yaygınlaştı. Bunlarla birlikte artık bir zararlı, sadece ilgili bulaşa maruz kalan bilgisayarı değil, bulunduğu ev ve işyeri ağındaki diğer bilgisayarları, mahalleyi, şehri, ülkeyi, kıtayı derken tüm dünyayı etkilemeye başladı.

The New York Times'ta 2020 yılının Eylül ayındaki bir habere göre hastane sistemlerine ransomware (fidye yazılımı) bulaşması sonucu geciken tedavi nedeniyle Alman bir kadının öldüğü üzerinde duruluyor. 2021 yılı Şubat ayında The Washington Post'ta çıkan habere göre Florida eyaletinde bir şehre su sağlayan arıtma tesisinde siber saldırgan tarafından sodyum hidroksit miktarı artırıldı. Son anda önlenmeseydi temizlemek için kullanılan bu kimyasal insan sağlığına zararlı olan sınıra gelecekti ve suyu içen kişilerin hayatları tehlikeye girecekti. Dolayısıyla buradaki gidişatı şöyle özetleyebiliriz:
Bilgisayar güvenliği -> Ağ Güvenliği -> Bilgi Güvenliği -> Siber Güvenlik -> Toplum Güvenliği
Sanal dünyadaki saldırıların gerçek dünyayı etkilediğinin anlaşılması bu kadar yeni bir kavram değil aslında. İran'ın nükleer çalışmalarının planlandığı gibi gitmemesi için kullanılan solucan yazılım olan Stuxnet ile birlikte sanal dünyada yaşanan bir olayın gerçek dünyada da doğrudan insan hayatına etki edebileceği gözlendi.

Tüm dünyayı etkileyebileceği somut olarak görüldüğünde, hacker grupları ve devletler kendi çıkarları için virüs geliştirmeye ve siber ordularını kurmaya başladılar. Adı üzerinde bir ordunun görevi, yeri geldiğinde yapılan saldırıyı püskürtmek ve savunma yapmak, yeri geldiğinde ise karşı atak yapmak ve önce davranıp saldırı planlamaktır. Nitekim şu an bulunduğumuz topraklarda yaşanan Truva Atı olayı da tam olarak günümüze uyarlanabilir durumdadır. Truva atı artık fiziki bir at değil, sanal ortamda geliştirilen ve hedefin içerisine sızan, sızdırılan yapılar olarak olarak karşımıza çıkmaktadır.

Dünya geneline baktığımızda pandemi ile birlikte market alışverişlerinden araç alımlarına, ofise gitmeden bir işe başlamaya, okula gitmeden eğitime başlamaya, fiziki ziyaretler yerine bilgisayar başından müze ziyareti ile konser, tiyatro gösterilerinin canlı yayın ile uzaktan takip edilmesinden, evde spor yapılmasına kadar evden çıkmadan hayat devam edilebilecek duruma geldi. İnsanların belki de evden çıkmalarını sağlayacak en temel konulardan bir tanesi bankalardı. Geçmiş zaman ifadesi kullandım çünkü BDDK'nın 1 Nisan 2021'de yayınlanan yeni yönetmeliği ile bankacılık işlemlerinde ıslak imza zorunluluğu da kalktı görünüyor. Sanırım sırada Noterde yapılan işlemler var.

> **Devletler kendi çıkarları için virüs geliştirmeye ve siber ordularını kurmaya başladı.**

Her yeni çözüm veya değişim beraberinde daima çözüm bekleyen yeni sorunları getirir. Bu minvalde giderek globalleşme hızı artan dünyada sayılamayacak kadar çok siber sorun olmakla beraber, bunlara karşı bir çok çözüm de geliştirilmektedir. Bu yazımızda bunlardan öne çıkanları şu şekilde sizlerle paylaşıyor olacağız;

√ VPN Güvenliği ve Yedekliliği
√ Video Konferans Güvenliği
√ Uçtan Uca Şifreleme ve Mesajlaşma Uygulamaları
√ Son Kullanıcı Cihaz Güvenliği ve IoT
√ Makine Öğrenmesi Modellerinin Güvenliği
√ Kaynak Kod Güvenliği ve Açık Kaynak Sistemler

VPN Güvenliği ve Yedekliliği

Evden çalışmaya başladığımız ve pandemi sonrasında da uzaktan çalışmayı gündemde tutacak iş modellerinin tasarlandığı bugünlerde en önemli konuların başında şüphesiz VPN kapasitesi, güvenliği ve yedekliliği gelmektedir.

2021 yılı Mart ayında ücretsiz bir VPN hizmeti sunan firmadan 1.2 TB boyutunda 21 milyon kullanıcının bilgilerinin çalındığı açıklandı. Şirketlerin veya kamu kurum ve kuruluşlarının iç ağına bağlantı için kullanılan VPN'lerin güvenliğinin ve yedekliliğin en üst seviyede sağlanması oldukça kritiktir. VPN sistemlerine girişlerde çok faktörlü doğrulama (multi factor authentication) seçeneklerinde SMS kullanımı yerine doğrulayıcı uygulamaları (authenticator) ya da kendi iç mesajlaşma uygulamaları ya da kuruma özel uygulamalara anlık bildirim (push notification) kullanılması gerekir.

Video Konferans Güvenliği

İş görüşmelerinden iş toplantılarına, eğitimlerden sınavlara kadar, devlet işleri dahil olmak üzere video konferans sistemi giderek yaygınlaşarak kullanılmaktadır. Devlet başkanları birbirleriyle video konferans sistemiyle görüşmekte, yerel idareler ile merkez birimleri, şirketlerin genel merkezleri ile bölge temsilcileri kritik toplantılarını video konferans sistemleri ile yapmaktadırlar. Görünen bu durum her geçen gün gittikçe yaygınlaşma eğilimindedir.

Video konferans sistemleri bu denli yaygın değilken veya bu denli herkes tarafından kullanılmadan önce bağlantı, ilgili kişi ile paylaşılıyor ve bağlantıya sahip kişiler bu sistemlere girebiliyorlardı. Aslında bu durumun başından beri güvenli olmadığı biliniyordu fakat pandemi ile birlikte toplantıların gündeminde gizli ve/veya stratejik bilgi içeren görüşmeler yapıldığı için önemi arttı. Bu hizmeti sunan şirketler; toplantıya girişlerde şifre kullanılması, ilgili kişiler toplantıya katılınca toplantının kilitlenmesi ve yeni gelecek kişilerin girişinin engellenmesi, katılımcıların öncelikli olarak lobide bekletilip sonrasında toplantıya kabul edilmesi gibi çözümleri hızlıca uyguladılar.

Bu durum yeterli olmadı çünkü görüşme trafiğine sızılıp, mesaj ekranındaki yazışmalara ulaşılmaya başlandı. Sonrasında şifre bilinmese bile toplantılara giriş yapıldı. Nihai olarak ise toplantıya katıldığına dair hiç bir iz bırakmadan herhangi bir toplantıya katılımcı olarak sızıp toplantı içeriklerine ulaşım söz konusu oldu. Bunun üzerine firmalar; ilgili trafiğin bu hizmeti sağlayan firmaların sistemleri tarafından bile erişilemeyecek şekilde uçtan-uca şifreleme seçeneklerini dahil ederek güvenliği en üst düzeyde tutmaya başladılar.

Uçtan Uca Şifreleme ve Mesajlaşma Uygulamaları

Mesajlaşma ve video konferans sistemlerinde gündeme gelen uçtan uca şifreleme, ilgili yazılı ve/veya görüntülü/sesli görüşmelerin şifreli olması ve bu şifrelerin yalnızca görüşmeyi yapanlarca çözülebilmesi, aradaki trafik taşıyıcılar tarafından çözülememesi anlamına gelmektedir. Uçtan-uca şifreleme denildiğinde bazı mesajlaşma sistemleri bunu sağladıklarını belirtiyor fakat aslında yaptıkları örneğin Ali, Ayşe'ye "Merhaba" diye bir mesaj gönderiyor. "Merhaba" mesajı şifreleniyor, ilgili mesajlaşma uygulamasının sunucusuna bu şifreli mesaj geliyor ve çözülüyor yani "Merhaba" metnine ulaşılıyor. Buradan tekrar Ayşe'nin çözebileceği bir yöntem ile şifrelenip gönderiliyor. Ayşe de "Merhaba" mesajını okuyabiliyor. Burada sunucu şifrelenmiş içeriği çözmeden de gönderebilir. Fakat ilgili mesajlaşma uygulaması istediği zaman bu şifrelenmiş mesajları çözebiliyorsa burada uçtan-uca şifrelemeden bahsedilemez. Zira uçtan uca şifrelemede mesajın, başta ifade edildiği gibi sadece taraflar tarafından çözülmesi gerekir.

Bu örneğimizde Ayşe ve Ali dışında her kim olursa olsun içeriğe erişim söz konusu oluyor ise uçtan uca şifrelemeden bahsedilemez. Bir süre önce 128-bit, 256-bit şifreleme söz konusu olduğunda oldukça güçlü diye bahsedilirken günümüzde 1024 bit ve hatta 2048 bit uzunluklardan bahsedilmektedir. Şifreleme işlemlerinde kullanılan şifreleme anahtarlarının uzunlukları arttıkça sunucular veya bilgisayar üzerindeki işleme gücü ihtiyacı da artmaktadır.

Bu alandaki çözümler görünen o ki daimi olarak gündememizde olacaktır. Hazır olarak kullanılan ve kullanan kişi veya kurumlar tarafından geliştirilmeyen uygulamalar düşünüldüğünde ne kadar güvenilir oldukları ile ilgili araştırma raporlarına veya yapılan bilimsel çalışmalara bakılması gereken bir konudur.

Son Kullanıcı Cihaz Güvenliği ve IoT

The Washington Post gazetesindeki 2021 yılı Mart ayındaki bir haberde Apple'ın uygulamaları barındıran mağazası olan App Store üzerinde yer alan bir uygulama aracılığıyla bir IOS kullanıcısından 600 bin dolar değerinde Bitcoin çalındığı yazıyordu. McAfee resmi blogunda 2019 yılı Eylül ayında yayınlanan bir yazıya göre Siber suçluların en çok istediği 4 mobil tehlike şöyle sıralanmış: SMS ile gelen oltalamalar, ücretsiz-halka açık WiFi'lar, sahte (fake) mobil uygulamalar ve reklam yazılımı, casus yazılım veya malware gibi birçok biçimde gelebilecek olan Grayware'lar.

Ayrıca bundan belki de çok değil 15 yıl önce bilgisayarlarda bile anti-virüs uygulamaları en azından Türkiye'de çok yaygın değilken, bugünlerde mobil telefonlara özel geliştirilmiş anti-virüs uygulamaları kullanılmaktadır. Kredi kartlarını barındıran cüzdan uygulamaları, bankacılık uygulamaları, eposta uygulamaları, kriptopara hesap uygulamaları, sosyal medya uygulamaları gibi bir insanın neredeyse tüm hayatının artık telefonlarda olması, siber suçluların hedefinde olması için çok geçerli bir nedendir. Türkiye'deki bir haber sitesinin 2013 yılı Şubat ayındaki haberinin başlığı "Cüzdanını unut cep telefonunu unutma"'dır.

Son kullanıcı cihazı dediğimizde sadece cep telefonları, tabletler ya da bilgisayarlar düşünülmemelidir. Evlerdeki yazıcılar, akıllı televizyonlar, web kameralar, çamaşır makineleri, oyuncaklar kısacası kendisi dışında bir cihaza öyle veya böyle bağlanma özelliği olan her cihaz için güvenlik tedbirleri düşünülmeli ve alınmalıdır.

2019 yılı Aralık ayındaki The Washington Post gazetesindeki haber bu konudaki olayların nereye gidebileceğini bizlere gösterdi. Bir hacker, 8 yaşındaki kız çocuğunun odasında bulunan bir kamerayı ele geçirdi ve küçük kız ile konuştu. Akıllı TV'lerin ele geçirilerek mahrem hayatı kaydettiği konusundaki haberlere ise neredeyse şaşırmıyoruz. Marketlerde bile satılan oyuncak gibi gözüken fakat işlev olarak oldukça yetenekli drone'lar varsayılan olarak Wi-Fi üzerinden bağlantı sağlar ve şifresi de yoktur. Herhangi bir kişi dronu kontrolünü ele geçirerek canlılara zarar verebilir, veya en iyi ihtimalle drone'u kendi mülkiyetine geçirebilir.

Hız değerleri ile hepimizi heyecanlandıran 5G ve IoT cihazlarının yaygınlaşması ile akıllı ev sistemlerinin, internete veya başka cihazlara bağlanan hemen her cihazın güvenliği son derece kritik hale gelmiştir. Ağ teknoloji şirketlerinin tamamı ve telekom şirketleri 5G güvenliği konusunda çalışmalarını giderek artırıyor, yeni projeler başlatıyor, patentler alıyorlar. Bu alanda yine kendisini gösteren akıllı fabrikalar ve otonom araçlar da bünyelerinde bulundurdukları IoT platformları ve siber atak yüzeyleri bakımından insan güvenliği ve emniyeti açısından son derece önemli hale gelmektedirler. Bu yüzden 5G ve IoT güvenliği günümüzün ve önümüzdeki yılların en önemli güvenlik çalışma alanlarından birisi olmaya devam edecektir.

Makine Öğrenmesi Modellerinin Güvenliği

Başta eposta spam filtreleri olmak üzere DLP gibi birçok güvenlik aracı makine öğrenmesinden faydalanmaktadır. Hatta şirketler ürünlerini pazarlama aşamasında makine öğrenmesi kullanarak çok daha "akıllı" filtrelemeler yaptıklarını ve buna göre sisteme otonom olarak kararlar aldırdıklarını aktarmaktalar. Örneğin bundan yaklaşık 4-5 yıl önce dünyanın en büyük teknolojileri şirketlerinden birine ait e-posta hesabından, bu şirkete ait epostalar spam olarak işaretlendiğinde, spam klasörüne düşmeye başlamış ve spam olarak bilinmeye başlanmıştı.

Bir makine öğrenmesi modelinin en temel dayanak noktalarından bir tanesi ve güvenlik açısından zayıf noktası ise dışarıdan aldığı girdilerdir. Modelin hatalı eğitilmesine sebep olan bu girdileri korumak amacıyla Tartışmalı Makine Öğrenimi(Adversarial Machine Learning) başlığı altında çalışmalar yapılmaktadır. Burada hedeflenen hem makine öğrenme algoritmasının eğitimi sırasında eğitim verisine hem de eğitim sonunda oluşan modele girdi olarak saldırı yapılmasıdır. Nihai olarak yanlış sınıflandırma yapılarak yapay zeka algoritmalarının amacı dışı kullanılması ya da kullanılamaz duruma gelmesi söz konusudur. Örnek vermek gerekirse DeepFool isimli akademik çalışmada paylaşılan örnekte orjinal resme, sınıflandırıcı yanıt olarak "whale" (balina) dönerken, orjinal resim + r (karışıklık (perturbation)) eklendiğinde ise sınıflandırıcı yanıt olarak "turtle" (kaplumbağa) dönmektedir.

Kaynak Kod Güvenliği ve Açık Kaynak Sistemler

Synopsys firmasının 2020 yılına ait yayınladığı rapora göre kod altyapısının %91'lik kısmı, 4 yıldan eski ve 2 yıldır herhangi bir şekilde geliştirme yapılmamış bileşenleri kullanıyor. Synk.io'un 2020 yılına ait Açık Kaynak Kod Güvenliği raporuna göre açıkların %35'i 20 günden önce, %36'ı 70 gün ve daha fazla sürede, ortalama ise 68 günde kapatılmaktadır.

2021 yılı Nisan ayında PHP'nin kaynak kodlarına saldırı düzenlenip "back door" yerleştirilmişti. Günümüzde şirketlerin en değerli varlıklarından birisi de sahip oldukları kaynak kodlarıdır. Çünkü kaynak kodlar kullanılarak farklı saldırılar düzenlenebilir. Bu yüzden başta açık kaynak kod güvenliği olmak üzere kaynak kod güvenliği konusunda farkındalık artışı ülkemizde ve globalde söz konusudur. Birkaç yıl öncesine kadar şirketlerde mevcut güvenlik operasyon birimlerinin içerisinde görev yapan kişilerin işlerine ek olarak kaynak kod güvenliği alanında da çalışma yapılırken, günümüzde artık sadece kaynak kod güvenliğine odaklanan birimler kurulmaktadır. Büyük teknoloji şirketlerinde doğrudan bu amaçla görev yapacak personel arayışlarını ilanlarda görmekteyiz.

Tüm bu konular biraz olsun farkındalık oluşturmak, güvenliğin çok boyutlu bir kavram olduğunu göstermek için paylaşıldı. Hiçbir zaman %100 güvenli diye bir sistem yoktur fakat alınabilecek önlemlerin %100'ünü almak diye bir durum söz konusudur. Bununla birlikte Gartner raporuna göre gelecekte yetkinlik ihtiyacı bitmeyecek 2 çalışma alanı bulunmaktadır; Siber Güvenlik ve Yapay Zeka.

Uç Nokta Güvenliği

BİLGEM SGE tarafından geliştirilen uç nokta güvenliği ürününe, Veri Kaçağı Önleme Sistemi (DLP) ve Son Kullanıcı Tespit ve Yanıt (EDR) yetenekleri kazandırılmış, böylece hem harici, hem de dâhili tehditlere karşı çözüm sunulmuştur.

Erdem Reşber – Uzman Araştırmacı, Mehmet Can Döşlü - Uzman Araştırmacı, Recep Esen - Uzman Araştırmacı, İsa Yurdagül - Araştırmacı, Neslihan Hanecioğlu - Araştırmacı / BİLGEM SGE

Uç nokta cihazları bir kurumsal ağa bağlanan, o ağ içinde etkileşimde bulunan bilgisayarlar, akıllı telefonlar ve yazıcılar dahil tüm cihazlardır. Kurumların sahip olduğu ve bu uç noktalarda işlenen veriler kurumun en önemli varlıkları arasındadır ve korunması gereklidir.

Uç nokta güvenliğinin en önemli bileşenleri arasında Veri Kaçağı Önleme Sistemi (DLP) ve Son Kullanıcı Tespit ve Yanıt (EDR) çözümleri yer almaktadır. DLP, bilgi sistem ağlarında bulunan gizlilik dereceli verinin korunması için kullanılan ve temel kullanıcı işlem kontrollerini barındıran çözümler içermektedir. İç tehditlere odaklı olan DLP uç nokta güvenliği için yeterli değildir. Gelişmiş teknik ve yöntemleri kullanan saldırılara karşı, yalnızca güvenlik için uyarılar oluşturmak yerine, kötü niyetli etkinlikleri tespit edebilecek ve engelleyecek yaklaşımlara da ihtiyaç duyulmaktadır. Bu noktada EDR çözümleri karşımıza çıkar. Bu çözümlerle uç noktalar sürekli izlenmekte, kayıt altına alınmakta, şüpheli etkinlikleri ve diğer sorunları araştırıp tespit etmeye odaklanılmaktadır.

BİLGEM SGE tarafından geliştirilen uç nokta güvenliği ürününe, ortak yönetim paneli ve uç noktada kurulan bir ajan yazılımı aracılığıyla DLP ve EDR yetenekleri kazandırılmış; böylece hem harici, hem de dâhili tehditlere karşı çözüm sunulmuştur. Çözümde, öncelikli olarak, kullanıcı hareketlerine göre veri elde edilir. Ardından, verinin içeriği incelenip analiz edilir ve her kurum için özel olarak belirlenen politikalarla karşılaştırılır. Analiz edilen veri politikaya göre hassas olarak sınıflandırılırsa işlem engellenir (Şekil 1).

Uç Nokta Güvenliğinde Kullanılan Veri Tipleri

Veri herhangi bir ölçüm, sayım, deney, gözlem vb. bir yöntem ile elde edilen bilgi parçacığına verilen isimdir. Veri, teknolojinin insan hayatına girmesi ile birlikte günden güne önemi artan bir kavramdır. Günümüzde verinin dijital olarak hızlı

bir şekilde işlenebilmesi ve silikon tabanlı donanımların hesaplama kabiliyetinin gelişmesi ile verilerin anlamlandırılması ve kullanılabilmesi kolaylaşmıştır. Sosyal medyanın yaygınlaşması, elektronik ticaret hizmetlerinin çoğalması ve birçok sektörün dijital dönüşümüyle birlikte veri alışverişi ve güvenliği oldukça önemli bir kavram haline gelmiştir. Dijital veriler işlenmeyi ve güvenlik sağlamayı kolaylaşmak için sınıflandırılmaktadır. Veriler, örneğin, Kullanılan Veri (Data in Use), Hareket Halinde Veri (Data in Motion) ve Durağan Veri (Data at Rest) olarak sınıflandırılabilir.

Kurum içindeki uç nokta cihazların, ihmal veya kötü niyet sonucu olası veri kaybı ve sızdırmalara karşı güvenliğinin sağlanması için alınan önlemler, uç nokta güvenliği kapsamındadır.

Durağan Veri bellekte veya transfer halinde olmayan veridir. Bilgisayarlarda depolama kapsamında kaydedilen birçok veri bu kategoridedir. Bir veri tabanında bulunan bir tablo, ağ sunucusunda yer alan bir doküman, fiziksel depolama aygıtlarında yer alan herhangi bir dosya bu kapsamda örnek olarak gösterilebilir. Bu durumda veri işleme yapılmaz. Veri durağan haldedir ve CPU tarafından kullanılmamaktadır.

Durağan verinin güvenliğinin sağlanabilmesi için verilerin şifrelenmesi, son kullanıcı koruma ürünlerinin (EDR, DLP) kullanılması, hiyerarşik şifre kullanımlı koruma, güvenli depolama ve verilerin dış ağda saklanması gibi çözümler uygulanmaktadır.

Hareket Halinde Veri (Data in Motion veya Data in Transit) aktif bir şekilde iletilmekte olan veri çeşididir. Bu veri bilgisayarın RAM'inde bulunur ve işlenmek için hazırdır. Ağ veya bulut sistemlerinde paylaşılan dosyalar da bu kategoridedir. Araya girme teknikleri ile verilerin açık bir şekilde izlenebilmesinin önüne geçmek ve olası bir veri kaybını önlemek için veri iletişiminin şifreli olması gerekmektedir.[2]

Kullanılan Veri (Data in Use) aktif bir şekilde işlenen veridir. Bu işleme sırasında bellekteki veri kullanılmakta ve herhangi bir güvenlik önlemi alınmamışsa açık bir şekilde görüntülenebilmektedir. Bu nedenle şifreleme gibi teknikler ile hassas içerikli bellek bölgelerinin korunması oldukça önemlidir. Ayrıca veriyi kullanan yazılım servisleri de kendi aralarındaki veri iletişimini yürütürken güvenli haberleşme esaslarına göre hareket etmelidir. Ek olarak, kimlik doğrulama ve yönetimi tekniklerinin de uygulanmasıyla verinin güvenliği büyük ölçüde sağlanabilmektedir.

Bu verilerin güvenliği için son kullanıcıya yönelik güvenlik ürünlerinin kullanılması da önemli çözüm yaklaşımlarındandır. Çeşitli kanunlar (KVKK, GDPR vb.) bu uygulamaları desteklemektedir. Siber Güvenlik Enstitüsü olarak geliştirilen DLP çözümü, verilerin güvenliğinin son kullanıcıda sağlanabilmesi ve bu alanda ulusal bir ürün geliştirilmesi hedefi ile ortaya çıkmıştır. Kamu ve özel kurumlardan gelen ek gereksinimler doğrultusunda geliştirilmesine devam edilen bir altyapıdır.

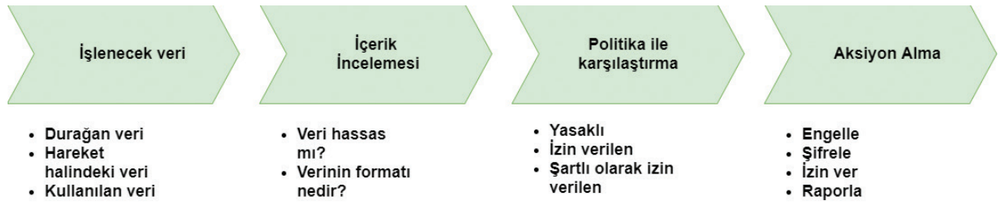
BİLGEM SGE Uç Nokta Güvenliği Sistemi

Kurum için hassas olarak belirtilen verilerin takibi için BİLGEM SGE olarak geliştirilmekte olan ürünümüzün özellikleri kısaca şöyle özetlenebilir: Genel olarak, kullanıcı işlem yaptığında bu işlem modüllerde, yani veri kontrol kanallarında incelenip gelen veri anlamlandırılır (kullanıcı davranışı analizi), tespit motoru bu veri için politika kontrolü yapar ve dönen cevaba göre kayıtlar yönetim merkezinde tutulur (Şekil 2). Ayrıca kullanıcı hareketlerine bakmadan, işletim sisteminde gerçekleşen olaylar da yakalanır ve raporlanır.

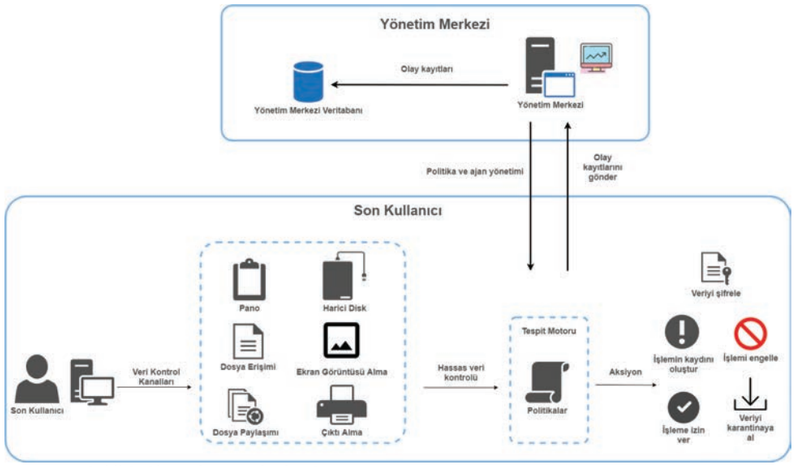
Kullanıcı Davranışı Analizi

Ajanın yüklü olduğu istemci bilgisayarda kullanıcı hareketleri takip edilip, bu hareketler kurum tarafından belirlenen politikalar üzerinden kontrol edilerek, herhangi bir politikayı ihlal eden bir durum varsa yapılan işlem ilgili modülde engellenmektedir.

Dosya Erişimi Kontrol Modülü: Uç noktalarda, kullanıcının herhangi bir dokümana erişmesi sırasında, işletim sistemi tarafında geliştirilen sürücü yazılımı ile bu işlem duraklatılır. Doküman incelenerek kurum politikalarına uymayan hassas bir



Şekil 1. Uç Nokta Güvenliği Akışı (1)



Şekil 2. Sistemin Detaylı Akış Şeması

içeriğe erişim sağlanıp sağlanmadığı kontrol edilir. Hassas veri tespiti durumunda uyarı verilerek kullanıcının dosyayı görüntülemesi engellenir ve bu durum işlem yönetim merkezine raporlanır.

Ekran Görüntüsü Kontrol Modülü: Uç nokta cihazlarında, kullanıcının klavyeden veya herhangi bir program aracılığıyla ekran görüntüsü almasını kontrol eden modüldür.

Pano Kontrol Modülü: Kurum için hassas veri içeren ve kopyalanmaması gereken içeriklerin kontrolü pano kontrol modülünde yapılır. Eğer kullanıcı hassas bir kelimeyi kopyalamayı denerse işlem engellenir.

Yazıcı Kontrol Modülü: Kurum için hassas veri içeren belgelerin yazıcıdan çıktılarının alınması engellenmektedir. Kullanıcı hassas bir veriyi dosyaya kaydedip çıktısını almayı denediğinde de çıktı alma işlemi engellenir.

Harici Disk Kontrol Modülü (HDKM): Hassas veri içeren dosyaların çıkarılabilir depolama cihazlarına kaydedilmesi engellenmektedir. Son kullanıcı bilgisayardan çıkarılabilir bir depolama cihazına çeşitli uygulamalar kullanarak dosya gönderebilir. Dosya hassas veri niteliğindeyse, henüz çıkarılabilir depolama cihazına yazılmadan işlem HDKM tarafından durdurulur. Gerekli politikanın tanımlanması durumunda harici diske dosyalar şifreli olarak gönderilebilir. Bu durumda da yalnızca ajanın yüklü olduğu bilgisayarlar şifreli dosyayı çözebilir. HDKM NTFS, FAT ve exFAT dosya sistemlerini destekler. İstemciye bir USB depolama cihazı takıldığında, HDKM çekirdek yazılımı sayesinde bunu tespit edip, USB üretici numarası, ürün numarası ve seri numarası bilgilerini bulur. Eğer bu bilgiler herhangi bir politikayı ihlal ediyorsa, harici cihazın işletim sistemine dahil olması yazılımsal olarak engellenir.

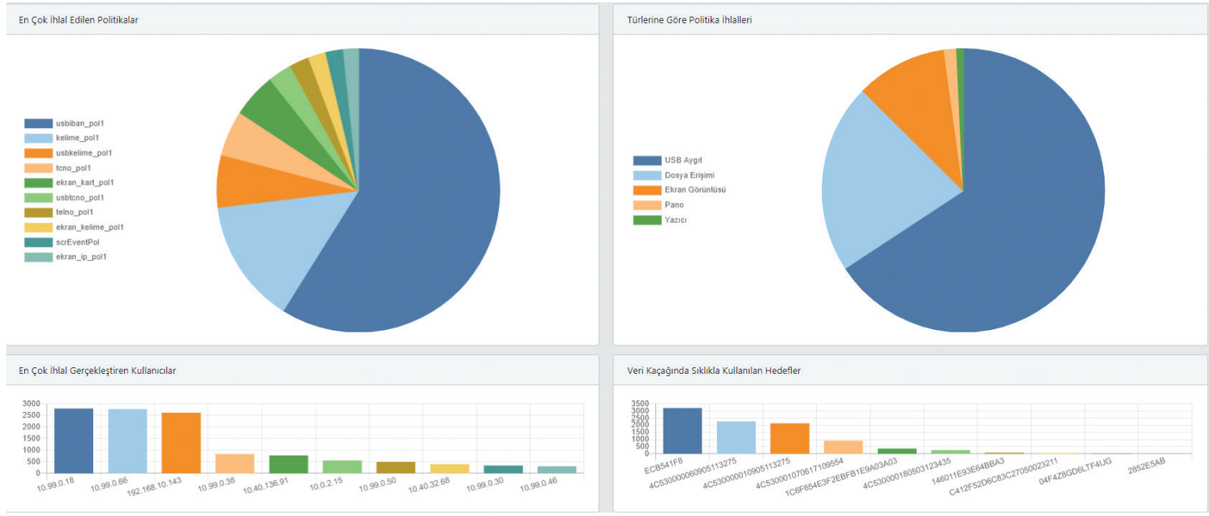
Ağ Dosya Paylaşımı Kontrol Modülü: Bu modül, kurum ağında bulunan riskli konak bilgisayarların kurum için hassas veri niteliği taşıyan dosyalara erişimini engeller. Sistem yöneticileri tarafından yönetim merkezinde, kurumun etki alanı ile ilgili konfigürasyon yapılır. Ajan, ağ üzerindeki dosya trafiğini izlemek için politikada yer alan etki alanı konfigürasyonundan faydalanır ve dosya paylaşımını tespit etmek için geliştirilen çekirdek yazılımını kullanır. Bazı riskli konak bilgisayarlar şunlardır:

- Kurum etki alanında olmayan istemciler (misafir konak bilgisayarlar) ve kullanıcılar.
- Kurum etki alanında bulunup kısıtlı kullanıcı grubuna üye olan istemciler veya kullanıcılar.
- Kurum etki alanında bulunup kısıtlı kullanıcı gruplarına üye olmayarak riskli kabul edilen istemciler veya kullanıcılar.

İşletim Sistemi Olay Takibi

Uç nokta cihazında, kullanıcı davranışlarının analiz edilmesine ek olarak, işletim sisteminde meydana gelen olaylar yakalanmakta ve raporları oluşturulmaktadır:

√ Yeni bir işlem başlatılması veya durdurulması,
√ Servis başlatılması, durdurulması veya kurulması,
√ Program kurulması, kaldırılması veya güncellenmesi,
√ Kullanıcı ile ilgili olaylar (kullanıcının aktif/pasif edilmesi veya kilitlenmesi/açılması, kullanıcı bilgilerinin değişmesi, hesap adının güncellenmesi, ekran koruyucu açılması/kapanması, kullanıcı değiştirme işlemleri vb.),
√ Kullanıcıların silinmesi, şifre değişikliği ve yeni kullanıcı eklenmesi,
√ Domain kullanıcısı eklenmesi ve silinmesi,
√ Dosya veya dizin oluşturulması, silinmesi, isim değişikliği yapılması, dosya içeriklerinin değiştirilmesi ve güvenlik ayarlarının yapılması,
√ Harici disk takılması/çıkarılması (telefon, hatta klavye gibi aygıtlar dâhil),
√ Harici disk içindeki dosyaların izlenmesi,
√ Kayıt değişikliği,
√ Dizinin veya sürücünün paylaşıma açılması/kapatılması,



Şekil 3. Yönetim Merkezi Ekran Görüntüsü

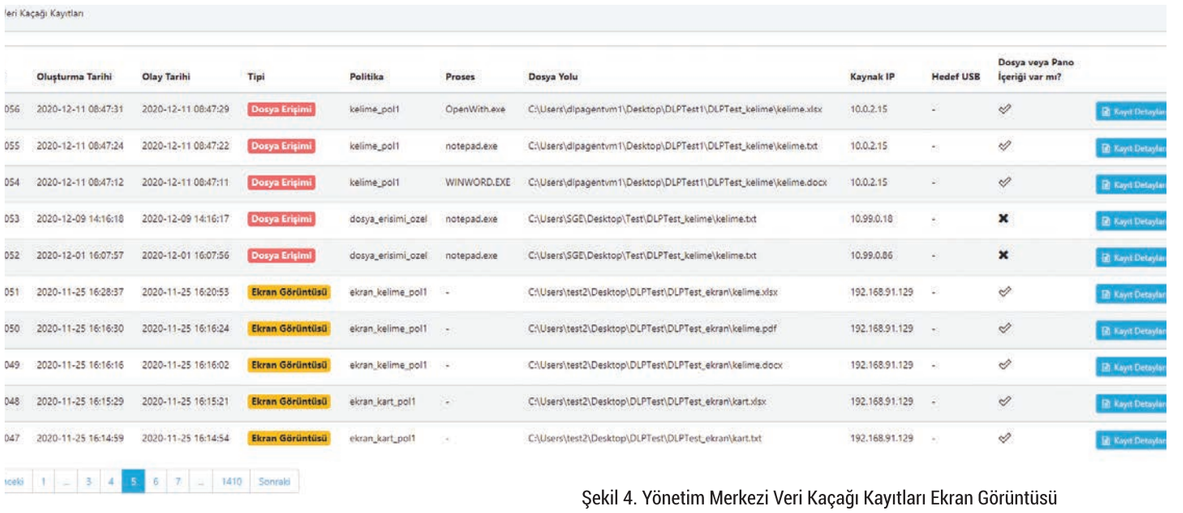
√ Şifreli sürücülerin açılması/kapanması ardından dosya/dizin olaylarını otomatik izleme işlemi,
√ Paylaşılan bir sürücü olduğunda dosya/dizin olaylarını otomatik izleme işlemi.

Kullanıcı Davranış Kayıtlarının Saklanması ve İncelenmesi

Olası bir veri kaçağı durumunda, geriye dönük incelemelerin yapılabilmesi için veri kaçaklarının sistemde kaydı tutulmaktadır. Bu kayıtlarda masaüstü istemcisinin kimliği, bilgisayarın IP adresi, hangi politikanın ihlal edildiği ve erişilmeye çalışılan dosya veya veri gibi bilgiler tutulur. Kayıtlardaki bu dosya veya veriler hassas içeriğe sahip olabileceğinden kimsenin direkt olarak açıp okuyamaması için istemcide şifrelenerek sisteme gönderilir ve sistemde şifreli olarak tutulur. Bu şifrelemenin anahtar altyapısı güvenliği artırmak için harici bir otorite tarafından sağlanır. Bu dosya veya verilerin incelenebilmesi için sistemdeki en yetkili kullanıcının izin vermesi gerekir. Yetkili kullanıcının izniyle şifreli tutulan bilgiler açılarak geriye dönük incelemeler yapılabilir.

Şekil 3 ve Şekil 4'de, BİLGEM SGE bünyesinde geliştirilen uç nokta güvenliği uygulamasına ait yönetim merkezi tarafının örnek ekran görüntüleri bulunmaktadır.

Kaynakça
[1]https://www.gartner.com/en/documents/3956073/building-an-effective-dlp-program
[2]https://www.endpointprotector.com/blog/how-to-protect-data-in-motion/



Şekil 4. Yönetim Merkezi Veri Kaçağı Kayıtları Ekran Görüntüsü

Veri Tabanı Sistemleri İçin Güvenlik Önerileri

Süleyman Muhammed Arıkan - Uzman Araştırmacı / BİLGEM SGE

"Veri tabanı sistemleri, barındırdıkları bilgiler sebebiyle her zaman saldırganların odağında olmuş ve günden güne artan tehdit vektörlerine ek olarak saldırı türlerinde de çeşitlilik yaşanmıştır."

Bir veri tabanı sisteminde, bilgi güvenliğinin üç temel ilkesi incelendiğinde, gizlilik ile mevcut verilerin yetkisiz kişilerin eline geçmemesi; bütünlük ile depolanan ve taşınan verilerin değiştirilmemesi ve erişilebilirlik ile sistemin ihtiyaç duyulduğunda kullanılabilir durumda olması ifade edilebilir. Veri tabanı güvenliği, bir veri tabanı sisteminin gizlilik, bütünlük ve erişilebilirlik ilkelerine zarar verebilecek, kazara veya kasıtlı her türlü olaya karşı alınan önlemler, gerçekleştirilen denetimler ve kullanılan araçlar olarak tanımlanabilir. Kullanılan araçların amacına uygun çalışması, denetimlerin verimli bir şekilde işletilmesi ve alınacak önlemlerin uygulanması için veri tabanı sisteminin ve ilişkili bileşenlerin doğru ve güvenli yapılandırılması gerekmektedir. Dolayısıyla, veri tabanı güvenliği yalnızca veri tabanı yönetim sisteminin değil, aynı zamanda işletim sisteminin ve bununla birlikte hizmet sunulan uygulamaların da yapılandırmasına doğrudan bağlıdır.

Veri tabanı güvenliğine yönelik saldırılar ve sebepleri incelendiğinde, şu gözlem ve tehdit türleri ortaya çıkmaktadır: iç tehditler, insan hataları, iletişimde araya giren saldırganlar, yazılım açıklıkları, hizmet dışı bırakma saldırıları ve yedeklere yönelik saldırılar. Kasıt olmadan ilgili sistemi saldırılara karşı açık hale getiren ihmalkâr yöneticiler veya kasıtlı olarak, zararlı bir amaç uğruna hareket eden kötü niyetli kullanıcılar iç tehdit kapsamında değerlendirilebilir. Kullanıcılar tarafından kazara gerçekleştirilen aktiviteler, zayıf parola kullanımı ve sosyal mühendislik gibi insan temelli saldırılara maruz kalınması da insan hatalarına birer örnek oluşturur. Veri tabanı sunucusu ile gerçekleştirilen bir trafiğin dinlenmesi, değiştirilmesi ve engellenmesi faaliyetleri iletişimde araya giren saldırgan aktivitelerindendir. Veri tabanı yönetim sistemi yazılımında mevcut olan güvenlik açıklıklarının istismar edilmesi ve hizmet sunulan uygulamalar üzerinden gerçekleştirilen SQL ve NoSQL enjeksiyonu gibi saldırılar da yazılım açıklıklarının bir tehdit türünü oluşturmaktadır.

Hizmet dışı bırakma saldırıları ilgili sunucunun, gerçek kullanıcılara hizmet veremeyecek büyüklükte bir trafiğe farklı kaynaklardan (ddos) veya tek noktadan (dos) maruz bırakılması saldırılarını kapsamaktadır. Ayrıca kasıtlı olarak, günlük kayıtlarının çok sayıda üretilmesini sağlayıp depolama alanını doldurarak sunucunun hizmet vermesini engellemek de bu tehdit türü ile ilişkilidir. Kullanımda olan veriler kadar güvenliği önemsenmeyen ve aynı derecede korunmayan yedeklenmiş veriler üzerinde; okuma, değiştirme, silme ve şifreleme gibi faaliyetler gerçekleştirebilecek her türlü işlem yedeklere yönelik saldırılar kapsamında ele alınabilir. Bahsi geçen tüm gözlemlere ve tehdit türlerine karşı önlem alarak veri tabanı güvenliğini sağlamak adına çeşitli kategoriler altında ele alınmış güvenlik önerileri uygulanabilir.

Kurulum Güncelleme ve Yamalar

Kurulum dosyalarının yetkili kaynaklardan temin edildiğinden emin olunmalıdır. Özellikle açık kaynaklı veri tabanı yönetim sistemleri internet üzerinde pek çok kaynak tarafından sunulabilmekte ve büyük çoğunluğunun içeriği ve işlevi değiştirilmiş olabilmektedir. Bu sebeple, ihtiyaç duyulan dosyalar yetkili kaynaklardan alınıp kurum bünyesinde oluşturulacak yerel depolar üzerinden kullanıma sunulabilir. Veri tabanı yönetim sistemi servisleri için atanacak kullanıcılar, ihtiyaç duyulan işlevlere uygun yetkilendirilmelidir. Dolayısıyla, servisler doğrudan yönetici haklara sahip kullanıcılar ile çalıştırılmamalıdır. Böylece en az yetki prensibi sağlanacak ve başarılı bir saldırı ardından gerçekleştirilebilecek işlemler kısıtlanabilecektir.

Güncelleme ve yamalar mümkün olan en kısa zamanda gerçekleştirilmelidir. Güncelleme işlemi ile veri tabanı yönetim sistemi bünyesinde oluşabilecek herhangi bir güvenlik açığı ile karşılaşma ihtimali düşürülürken yamalar ile mevcut açıklıkların kapatılması sağlanabilir. Kurulum işlemi ile gelen örnek veriler ve varsayılan kullanıcılar ise, ivedilikle sistemden kaldırılmalıdır. Böylece saldırganların veri tabanının barındırdığı veriler ve kullanıcılar hakkında ön bilgi sahibi olması engellenir.

"Veri tabanı güvenliğine yönelik saldırılar, iç tehditler, insan hataları, iletişimde araya giren saldırganlar, yazılım açıklıkları, hizmet dışı bırakma ve yedeklere yönelik saldırılardır."

Kimlik Doğrulama ve Yetkilendirme

Kurulumun ardından varsayılan kullanıcı adı ve parola barındıran tüm kullanıcılar (örneğin, system admin, root, cassandra, oracle vb.) tespit edilerek silinmeli veya kullanıcı adı ile parolası değiştirilmelidir. Parola belirlenmesi sürecinde, bir parola politikası ile kullanıcılar güçlü parolalar kullanmaya zorlanabilir. Bu politikalar ile bir parolanın geçerlilik süresi, uzunluğu ve barındırılması zorunlu karakterler gibi çeşitli parametreler belirlenebilir. Buna ek olarak, belirlenen politikalar ile boş parolaya sahip kullanıcının bulunmadığından da emin olunur.

Kimlik doğrulama aşamasında gerçekleşen belirli sayıdaki yanlış girişlerin ardından kullanıcı ön tanımlı bir süre için veya süresiz olarak kilitlenebilir. Başta yönetici hesapları olmak üzere, kullanıcılar için oturum açabilecekleri IP adresleri belirlenmeli ve yalnızca bu kaynaklardan bağlantı sağlamalarına izin verilmelidir. Böylece kurum dışından veya kurum içindeki farklı kaynaklardan kullanıcılara yönelik parola tespiti saldırılarının önüne geçilebilir. Ayrıca, kullanıcıların aynı anda açabileceği oturum sayısı kısıtlanarak sistem kaynaklarının kasıtlı veya kasıtsız tüketilmesinin önüne geçilebilir. Aksi halde çok sayıda oturum açılıp yüksek hesaplama gücüne ihtiyaç duyan işlemler üzerinden sistem kaynakları tüketilip servis dışı bırakma saldırısı gerçekleştirilebilir.

Verilen yetkiler periyodik olarak kontrol edilerek yetkisi değiştirilmiş kullanıcılar tespit edilebilir. Yetkilendirme sürecinde ise kurulum ile gelen varsayılan roller kullanılmamalıdır. Bu roller güncelleme veya yamalar ile değişikliğe uğrayabilir. Bu kapsamda amaca özgü oluşturulmuş rollere en az yetki prensibi gereği ayrıcalıklar tanımlanmalıdır. Her kullanıcı ihtiyaç duyduğu işleve göre de bu rollere atanmalıdır. Mevcut tüm kullanıcılara ayrıcalık tanımlayabilecek herkesin atandığı ortak rollerin (örneğin: "Public" roller) yetkileri mümkün olduğu kapsamda tamamen kaldırılmalıdır.

Denetleme ve Günlük Kayıtları

Veri tabanı sistemi üzerinde gerçekleşen aktivitelerin takibi için günlük kayıtları büyük öneme sahiptir. Bu kayıtların oluşturulması için denetleme mekanizması aktif hale getirilmelidir. Unutulmamalıdır ki, birçok ücretsiz olarak sunulan açık kaynaklı veri tabanı yönetim sistemi; denetim mekanizması gibi birçok özelliği de ücretli sürümlerinde sunmaktadır. Dolayısıyla açık kaynaklı alternatifler değerlendirilirken bu husus göz önünde bulundurulmalıdır.

Denetleme mekanizması sayesinde, kullanıcı tarafından çalıştırılan komutlar kayıt altına alınabilir ve kimin hangi komutu ne zaman çalıştırdığı bilgisine doğrudan ulaşılabilir. Özellikle kritik öneme sahip komutlar (DROP TABLE, ALTER USER vb.) için denetim mekanizmasının aktif olması önerilmektedir. Oluşturulmuş denetim kayıtlarının ve veri tabanı sistemi tarafından üretilen günlük kayıtlarının disk üzerinde sistem bölümünden farklı bir bölümde tutulması sağlanarak, depolama alanının dolması engellenebilir ve günlük kayıtları üzerinden gerçekleştirilebilecek servis dışı bırakma saldırılarından kaçınılabilir.

Veri Şifreleme

Kullanıcılar ile veri tabanı sistemi arasında gerçekleşen iletişimin dinlense dahi anlaşılamaması, değiştirildiğinde ise tespit edilebilmesi amacıyla şifreli iletişim tercih edilmelidir. Benzer olarak, yapılandırılmış küme (cluster) bünyesindeki sunucular arasında da şifreli iletişim kullanılarak bilginin ifşasının ve bozulmasının önüne geçilebilir. Sunucunun fiziksel olarak çalınması, veri tabanı dosyalarının ele geçirilmesi gibi faaliyetler neticesinde saldırganların bilgiye ulaşmasını engellemek adına durağan verinin güvenliği için önlem alınmalıdır. Bu kapsamda, verinin önceden şifrelenerek kaydedilmesi, veri tabanı yönetim sisteminin veri tabanı dosyalarını şifreli tutması için yapılandırılması ve disk seviyesinde şifreleme kullanılması sağlanabilir.

Yüzey Alanı Küçültme

Kurulumlar için veri tabanı yönetimi işlevinden başka herhangi bir amacı olmayacak şekilde yapılandırılmış olan adanmış sunucular (dedicated server) kullanılmalıdır. Bu sayede, farklı sistemler üzerinden sunucunun ifşa olması ve veri tabanı sisteminin zarar görmesi engellenebilir.

Veri tabanı yönetim sistemi, ihtiyaçlara göre yapılandırılmalı ve gereksiz özellikleri devre dışı bırakılmalıdır. Bu kapsamda, veri kaçırma faaliyetlerini önlemek için kullanılmayan e-posta servisleri ve olası gerçekleştirilebilir uzak bağlantılar (SSH, RDP vb.) kapatılmalıdır. Buradan hareketle kullanılmayan bağlantı protokolleri de (TCP/IP, VIA, paylaşılan bellek vb.) devre dışı bırakılmalıdır. Kullanılan bağlantı protokolleri kapsamında ise varsayılan ayarlar (örneğin: varsayılan port bilgisi) değiştirilmelidir. Saldırganların farklı bileşenler üzerinden veri tabanını hedef almasını engellemek adına mümkün olduğunca; üçüncü parti prosedür, kütüphane veya uygulama kullanımından kaçınılmalı, işletim sistemi üzerinde komut yürütme devre dışı bırakılmalı ve diğer veri tabanı sistemleri üzerinde dağıtık sorguları çalıştırma işlevi kapatılmalıdır.

İşletim Sistemi Sıkılaştırma

İşletim sistemi üzerinde tutulan ortam değişkenleri bünyesinde veri tabanı sistemi için kullanıcı adı ve parola bilgisi bulundurulmamalıdır. Başta şifreleme işlemlerinde kullanılan anahtar dosyaları ile kayıtları barındıran veri tabanı dosyaları olmak üzere, veri tabanı yönetim sistemine ait dosya ve dizinler için ilgili izinler periyodik olarak kontrol edilmelidir. Mümkün olduğunca diğer kullanıcıların okuma, yazma ve yürütme hakları kaldırılmalıdır.

Veri tabanı yönetim sisteminde çalıştırılan komutların geçmişini tutan dosyalar (örneğin: ".mysql_history" dosyası) işletim sistemi üzerinden belirli zamanlarda silinmeli veya oluşturulması engellenmelidir. İşletim sistemi kaynakları, veri tabanı sistemi için sınırlandırılarak hizmet dışı bırakma gibi saldırılar neticesinde işletim sisteminin beklendiği gibi çalışmaya devam etmesi sağlanabilir. Veri tabanı sistemi özelinde alınacak bu önlemlere ek olarak ilgili işletim sistemi için ulusal ve uluslararası otoriteler tarafından standart olarak sunulan sıkılaştırma tedbirleri de uygulanmalıdır.

Uygulama Geliştirme

Veri tabanı sisteminin hizmet sunduğu uygulama, amaçlanan işlevlerinin haricindeki faaliyetleri engellemek adına girdi ve çıktı denetimi yapmalıdır. Girdi denetimi ile sorgu sırasında gerçekleşecek SQL ve NoSQL enjeksiyonu gibi saldırılar engellenebilirken, çıktı denetimi ile veri tabanından alınmış veriler üzerinden gerçekleştirilecek XSS (cross site scripting) gibi saldırıların da önüne geçilebilmektedir. Veri tabanı sistemine ait erişim adresi, kullanıcı adı ve parola bilgileri doğrudan kaynak kod üzerinde tanımlanmamalıdır. Bu bilgilerin çalışma zamanında elle veya bir konfigürasyon yönetim aracı üzerinden elde edilmesi sağlanmalıdır.

Yedekleme ve Felaket Kurtarma

Replikasyon ve yedekleme sürecinde, ilgili işlevlere uygun haklar barındıran kullanıcılar oluşturulmalıdır. Yönetici haklara sahip kullanıcılar, bu işlevleri yerine getirme amacıyla kullanılmamalıdır. Yedekler, veri tabanı sisteminden farklı bir lokasyonda (fiziksel veya sanal) şifreli olarak depolanmalı ve bu dosyalar üzerindeki izinler periyodik olarak kontrol edilmelidir. Yedeklerin düzgün alındığından ve olası bir sebeple bozulmadığından emin olmak için belirli zamanlarda yedekten dönme testleri gerçekleştirilmelidir.

Sonuç

Veri tabanı sistemleri barındırdıkları bilgiler sebebiyle her zaman saldırganların odağında olmuş ve günden güne artan tehdit vektörlerine ek olarak saldırı türlerinde de çeşitlilik yaşanmıştır. Bu sebeple, veri tabanı güvenliğini sağlamak adına basit sayılabilecek çeşitli önlemlerin hayata geçirilmesi ile saldırganların amaçlarına ulaşması ve iş sürekliliğinin kesintiye uğraması engellenebilir. Çalışmaya konu olan güvenlik önerileri ile gözlem ve tehdit türleri ışığında;

- İç tehditleri engellemek için: "kimlik doğrulama ve yetkilendirme, denetleme ve günlük kayıtları ile yüzey alanı küçültme";
- İnsan hatalarından korunmak için: "kimlik doğrulama ve yetkilendirme";
- İletişimde araya giren saldırganları engellemek için: "veri şifreleme";
- Yazılım açıklıklarını ortadan kaldırmak için: "kurulum, güncelleme ve yamalar ile uygulama geliştirme";
- Hizmet dışı bırakma saldırılarına karşı: "işletim sistemi sıkılaştırma, denetleme ve günlük kayıtları ile kimlik doğrulama ve yetkilendirme";
- Yedeklere yönelik saldırılardan korunmak için: "yedekleme ve felaket kurtarma" önlemleri, etkili ve uygun seçenekler olarak görülmektedir.

Kaynakça

- https://cbddo.gov.tr/bgrehber
- https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html
- https://www.cisecurity.org/cis-benchmarks/
- https://www.ibm.com/cloud/learn/database-security

Oltalama Saldırılarının Tespitinde Makine Öğrenimi

Ferdi Gül – Araştırmacı / BİLGEM SGE

> Saldırganların siber saldırılardaki motivasyonları, kendi kişisel tatminlerinin yanında maddi kazançlar elde etmek ya da hedef kurum/kişilere maddi kayıplar yaşatmaktır.

Günümüzde dijital dünyanın gelişmesi ile birlikte kurum veya kişi özelinde yapılan birçok iş internet ortamına bağlanmıştır. Yaşamı kolaylaştıran sosyal ağlar, e-posta kullanımı, elektronik bankacılık, e-ticaret gibi alanlar dijital dünyada gelişmeye ve yaygınlaşmaya devam ederken, eş zamanlı olarak bu sistemlere yapılan saldırılar da her geçen gün artmaktadır. Eskiden savaş alanları; kara, deniz, hava ve uzay olarak sınırlandırılırken artık bu alanlara siber uzay olarak yeni bir savaş alanı eklenmiştir. Ülkeler yıl sonu gerçekleştirdikleri ekonomi, askeri planlamalarında artık bu alana yatırımlarını da göz önünde bulundurmaktadırlar.

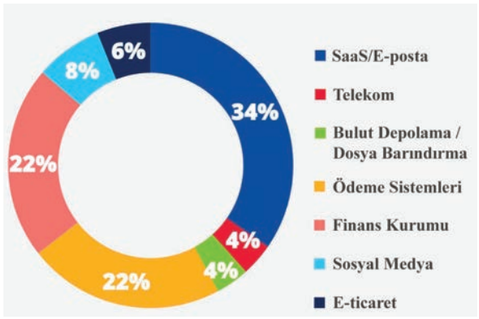
Oltalama (Kimlik avı), güvenilir kaynaklardan geliyormuş gibi görünen, çeşitli saldırı vektörlerinin kullanılarak (e-posta vb.) kurbanın kişisel bilgilerini elde etmek veya saldırı yüzeyini genişletmeyi amaçlayan siber ataklardan biridir. Sosyal mühendisliği ve teknik hileyi birleştirir. Kötü amaçlı yazılım indirmeniz veya kişisel bilgilerinizi vermeniz için sizi kandırabilecek meşru olmayan bir web sitesine referans olacak bir bağlantı da içerebilir.

Hedefli kimlik avının tespit edilmesi, diğer oltalama saldırılarına göre daha zor olabilir. Bir bilgisayar korsanının hedefli kimlik avı saldırısı gerçekleştirmesinin en basit yollarından biri, sizin veya kurumunuzun iş yaptığını düşündüğü firmaları taklit etmesidir. Dolandırıcıların saldırı senaryolarına güvenilirlik katmak için kullandıkları başka bir teknik de web sitesi klonlamadır.

Saldırganların siber saldırılardaki motivasyonları, kendi kişisel tatminlerinin yanında maddi kazançlar elde etmek ya da hedef kurum/kişilere maddi kayıplar yaşatmaktır. Bu konuda gerçekleştirilen siber saldırılara bakıldığında oltalama saldırıları önemli bir yüzdeliği kapsamaktadır. Oltalama saldırılarının, günümüzde son kullanıcılara en çok e-posta ile iletildiği bilinmektedir.

PhishLabs tarafından sağlanan ülkemize yönelik 2018 yılı oltalama saldırıları verileri baz alındığında, oltalama saldırıları 2014 yılına göre %621 artmış iken 2017 yılına göre ise %149 artmıştır. 2020 yılında ise tüm dünyayı etkisi altına alan Covid-19 salgınının etkisiyle tüm dünyada bu yüzdeliğin daha da arttığı gözlenmiştir.

2020 yılı oltalama saldırılarının hedef aldığı sektörler incelendiğinde SaaS (İnternet üzerinden bulut tabanlı erişimi olan uygulamaları temsil eder)/Web mail %34 ile en başta yer almaktadır. Onu ise beklendiği gibi finans sektörü takip etmektedir [1].



Şekil 1 Oltalama Saldırılarının Sektörel Dağılımı

Kimlik avı riskini azaltmak için şu teknikler kullanılabilir.

Eleştirel düşünme: Çok sayıda gelmiş e-posta üzerinde aksiyon almadan önce analiz etmeyi unutmayınız.

Bağlantıların üzerine gelme: Farenizi tıklamadan bağlantının üzerine getirerek sizi gerçekte nereye yönlendireceğini görebilirsiniz. URL daha önce tehdit analiz beslemelerine düştüyse "virustotal.com" başta olmak üzere "any.run", "hybred-analysis" gibi faydalı kaynaklardan yararlanabilirsiniz.

E-posta header analiz etme: E-posta headerları, bir e-postanın adresinize nasıl ulaştığını tanımlar. "Yanıtla" ve "Dönüş Yolu" parametreleri, gelen e-postada belirtilenle aynı etki alanına yönlendirilmesi beklenmektedir.

Korumalı Alan: E-posta içeriğini korumalı alan ortamında test edebilirsiniz. Bu her zaman mümkün olmayabilir.

Oltalama Saldırıları Kill Chain Gösterimi

Cyber Kill Chain çerçevesi, bir saldırının yapısıyla ilgili askeri bir konseptten uyarlanmış ve Lockheed Martin tarafından geliştirilmiştir. Belirli bir saldırı vektörünü incelemek için, sürecin her adımını haritalamak ve saldırgan tarafından kullanılan araçlara, tekniklere ve prosedürlere referans vermek için Şekil 2'deki "kill chain" diyagramı kullanılmaktadır.

Şekil 2 Oltalama Saldırısı ve Kill Chain Gösterimi

Saldırgan, hedef sistem veya kullanıcı hakkında ilk önce aktif ve pasif olarak gerçekleştirdiği araştırmaları sonucunda bazı anlamlı ve anlamsız verilere ulaşır. Bu veriler ışığında bilgileri gruplandırır. Bunun sonucunda çeşitli saldırı araçlarını kullanarak hedef kullanıcıya karşı başta sosyal mühendislik olmak üzere örnek bir web sitesini oluşturur. Oluşturulan bu site, saldırı yüzeyinin hedefine göre çeşitli saldırı senaryolarını içinde barındırabilir. Son kullanıcı bilerek veya bilmeyerek tıkladığı e-posta içerisindeki link aracılığı ile gerçeğinden ayırt edilmesi zor sahte siteye yönlendirilir. Son kullanıcı, kendi kimlik verilerini ya da sistemden sorumlu bir kişi ise sistemin bilgilerini saldırganla paylaşabilir. Eğer saldırgan, sistem veya kullanıcı verilerini ele geçirmenin ötesinde sisteme zarar vermeye yönelik bir senaryo geliştirdiyse ziyaret edilen linkten aynı zamanda C&C denilen komuta kontrol sunucusundan zararlı dosyalar (dropper) indirilmesini sağlayabilir ve sistemi ele geçirebilir. Ele geçirilen makineden yanal hareket ile bu sisteme bağlı diğer kullanıcı veya sistemler aracılığı ile diğer sistemlere yayılım gerçekleştirebilir.

Oltalama Saldırıları Tespit Yöntemleri

Kara Liste ve Beyaz Liste Tabanlı Tespit Yöntemi

Bilinen zararlı URL veya IP adreslerinin oluşturduğu veri kümelerine dayanmaktadır. Daha önce çeşitli güvenlik mekanizmaları tarafından tespit edilen zararlı URL veya IP adreslerinin bir güvenlik sisteminde (güvenlik duvarı vb.) veri tabanına eklenerek her güvenlik sistemi üzerinde kendi kara listeleri oluşturulabilmektedir. Kara Liste tabanlı

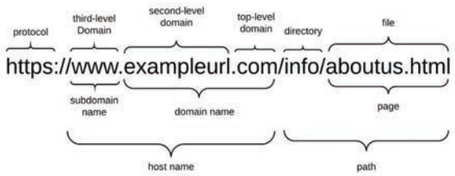
tespit yöntemi verimli gibi görünse de banka gibi sürekli oltalama saldırılarına maruz kalan sistemlerde sürekli güvenlik duvarı bloklaması yapılması veri tabanın şişmesine neden olabilmektedir.

Bu yöntemin verimliliğini ve güvenliğini arttırmak için genelde kurumsal firmalarda eğer kurumun iş yaptığı firmalarla bir bağlantısı yoksa dns tabanlı bloklamalar yapılmaktadır. Bu tarz sistemlerin eksiği ise, daha önce gerçekleşen saldırıları ya da tespit edilmemiş olan saldırıları algılama yeteneğine sahip olmamalarıdır. Kara Liste tabanlı oltalama saldırıların tespit edilme başarıları %20 civarındadır [2]. PhishNet, Automated Individual White-List, DNS-Based Blaklist (dnspedia vb.), Google Safe Browsing API gibi uygulamalar bu konuda yardımcı olmaktadır.

Beyaz liste tabanlı tespit yöntemi ise kara liste tabanlı tespit yönteminin aksine şüpheli veya zararlı olmadığı bilinen adreslerin oluşturduğu listeye dayanmaktadır. Beyaz liste oluşturmak, kara listeye göre daha kolaydır.

Makine Öğrenimi Tabanlı Tespit Yöntemi

Makine Öğrenimi ve Derin Öğrenme Tabanlı sistemlerin bu noktadaki amacı verimliliği ve güvenliği artırmanın yanında, yanlış pozitif oranını minimum seviyeye düşürmektir. Makine Öğrenimi sırasında gerçekleştirilen testlerde Random Forest, Decision Tree, kernel tabanlı Sıralı Minimum Optimizasyon (SMO), istatiksel tabanlı bir algoritma olan Naive Bayes(NB), Support Vector Machine (SVM) ve diğer algoritmalar kullanılabilir. Random Forest algoritmasının, SVM ve Decision Tree'ye göre biraz daha doğruluk oranına sahip olduğu yapılan çalışmalarda gözlemlenmiştir. Daha fazla doğruluk oranı yakalayabilmek için birden fazla algoritmanın bir arada kullanıldığı hibrit yaklaşımlar tercih edilebilir.



Şekil 3 URL Adresi Bölümleri

Bu yöntemlerde tespiti zorlaştıran etmenler aşağıda sıralanmıştır.

Typosquatting: Kurumun gerçek adresine benzer domain adreslerin saldırgan tarafından satın alınması durumu. Örneğin "linked1n.com", "goggle.com".

Cybersquatting: Kurumun var olan alan adının aksine farklı uzantıların saldırgan tarafından satın alınması durumudur. "ozelkurum.com" bir kuruma aitken, "ozelkurum.net", "ozelkurum.org" gibi farklı uzantılara sahip alan adlarını içermektedir.

Birleşik Kelime Kullanımı: Kelimelerin bitişik yazımına dayanmaktadır. Saldırganların çok sık tercih ettiği yöntemlerden biridir. Örneğin, "xbanksecurelogin.com". Doğal Dil İşleme (DDİ) yöntemleri belirli ayraçlar ile kelimelerin ayrılmasına dayanır. Kelimelerin bitişik yazılması analizi zorlaştırmaktadır. Bu zorluk bilgisayarların bunu analiz etme zorluğuna dayanmaktadır. İnsanlar tarafından bitişik kelimelerin tespit edilmesi ise kolaydır.

Rastgele Karakterlerden Oluşan Kelimeler: Alan adlarının rastgele oluşturulmasına dayanmaktadır. Örneğin, "qwrtyght.com". Kullanıcı tarafından tespit edilmesi kolay gibi görünse de saldırgan rastgele karakterlerden oluşturduğu bu alan adına uzun alt alan adları ve çok uzun dosya yolu ekleyerek URL adresinin tarayıcıda görünmesini zorlaştırabilir.

Oluşturulan veri kümelerinden zararlı ve normal olmak üzere iki çıktı alınırken test aşamasında, doğru negatif, yanlış pozitif, yanlış negatif, doğru pozitif dediğimiz ikili sınıflandırma problemleri ile karşılaşılabilmektedir.

Makine Öğrenimi gerçekleştirilirken kullanılan veri setinin zararlı URL/IP ve güvenilir URL/IP adreslerini içerebilir. Zararlı URL adreslerinin oluşturduğu kümeler için "phishtank.org" gibi ücretsiz sitelerden yararlanılabilir. Temiz URL adresleri için ise "Google Trend API, Yandex Search API" gibi arama motorlarından yararlanılabilir. Arama motorları güçlü skorlama algoritmaları kullandığı için arama motorlarında karşımıza çıkan ilk sonuç en güvenilirdir diye basite indirgeyebilir ve bunu başka indikatörlerle çoğaltabiliriz. Zararlı URL ve Temiz URL veri kümelerini daha da güçlendirmek için örneğin

marka isim listesi oluşturup bundan yararlanabiliriz. Bunun için dünyada en çok kullanılan bankalar, Telekom şirketleri, sosyal medya şirketleri, Alexa üzerinde üst sıralarda sıralanmış markalar gibi amaca uygun veri kümelerini oluşturabiliriz.

Veri Ön İşleme aşaması, öznitelik çıkarımını başarılı bir şekilde sağlayabilmek için kullanmak mantıklı olabilir. URL adresinin içerisinden özel karakterlere göre parçalanabilir ardından sisteminize uygun belirlediğiniz anahtar kelimeleri veya marka isimlerini içerip içermediği tespit edilir. Bilinen bir kelime içeriyorsa bu kelimelerin sayısı, firma sayıları çıkarılır. Bilinmeyen bir kelime içeriyorsa rastgele kelime içerip içermediği tespit edilir. Uzunluğuna göre kelime listesine eklenir. Belli uzunluğu geçiyorsa rastgele kelime kümesinden kelimeler ayrıştırılır ("fastpaylogin" verisinden "fast","pay","login" kelimelerinin çıkartılması gibi). Oluşturulan tüm bu listelerden zararlı olup olmadığı analizi gerçekleştirilir ve öznitelik çıkarımı yapılır.

Öznitelik çıkarımı aşamasında ise kelime tabanlı özniteliklerden yararlanılabilir. DDİ teknikleri bu konuda yardımcı olmaktadır. Özel karakterlere ayrıştırılan URL içerisinde sözlükte geçen kelime sayısı, en uzun ve en kısa kelime uzunluğu, marka isim kontrolü, bulundurduğu rakam sayısı, URL uzunluğu, alan adında geçen "www" ve "com" gibi kelimelerin kullanılıp kullanılmadığı, özel karakterler içermesi durumu (@ , ? & , = vb.), alt alan adı sayısı, punnycode içermesi ("tubitak.gov.tr" yerine "xn--tbitak-3ya.gov.tr" kullanılması durumu), domainin yaşı, URL adresin IP adres içerip içermediği gibi 40'tan fazla öznitelik çıkarımı yapılabilmesi mümkündür.

Oltalama saldırılarının tespit edilmesinde Makine Öğreniminin yanı sıra Derin Öğrenme yöntemlerinin de başarılı olduğu gözlemlenmiştir ancak Derin Öğrenme yönteminin tercih edilmesi, bazı nedenleri içinde barındırmaktadır. İki farklı yöntem üzerindeki yapılan tartışmalara bakıldığında şu an için henüz bir fikir birliği oluştuğunu söylemek güçtür.

Makine Öğrenimi ve Derin Öğrenme yöntemlerinde kullanılan en temel fark performanstır. Veri kümelerinin ayrıştırılması, ayrıştırılan verilerden öğrenilmesi ve öğrenilen veriler üzerinden kararların verilmesi için iki yöntem de kullanılabilmektedir. Derin Öğrenme algoritmalarına bakıldığında temel olarak kendi başına kararlar verebilen bir Yapay Sinir Ağı (YSA) oluşturmak için kullanılır. Makine Öğrenimi, Derin Öğrenme'yi kapsamaktadır. Derin Öğrenme'de, oltalama saldırılarının tespit edilmesinde Multi Dimensional Feature Selection (MDFS) kullanılabilir. Derin Öğrenme uyguladığımız sistemlerde Makine Öğrenimi yapıldığı söylenebilir ancak her Makine Öğrenimi uygulandığında sisteme bir Derin Öğrenme yöntemi uygulandığı söylenemez. Öznitelikler Makine Öğrenimi'nde manuel olarak verilir. Derin Öğrenme'de ise bu öznitelikleri sistem, verilerden doğrudan öğrenebilmektedir.

Derin Öğrenme kullanılmasındaki en temel amaç, eskiden verilerin büyüklüğünü tanımlamak için kullanılan sayısal tanımlamaların değişmesidir. Son 10 yılın üzerinde büyümekte olan veriler Makine Öğrenimi ile sonuç vermemeye başlamıştır. Bugün 1 milyon seviyesindeki veriler "big amount of data" olarak tanımlanmaktadır. İleride genişleyen veri kümeleri ışığında bu kavramın da değişeceğini söylemek zor değildir. Veri sayısı düşme eğilimi gösterdikçe, Derin Öğrenme algoritmaları performans noktasında kayıp yaşamaktadır. Derin Öğrenme algoritmalarının iyi çalışması için büyük miktarda veriye ihtiyaç vardır. Daha az veriyle işlem yapılıyorsa Makine Öğrenimi'nin daha iyi sonuçlar vermesi beklenmektedir.

Oltalama Saldırılarında Riski Minimize Etmek için Alınabilecek Önlemler

- Personeli sahte ve kötü niyetli e-postaları belirleme ve tetikte olma konusunda eğitilebilirsiniz. Kuruluşun altyapısını ve personelin yanıt verme yeteneğini test etmek için taklit edilmiş kimlik avı kampanyaları başlatılabilirsiniz.
- Filtrelerin düzenli bakımıyla bir güvenli e-posta ağ geçidi kullanabilirsiniz.
- Kimlik avı sitelerini gerçek zamanlı olarak belirlemek için makine öğrenimi tekniklerini kullanan güvenlik çözümleri uygulamayı düşünebilirsiniz.
- Posta istemcilerinde kodun, makroların, grafiklerin otomatik olarak çalıştırılmasını ve postalanan bağlantıların önceden yüklenmesini devre dışı bırakın ve bunları sık sık güncelleyin.
- İstenmeyen e-postaları azaltmak için şu standartlardan birini uygulayabilirsiniz: SPF, DMARC ve DKIM.
- Kritik finansal işlemler veya hassas bilgileri paylaşırken dijital imzalar veya şifreleme aracılığıyla güvenli e-posta iletişimi tercih edilebilir.
- Rastgele bağlantılara, özellikle sosyal medyada bulunan kısa bağlantıları tıklamaktan kaçınılmalıdır.
- Bir e-postanın kaynağı konusunda kesinlikle emin değilseniz, bağlantıları tıklamayınız veya ekleri indirmeyiniz.
- Kişisel bilgileri sosyal medyada aşırı paylaşmayınız.
- Özellikle banka gibi hassas siteler için, ziyaret ettiğiniz sayfanın alan adlarını kontrol ediniz. HTTPS bağlantı olması her zaman güvenli olduğu anlamına gelmez.
- Hesap devralmalarında iki faktörlü kimlik doğrulamayı etkinleştiriniz.
- Her çevrimiçi hizmet için güçlü ve benzersiz bir parola kullanınız.
- Şifrelenmemiş ve imzalanmamış e-postalara, özellikle banka verileri gibi hassas paylaşım durumlarında güvenmeyiniz.

Kaynakça
[1]https://www.enisa.europa.eu/publications/phishing/at_download/fullReport
[2] Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. IEEE Communications Surveys & Tutorials, 15(4), 2091-2121.
[3] https://cipher.com/blog/phishing-protection-spf-dkim-dmarc/
[4] https://www.phishing.org/10-ways-to-avoid-phishing-scams

Android Cihazlardaki Ön Yüklü Uygulamalar

Abdullah Özbay – Araştırmacı / BİLGEM SGE

Kutusundan çıkarılan bir Android işletim sistemine sahip akıllı telefonda, ortalama 100-500 arası ön yüklü uygulama bulunmaktadır.

Android işletim sistemi, açık kaynak kodlu olması sebebiyle, ilgili üreticilerin cihazlara özelleştirilmiş işletim sistemi versiyonları koymasına olanak sağlar. Bu versiyonların bazılarında, kullanıcıların gizliliğini ve güvenliğini tehdit eden çeşitli ön yüklü uygulamalar tespit edilmiştir. Bu uygulamalar; cihazlarda ön yüklü olarak bulunduğu için birçok kullanıcı, cihazlarında bulunan bu tehlike hakkında bilgi sahibi değildir. Kutusundan çıkarılan bir Android işletim sistemine sahip akıllı telefonda ortalama 100-500 arası ön yüklü uygulama bulunmaktadır.

Bu kapsamda yapılan araştırmanın içeriği de üç bölüm altında şu şekilde incelenmiştir:

- Problem tanımı bölümünde, Android cihazlardaki tedarik zincirinden ve bu cihazlarda tespit edilen Potansiyel Zararlı Uygulamalardan bahsedilecektir.
- Araştırma bölümünde, Android cihazlardaki ön yüklü uygulamalar hakkında yapılan araştırma ve bulgulardan bahsedilecektir.
- Sonuç bölümünde ise çalışma sonunda bulunan bulgular yorumlanacaktır.

Problem Tanımı

Tedarik Zinciri

Android cihazlara konulacak işletim sistemi versiyonları için Google tarafından geliştirilen çeşitli sertifika programları bulunmaktadır. Bunlardan en önemlileri; Android Sertifikalı Partner Programı ve Android Uyumluluk Programı'dır.

Android Uyumluluk Programı'nda cihaza konulacak işletim sistemi versiyonunun Google tarafından tanımlanan donanımsal ve yazılımsal uyumlulukları sağlaması gerekmektedir. Bu program kapsamındaki cihazlar AOSP (Android Open Source Project) üzerinde inşa edilmiştir. Bu AOSP versiyonları önceden de belirtildiği gibi cihaz üreticileri tarafından özelleştirilebilir. Bu özelleştirilmiş işletim sistemi versiyonlarının da Google tarafından tanımlanan CDD (Compatibility Definition Document) gereksinimlerine uyumlu olması gerekmektedir.

Üreticiler, cihazlara koyacakları yazılımların CDD'ye uyumluluklarını yine Google tarafından geliştirilen CTS (Compatibility Test Suite) paketini kullanarak test edebilirler. CDD ve CTS kriterlerini sağlayan cihazlar Android Uyumluluk Sertifikası alabilir. Bu cihazlarda Google uygulamaları (Gmail, Google Play, Youtube vb.) bulunmamakta olup, ilgili sertifika programı kapsamında herhangi bir güvenlik analizi yapılmamaktadır.

Android Sertifikalı Partner Programı'ndaki cihazlarda ise Google uygulamaları ön yüklü olarak gelir. Ayrıca bu sertifika programını almak isteyen cihazlardaki dosyalar, Google tarafından güvenlik ve gizlilik açısından test edilir ve programların güncel olup olmadıkları kontrol edilir. Bu sertifikasyon programına kabul edilmek için cihazların, CTS'nin yanında; GTS (GMS Requirement Test Suite), VTS (Vendor Test Suite), BTS (Build Test Suite) ve STS (Security Test Suite) gibi testlerden geçmesi gereklidir. İlgili testler arasında yer alan BTS kapsamında, cihazlarda bulunan Potansiyel Zararlı Uygulamalar (Potentially Harmful Applications) ve zararlı davranış sergileyen programların tespit edilmesi amaçlanır. STS kapsamında ise cihaz yazılımı üzerindeki güvenlik yamalarının yapılıp yapılmadığı kontrol edilir. Tüm bu testlerden geçen cihazlar Android Sertifikalı Partner (Play Protect Certified) olarak isimlendirilebilir. Bu cihazlara; "Pixel, Samsung ve Xiaomi" gibi üreticilerin cihazları da örnek olarak verilebilir.

Android cihazlara konulacak işletim sistemi versiyonları için Google tarafından geliştirilen çeşitli sertifika programları bulunmaktadır. Bunlardan en önemlileri, Android Sertifikalı Partner Programı ve Android Uyumluluk Programı'dır.

Bazı Ön Yüklü Potansiyel Zararlı Uygulama Örnekleri

Tecno W2 model cihazlarda; "Triada ve xHelper" zararlı yazılım ailelerinin örnekleri bulunmuştur. Bu model daha çok Afrika ülkelerinde satılmaktadır ve Çinli bir firma tarafından üretilmektedir.

Blu R1 model cihazlarda, FOTA (Firmware Over The Air) özelliğine entegre edilmiş Çinli ADUPS Teknoloji Şirketi'ne ait uygulamalar bulunmuştur. FOTA özelliği; USB kablosu ile bağlantı olmadan uzaktan telefonunuzun yazılımını yeni bir sürüme güncellemek için kullanılır. Ancak bu özellik sayesinde ilgili uygulamaların, kullanıcıların "Kişisel Tanımlanabilir Bilgilerini (Personally Identifiable Information)" şifreli bir şekilde bu şirketin sunucularına gönderdiği tespit edilmiştir.

OnePlus firmasına ait telefonlarda kullanıcıların kişisel bilgilerini toplayan, cihazlara uzaktan erişime imkân sağlayan ve cihazlarda yetki yükseltmeye izin veren uygulamaların bulunduğu ortaya çıkarılmıştır. Yapılan araştırmalar kapsamında, Facebook ile telefon üreticileri arasında iki taraflı iş birliği tespit edilmiştir.

Araştırma

Veri Seti

Android cihazlarda bulunan ön yüklü uygulamalara, Google Play gibi uygulama marketleri üzerinden açık bir şekilde erişim sağlanamamaktadır. Bundan dolayı cihazlardan bu uygulamaların toplanması gerekmektedir. Bu amaç doğrultusunda, bir Android uygulaması geliştirilmiş ve bu uygulama Google Play Store'a yüklenmiştir.

Geliştirilen bu uygulama, yüklü olduğu cihaz üzerinde; "/system, /odm, /oem, /vendor ve /product" dizinlerini taramakta ve bu dizinlerde bulunan dosyaların özet (hash) bilgilerini sunucuya göndermektedir. Yani sunucuda bulunmayan ilgili dosyalar, uygulama tarafından sunucuya gönderilmektedir. Şu ana kadar toplanan veri seti hakkında bazı bilgiler şu şekildedir:

- Veri setine 22 farklı üreticinin, 76 farklı modelinden dosya yüklenmiştir.
- 10 farklı ülkedeki cihazlara uygulama yüklenmiştir.

- Toplam 126.418 dosya toplanmıştır. Bunlardan;
  - 11.814 tanesi uygulama dosyası,
  - 416 tanesi "root" sertifika dosyası,
  - 53.895 tanesi paylaşımlı kütüphane dosyasıdır.
- Toplanan uygulamalardan sadece %10'u Google Play Store'da bulunmaktadır.

Uygulama Ekosistemi

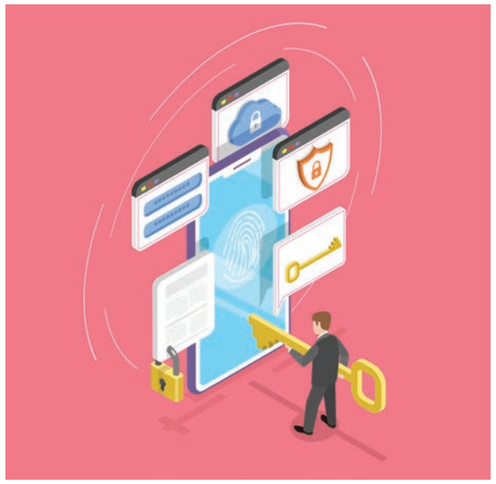
Araştırma kapsamında ilk olarak uygulama ekosistemi çıkarılması amaçlanmıştır. Bu amaç doğrultusunda, uygulamaları imzalamada kullanılan sertifikalar incelenmiştir. Aynı firmaların uygulamalarını imzalarken farklı ve çeşitli sertifikalar kullandıkları görülmüştür. Ayrıca bazı uygulamaların sertifika bilgilerinde eksikler olduğu veya sadece "Android" gibi genel bilgiler bulunduğu için hangi firma veya kişi tarafından geliştirildikleri tespit edilememiştir.

Ek olarak bazı uygulamaların, "Android Debug Sertifikası" ile imzalandığı tespit edilmiştir. Ayrıca bu sertifika, Android uygulama geliştirme sürecinde kullanılmaktadır ve üretimdeki uygulamalarda önerilmemektedir.

İnceleme sonucunda; Samsung: 5477, Xiaomi: 1024, Oppo: 760, Google: 734, OnePlus: 506, Huawei: 478, Realme: 249, Nokia: 217 gibi çeşitli sayılarda farklı üreticilere ait uygulamalar tespit edilmiştir. Bunların yanı sıra, 3. parti firmalar veya kişiler tarafından geliştirilen 513 uygulama bulunmuştur. Bu uygulamalardan 50 tanesi Facebook tarafından geliştirilmiştir. Bu şirketin kullanıcıların kişisel verilerini topladığı ve 3. parti firmalarla paylaştığına dair çeşitli çalışmalar bulunmaktadır. Ayrıca, Digital Turbine reklam firmasına ait çeşitli uygulamalar tespit edilmiştir. Bu firmanın, UID (User Identification) bilgisinden trafik kayıtlarına kadar çeşitli bilgileri topladığı ve bu bilgileri iş ortakları ile paylaştığı gizlilik politikasında belirtilmiştir.

Yine "IronSource" isimli reklam firmasına ait birden fazla uygulama cihazlar üzerinde saptanmıştır. Ek olarak, "Buzzebees" firmasına ait uygulamalar da bulunmuştur. Bu firma; CRM (Customer Relationship Management) olarak bilinen müşteri ilişkileri yönetimi, dijital pazarlama ve mobil ticaret alanlarında faaliyet göstermektedir. Firma, çalışma alanları kapsamında müşteri verilerini toplayarak, bu verileri analiz etmekte ve bunun sonucunda elde ettiği bilgileri işleyerek hizmet verdiği firmaların iş sonuçlarını iyileştirmek için kullanmayı amaçlamaktadır.

Ayrıca "id.co.babe" paket isimli uygulama, VirusTotal platformundaki 3 farklı anti virüs yazılımı tarafından Adware (Reklam Yazılımı) olarak tanımlanmıştır. ADUPS şirketinin kullanmış olduğu FOTA özelliğini kullanan uygulamaların örnekleri tespit edilmiştir. Bunun yanında, OnePlus firmasına ait cihazlarda uzaktan erişime olanak sağlayan ve kullanıcıların kişisel verilerini toplayan uygulama paketleri (OPDeviceManager ve EngineerMode) saptanmıştır.



Android İzleyiciler (Trackers)

İzleyiciler (Trackers), kullanıcı veya kullanıcının davranış biçimleri hakkında bilgi toplamak amacı ile kullanılan yazılımlardır. Araştırma kapsamında, Android platformunda kullanılan çeşitli "izleyiciler" tespit edilmiştir. Analiz edilen uygulamalardan 836 tanesinde en az bir izleyici tespit edilmiştir. En çok tespit edilen izleyiciler ve kaç uygulamada bulundukları şu şekildedir; Google Firebase Analytics: 476, Google AdMob: 315, Google CrashLytics: 153, Google Tag Manager: 107, Facebook Login: 99, Facebook Share: 87 ve AutoNavi / Amap: 80.

Bazı dikkat çeken izleyiciler şunlardır:

Google AdMob: Google'ın mobil uygulamalardan para kazanmak ve uygulama içi reklam amacıyla kullanılan izleyicisidir. Bu izleyici 315 uygulamada bulunmuştur.

AutoNavi / Amap: Çinli Alibaba firmasına ait ağ haritalama, navigasyon ve konum tabanlı servis sağlayıcısıdır. Amap.com ve Amap mobil uygulaması üzerinden harita servisleri sunmaktadır. Ayrıca firma, 2006 yılından beri Google firmasına konum bilgileri sağlamaktadır.

Facebook Ads: Facebook firmasına ait reklam servislerinde kullanılan izleyicidir. Firmanın daha önce, kullanıcıların gizliliğini ihlal ettiğine dair çalışmalar bulunmaktadır.

InMobi: Hindistan'da kurulan ve hedeflenmiş reklamcılık, e-ticaret, uygulama içi mobil reklamcılık ve pazar araştırma platformu gibi alanlarda faaliyet gösteren bir firmadır. Firmanın gizlilik politikası incelendiğinde cihaz tipi (akıllı telefon, tablet vb.), işletim sistemi (iOS, Android vb.), ağ sağlayıcı, kullanılan mobil tarayıcı, cihaz modeli, cihaz üreticisi, cihaz işletim sistemi versiyonu ve cihaz konumu gibi bilgileri topladığı belirtilmiştir. Bunların yanında, reklamın içerik türü (oyun, finans, eğlence, haber vb.), reklam tipi (metin, resim, video), reklamın hangi site üzerinden gösterildiği ve kaç kez tıklandığı gibi bilgiler de toplanmaktadır. Toplanan bu bilgilerin uygulama yayınlayıcılar, geliştiriciler, reklamcılar, veri ortakları, ölçüm firmaları, InMobi iştirakleri, kolluk kuvvetleri ve danışmanlar gibi 3. parti firmalarla paylaşılabileceği söylenmiştir.

Flurry: ABD'li Yahoo firmasına aittir ve mobil analitik, para kazanma (Monetization) ve reklamcılık servisleri sunmaktadır. Çeşitli kullanıcı bilgilerini toplamakta ve iş ortakları ile paylaşmaktadır.

Baidu Location: Palo Alto Networks firması tarafından yapılan araştırmaya göre Çinli Baidu firmasının bazı servisleri, kullanıcıların MAC (Media Access Control) adresleri ve IMSI (International Mobile Subscriber İdentity) numarası gibi bilgilerini toplamaktadır.

ironSource: Para kazanma, analitik gibi alanlarda faaliyet gösteren İsrail merkezli reklam firmasıdır. Bunların yanında, uygulamalarda başka izleyiciler de tespit edilmiştir.

Ayrıca bazı uygulamalarda fazla sayıda izleyici tespit edilmiştir. Bunlara örnek olarak; deezer.android.app: 23, de.axelspringer.yana.zeropage: 20, com.picmix.mobile: 17, flipboard.boxer.app: 17 ve com.jakarta.baca.lite: 15 izleyici barındırmaktadır. Bu uygulamaların tamamının sertifikaları incelendiğinde cihaz üreticilerine ait olmadıkları, yani 3. parti uygulamalar oldukları görülmüştür.

Sonuç

Android tedarik zincirindeki denetim eksikliğinden dolayı cihazlarda bulunan ön yüklü uygulamalar kullanıcıların gizlilik ve güvenliğini tehdit etmektedir. Yapılan tekil analiz çalışmaları, bu tehlikeyi doğrulasa da söz konusu çalışmalar kapsayıcı olmaktan uzaktır. Bu yazıda anlatılan çalışma doğrultusunda ise Android cihazlardaki ön yüklü uygulamalardan oluşan kapsayıcı bir veri seti oluşturulması ve bu veri setindeki uygulamaların analizi hedeflenmiştir.

Hâlihazırda devam etmekte olan bilimsel çalışmaya destek olmak için yukarıda verilen QR kod ile yazar tarafından geliştirilen Android uygulamasını Google Play Store üzerinden indirebilirsiniz. (Not: Uygulama hiçbir şekilde kişisel verilerinize erişmemekte ve sunucuya göndermemektedir.)

Kaynakça

- https://source.android.com/compatibility/cdd?hl=en
- https://source.android.com/compatibility/cts/downloads?hl=en
- https://www.android.com/certified
- https://lab.secure-d.io/triada/
- https://www.kryptowire.com/kryptowire-discovers-mobile-phone-firmware-transmitted-personally-identifiable-information-pi-i-without-user-consent-disclosure/
- https://www.theregister.com/2017/11/14/oneplus_backdoor/
- https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html

Wi-Fi Güvenlik Teknolojileri

Anıl İpek - Uzman Araştırmacı / BİLGEM SGE

> Wi-Fi, aslında teknolojik cihazların kablosuz (wireless) bağlantı sağlayabildiğini belirten bir uyumluluk (fidelity) göstergesidir.

Hayatın vazgeçilmez bir parçası hâline gelerek iş, iletişim, eğlence gibi alanlarda sıklıkla ihtiyaç duyulan internet bağlantısı, Wi-Fi (Wireless Fidelity) adı verilen kablosuz ağlar sayesinde teknolojik cihazlarda neredeyse zorunlu bir hal aldı.

Kullanıcı veya misafirlerin taleplerini karşılamak için, mevcut kablosuz ortak ağların şifrelerini ilgili kişilerle irtibata geçerek temin ediyor ve o ağlara dâhil oluyoruz. Evimizdeki kablosuz ağın şifresini birbirimizle ve çevremizle paylaşıyoruz. Bunun yanında kamuya açık yerlerdeki ortak ağları da kullanıyoruz. Bu noktada pek çok kullanıcı doğal olarak mahremiyet ve güvenlikle ilgili tedirginlik yaşıyor.

Kablosuz teknolojide güvende miyiz?

Wi-Fi, teknolojik cihazların kablosuz (wireless) bağlantı sağlayabildiğini belirten bir uyumluluk (fidelity) göstergesidir. Temelde, kablosuz ağ üzerinden iletişim kurabilen bütün teknolojik cihazlar, IEEE (Institute of Electrical and Electronics Engineers) organizasyonunun geliştirdiği 802.11 standartlarından birini destekler. Bu standartlara 802.11a, 802.11b ve 802.11g örnek verilebilir. Ancak Wi-Fi İttifakı (Alliance), akılda kalıcılık amacıyla daha yeni standartları Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac) ve Wi-Fi 6 (802.11ax) şeklinde isimlendirme kararı almıştır. Kullanıcıların belirlenen bu standartlarla ilgili bilmesi gereken en önemli şey, ilgili standardın son sürümünün en iyi performansı sağladığı ve çalıştırılacak cihazların ortak olarak aynı standarda uyumlu olması gerektiğidir.

Güvenlik tarafı ise kablosuz ağların kullanıldığı ilk zamanlarda büyük bir sorun olarak değerlendirilmiyordu. Çünkü donanımlar üreticilere özel, pahalı ve bulunması zordu. Teknolojinin yaygınlaşmasıyla Wi-Fi güvenliği ile alakalı araştırmalar birtakım mekanizmalara olan ihtiyacı ortaya çıkardı. Erişim noktaları üzerinde etkin olan SSID (Service Set IDentifier) gizleme, MAC (Media Access Control) filtreleme gibi güvenlik seçenekleri bunlardan bazıları ise de Wi-Fi ağlarının istenmeyen kişilerden uzak tutulması ve emniyetinin sağlanması adına geliştirilen şifreleme algoritmaları, mevzubahis teknolojiler arasında bugün için en değerlisi denilebilir.

Wi-Fi Teknolojisi nasıl bir güvenliğe sahip?

Wi-Fi ağlarında şifreleme çeşitleri, şu an için WEP, WPA, WPA2 ve WPA3 olarak değişiyor. Bu teknolojiler, kablosuz ağın yetkisiz kullanımını önlemek üzere güvenliğini sağlamak için kullanılır. Kimi zaman "güvenlik anahtarı" olarak da karşımıza çıkabilen şifreleme protokolleri, erişim noktasında yapılandırılır. Yıllar geçtikçe, türlü sebeplerle bir yenisi ve daha iyisi çıkan bu algoritmalar, ilgili cihazda desteklenmezse devreye alınamaz. Dolayısıyla söz konusu erişim noktasının destek verdiği kapsam, güvenliğini artırmak istediğimiz ağ için gerekli unsurların başında yer alır.

İlk etapta WEP (Wired Equivalent Privacy), 1999 yılında Wi-Fi Güvenlik Standardı olarak kabul edilmişti. Fakat Fluhrer, Mantin ve Shamir (FMS) üçlüsünün öncülük ettiği atak yöntemleriyle algoritmanın kolayca kırılabilir olduğunun ispatlanmasıyla tahtını sadece 4 yıl koruyabilmiştir. 30 Haziran 2010'dan bu yana ise WEP protokolünün herhangi bir kredi kartı işleminin parçası olması, Payment Card Industry Data Security Standartlarına(PCI DSS) göre de yasaktır.

Bilinen ciddi zayıflıkları kapatmaya yönelik geçici çözümler sunmak amacıyla pratik bir ara önlem olarak 2003 yılında, Wi-Fi İttifakı tarafından geliştirilen Wi-Fi Protected Access(WPA) boy göstermiştir.. Nispeten daha güvenilir kabul edilse de mevcut modemlerin algoritmayı desteklemek için güncellenmesi, hayal edildiği ölçüde başarılamadığından yaygınlaşması sağlanamamıştır.

Önceki protokollerde güvenlik problemlerine yol açan şifreleme yöntemi (RC4)'ün kökünden değiştirilmesiyle (AES), hem gizlilik hem de bütünlük açısından daha güçlü olan WPA2, 2006'dan itibaren tüm yeni cihazlarda zorunlu kılındı. WPA için de birtakım saldırılar yayımlayan Piessens ve Vanhoef ikilisinin 2017 yılında duyurduğu, ağa dâhil olunmadan havadaki paketler koklanarak (sniff) yapılan ve "KRACK" atağınca sömürülen bir dizi güvenlik açığı mevcuttu. Bazı modem üreticileri, güncellemeler yayımlayarak bu zafiyetin önüne geçse de Ekim 2018'deki bir çalışmaya göre, bu teknolojiye sahip birçok cihaz istismar edilebilir durumdadır.

Eski sistemlerdeki ileri mahremiyet (forward secrecy) eksikliğini gidermek ve mevcut güvenlik açıklarını kapatmak için 2018 yılında WPA3 duyurulmuştur. Daha güvenli ve kişiselleştirilmiş şifreleme sağlayan, Simultaneous Authentication of Equals (SAE) özelliği sayesinde iyileştirmeler sergileyen WPA3, daha işlevsel bir görüntü çizmekte. Ağdaki kullanıcıların da bir başkasının trafiğini izlemesi zorlaştığından, kamuya açık ağların daha özel hâle geleceği bile söylenebilir.

Sonuç olarak kablolu şekliyle karşımıza çıkan ağlar, talep artışı ve gelişen teknolojiyle kablosuz olarak yaşantımızda yerini almaya başlamıştır. Ortaya çıkmasından bu yana çok hızlı aşama kaydeden Wi-Fi ağlarında, bu ilerlemeyle birlikte güvenlik açıkları da belirmiştir. Son nesil protokollerse kablosuz ağlarda güvenliği zorunlu hâle getirmiştir. WPA3, 1 Temmuz 2020 tarihi itibarı ile yeni cihazlarda mecburi tutulmuştur.

Mevcut olan en önemli Wi-Fi güvenlik önlemi WPA3 yaygın bir şekilde benimsenene kadar güvenlik bilincine sahip kullanıcılar halka açık ağlarda VPN vb. çözümler kullanmayı bir süre daha sürdürecekler gibi görünüyor.

Kaynakça
- https://bidb.itu.edu.tr/seyir-defteri
- https://dspace.gazi.edu.tr
- https://www.cs.umd.edu
- https://www.pcisecuritystandards.org
- https://openxtra.org
- https://www.usenix.org
- https://www.wi-fi.org

Şüpheli e-Posta İnceleme Süreci ve Otomasyonu

"Günde ortalama 14,5 milyar spam e-Posta, internet ortamında dolaşmaktadır. Bu sayı toplam e-Posta trafiğinin %45'ine eşit olmakla beraber, kötücül yazılım, oltalama gibi istenmeyen diğer e-Posta türleriyle birlikte oran daha da yükselmektedir."

Dr. Samet Ganal – Kıdemli Mühendis / Kuveyt Türk Katılım Bankası

Kurumsal yapılar korumaları gereken veri boyutu ve önemi nedeniyle bireysel siber güvenlikten farklı olarak çok katmanlı koruma yapısı kullanmaktadır. Çok katmanlı koruma yapısında, internet üzerinden kurum iç ağına girecek paket farklı güvenlik ürünleri tarafından tekrar tekrar kontrol edilir. Bu sayede kötücül bir dosya ilk katmanda tespit edilemese bile ikinci veya üçüncü katmanda tespit edilmekte ve kurum iç ağına girişi engellenmektedir.

Kurum iç ağına erişimin bir diğer yolu olan e-Posta koruma sistemi ise genellikle tekil bir yapıya sahiptir. Kurumlar çalışanlarına gönderilen e-Postaların kontrolünde birden fazla katman kullanmayı tercih etmemektedir. Bunun sebebi ekstra maliyetin yanı sıra hatalı tespitlerin önüne geçmektir.

Siber saldırganlar, e-Posta adreslerinin kolay ele geçirilebilmesi ve kullanıcılar ile direkt etkileşim sağlaması nedeniyle e-Posta üzerinden saldırı tekniklerini sıklıkla kullanmaktadır.

e-Posta Saldırılarına Karşı Çözümler

e-Posta ortamındaki güvensiz duruma karşılık olarak siber güvenlik uzmanları kurum personel ve değerlerini korumak için e-Posta koruma ve sandbox teknolojilerinden yararlanmaktadır. Kullanılan güvenlik yöntemleri istenmeyen e-Postaları büyük oranda engellese de hiçbir koruma yöntemi %100 doğru sonuca ulaşamadığı için kurum içine istenmeyen e-Posta girişi olmaktadır.

Spam (istenmeyen e-Posta), oltalama veya kötücül yazılım içeren tüm e-Postalar kurumların gözünde "istenmeyen" kategorisinde değerlendirilmektedir. Kurum çalışanlarının bu tür e-Postalara karşı bilinçli olması için düzenli olarak bilgilendirmeler yapılmalı ve istenmeyen türde bir e-Posta almaları durumunda ilgili güvenlik birimine bilgi vermeleri istenmelidir.

Ek olarak çalışanlarda e-Posta güvenliği konusunda bilinç oluştuğunda, istenmeyen türdeki e-Posta bildirimleri için bir yol gösterilmelidir. Siber güvenlik uzmanları kullanıcılara net ve kolay bir bildirim yöntemi sunmaz ise kullanıcılar bildirimleri farklı formatlarda ve yöntemlerde yapacak, bu durum da şüpheli e-Posta inceleme ve önleme sürecini zorlaştıracaktır. Çalışanların e-Postaları tam ve tekdüze bir biçimde iletmesi için güvenlik uzmanları tarafından çalışmalar yapılmaktadır. Örnek olarak

"Bir e-Postanın kötücül olması durumu, içerisindeki IP, URL veya ek dosyasının kötücül yazılım içermesi veya yönlendirmesi durumuna bağlıdır. Bu bakımdan e-Posta içerisindeki IP, URL ve ek dosyaları ayrıştırılmalı ve kontrol edilmelidir."

kullanıcı e-Posta kutularına, tıklandığı takdirde seçili e-Postayı ek şeklinde güvenlik uzmanlarına ileten buton yerleştirilmesi her iki taraf için de süreci daha kolay hale getirebilmektedir.

Bununla birlikte şüpheli e-Posta inceleme süreci bir otomasyon ve çağrı yönetimi uygulaması üzerinden yapılmalıdır. Bu tür bir uygulamanın kullanılması e-Posta inceleme sürecini önemli ölçüde daha kolay hale getirecek, gözden kaçırma ihtimalini düşürecek ve hızlı aksiyon imkanı vererek zaman kazancı sağlayacaktır.

Siber olay yönetim uygulaması kullanıcıların şüpheli e-Postaları yönlendirdiği e-Posta kutusunu takip etmeli ve buraya gelen her yeni bildirim için otomatik olarak olay kaydı açılmalıdır. Oluşan olay kaydı için daha önceden hazırlanmış senaryo otomatik olarak çalıştırılmalıdır. Senaryo içerisinde ilk olarak bildirimde bulunan kullanıcı bilgileri, bildirimi yapılan e-Postanın gönderici adresi ve konusu ayrıştırılarak olay kaydı içerisinde doğru alanlara

yazılmalıdır. Geribildirim olarak bildirimi yapan kullanıcıya yönlendirdiği e-Postanın alındığı ve üzerine çalışılmaya başlandığına dair bilgilendirme e-Postası gönderilmelidir.

Bildirimi yapılan e-Postanın kurum dışından gelen şüpheli bir mail mi olduğu yoksa kurum iç yazışmalarına ait sehven bir gönderim mi olduğu tespit edilmelidir. e-Posta güvenlik cihazları kurum dışından gelen e-Postaları işaretleyebilmektedir. Bildirimi yapılan e-Postanın kaynağının neresi olduğu bu işarete bakılarak öğrenilebilmektedir. Eğer e-Posta kuruma dışarıdan gelmemiş ise şüphe içeren bir durum olmayacağı için kullanıcıya, ilgili e-Posta içerisinde şüphe edilecek bir durum olmadığını belirtilen bildirim gönderilerek olay kaydı kapatılmalıdır.

e-Postaların Kategorizasyonu

Bildirimi yapılan e-Postalar incelenip şu dört kategoriye ayrılmalı ve bu duruma istinaden karar alınmalıdır.

- Kötücül içermeyen iyi huylu e-Postalar,
- Kötücül içermeyen reklam vs. türü spamlar,
- Kötücül içermeyen oltalama vs. türü spamlar,
- Kötücül içeren veya yönlendiren tehlikeliler

Kullanılan senaryo ve olay yönetimi uygulaması sayesinde incelenen tüm şüpheli e-Posta bildirimlerinin gönderici adresi, konusu ve inceleme sonucu, tekrar kullanılmak üzere kaydedilmektedir. Yeni gelen şüpheli e-Posta bildiriminin gönderici adresi ve konusu bu listede aratılmalı ve önceki ihbarlardaki inceleme sonucu kontrol edilmelidir. Eğer aynı gönderici adresi ve e-Posta konusu için daha önceden inceleme yapılmış ise aynı karar yeniden otomatik olarak uygulanmalıdır. Bu sayede güvenlik analistinin aynı şüpheli e-Postayı tekrardan incelemesi önlenmiş, zaman kazancı sağlanmış ve süreç tam otomatik çalışmış olacaktır.

Tespit sürecini kolaylaştırmak için bildirimi yapılan e-Postanın kurum içerisinde kaç kullanıcıya iletildiğinin kontrolü de yapılmalıdır. Bu işlem için olay yönetimi uygulamasında daha önceden hazırlanan sorguya, bildirilen e-Postanın gönderici adresi ve konu bilgileri eklenerek kurum e-Posta güvenliği veya iz kaydı sistemi üzerinde aratılması sağlanmalıdır. Elde edilen sonuç olay yönetimi uygulamasına geri alınmalı ve doğru alanlara yazılmalıdır.

Siber Tehdit İstihbaratı ile Entegrasyon

Bileşenlerin kontrolü sürecinde, kullanılan olay yönetimi uygulamasında siber tehdit istihbarat ürün entegrasyonu varsa IP ve URL adresleri burada otomatik sorgulanmalı ve kötücül itibar sahibi olma durumları kontrol edilmelidir. Ek dosyalarına ait özet(hash) bilgileri de tehdit istihbarat ürünleriyle sorgulanıp kötücül itibar sahibi olması durumu kontrol edilmelidir. Kurumsal veri kaybı olmaması adına ek dosyaları tehdit istihbaratı amacıyla da olsa kurum dışına çıkmamalı, sadece özet bilgisi üzerinden bilgi edinilmeye çalışılmalıdır. Kurum içerisinde sandbox teknolojisi kullanılıyorsa tüm IP, URL ve ek dosyaları burada taratılarak kötücül içerme veya yönlendirme durumları kontrol edilebilmektedir.

Ayrıca ilgili olay kaydını inceleyecek siber güvenlik uzmanının işini kolaylaştırmak için şüpheli e-Posta içerisinden ayrıştırılan URL adreslerinin ekran görüntüleri de otomatik olarak alınmalı ve olay kaydı içerisine eklenmelidir.

Elde edilen bilgiler ışığında, olay yönetim uygulaması kullandığı senaryoya bağlı kalarak önceden tanımlı kıstaslara uyan e-Postalar için karar verip otomatik aksiyon başlatabilmektedir. Örnek olarak eğer e-Posta içerisindeki herhangi bir URL adresi tehdit istihbarat servislerinde 7'den büyük bir skora sahipse veya ek dosya sandbox'ta kötücül olarak tespit edilmiş ise e-Postayı kötücül olarak işaretle ve karar ağacını bu kırılımdan devam ettir denilebilmektedir.

Seçenek Bazlı İşlemler

Elle inceleme durumlarında ise siber güvenlik analistine karar verebileceği dört adet seçenek sunulmuştur. Analist bu seçeneklerden herhangi birini işaretlediğinde geri kalan tüm işler, kullanıcıya yapılacak bildirim, mail silinmesi gibi işlemler otomatik olarak yapılacaktır.

Kötücül içermeyen iyi huylu e-Postalar: Bildirimi yapılan e-Posta içerisinde kötücül olabilecek bir bileşene rastlanmaması durumudur. Kullanıcıya e-Postada şüphe edilecek bir durum olmadığı bildirilmekte ve olay kaydı kapatılmaktadır.

Kötücül içermeyen reklam vs. türü spamlar: Bildirimi yapılan e-Posta reklam ve bilgilendirme amacıyla gönderilmiş olup az sayıda kullanıcıya ulaşmışsa bu kategoride olduğuna karar verilmektedir. Kullanıcıya e-Postanın herhangi bir tehdit içermediği ve bu gönderici adresini kişisel olarak engelleyebileceği bilgisi verilmektedir.

Kötücül içermeyen oltalama vs. türü spamlar: Bildirimi yapılan e-Posta kötücül yazılım içermiyor ama çok fazla sayıda kullanıcıya gelmiş veya kullanıcıyı aldatmaya yönelik içeriğe sahip ise bu kategoride olduğuna karar verilmektedir. Bu durumda bildirimi yapan kullanıcıya gerekli tüm işlemlerin siber güvenlik uzmanları tarafından yapılacağına dair geribildirim verilmektedir. Eğer yapılabilme imkanı varsa olay yönetimi uygulaması üzerinden, yapılamıyorsa e-Posta yöneticisinden ilgili e-Postaların kullanıcı kutularından silinmesi istenmektedir.

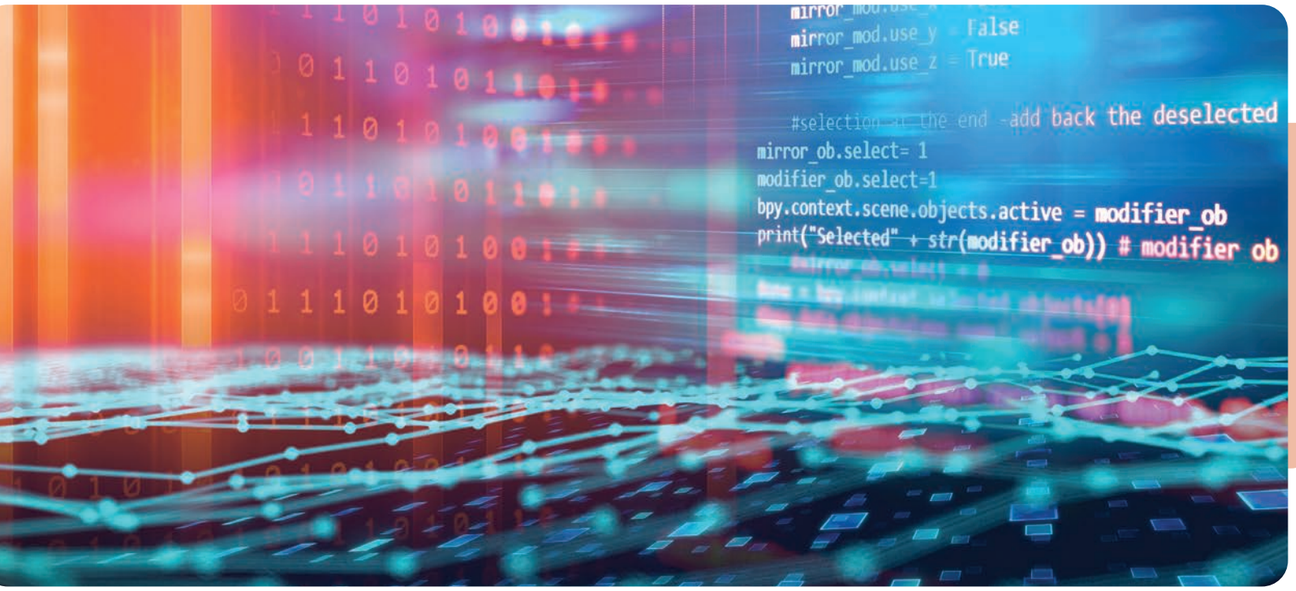
Kötücül içeren veya yönlendiren tehlikeliler: Bildirimi yapılan e-Posta içerisindeki IP, URL veya ek dosyası kötücül bir aktiviteyi gösteriyorsa bu kategoride olduğuna karar verilir. Bu durumda yine bildirimi yapan kullanıcıya gerekli tüm işlemlerin siber güvenlik uzmanları tarafından yapılacağına dair geribildirim verilmektedir. Yanıt ve kurtarma süreci içinse ilgili e-Postaların kullanıcı kutularından acilen silinmesi süreci başlatılmakta ve içerisindeki kötücül bileşenle iletişime geçen başka kullanıcı olması durumu kontrol edilmektedir. Elde edilen bulgular ışığında kurtarma süreci genişletilebilmektedir.

Tüm bu işlemler ile birlikte kullanıcı tarafından yönlendirilen e-Posta içeriği ayrıştırılmış, incelenmiş, oluşturduğu trafik görülmüş ve tehdit içermesi durumuna karar verilmiştir. Bu sayede şüpheli e-Posta incelemesi süreci büyük oranda otomatik hale getirilmiş ve hem hız hem analist eforu açısından büyük kazanç sağlanmıştır.

Kaynakça

[1] SPAMLAWS, 2021. Spam Statistics and Facts. Retrieved from https://www.spamlaws.com/spam-stats.html.

Yazılım Geliştirme Yaşam Döngüsünde Hız ve Güvenlik: DevSecOps



Süleyman Muhammed Arıkan - Uzman Araştırmacı / BİLGEM SGE

DevSecOps (Development-Security-Operations), DevOps uygulamalarında geliştirme sürecini yavaşlatmadan güvenliği artırmak için sunulmuştur.

Yazılım geliştirme yaşam döngüsü (YGYD), müşteri beklentilerini karşılayan yazılımların mümkün olan en yüksek kalitede, en düşük maliyet ile en kısa zamanda üretilmesi için izlenen sistematik bir süreçtir. Geçmişten günümüze sıkça tercih edilen geleneksel YGYD yöntemleri incelendiğinde ilk olarak 1956 yılında sunulmuş ve 1985 yılında Amerika Birleşik Devletleri Savunma Bakanlığı tarafından yazılım geliştirme için standart bir yaklaşım olarak tanımlanmış şelale modeli öne çıkmaktadır. Bu modelde tamamen sıralı ve doğrusal bir yaklaşım üzerinden planlama, analiz, tasarım, geliştirme, test ve bakım aşamaları birbiri ardına gerçekleştirilir. Dolayısıyla tüm gereksinimlerin açık ve sabit olduğu projeler için uygundur.

Ancak, zaman içinde bilişim teknolojilerinin gelişmesi ile ihtiyaçlar çeşitlenmiş ve yazılım projeleri büyüyerek tamamlanma süreleri uzamıştır. Müşterilerin son ürüne ulaşması için geçen sürenin artması ve ihtiyaçların değişken yapısı, daha sık teslimatlara imkan tanıyan, değişime hızlı ve esnek yanıt verebilen yeni yöntemlere olan ihtiyacı ortaya çıkarmıştır. Ayrıca güvenlik amacıyla gerçekleştirilen testlerin projenin ilerleyen aşamalarında ele alınması, yazılım projelerinin bütçesi ve zamanı içinde gerekli düzeltmelerin yapılmasını ve ilgili önlemlerin uygulanmasını zorlaştırmıştır.

Çevik Yöntemler

2001 yılında 12 prensipten oluşan çevik bildiri (agile manifesto) yayınlanmıştır. Zaman içinde bu prensiplere dayanan çeşitli yöntemler (Scrum, Kanban, vb.) geliştirilmiş ve proje süresince çeşitlenen ve değişen müşteri ihtiyaçlarını karşılamak için yazılım geliştirme projelerinde tercih edilmeye başlanmıştır. Çevik yöntemler, yazılımın erken ve devamlı teslimini amaçlarken son aşamalarda dahi değişen gereksinimlere hazır olmaya çalışır. Personelin motivasyonuna ve ihtiyaçlarına, ekibin performansına ve verimini artırmaya yönelik çözümlere, gereksiz süreçlerin ikinci plana atılmasıyla sadeliğin sağlanmasına ve çalışan yazılımın varlığına odaklanır. Çalışan yazılım ile test faaliyetleri işletilmiş ve tümünden başarılı şekilde geçmiş yazılım ifade edilmektedir. Dolayısı ile paydaşlara olan ürün teslimatı sıklaştırılmış, test faaliyetleri geliştirme süreci ile paralel hale getirilmiş, değişen gereksinimlere karşı esneklik sağlanmıştır.

DevOps

Çevik yöntem ile geliştirme sürecine odaklanılarak geliştirme ve test ekiplerine çeviklik kazandırılmış olsa da ele alınmayan operasyon süreçleri darboğaz oluşturmuştur. Ayrıca çevik yöntemlerde kişilere, yazılımın işlevselliğine ve müşteri beklentilerine odaklanılırken güvenlik doğrudan ele alınmamıştır. Bu durum güvenliğin, doğrudan iş değeri sunmadığını ve/veya sonradan ele alınabilecek bir konu olduğunu düşünen projelerde açıklık barındıran yazılımların oluşmasına sebep olmuştur. Ayrıca kısa yinelemelerin gerekli güvenlik testlerini işletmek için yeterli olmaması; personelde ve müşteride bilgi, tecrübe veya farkındalık eksikliği güvenliğin çevik yöntemlere dahil edilmesini zorlaştırmaktadır.

Geliştirme ve operasyon süreçlerinin her ikisine birden çeviklik kazandırabilmek amacıyla 2009 yılında DevOps (Development-Operations) yaklaşımı ortaya çıkmıştır. DevOps, yazılımların ve hizmetlerin hızlı sunulabilmesi amacıyla kullanılacak kültürel felsefelerin, yöntemlerin ve araçların birleşimi olarak tanımlanabilir. DevOps, geliştirme ve operasyon ekipleri arasındaki engelleri kaldırarak geliştirmeden teste, dağıtımdan operasyona kadar bir yazılımın yaşam döngüsü boyunca çalışacak tek bir ekip üzerinden faaliyetlerin yürütülmesine imkan sağlar. Böylece yazılım geliştiricilerin, test personelinin, sistem yöneticilerinin ve kalite güvence mühendislerinin uyum içinde aralarında kopukluk olmadan çalışması neticesinde iş hedeflerine kaliteden ödün vermeden daha hızlı ulaşılır.

Unutmamak gerekir ki; çevik yöntemler, şelale modeli gibi geleneksel YGYD modellerinin yerini alsa da DevOps, çevik yöntemlerin yerini alacak bir model olmaktan ziyade daha fazla süreci kapsayan bir iyileştirme/geliştirme olarak görülmelidir. Dolayısı

DevOps yaklaşımının çevikliğinden ve esnekliğinden faydalanabilmek için; güvenliğin, tüm yazılım geliştirme yaşam döngüsü (YGYD) boyunca entegre bir rol olarak yer alması gerekmektedir.

ile DevOps, yazılıma odaklanan çevik yöntemler için tamamlayıcı niteliktedir. DevOps uygulamaları, hız ve işlevsellik açısından güçlü yaklaşımlar barındırsa da önceden olduğu gibi güvenlik ikinci planda kalmış ve yeterince vurgulanmamıştır. DevOps yaklaşımının çevikliğinden ve esnekliğinden faydalanabilmek için güvenliğin tüm YGYD boyunca entegre bir rol olarak yer alması gerekmektedir. DevSecOps (Development-Security-Operations), DevOps uygulamalarında geliştirme sürecini yavaşlatmadan güvenliği artırmak için sunulmuştur.

DevSecOps ve Avantajları

DevSecOps yazılım geliştirme projelerinde ihtiyaç duyulan güvenlik için doğal evrimi temsil eder. Yazılım ve altyapı güvenliğinin projede en baştan itibaren ele alınması gerektiğini belirtir. Güvenliğin, geliştirme ve operasyon ile eşit öneme sahip olduğunu vurgulayarak yazılım geliştirme yaşam döngüsünün her aşamasında mevcut olmasını amaçlar. Dolayısı ile güvenliğin sağlanmasına yönelik faaliyetleri, geliştirilmesi tamamlanmış bir ürüne uygulamak yerine çevik yazılım geliştirme süreçlerine ve DevOps iş akışlarına entegre ederek üründe yerleşik (built-in) güvenliğin oluşturulmasını sağlar. Güvenliğin tek bir ekibin yegane sorumluluğu olmasından ziyade geliştirme, güvenlik ve operasyon ekiplerinin ortak sorumluluğunda oldu-

ğunu belirtir. Bu sebeple güvenlik, bir DevSecOps ekibinde her personelin odaklanması gereken bir konudur. Bu durum güvenlik sorunlarının; kolay, hızlı ve düşük maliyet ile çözülebileceği geliştirme sürecinde ele alınmasını mümkün kılar.

DevSecOps, yeni tanımlanan bir açıklığın ne kadar hızlı yönetildiği ile ilgilidir. Dolayısı ile DevSecOps'un iki ana avantajı hız ve güvenliktir. Yazılım geliştirme yaşam döngüsünü yavaşlatmamak için diğer süreçlerde olduğu gibi güvenlik odaklı faaliyetler de otomatikleştirilir. Otomasyonun sağlanmasıyla veya daha verimli kullanılmasıyla güvenlik sorunları daha etkin ve hızlı şekilde tespit edilir. Tüm geliştirme süreci boyunca kaynak kod, karşılaşılabilecek muhtemel açıklıklara ve tehdit aktörlerine karşı sürekli olarak gözden geçirilir, denetlenir ve test edilir. Bu durum, meydana gelebilecek hataları ortadan kaldırır ve başarıya ulaşabilecek saldırı ihtimalinin azaltılmasına katkı sunar. Ayrıca, başarılı saldırılar neticesinde işletilecek olay müdahale sürecinin daha etkin gerçekleştirilmesini sağlar. Gelişmiş izleme ve denetimler ile muhtemel yeni tehdit aktörleri ve türleri daha hızlı tespit edilebilir.

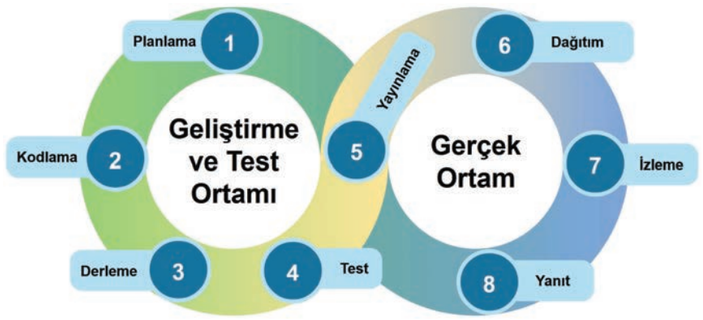
DevSecOps; insan, zaman ve iş gücü gibi tasarruf edilen kaynaklar, iyileştirilmiş ve çeviklik kazandırılmış çeşitli süreçler, azaltılmış güvenlik tehditleri, işletilmiş otomatik testler sayesinde artan kalitenin yanı sıra projelerin ve ürünlerin müşteriye daha erken ve sık periyotlar ile teslim edilmesi yoluyla iş değerine önemli katkıda bulunur.

DevSecOps Yaşam Döngüsü ve İşlem Hattı

DevSecOps, DevOps işlem hattı üzerinden sunduğu yüksek geliştirme hızı ve çevikliğe karşın güvenlikten ödün vermez. Döngüsel bir süreç olan DevSecOps için işlem hattı Şekil-1 üzerinde gösterilmiştir.

Süreklilik, DevOps'da olduğu gibi DevSecOps işlem hattının da vazgeçilmez bir karakteristiğidir. Bu sürekliliği sağlamaya yönelik olan DevSecOps yaşam döngüsü; sürekli geliştirme (continuous development), sürekli entegrasyon (continuous integration), sürekli test (continuous testing), sürekli dağıtım (continuous deployment), sürekli izleme (continuous monitoring) ve sürekli geri bildirim (continuous feedback) gibi fazlardan oluşarak işlem hattı aşamalarını işletir.

Yaşam döngüsünün ilk aşaması, planlamanın ve yazılım için kaynak kodun geliştirilmesi faaliyetlerinin işletildiği sürekli geliştirmedir. Yazılım güvenliği odağında DevSecOps işlem hattının incelenmesi gerekirse planlama, otomatizasyonun en az işletildiği aşamadır ve tehdit modellemesi gibi faaliyetleri içerir. Bu aşamada güvenlik analizi faaliyetleri uygulanarak güvenlik testlerinin ne zaman, nerede ve nasıl gerçekleştirileceğine dair plan oluşturulur. Geliştirme olarak da adlandırılan kodlama; personelin daha güvenli kod geliştirmesine odaklanan aşamadır. Geliştirilen kodun, sürüm kontrol sistemine (Git, Apache Subversion, Mercurial vb.) gönderilmeden önce üzerinde gerçekleştirilecek analizlerin/incelemelerin yapılmasını, sürüm kontrol sistemine gönderildikten sonra işletilen gözden geçirme (review) çalışmalarını ve statik kod analizi faaliyetlerini içerir.



Şekil 1. DevSecOps Yaşam Döngüsü

Derleme ve test aşamalarını barındıran sürekli entegrasyon aşaması, yazılım geliştirme personeli tarafından oluşturulmuş/iyileştirilmiş kodun mevcut kaynak kod ile birleştirilmesidir. Derleme, kodun mevcut kaynak kodlara entegre edilerek yazılımın derlenmesini ve derlenmiş yazılımın üzerinde yazılım bileşimi analizi (yazılım kompozisyon analizi olarak da bilinir - SCA), statik uygulama güvenlik testleri (SAST) ve birim testleri gibi faaliyetlerin işletilmesi süreçlerinden oluşur. Test aşamasında ise özellikle yaygın olarak bilinen yüksek öncelikli güvenlik sorunlarına karşı dinamik uygulama güvenliği testleri (DAST) gerçekleştirilir. Sürekli test aşaması ise entegrasyonu başarıyla sağlanmış kod üzerinde entegrasyon testlerinin, performans testlerinin, regresyon testlerinin ve/veya kabul testlerinin manuel işlemlere gerek duymadan gerçekleştirilmesidir.

İlgili testlerden başarıyla geçen ve son halini alan kaynak kodun gerçek ortama kurulması sürekli dağıtım aşaması ile gerçekleşir ve yayınlama ile dağıtım aşamalarını barındırır. Yayınlama (release) aşamasında, çalışma ortamı altyapısının güvenli hale getirilmesine odaklanılır. Bu kapsamda, altyapı bünyesinde kullanılan teknolojilerde (işletim sistemi, veri tabanı, güvenlik duvarı vb.) güvenliğin sağlanmasına yönelik yayınlanmış rehberler ve en iyi uygulama (best practices) önerileri ışığında sıkılaştırma (hardening) faaliyetleri işletilir.

Dağıtım aşamasında geliştirme ortamı ile gerçek ortam arasındaki konfigürasyon farklılıkları kontrol edilerek uygun yapılandırmalar ve kaynaklar (gerçek ortam için hazırlanmış sertifikalar, erişim bilgileri vb.) ile yazılımın hizmet verdiğinden emin olunur. Çalışma ortamının beklendiği gibi hizmet verdiğinden emin olmak için ise çalışma zamanı doğrulama araçlarından (Osquery, Falco vb.) faydalanılabilir. Bunlara ek olarak çöken sunucular, kopan ağ bağlantıları ve sabit disk üzerinde meydana gelebilecek hatalar gibi çeşitli gerçek dünya olayları simüle edilerek yazılımın davranışları incelenebilir ve güvenlik zafiyetine sebep olabilecek durumlar tespit edilerek önlem alınabilir.

> **DevSecOps, yeni tanımlanan bir açıklığın ne kadar hızlı yönetildiği ile ilgilidir. DevSecOps'un iki ana avantajı hız ve güvenliktir.**

Yazılımın kullanım verilerinin kaydedildiği ve her işlevin takip edildiği sürekli izleme fazında izleme ve yanıt aşamaları işletilir. Dağıtım aşamasının başarılı bir şekilde tamamlanmasının ardından gerçek ortamda çalışmaya başlayan yazılım için günlük kayıtları toplanır ve mevcut/muhtemel tehditlerin tespit edilmesi amacıyla bu kayıtlar üzerinde analizler gerçekleştirilir. Kurum personeli veya harici kaynaklar üzerinden sızma testleri de işletilebilir. Son olarak yanıt aşamasında, gerçekleştirilen saldırılar engellenir veya engellenemeyen saldırıların ardından sistemin tekrar düzgün çalışır duruma getirilmesi için süreç işletilir.

DevSecOps yaşam döngüsünün son aşaması olan sürekli geri bildirimde ise geri dönüşler ve öğrenilen dersler elde edilerek bir sonraki yinelemeye aktarılır. Böylece, sürekli tekrarlanacak olan yinelemelerin ardından yazılım iyileştirilerek amaçlanan kalitede ve işlevde güvenli yazılımların hızlıca oluşturulması sağlanır. Müşterilerden alınacak geri dönüşler, ihtiyaçları karşılayan yazılımların oluşturulmasında ve kullanıcıların memnuniyetine giden yolda bir adım daha atılmasında büyük öneme sahiptir.

DevSecOps sayesinde personel, hızdan ödün vermeden güvenlik sorunlarını yalnızca tespit etmekle kalmayacak aynı zamanda çözümlerini de uygulayacaktır. Bu sebeple temel güvenlik bilgisinin sağlanması için eğitimlere ihtiyaç duyulacaktır. Ayrıca yeni araçların temini kadar kurumsal kültürün değişimini de gerektirecektir.

Kaynakça

•Bartsch, Steffen. "Practitioners' perspectives on security in agile development." 2011 Sixth International Conference on Availability, Reliability and Security. IEEE, 2011.
•https://aws.amazon.com/tr/devops/what-is-devops/
•https://www.atlassian.com/devops/devops-tools/devsecops-tools
•https://www.contino.io/insights/devsecops-best-practices
•https://www.coveros.com/devsecops-incorporate-security-devops-reduce-software-risk/
•https://www.cuelogic.com/blog/devops-lifecycle
•https://www.forcepoint.com/tr/cyber-edu/devsecops
•https://www.ibm.com/cloud/learn/devsecops
•https://www.javatpoint.com/devops
•https://www.linkedin.com/pulse/all-you-need-know-waterfall-model-rafayel-mkrtchyan/
•https://www.redhat.com/en/topics/devops/what-is-devsecops

Sistem ve Kütüphane Çağrı Verileri ile Zararlı Davranış Tespiti

İlk olarak 1990'lı yıllarda UNIX üzerinde çalışan işlemlerin modellenmesi ve oluşturulan istatistiksel model üzerindeki sapmalar vasıtasıyla zararlı davranışların tespit edilmesi üzerine çalışmalar yapılmıştır.

Kerim Can Kalıpcıoğlu – Araştırmacı / BİLGEM SGE

Günümüz bilgisayar sistemleri, gelişen hesaplama, bilgi işleme ve problem çözme kabiliyetleriyle birçok alanda yaygın olarak kullanılmaktadır. Bu işlemler gerçekleştirilirken işlenen verilerin güvenliği ise bilgisayar sistemlerinin güvenliğinden geçmektedir. Veri güvenliğinin sağlanması amacıyla, özellikle kurumsal sistemlerde kullanılmak üzere, yazılım ve donanım ürünleri geliştirilmiştir. Farklı yaklaşımlar kullanarak bilgisayar sistemlerinin güvenliğini sağlamaya çalışan bu güvenlik ürünleri gelişen bilgisayar teknolojisine rağmen uzun süredir benzer yöntemler kullanmaktadır.

Bilgisayar teknolojisinin gelişmesi ile birlikte bilgisayarlar insanlara benzer şekilde örüntüleri tanıma yeteneğine sahip olmuşlardır. Çoğunlukla yapay zekâ olarak adlandırılan bu örüntü tanıma yöntemleri sayesinde insan dilinin bilgisayar tarafından yorumlanması ve görüntülerden objelerin tespit edilmesi gibi işler gerçekleştirilebilmektedir. Yapay zekâ tekniklerini kullanan sistemler bilgisayar güvenliği araştırmalarında da kabul görmüştür. Bu araştırmalara konu olan başlıklardan birisi de sistem çağrıları ve kütüphane çağrıları kullanılarak yapılan zararlı davranış tespitidir.

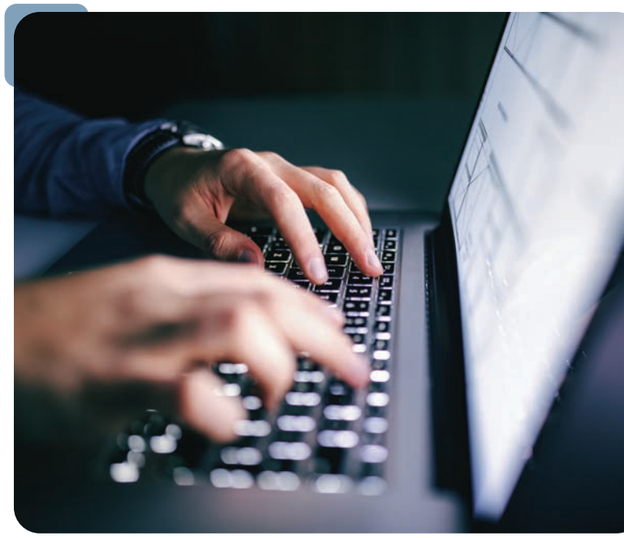
Bu kapsamda ilk olarak 1990'lı yıllarda UNIX üzerinde çalışan işlemlerin modellenmesi ve oluşturulan istatistiksel model üzerindeki sapmalar vasıtasıyla zararlı davranışların tespit edilmesi üzerine çalışmalar yapılmıştır. 2000 yılına kadar yapılan çalışmalar, çoğunlukla işlemlerin modellenmesinde sistem çağrı verisinin kullanımının etkinliği ve bilgisayar güvenlik yaklaşımlarının felsefesi üzerine yapılmıştır. Sistem çağrı verisinin modelleme için yeterli ve verimli olup olmadığının araştırılmasının yanında bu verinin modelleme için nasıl kullanılacağı da cevap aranan önemli bir problemdir. Günümüzde ise özellikle finans, doğal dil işleme ve sinyal işleme alanlarında geliştirilen modeller ile ardışık verilerin modellenmesi için önemli gelişmeler sağlanmıştır. Bu yöntemler benzer özellik gösteren sistem ve kütüphane çağrılarına da uygulanmaktadır.

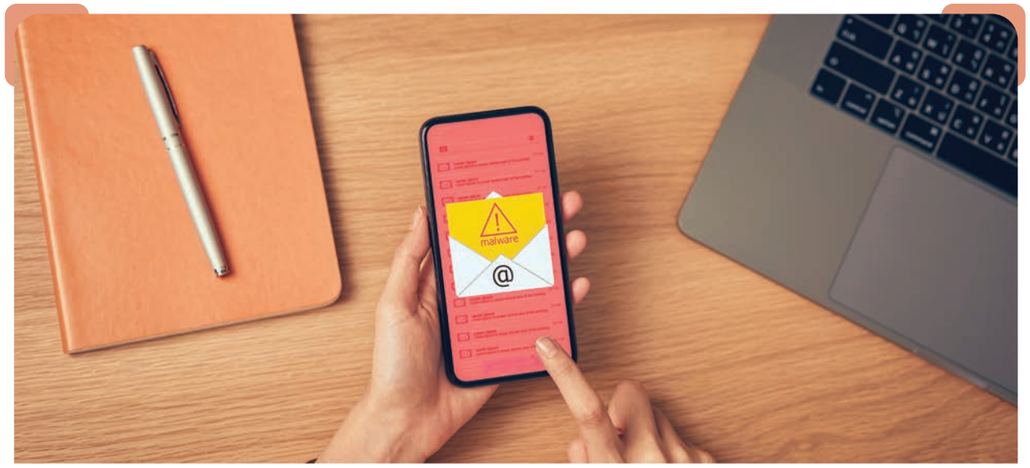
Zararlı davranış tespiti

Bilgisayar güvenliği çalışmalarının başlangıcından beri zararlı davranış tespiti problemi üzerine araştırmalar yürütülmektedir. Bilgisayar sistemlerine karşı yapılan saldırıları zararlı davranışın kaynağı olarak kabul etmenin diğer yöntemlere göre faydalı bir yönü bulunmaktadır. Bu da zararlı davranışın kaynağının zararlı yazılım veya bilgisayarın başındaki bir kişi olup olmamasının bu yaklaşım açısından önem arz etmemesidir. Çalışmalara konu olan "zararlı" davranışları tespit etmek ise çoğu zaman karmaşık örüntülerin belirlenmesine dayanmaktadır. Örneğin Linux sistemlerindeki /etc/shadow ve /etc/passwd dosyalarını ele alalım. Bu dosyalar kullanıcı bilgilerinin saklandığı dosyalardır. Peki bu dosyalara erişim bilgisayar sistemine bir saldırı mıdır? Halihazırda sshd(8) ve passwd(1) gibi birçok program bu dosyalara erişim ihtiyacı duymaktadır. Kullanıcıların doğrulanması, grupların belirlenmesi ve kullanıcı bilgilerinin elde edilmesi gibi masum işlemler için de kullanılan bu dosyalara erişimin saldırı olarak nitelendirilmesi olanaklı değildir. Bu durumda şüpheli olayların değerlendirilmesi için aşağıdaki iki yaklaşımdan biri seçilebilir.

- Bütün olayları saldırı olarak değerlendirerek durumu insanlara sevk etmek
- Kayıtları ilişkilendirmek için kurallar belirlemek ve veri içerisinden çıkarım yapmaya çalışmak

Günümüzde özellikle finans, doğal dil işleme ve sinyal işleme alanlarında geliştirilen modeller ile ardışık verilerin modellenmesinde önemli gelişmeler sağlanmıştır.





Bu yaklaşımları incelemek gerekirse, ilk yaklaşım çok fazla yanlış-pozitif üretilmesine yol açacaktır. Bu da hem sistemin güvenilirliğini zedeleyecek hem de inceleyen kişilerin zamanına mâl olacaktır. Bu tip yaklaşımda bazı güvenlik ürünleri kullanıcılara tek tek olayları göstererek, kullanıcının olaya izin vermesini veya engellemesini istemektedir. Kullanıcıdan alınan bu bildirimler ile kurallarda iyileştirme yapılmaktadır. Örneğin burada ssh "daemon"ı güvenilir yazılım listesine alınabilir. Ancak kullanıcılar her zaman tekil olayları yorumlayabilecek durumda olmayabilirler. Bu nedenle iyileştirmeler bu yaklaşımı kullanılabilir kılmamaktadır.

İkinci yaklaşımda ise yaygın olarak kullanılan kayıt yönetim yazılımları, farklı kaynaklardan elde ettiği kayıtları ilişkilendirerek saldırıları tespit etmeye çalışmaktadır. Ancak kayıtlar kayıplı ve tekrarlı bilgi içerdiğinden bu tip yaklaşımlar eğreti çözümler ortaya çıkarmaktadır. Bunun yanında bu yazılımları üretmek için harcanan emeğin çoğu farklı biçimdeki verileri anlamlandırmaya çalışmak ve eldeki veri yığınını yönetmeye harcanmaktadır. Sonuç olarak üretilen yazılımda ise yine insanların oluşturacağı kurallar ile gürültülü veri üzerinde saldırılar tespit edilmeye çalışılır. Ayrıca ikinci yaklaşımda yapay zekâ kullanımıyla kuralların otomatik üretimi üzerinde çalışmalar yapılmaktadır.

Bilindiği gibi son yıllarda makine öğrenmesi çalışmalarında insan güdümlü özellik mühendisliğinin yeri azalmış bunun yerine özellikleri makinelerin öğrenebilmesi üzerine çalışmalar yapılmıştır. Çoğunlukla yapılan bu çalışmalar sayesinde yapay zekâ uygulamaları günlük hayatımızda kullanabileceğimiz kalitede ürünler ortaya çıkarabilmiştir. Buradan da anlaşılabilir ki; insan eliyle yapılan özellik mühendisliği sonucunda elde edilen verilerden yola çıkarak yorum yapmaktansa, saf verinin yorumlandığı yöntemler daha başarılı olmaktadır.

Sorular	İşletim sistemi çağrıları	Kütüphane çağrıları
Muhatabı kimdir?	İşletim sistemi çekirdeği	İşletim sistemi çekirdeği Dinamik kütüphane fonksiyonları
Nasıl tetiklenir?	Yazılım kesmesi ve işlemci komutlarıyla	Program içerisinde ilgili fonksiyonun çağırılmasıyla
Çalışması için gereken mekanizmalar nelerdir?	Kesme yönetimi ve işlemci sistem çağrı mekanizmaları	Dinamik bağlayıcı
Amacı nedir?	İşletim sisteminin sunması gereken temel özellikleri sağlamak	Yönetilebilir, iyi tanımlanmış ve basit bir arayüz sunmak; kullanıcı uzayında gerçeklenebilecek servisleri sağlamak

İşte bu noktada sistem ve kütüphane çağrılarından yararlanma ihtimali doğmuştur. Sistem çağrıları kullanıcı uygulamalarının* işletim sistemi arayüzünü oluşturduğundan, uygulamanın sistem kaynaklarına erişim taleplerini ifade etmektedir. Bu şekilde kullanıcı uzayında çalışan programlar dosya sistemi, aygıtlar ve bellek alanı gibi kaynaklara erişebilmektedir. Yazılım kütüphaneleri ise basit kullanımlı işletim sistemi arayüzü sunmak ve programlara çalışma zamanı ortamı sağlamak amacıyla oluşturulan yazılımlardır. Çoğunlukla çalışma anında işletim sistemi tarafından belleğe yüklenen dinamik kütüphaneler** olarak bulunmaktadırlar.

İşletim sistemlerinin iki temel işlevi vardır. Bunlardan ilki sahip olduğu donanım kaynaklarını yönetmektir. İkincisi ise sistem üzerinde çalışan uygulamalara arayüz sağlamaktır. Bu işlevi çoğunlukla sistem ve kütüphane çağrıları aracılığıyla yerine getirir. Bu nedenle bu çağrılar program kodunun sistem ve çalışma ortamı ile etkileşimini göstermektedir. Bir programın sırasıyla hangi dosyalara eriştiğini, hangi işlemleri başlattığını, ne şekilde bellek tahsis ettiğini ve hangi ağ arayüzleriyle haberleştiğini sisteme yapılan çağrılar üzerinden görebiliriz. Bu nedenle sistem ve kütüphane çağrıları zararlı davranışı göstermesi açısından bahsi geçen ve belirli kurallara göre oluşturulan alarmlardan daha detaylı bilgi sağlamaktadır. Programın dinamik ortamda çalıştırılması sonucunda elde edilen sistem ve kütüphane çağrı verileri ile ilgili bilgiler yan sayfadaki tabloda görülmektedir.

Sistem ve kütüphane çağrılarının benzer özelliklerinin yanında birbirlerinden farklı özellikleri de vardır. Örneğin kütüphane çağrıları birbirlerinin yerine kullanılabilir. Bir işlevi gerçekleştirebilecek birden fazla kütüphane fonksiyonu vardır. Ancak sistem çağrıları bu özelliğe sahip değildir. Bu da sistem çağrılarının kullanımını yararlı kılmaktadır.

Zararlı davranış tespitinde yaklaşımlar ve zorluklar

Zararlı davranış tespiti ile ilgili güncel uygulamalar incelendiğinde görülmüştür ki günümüzde yaygın olarak kullanılan yaklaşımlar zararlı davranış tespiti problemine tatmin edici bir çözüm bulmamaktadır. Bunun yanında sistem ve kütüphane çağrılarının zararlı davranışları tespit etmek için gereken bilgiyi barındırdığı ifade edilmiştir. Bu nedenle sistem ve kütüphane çağrı verileri kullanılarak oluşturulan modeller zararlı davranışların tespiti için kullanılmalıdır.

Sistem ve kütüphane çağrılarını kullanarak zararlı davranış tespitini hedefleyen sistemler, verileri iki açıdan ele almaktadırlar. Bunlardan ilki, farklı işlemler için verilerin ayrı olarak değerlendirilmesidir. Bu yaklaşımda her bir işlem için toplanan veri kendi özelinde değerlendirilir. Örneğin cmd.exe ve explorer.exe işlemlerinin ürettiği sistem çağrıları ayrı ayrı incelenerek ilgili işlemin zararlı davranışa sahip olup olmadığı denetlenir. Diğer bir yaklaşımda ise, işletim sistemine yapılan tüm çağrıların bir kaynak tarafından üretildiği kabul edilerek değerlendirme yapılmaktadır. Bu yaklaşımda uygulamaların sergilediği zararlı davranışın kaynağını bulmak zorlaşacaktır. Ancak zararlı davranışı sergileyen program birden fazla yazılım parçasından oluşuyor ise bu davranışı tespit etmek mümkün olabilir.

Sistem çağrı dizisi çalışma şekli itibariyle rastgele olmak durumundadır.Bunun en basit nedenlerinden biri kullanıcı yazılımı tarafından sistemden talep edilen kaynakların mevcut olmamasıdır. Bu duruma örnek olarak brk(2) veya mmap(2) çağrılarının başarısız sonuçlanması gösterilebilir. Yeterli belleğin olmadığı durumlarda çoğunlukla programın sonlandığı görülmektedir. Bu da programın dinamik davranışının çevresel etkilere göre değişebileceğini göstermektedir. Bir yandan da çok çekirdekli ve işlem parçacıklı bilgisayar sistemleri işlemlerin çalışma sırası açısından rastgele olmak durumundadır. Bu nedenle çok işlem parçacığı ile çalışan bir program için sistem çağrı dizisi farklı şekillerde oluşabilir. Ancak örüntü tanımada kullanılan uygun makine öğrenmesi algoritmalarının bu sorunların üstesinden geldiği görülmüştür.

Açıklamalar

* Kullanıcı uygulamaları, uzun adıyla kullanıcı uzayı uygulamaları çekirdek uzayı ve kullanıcı uzayı olarak ayrılan yetki bölgelerinde çalışan yazılımları sınıflandırmak için kullanılan bir terimdir. Özellikle günümüz işlemcilerinin bellek bölgelerine erişimi kısıtlayan özellikleri sayesinde gerçekleştirilen bu ayrım, işletim sistemi çekirdeğinde çalışan yazılımları korumak için kullanılan bir mekanizmadır.

** Bahsedilen yazılım kütüphaneleri yaygın olarak işletim sistemi kütüphaneleri olarak da adlandırılırlar. Örneğin Microsoft Windows kütüphaneleri olarak bahsedilen kütüphaneler Microsoft'un Windows işletim sistemleri için oluşturulmuş kütüphanelerdir. Benzer bir örneği ise GNU C kütüphanesi (glibc) olarak adlandırılan Linux kütüphaneleridir.

Kaynakça
• syscalls(2) — Linux manual page
• Programming reference for the Win32 API - https://docs.microsoft.com/en-us/windows/win32/api
• Computer Immune Systems - https://www.cs.unm.edu/~immsec

Yazılım Güvenlik Fuzz (Bulandırma) Testleri

Şerafettin Şentürk – Başuzman Araştırmacı / BİLGEM BTE

"Yazılım sistemlerinde kritik hatalar güvenlik açıklarına yol açar. Bunlara karşı yürütülen Fuzz (Bulandırma) Testleri, hem araştırma dünyasında hem de endüstride popüler bir güvenlik açığı keşif yöntemidir."

RFC 2828'de (Shirey 2000) tanımlanan güvenlik açığı, bir sistemin tasarımında, uygulanmasında, işletiminde ve yönetiminde, sistemin güvenlik politikasını ihlal etmek için yararlanılabilecek bir kusur veya zayıflıktır. Yazılım sistemlerinde kritik hatalar güvenlik açıklarına yol açar. Yazılım güvenlik açıkları, saldırganların veri yapılarını bozmasına, kötü amaçlı kod çalıştırmasına ve hattâ yazılımın çalıştığı tüm sistemi kontrol etmesine olanak tanır. Sıfır gün güvenlik açıkları gibi güvenlik açıklarına yönelik saldırılar, ciddi zararlara ve etkilere neden olabilir.

Güvenlik açıklarının neden olduğu ciddi zararlarla ilgili olarak, bilgi ve yazılım sistemlerine yönelik güvenlik açığı keşif teknikleri ile ilgili çok sayıda çalışma yapılmış, pek çok yöntem ve yaklaşım geliştirilmiştir. Diğer yöntemlerle karşılaştırıldığında, Fuzz (Bulandırma) Testi, test edeceği sistemle ilgili fazla sayıda bilgi gerektirmez ve büyük uygulamalara kolayca ölçeklendirilebilir. Bu nedenle son zamanlarda özellikle endüstride en popüler güvenlik açığı keşif yöntemi haline gelmiştir. Ayrıca, bu tip testler gerçek uygulamalar üzerinde yapılabildiğinden yüksek doğruluk oranına sahiptir.

Etkili bir güvenlik açığı tespiti ve sistem dayanıklılığı (robustness) testi yöntemi olan Tüy Testi sırasında daha fazla hata türü bulmak önemlidir. Tüy testi işleminde test edilen sistem ya da program çok fazla sayıda ve farklı stratejiler ile üretilen girdi değerleri ile sınanmaktadır ve sistemin çalışmaz hale geldiği durumlar bulunmaktadır. Özellikle rasgele üretim, mutasyona dayalı veya sistem gramerine göre model bazlı girdi üretim yöntemleri ile sisteme girişte geçerli olacak, yani sisteme giriş kapısının daha ilkinden çeşitli doğrulama yöntemleri sonucunda elenmeyecek, fakat sisteme girdikten sonra sistemi çalışmaz hale getirebilecek hataları bulan bir girdi üretimi, tüy testi süreçlerinin ana amaçlarındandır.

Ek olarak, bu tip bir zafiyet ve dayanıklılık tespit sisteminde daha spesifik olarak güvenlikle ilgili sorunları ve hataları bulmak oldukça önemlidir. Diğer yandan, yapılan bu testler ile bilgi sızıntılarının, zamanlama veya enerji ile ilgili yan kanal güvenlik açıklarının keşfi aktif bir araştırma konusudur. Ayrıca sistemlerde yetki artırmayı, uzaktan kötücül kod çalıştırmayı ve diğer güvenlik açıklarını otomatik olarak algılayıp bunları tetikleyen yeni teknikler de olmalıdır.

Fuzzingin Tarihi

İlk Fuzzing (Bulandırma Testi) aracı Miller ve arkadaşları tarafından 1990 yılında geliştirilmiş ve UNIX araçlarının güvenilirliğini test etmek için tasarlanmıştı. İlk tüy testlerinin üzerinden yaklaşık 30 yıl geçti ve geçen süre zarfında bu test yaklaşımında her zamankinden daha sofistike hale gelen teknikler geliştirildi. İlk test yaklaşımı tipik olarak rasgele üretilen mutasyonlara dayalıydı. Bu yüzden, geliştirilen bu sistemin erken dönemleri, ürettikleri sonuçlar açısından biraz verimsizdi. Bu nedenle, zamanla verimliliği artırmak adına yeni teknikler ve daha modern yaklaşımlar ortaya çıkmıştır.

Fuzzingin genel bir tarihçesine bakıldığında, dönemlere göre gelişimi görülebilmektedir:

√ 2005 yılından önce, sadece temel rasgele mutasyona dayalı Fuzzing vardır. Bir süre sonra testlerin etkinliğini artırmak için Gramer tabanlı Fuzzing uygulanmaya başlanmıştır.

√ 2006 ve 2010 yılları arasında Beyaz Kutu Fuzzing ve Dinamik Sembolik çalıştırma yaklaşımları geliştirilmiştir. Buna paralel olarak, Bozulma Analizi (Taint Analysis) teknikleriyle ilgili bazı çalışmalar da kullanılmaya başlanmıştır.

√ 2011-2015 yılları arasında yine verimliliği artırmak adına Kapsam Yönlendirmeli (Coverage Guided) Fuzzing ve Çizelgeleme Algoritmaları kullanılmaya başlanmıştır.

√ 2016-2017 yılları ve sonrasında birden fazla Fuzzing tekniğinin bir arada karma olarak kullanılması yaygın hale gelmiştir. Testlerde etkililiği ve doğruluğu artırmak için fuzzing sürecinde makine öğrenimi yaklaşımları da devreye girmiştir. Diğer yandan gri kutu testleri, sistemi hem endüstride hem de akademide kullananların çoğunluğu tarafından büyük ilgi görmeye başlamıştır.

"1990'lı yıllarda ismi duyulan Fuzz (Bulandırma) Testleri ile yazılımlar, çok fazla sayıda ve farklı stratejiler ile üretilen girdi değerleriyle sınanmakta ve sistemin çalışamaz hale geldiği, güvenlik zafiyeti gösterdiği noktalar saptanmaktadır."

Bulandırma Testleri Sınıflandırması

Bulandırma testi teknikleri, farklı bakış açıları açısından sınıflandırılabilir: Bulandırma testi teknikleri, hedef sistem hakkında bilgi sahibi olma açısından kara kutu, beyaz kutu, gri kutu olmak üzere üç farklı gruba ayrılabilir. Teknikler girdi verisi oluşturma türüne göre de iki grupta sınıflandırılabilir; bu gruplar mutasyon temelli ve nesil tabanlı testlerdir. Geri bildirim türüne göre ise, tüy testi teknikleri, geri bildirimli ve geri bildirimsiz sistemler olarak tanımlanmaktadır.

Kara Kutu Testleri

Kara Kutu Bulandırma Testleri, test edilen programın dâhili iş mantığıyla ilgilenmemektedir. Bu tip sisteme girdiler verilir ve verilen girdilere karşılık gelen çıktılar toplanarak incelenir. Özellikle mutasyonel kara kutu testlerinde, süreç bir veya daha fazla tohum girdisi adı verilen veri kümeleri ile başlatılır. Tohumlar daha sonra yeni girdiler oluşturmak için değiştirilir, yani mutasyona uğratılır. Girişteki veri üzerinde seçilen rasgele konumlara rasgele mutasyonlar uygulanabilir.

Örnek vermek gerekirse, giriş verisi bir dosya olan sistemde, dosya girdisindeki mevcut olan rasgele bitler çevrilip yerleri değiştirilerek yeni girdi dosyaları üretilir ve sisteme yeniden çalıştırması için verilir. Mutasyon tabanlı kara kutu testlerindekinden farklı olarak bir diğer test çeşidi olan nesil tabanlı kara kutu tüy testlerinde ise girdiler sıfırdan üretilir. Test edilecek sistemin kabul ettiği girdilerin biçimsel olarak yapısal özellikleri, yani bir deyişle gramer bilgileri verilirse, girdi dilbilgisi biçimine uygun olacak bir biçimde yeni girdiler oluşturularak tüy testleri sürdürülür.

Beyaz Kutu Testleri

Beyaz Kutu Bulandırma Testleri test edilen programın iç bileşenlerini bilir. Bu tip testlerde, test edilen sistemin kaynak kodu hakkında bilgi, ayrın-

tılı çalışma zamanı bilgileri ve programın tasarımı hakkında bazı veriler bilinmektedir. Beyaz kutu testleri, sembolik yürütme adı verilen bir tekniğe dayanmaktadır. Bu teknik, program yollarını sistematik olarak numaralandırmak için program analizi ve kısıtlama çözücüleri kullanmaktadır.

Beyaz kutu bulandırma testleri sisteme verilen bir girdi verisinin yol koşulunun hesaplamasını yapar; yani verilen girdi ile sistem içerisinde kodsal olarak nerelere gidileceği, nasıl bir yol izleneceği sembolik olarak bilinebilmektedir. Buradan yola çıkarak sistemde hesaplanan yol koşulları, mutasyon tabanlı yöntemlerle değiştirilerek sisteme daha sonraki test adımlarında ne tip veriler girilmesi açısından yönlendirici olmaktadır. Bununla birlikte, beyaz kutu tüy testlerindeki en büyük sorunlardan bir tanesi yol patlaması (Path Explosion) problemi olarak adlandırılan sembolik yürütme sorunlarıyla ilgilidir. Bunun nedeni, hedef programdaki koşullu dalların genellikle çok sayıda olmasıdır; küçük boyutlu bir uygulamada bile çok sayıda yürütme yolu üretilebilir. Dolayısıyla, orta ve büyük ölçekli uygulamalarda beyaz kutu testleri çalıştırıldığında sistemde gidilmesi gereken tüm olası yollar zamanla çok fazla artacağı için, her birinin çalıştırılması sistemin performansı açısından neredeyse olanaksız hale gelmektedir.

Gri Kutu Testleri

Gri kutu bulandırma testleri, test edilen program hakkında kısmi bilgiler içeren yazılım hatalarını etkili bir biçimde bulabilmek için kara kutu ve beyaz kutu testlerinin ortasında bir yerdedir. Gri kutu testlerde yaygın olarak kullanılan yöntem kod enstrümantasyonudur. Bu tür enstrümantasyonla, gri kutu test aracı, çalışma zamanında hedef programın kod kapsamını elde edebilir; bu bilgiyi, örneğin, genetik algoritmalar yardımıyla mutasyon stratejilerini güncellemek ve daha fazla yürütmeyi kapsayabilecek test senaryoları oluşturmak için kullanır. Gri kutu tüy testleri yardımıyla Google, Chrome tarayıcısında sekiz yıllık bir süre içerisinde 16.000'den fazla hata ve üç yıl boyunca 160'ın üzerinde açık kaynaklı yazılım projesinde 11.000'den fazla hata tespit etmiştir [1].

Bununla birlikte, AFL (American Fuzzy Lop) adıyla bilinen ve yaygın kullanımı olan gri kutu tüy testi aracında, yol kapsama bilgisi gibi çalışma zamanı bilgileri ikili enstrümantasyonla toplanır. Bu bilgiler, test senaryosu oluşturma sürecine rehberlik etmesi için Test Durumu Üretme Modülüne aktarılır. AFL aracının bulduğu hatalar, genellikle programın çökmesine neden olan veya korsanlar tarafından istismar edilebilen arabellek taşması, erişim ihlali, yığın parçalama gibi bellek işlemleriyle ilgilidir.

Bulandırma Testi Uygulama Alanları

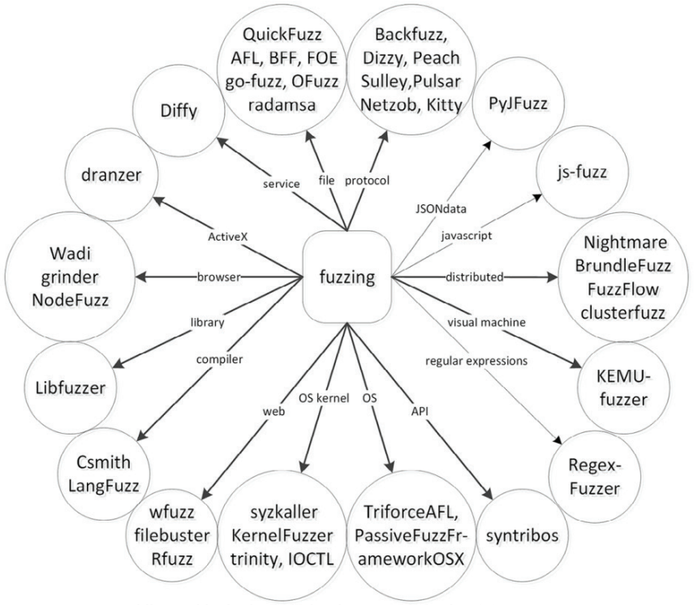
Bulandırma Testleri, girdi verisi olarak dosya alan sistemler, işletim sistemi çekirdeği, protokoller, API'lar, web uygulamaları, ActiveX uygulamaları, sanal makineler, web tarayıcıları, JSON verileri, Javascript derleyiciler, dağıtılmış sistemler gibi birçok farklı uygulama alanında yürütülebilir. Yaygın olarak komut satırı araçlarında, dosya ayrıştırıcılarında yapılan tüy testlerinin yanı sıra, çevre ile etkileşimde olan siber-fiziksel sistemlerde ve IoT platformlarında yapılan tüy testi çalışmaları da son zamanların ilgi odağı haline gelen çarpıcı konulardandır. Ayrıca, davranışları eğitim verileriyle belirlenen makine öğrenimi sistemleri üzerinde devam eden bulandırma testi çalışmaları da mevcut olup, bir girdi için çeşitli çıktılar üretebilen protokol uygulamalarında durum bilgili yazılımın nasıl test edilebileceği gibi konularda zorluklar ve açık problemler de bulunmaktadır. Olaylar dizisi olarak girdiler alan GUI tabanlı sistemlerin testleri de bir diğer çözüm bekleyen zor problemler arasındadır.

Tüy Bulandırma yapılan başlıca uygulama alanlarından bir tanesi de dosya formatı testleridir. Dosya formatı tüy testlerinin önemli bir alt alanı da web tarayıcılarında yapılan testlerdir. Tarayıcılar tarafından işlenen dosya türleri, HTML, CSS, Javascript dosyaları olarak öne çıkmaktadır. Özellikle, tarayıcıların DOM yapılarının ayrıştırılması ve sayfaların görüntülenmesi şu anda bulandırma testi yapılan popüler alanlardır. Web tarayıcılarına yönelik iyi bilinen tüy testi araçları, Grinder çerçevesi altında COMRaider ve BF3'tür. Diğer yandan, ağ sistemlerinde kullanılan protokol testleri de çarpıcı tüy testi alanlarındandır.

Protokol üzerinde yapılan testlerin zor kısmı, servislerin kendi haberleşme protokollerini belirleyebilmesidir. Ayrıca, bu tip protokollerin standartlarının belirlenmesi de zordur. Dahası, tanımlı dokümante edilmiş protokoller için bile RFC dokümanı gibi spesifikasyonları takip etmek hâlâ zor bir iştir. Bazı temsili protokol tüy testi araçlarına örnek vermek gerekirse; SPIKE, AutoFuzz, ve SNOOZE bu alanda sık kullanılanlar arasındadır. SPIKE, ağ protokolü stres testlerini hızla oluşturabilir. AutoFuzz, Sonlu Durum Otomatı oluşturarak protokol uygulamasını öğrenebilir ve öğrenilen bilgileri test senaryoları oluşturmak için daha fazla kullanabilir. SNOOZE aracı ise durum bilgisine dayalı bir tüy testi yaklaşımı ile protokol kusurlarını tanımlayabilir.

Bulandırma Testlerinin Geleceği

İlk ortaya çıktığı yıllarda sadece bir kara kutu testi ve rasgele girdi üretimi ile kendisini gösteren bulandırma testleri, daha sonraki yıllarda, sistemlerde mevcut olan ve bilinmeyen hataları bulmadaki verimliliğini artırmak adına birçok farklı teknik ile bir arada kullanıldı. Özellikle son yıllarda farklı bulandırma testi yaklaşımlarının karma olarak bir arada kullanılması popüler bir hale geldi ve bir süre daha bu şekilde gideceği açıktır. Bununla birlikte tüy testlerinin daha akıllı hale gelmesi, sistemlerde bilinmeyen ve daha derinlerde saklı hataları daha fazla sayıda bulabilmesi için makine öğrenimi ve derin öğrenme yöntemleri sıcak bir gündem olarak kendini göstermektedir. Bu şekilde etkinliği, bilinirliği ve verimliliği artan tüy testlerinin kullanımı, son yıllarda önemi giderek artan IoT uygulamalarında, kritik altyapı özelliği gösteren sistemlerde, otonom araçlarda ciddi anlamda artış göstermektedir.

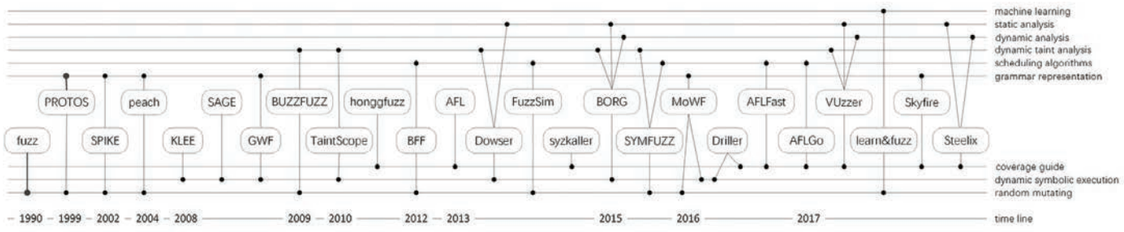


Şekil1. Farklı alanlarda bulandırma testi araçları (2).

Kaynakça

[1] M. Böhme, C. Cadar and A. Roychoudhury, "Fuzzing: challenges and reflections," IEEE Software, vol. 38, no. 3, pp. 79 186, May June 2021.

[2] C. Chen et al., "A systematic review of fuzzing techniques," Computers & Security, vol. 75, pp. 118 137, June 2018.



Şekil 2.Test araçlarında verimliliği artırıcı yardımcı teknikler (2).

Bilgi Güvenliği Risk Yönetimi

> Risk, iş hedeflerine ulaşılmasını olumsuz etkileyebilecek her türlü olaydır.

Sabri Safa Paksu - Başteknisyen, Rumeysa Bozdemir - Teknisyen / BİLGEM İGBY

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı ve Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi, risk yönetimi stratejileri için ihtiyaç ve gereksinimleri ele alır. Kurum ve Kuruluşlarda bilgi güvenliği süreçlerinin yürütülebilmesi için bu dokümanların dikkate alınması gereklidir.

Ayrıca BİLGEM kapsamında bilgi güvenliği risk yönetiminin değerlendirildiği ve uygulandığı BGYS Risk Değerlendirme Kılavuzu'nda konu ile ilgili tüm bilgilendirmeler mevcuttur. Bilgi güvenliğinin 3 temel unsuru aşağıda maddeler halinde belirtilmiştir. Bu unsurlar varlık değerini belirlerken riskin değerine de etki etmektedir.

- **Gizlilik:** Bilginin sadece yetkili kişilerce erişilebilir olmasının sağlanmasıdır.
- **Bütünlük:** Bilginin yetkisiz kişiler tarafından değiştirilmemesidir. Bulunduğu ya da iletildiği ortamda içeriğinin bozulmama özelliğidir.
- **Erişilebilirlik:** Bilginin ihtiyaç duyulduğunda yetkili kişilerce kullanıma hazır durumda olmasıdır.

Risk Nedir?

Risk, iş hedeflerine ulaşılmasını olumsuz etkileyebilecek her türlü olaydır. Riskler zamana bağlı olarak değişir. Risklerin birçok boyutu vardır. Çoğu zaman riskler tehdit odaklı yazılır fakat beraberinde fırsatlar da oluşturur.

Risk Yönetimi Nedir?

Bilgi güvenliği risk yönetimi bilgi teknolojisinin kullanımıyla ilişkili riskleri yönetme sürecidir. Bir kuruluşun varlıklarının gizliliği, bütünlüğü ve kullanılabilirliği ile ilgili risklerin tanımlanmasını, değerlendirilmesini ve ele alınmasını içerir. Bu sürecin nihai amacı, riskleri bir kuruluşun genel risk toleransına göre ele almaktır. İşletmeler tüm riskleri ortadan kaldırmayı beklememelidir. Bunun yerine, kuruluşları için kabul edilebilir bir risk seviyesi belirlemeye ve belirlenen risk aralığında kalmaya çalışmalıdırlar.

Bilgi Güvenliği Risk Yönetimi Sürecinin 5 Önemli Adımı

Siber suçları önlemek ve iç tehditleri durdurmak zorlu bir süreçtir. Kurumsal risk yönetiminize gizlilik, bütünlük ve erişilebilirlik kavramlarını dahil etmek, etkili bir bilgi güvenliği risk yönetiminin temelini oluşturur. Bu yapı kuruluşunuz, çalışanlarınız ve paydaşlarınız için çok önemli bir süreçtir. Risk yönetim sürecinizi oluşturmak ve bilgi güvenliğini bir iş haline getirmek için stratejik adımlar atmak ve bu adımları bir süreç şeklinde uygulamak gerekmektedir. Bu süreç ISO 27005

> Kuruluşlar tüm riskleri ortadan kaldırmayı beklememeli, kabul edilebilir bir risk seviyesi belirlemeye ve belirlenen risk aralığında kalmaya çalışmalıdır.

Bilgi Güvenliği Risk Yönetimi standardı dikkate alınarak yönetilir.

1.Tanımlama

Varlıkların Tanımlanması

Kuruluşlarda hangi verilerin, sistemlerin ve diğer varlıkların önemli / kritik kabul edileceğinin belirlenmesi gerekir. Bu kapsamda "hangi varlıkların gizliliği, bütünlüğü veya erişilebilirliği tehlikeye girerse kuruluşunuza en büyük etkiyi verir?" sorusunun cevabını aramalıyız. Kimlik numaralarına kötü niyetli kişilerin ulaşması, finans sektöründeki bir firmanın hazırladığı rapordaki küçük bir bütünlük sorununun yüksek maliyetle sonuçlanması, çevrimiçi müzik hizmeti veren bir firmanın erişilebilirliği tehlikeye girdiğinde abone kayıplarına neden olabileceği düşünüldüğünde gizlilik, bütünlük ve erişilebilirlik kavramlarının hayatımızın içinde yer edindiğini görüyoruz. İşte bu sebeple hangi varlıkların ne derecede önemli olduğunu tanımlamamız ve buna göre değerlendirme yapmamız gerekiyor.

Güvenlik Açıklıklarının Tanımlanması

Tanımladığınız varlıklar üzerinde gizlilik, bütünlük ve erişebilirliği riske atan yazılımsal ve diğer sistemsel güvenlik açıklıklarının belirlenmesi gerekiyor. Bu süreçte hangi zayıflıkların ve/veya eksikliklerin bilginin tehlikeye atılmasına neden olabileceğinin araştırılması bu tanımlamayı kolaylaştıracaktır.

Tehditlerin Tanımlanması

Varlıkların veya bilginin tehlikeye atılmasının olası nedenlerinin belirlenmesi gerekiyor. Bu kapsamda şu soruları sorabiliriz: "kuruluşun bağlı olduğu veri merkezleri sel ve deprem gibi fiziksel / çevresel tehditlerin bulunduğu bölgelerde mi konumlandırılmış?", "kuruluştaki çalışanlar bilinen bir suç örgütü, bilgisayar korsanları veya bazı kuruluşlar tarafından hedefleniyor veya saldırıya uğruyor mu?"

Tehdit modellemesi, riskleri bilinen tehditlerle ilişkilendirir. Yapısal güvenlik açıkları gibi potansiyel tehditlerin varsayımsal bir saldırganın bakış açısından tamamlanabileceği, sayılabileceği ve önceliklendirilebileceği önemli bir süreçtir. Buradaki amaç, kuruluşlara olası tehdit profilini, en muhtemel saldırı vektörlerini ve bir saldırgan ta-

rafından en çok istenen varlıkların sistematik bir şekilde analiz edilmesini sağlamaktır.

Kontrollerin Tanımlanması

Kuruluşunuzda tanımladığınız varlıklarınızı korumak adına hali hazırda nelere sahip olduğunuzu öncelikle belirlemeniz gerekiyor. Bu kapsamda gerçekleştireceğiniz bir denetimle tanımlanmış bir güvenlik açığını, tümüyle düzelterek (iyileştirme), riskin olasılık ve/veya etki değerlerini azaltarak (azaltma) doğrudan ele alabilirsiniz. Örneğin; Sözleşmesi feshedilen bir kullanıcının belirli bir uygulamaya erişiminin devam etme riskini belirlediyseniz, bu kapsamdaki kontrolünüz kullanıcının feshi ile tetiklenen bir otomatik yetki kaldırma işlemi olabilir.

Telafi edici bir kontrol, riski dolaylı olarak ele alan bir güvenlik kontrolüdür. Aynı örnekten devam edersek; Telafi edici bir kontrol, üç aylık bir erişim inceleme süreci olabilir. Bu inceleme sırasında uygulamaya giriş yetkisi olan kullanıcılar kontrol edilerek, yetkisi olmaması gereken kullanıcılar tepkisel olarak kaldırılır. Bu süreç kuruluşun kullanıcı listesi ile feshedilen kullanıcı listesinin çapraz kontrolü ile gerçekleştirilir.

Çıktılar

Yukarıda belirtilen tanımlamalar sonucunda ortaya çıkacak varlık, açıklık ve tehdit listeleri ile risk tanımlamaları yapılarak kuruluşun risk listesi oluşturulur.

2. Analiz Etme

Risk Analizi, varlıkların kritikliğine, bilinen güvenlik açıklıklarının kapsamına ve kuruluşta yaşanan önceki olaylara bağlı olarak değişen detaylarda gerçekleştirilebilir. Bir risk analizi metodolojisi, koşullara bağlı olarak nitel, nicel

> **Kurumsal risk yönetimine gizlilik, bütünlük ve erişilebilirlik kavramlarını dâhil etmek, etkili bir bilgi güvenliği risk yönetiminin temelini oluşturur.**

veya ikisinin de kombinasyonu olabilir. Nitel analiz daha çok gözleme dayalı, sayısal olarak ölçülemeyen özelliklere ilişkin bir analiz türüdür. Öte yandan nicel analiz ise daha çok istatistiksel olarak değerlendirilen ve analiz edilen yöntemleri kapsamaktadır. Nitel analiz yöntemi, nicel analiz yöntemine göre daha az karmaşık ve daha ucuz bir yöntemdir. Analiz şekli, bağlamı oluşturmanın bir parçası olarak geliştirilen risk değerlendirme kriterleriyle tutarlı olmalıdır.

3. Değerlendirme

Risk değerlendirmesi "varlıklar", "güvenlik açıklıkları" ve "kontrollerin" bir araya getirilmesidir. Risk değerlendirmesi kuruluşunuzdaki riskleri sıralamanıza ve risklerin önem derecesini belirlemenize olanak sağlamaktadır. Hangi riskleri öncelikli olarak ele alacağınız konusunda size yardımcı olacaktır. Risk değerlendirmesi rakamlarla değil mantıksal yapılarla ilgili olsa da, bunu bir formül şeklinde göstermemiz gerekiyor. Bu formüller kuruluşların neyi değerlendirmeye almak istediğine göre şekillenebilir. Genelde kullanılan formül şu şekildedir:
Risk = (Tehdit x Güvenlik Açığı (Olasılık x Etki) x Varlık Değeri) - Güvenlik Kontrolleri

4. Tedavi Etme

Bir riski değerlendirip analiz ettikten sonra, kuruluş bu riskin tedavi sürecini başlatmalıdır ve bu süreçte her risk için aşağıdaki tedavi seçeneklerinden biri seçilmelidir.

Riski İyileştirme: Riskin olasılık ve etki değerlerinin tümüyle ortadan kalkması diyebiliriz. Bu maddeye kritik verilerin depolandığı bir sunucuda bulunan açıklığın yayınlanan bir yama ile giderilmesi şeklinde örnek verilebilir.

Riski Azaltma: Riskin olasılık ve etkisini azaltmak için kullanılan risk tedavi tekniğidir. Bu teknik seçildiğinde riskin mevcut seviyesinden kabul edilebilir risk seviyesine getirilmesi amaçlanır.

Riski Kabul Etme: Riskin olasılık ve etkisinin düşük olduğu ve risk maliyetlerini düzeltmek için gereken zaman ve çabanın, riskin gerçekleşmesi durumunda oluşacak maliyetlerden daha fazla olduğu durumlarda uygundur. Bu durum yapılan risk değerlendirmesi sonucunda, önceden belirlenmiş kabul edilebilir risk seviyesinin altında kalan riskler için değerlendirilebilir.

Riski Transfer Etme: Riskin kabul edilebilir risk seviyesinin altına düşürülmesi mümkün olmadığında veya bunu gerçekleştirmek için gereken kontrollerin uygulanması yüksek maliyet gerektirdiğinde, riskin üçüncü bir tarafa transferi ele alınır. Örneğin; Bir varlık için sigortalama işlemi verilebilir. Bu yöntem tercih edildiğinde güvenlik ihtiyaçlarının, kontrol hedeflerinin ve ilgili kontrollerin sözleşmelerde yer almasına dikkat edilir.

Riskten Kaçınma: Riskli kabul edilen varlığı kullanmaktan vazgeçerek riskten kaçınmak mümkün olabilir. Bu yaklaşım sonucunda riski oluşturan sebep ortadan kalkar. Bir yazılımın risk oluşturan kısmının yüklenmemesi, belirli işlemler için internetin kullanılmaması riskten kaçınma için verilebilecek örneklerdir. Riskten kaçınma seçeneği düşünülürken iş gereksinimleri ve güvenliğin sağlanması konusunda bir denge sağlanmalıdır. İş süreçlerinde ciddi değişiklikler getirecek ve/veya kuruluşun çalışmasını olumsuz etkileyecek şekilde riskten kaçınma metodu uygulanmamalıdır.

5. İzleme ve Gözden Geçirme

Bilgi Güvenliği Risk Yönetiminin benimsenmesi, varlıklarınıza güvenli bir ortam sağlamak için kritik öneme sahiptir. Bu nedenle sürekli izleme ve gözden geçirme çok önemlidir. Kötü niyetli kişi ve kuruluşlar, ağınıza ve bilgi varlıklarınıza saldırmak için her gün, her saat yeni yöntemler geliştirmektedirler. Bu saldırılara ayak uydurmak ve tedbirlerinizi buna göre belirlemek için varlıklarınızı, tehditlerinizi, kontrollerinizi ve risklerinizi sürekli olarak gözden geçirmelisiniz.

Kaynakça
- ISO 27005 Bilgi Güvenliği Risk Yönetimi Standardı
- BİLGEM BGYS Risk Değerlendirme Kılavuzu
- https://www.rapid7.com/fundamentals/information-security-risk-management/
- https://www.isaca.org/resources/isaca-journal/past-issues/2010/developing-an-information-security-and-risk-management-strategy
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
- https://en.wikipedia.org/wiki/IT_risk_management

Oturum Yönetimi

> "Oturum bilgisi, günümüz uygulamalarının istemcileri tanımak için kullanmış oldukları bir bilgidir."

Ufuk Yenigün – Uzman Araştırmacı, M. Sabri Elmastaş - Araştırmacı, M. Sadık Karabay - Araştırmacı,
Abdullah Özkan - Uzman Araştırmacı / BİLGEM İGBY

Oturum bilgisi, günümüz uygulamalarının istemcileri tanımak için kullanmış oldukları bir bilgidir. Uygulamada kimlik doğrulama işlemi gerçekleştirilirken kullanıcı adı ve parola kullanılır. Hedef uygulama size başka kimseye verilmeyecek bir SessionID (oturum anahtarı) verir. Daha sonra browser (tarayıcı) yapılan her istekte bu anahtarı göndererek istemcinin kim olduğunu bildirir ve sunucu da bu bilgiye göre gelen isteği değerlendirir. Bu bilginin taşınması da cookie (çerez), URL veya gizli form elemanları ile sağlanabilir. Oturum anahtarının en yaygın taşıma yöntemi olan Cookie' nin işleyiş süreci aşağıdaki şekilde belirtilmiştir.

Kimlik doğrulama isteğinden sonra sunucu tarafından verilen oturum bilgisi Cookie bilgisi istemcinin tarayıcısında saklanır. Bu değer aynı zamanda www.example.com üzerinde bulunan Cookie Storage alanında da tutulacaktır. Dolasıyla kullanıcı www.example.com 'a istek gerçekleştirdiği anda ilgili domain için bulunan Cookie de gerçekleştirilen isteğe tarayıcı tarafından eklenir. Cookie değeri için her bir GET/POST isteğine Cookie: Cookies=12345 gibi bir başlık eklenerek gönderilir(bkz Resim 1.1). Bu kullanım, web uygulamalarında en yaygın oturum bilgisi taşıma yöntemidir.

Oturum bilgisinin yukarıdaki şekilde kullanılmasının en önemli nedeni ise HTTP protokolünün yapısından kaynaklanmaktadır. Çünkü bu protokol üzerinden gerçekleştirilen isteğe cevap geldikten sonra aradaki tüm bağlantıları sonlanır. Bu nedenle bir sonraki istekte uygulamanın istemciyi tanıyabilmesi için oturum bilgisini tekrar göndermesi gerekir.

Oturum Anahtarı

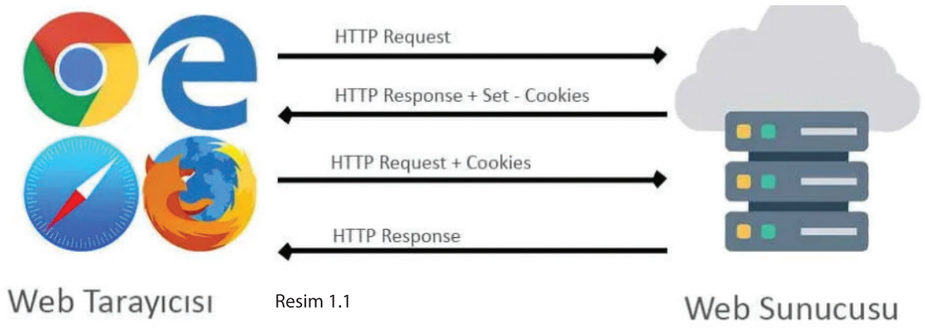
Oturum anahtarları uygulamalar tarafından benzersiz olarak tasarlanıp kullanıcılara atanan bir değerdir. Resim 1.1'de görüleceği üzere oturum anahtarı Cookie üzerinden taşınır. Bu değişken uygulamadan uygulamaya farklılıklar gösterebileceği gibi kullanılan uygulama çeşidine göre varsayılan oturum anahtarı değişkenleri de bulunabilir (PHPSESSID, JSESSIONID, ASP.NET_SessionId). Günümüz uygulamalarının birçoğunda oturum anahtarı, kullanılan programlama dillerinin varsayılan kütüphaneleriyle veya kullanılan uygulama geliştirme platformları (framework) ile oluşturulmaktadır. Fakat kendi oturum anahtarını oluşturmayı tercih eden uygulamalar da görülebilmektedir. Bununla birlikte uygulama geliştirme platformları tarafından varsayılan olarak sağlanan uygulama anahtarına ilave olarak ek özelleştirilmiş oturum anahtarları da kullanılabilmektedir.

Zayıf Oturum Anahtarları

Daha önce verilen örneklerde de görüleceği üzere oturum anahtarı belli uzunlukta bir karakter kümesidir. Bu karakter kümesinin uzunluğunun yeterli uzunlukta olmaması veya kullanılacak küme elemanlarının yeterli karakter seçiminden oluşmaması gibi durumlar oturum anahtarlarının kolayca tahmin edilmesine dayanan zafiyetleri de beraberinde getirmektedir. Zayıf oturum anahtarına örnek Resim 1.2'de belirtilmiştir. Resim 1.2' de tespit edilen zafiyet, oturum anahtarının yeterli uzunlukta olmamasıdır. Bununla birlikte oturum anahtarını oluşturan elemanların sadece sayılardan oluşması kolay tahmin edilmesine yol açar.

Cookie Özellikleri

Cookie'ler oturum anahtarının taşınmasında ve istemcide saklanmasında yaygın olarak kullanılan yöntemdir. Oturum anahtarlarının hem gü-



Resim 1.1

Resim 1.2

venli taşınması hem de güvenli saklanması için Cookie'ler farklı özel parametreler sunarlar.

Secure Özelliği
Genel olarak tarayıcılar Cookie gönderirken özel bir tanımlama yok ise oturum anahtarını http kullanarak gönderirler. Bu durum ağ trafiğini dinleyen saldırganlara trafiği açık olarak izleme olanağı tanır. Bu durumun oluşmaması için HTTPS üzerinden gönderilerek "Secure" özelliği aktif edilmelidir.

Httponly Özelliği
Cookide taşınan bilgiler istemci tarafında Javascript dili kullanılarak değiştirilebilmektedir. Özellikle XSS saldırılarında karşılaşılmaktadır. HttpOnly özelliği aktif edilirse cookilere javascript dili kullanılarak erişilemez.

Cookie oluşturulurken kullanılan domain ilişkili Cookie bilgisine hangi domainlerden erişim yapılabileceğini gösterir. Tarayacılar domain bilgisinde belirtilen kapsamdaki tüm domain'lere, istekler içinde geçen Cookie bilgisini otomatik olarak gönderirler. Aynı zamanda alt domain'ler istemci taraflı scripting dilleri ile bu Cookie değerine de erişim sağlayabilirler. Eğer Cookie için domain tanımı geniş tutulursa, tüm alt domain'ler atanmış Cookie değerine erişim yapabilir. Bu durum Cookie içinde bulunan oturum anahtarının risk

> **Oturum anahtarları, uygulamalar tarafından benzersiz olarak tasarlanıp kullanıcılara atanan değerlerdir.**

altına girmesine neden olur. Dolayısıyla Cookie oluştururken eğer ihtiyaç yok ise sadece belirtilen domain veya alt domain (subdomain) için Cookie kullanımı tercih edilmelidir.

Path özelliği de domain'e benzemektedir. Eğer aynı domain içinde farklı klasörlerde iki uygulama var ise ve Cookie değerlerinin karışmaması için Path =/dashboard-1 ve Path=/dashboard-2 gibi kullanılması gerekmektedir. Özellikle yönetim panelleri bu tür yapılarda bulundurulabilir. Bu nedenle yönetim panelleri için kullanılan Cookie değerlerinin ilgili Path'ler için atanması doğru bir yol olacaktır.

Expires Özelliği
Cookie'de bulunan Expires değeri ile Cookie içerisinde bulunan değerlerin yaşam süresi belirlenir. İstemciler bir internet sayfasına istek gerçekleştirdiğinde belirtilen Domain ve Path için Cookie değerinin olup olmadığına bakar. Eğer ilgili bilgiler için bir Cookie değeri var ise tarayıcı Expires değerini kontrol eder. Expires değeri istek yapılan zamanın ilerisinde ise Cookie değerini ekleyerek isteği gerçekleştirir.

Cookie'ler yaşam süresine göre iki çeşide ayrılır.
Session Cookie: Herhangi bir Expires veya Max-Age değeri atanmamış Cookie'lerdir. Bu Cookie'ler oturum açılınca bellekte tutulur ve tarayıcı kapatılınca bellekten silinirler.

Persistent Cookie: Bu tür Cookie' lerin Expires veya Max-Age değerleri atanmıştır. Dolayısıyla Cookie tarayıcı kapatılsa bile tarayıcının Cookie depolama alanında saklanır ve Expires ile belirtilen zamandan önce tekrar istek yapılır ise bir önceki Cookie değeri de sunucuya gönderilir.

Httponly Özelliği

```
Set-Cookie: JSESSIONID =SAe2B5t7altgedadfc12nvbi681; domain=test.local; path=/; httpOnly
```

Httponly Özelliği

```
Set-Cookie: JSESSIONID =SAe2B5t7altgedadfc12nvbi681; domain=test.local; path=/ dashboard;
httpOnly
```

Expires Özelliği

```
Set-Cookie: JSESSIONID =SAe2B5t7altgedadfc12nvbi681; domain=test.local; path=/ dashboard;
httpOnly ; expires=Sun, 13-02-2021 08:25:01 GMT
```


Güvenli Oturum Yönetimi Nasıl Olmalıdır?
Oturum Anahtarı İsmi
Oturum anahtarının ismi, kullanıcıya herhangi bir bilgi vermemelidir. PHPSESSIONID (PHP), JSESSIONID (J2EE), CFID ya da CFTOKEN (ColdFusion), ASP.NET_SESSIONID (ASP.NET) gibi uygulama geliştirme platformu hakkında bilgi veren oturum anahtarları bulunmaktadır. Bu isimler yerine genel bir ifade ile "id" olarak isimlendirilerek kullanılmalıdır.

Oturum Anahtarı Boyutu ve Entropisi
Kaba kuvvet saldırılarından kaçınma amaçlı oturum anahtarı boyutunun yeterli boyutta olması gerekmektedir. Günümüzde 128 bit uzunluklu anahtarlar yeterli gelmektedir. Oturum anahtarları tahmin edilebilir yapıda olmamalıdır. Her hangi bir istatistik veya korelasyon ile tespit edilememelidir. Yeterli karmaşıklıkta olmalıdır.

Oturum Anahtarı Değeri
Oturum anahtarı değeri ve içeriği her hangi bir anlam ve bilgi ifade etmemelidir. Bilgi ifşasına neden olacak bir değer olmamalıdır.

Oturum Anahtarı Üretimi
Oturum anahtarları üretilirken, rastgele sayı üreteçleri kullanılıp özetleri (hash) alınmalıdır. Her giriş esnasında yeniden üretilmelidir.

Güvenli Cookie Oluşturmak
Cookie'lerin özellikleri yardımı ile oturum anahtarının güvenliği amaçlanmaktadır. Dolayısıyla güvenli bir Cookie için aşağıdaki özelliklerin sağlanması gerekir.

- Güvenli iletişim (HTTPS) kullanan uygulamalarda da Secure özelliği aktif edilmelidir.
- HTTPS üzerinden gelmeyen HTTP üzerinden gelmesi sebebiyle meydana gelebilecek MITM ataklarını engellemek için de 'HTTP Strict Transport Security (HSTS)' kullanılmalıdır.
- İstemci taraflı scripting dillerine erişimin kapatılması için HttpOnly özelliği aktif edilmelidir.
- Gerekmedikçe Persistent Cookie kullanılmamalıdır.
- Bir Cookie'nin sadece belirtilen uygulamalarda kullanılması için Domain ve Path bilgileri sadece uygulamaya özgü bilgiler (uygulamanın çalıştığı Domain ve Path) ile doldurulmalıdır.
- Cookiler her zaman cookie bölümünde taşınmalıdır. URL üzerinden taşınması engellenmelidir.

Güvenli Olarak Oturum Sonlandırma ve Zaman Aşımı
Uygulamada kullanıcının her hangi bir zamanda oturumunu sonlandırması Çıkış butonu gibi bir buton entegre edilmelidir. Bu butona tıklanması ile oturum anahtarı geçersiz hale getirilmelidir. Bu önleme ek olarak oturum sonlandırma için aşağıdaki önlemlerden en az birinin uygulamada kullanılması gerekmektedir.

- Kullanıcıdan belli bir süre yanıt alınamadığı zaman oturum sonlandırılabilir. HTTP isteklerinin gelme durumu dikkate alınır.
- Kullanıcı uygulamaya giriş yaptıktan sonra, herhangi bir aktivite olup olmadığına bakmaksızın, belli bir toplam süreyi geçince oturum sonlandırılması yapılabilir.

Güvenli Oturum İçin Ek Tedbirler
Kullanılan uygulamanın kritikliğine göre bazı hususlarda ek tedbirler alınabilir.

- Kullanıcıya IP adresi limitleme seçeneği verilebilir. Kullanıcıya sadece belli IP adresleri üzerinden giriş yapmasına izin verilebilir.
- Çift faktörlü doğrulama etkinleştirilebilir. Kullanıcı adı ve parolaya ek olarak SMS mesajı gibi doğrulamalar kullanılabilir.
- Uygulama sunucusundaki tüm iletişimin güvenli protokol olan HTTPS ile yapılması gerekmektedir.

Kaynakça
- https://docs.microsoft.com/en-us/previous-versions//ms533046(v=vs.85)?redirectedfrom=MSDN
- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
- https://www.netsparker.com.tr/blog/web-guvenligi/http-isleyisi-ve-guvenligi-acisindan-cookie-ve-session-yonetimi/

BATUTA PROJESİ
Coğrafi Büyük Veri Portalı

İbrahim Sarıçiçek – Başuzman Araştırmacı / BİLGEM YTE

> Batuta Projesi, büyük coğrafi veri için saklama ve görselleştirme platformu oluşturulması amacıyla TÜBİTAK BİLGEM bünyesinde hayata geçirildi.

Batuta Uygulaması, coğrafi verinin saklanmasını, kolay ulaşımı, yaklaşık 5 milyon noktanın ve binlerce çizgi ve poligonun web üzerinde gösterimini ve farklı görselleştirme metotlarıyla analiz edilmesini sağlayacak şekilde tasarlandı. Ek olarak sayısal ve sözel bilgilerden grafikler üretmeyi, listeler oluşturmayı, en düşük, en yüksek, ortalama değerler gibi istatistiki bilgilere ulaşmayı ve tüm bunları izleme ekranlarından (dashboard) takip etmeyi sağlar.

Projenin gelişme sürecini, coğrafi bilgi ve coğrafi bilgi sistemlerini açıklamak ve coğrafi zekaya geçişin nasıl olduğunu özetlemekte fayda var. Böylece projenin hangi sektörlerde ve hangi konularda kullanıcılara fayda sağlayacağı daha iyi anlaşılacaktır.

Coğrafi bilgi nedir?

Coğrafi bilgi, yeryüzü üzerindeki doğal ve yapay detaylara ilişkin, belli bir referans sistemindeki konum koordinatları ile ifade edilen mekansal veriler ve bunlara ait öznitelik verilerinden oluşur. Yani oturduğunuz binanın arazide kapladığı geometri, bunun yanında binanın yaşı, kat bilgisi, toplam daire sayısı gibi sözel bilgiler coğrafi bilgiyi oluşturur.

Coğrafi bilgi sistemi(CBS) nedir?

Coğrafi bilginin bir sisteme dönüşebilmesi için her türlü coğrafi referanslı bilginin elde edilmesi, depolanması, güncellenmesi, kullanılması, analizi ve görüntülenmesini sağlamak gerekir. Bunu da bilgisayar donanımı, yazılımı, ilgili personel ve yöntemlerin bir arada toplanması ile yaparız. Coğrafi bilgi sistemleri temelde bilgi sistemleridir, ek olarak coğrafi referanslar içerir.

Coğrafi bilgi sistemi ve Coğrafi zeka ayrımı

Coğrafya bilgisayarlar (ki yaratıcılarının ana dili olan ingilizcede "computer" yani hesaplayıcı olarak geçer) ile hesaplar yapan kompleks bir bilim olmaya başlayalı çok olmadı. Haritalama da arazide zaman harcanan bir meslek olmaktan daha çok, mekan ile ilgilenen birçok bilim dalında olduğu gibi, uydu görüntüleri / drone çekimleri kullanan ve kodlama, veri analizi, süreç otomasyonu yapan bir iş alanı haline geldi.

CBS ve coğrafi zeka farkı yakın zamanda oluşmaya başladı. Forbes'da 2019'da yayınlanan "Geospatial Is Not GIS" makalesine göre CBS, her zaman bir kimlik krizi yaşadı. CBS çalışanları olarak tam anlamıyla ne işle ilgilendiğimizi anlatmakta zorlandık. Google Earth ve Haritalar sayesinde ancak biraz olsun ne tür işler ile ilgilendiğimizi anlatabilir olduk.

CBS alanında, kartografik tasarım (harita görselleştirme sanatı) veya analitik sonuçlar oluşturmak için bilgisayar operatörü seviyesinde masaüstü ve mobil uygulamalar kullanılıyor. Coğrafi zeka alanında, kartografik veya analitik ürün akışları oluşturmak için kodlama kullanılıyor. Tanımlı tek bir iş için, örneğin orta büyüklükte bir kentteki mahalle bazında nüfus dağılımını hesaplamak ve haritalamak için CBS'nin kullanılacağını düşünebiliriz. Ancak iş akışı tekrarlanan, örneğin bir market zincirinin şubelerinden gün içinde aktarılan verileri saklamak ve saatlik satışlarının anlık haritada izlendiği bir sürece dönüştürmek coğrafi zeka işidir.

> Yakın dönemde Coğrafya, bilgisayarlar ile hesaplar yapan kompleks bir bilim olmaya başladı. Haritalama da arazide zaman harcanan bir meslek olmaktan daha çok, mekan ile ilgilenen birçok bilim dalında uydu görüntüleri / drone çekimleri kullanan ve kodlama, veri analizi, süreç otomasyonu yapan bir iş alanı haline geldi.

Coğrafi zeka alanında büyük veri dediğimiz ölçekte sürekli akan veriyi üreten aktör ve uygulamaları aşağıdaki gibi sıralayabiliriz.

- Coğrafi bilgi üretiminden ve paylaşımından sorumlu ya da işlemlerinde konum kullanan kurumlar
- Navigasyon, adresleme ve online haritalama için yol, bina ve işletmelerin konumlarını üreten firmalar
- Mobil uygulamalarda GPS kullanan ve bilgiyi kaydedebilen uygulamalar; Twitter, Instagram, mobil harita uygulamaları, Foursquare ya da kurumların kendi çözümleri için geliştirdiği GPS kullanan tüm uygulamalar,
- Pos cihazları
- IoT cihazlar (akıllı ev çözümleri, araç takip cihazları, vb)
- Sensörler, beaconlar

Coğrafi durum(geospatial) analizi ne işe yarar?

Coğrafi veriler kullanılarak farklı sektörlerde çeşitli çözümler üretiliyor. Bunlara bazı örnekler verelim.

Ulaşım örneği

Uber, mobil uygulama üzerinden araç çağrısı yapılması ile ulaşım hizmeti sağlayan bir firma. Birçok ülkede faaliyet gösteriyor. Sürücülerde ve kullanıcılarda mobil uygulama bulunuyor. Sürücülerin kullandıkları uygulamadan araçların anlık konum, hız, kullanımda ya da boşta bilgisi gibi veriler toplanıyor.

2018 Open Summit organizasyonunda "Urban Computing with Advanced Visualization" konulu oturumda Uber katılımcıları, ihtiyaç analizlerine göre geliştirdikleri ürünleri tanıtırken lokasyon bazlı verileri nasıl kullandıklarına örnekler verdiler. Örneğin Londra'da en çok hangi saatte ve nereden nereye gitmek için hizmet kullanıldığının bilgisine erişiyorlar. Bu şekilde belirli saatlerde belirli bölgelerdeki yoğunlukları önceden tahmin edip boşta olan sürücüleri ilgili noktalara yönlendiriyorlar. Takip ettikleri araçlardan gelen mesaj sayısı bir günde bir kentte milyarlarca konuma ulaşabiliyor. Bunları ısı haritaları, grid gruplamalar ve dairesel gruplamalar ile gözle analiz edilebilir hale getiriyorlar.

Lojistik örneği

Birkaç sene önce içinde bulunduğum bir projede, bir kargo firmasının araçlarında bulunan takip cihazlarından gelen son 1 aylık (1-5 milyon arası nokta) verilerin ısı haritalarında gösterilmesi istenmişti. Böylece mevcut şubelerini ve araçlarının gün içinde en çok bulunduğu alanları aynı ekranda görebileceklerdi. Projeyle, yanlış konumlanmış şubeleri taşıma ya da yeni şube açma kararı için ihtiyaç duyulan veri analizine erişim sağlanmıştı.

Mekan seçimi

Günümüzde birçok büyük market zinciri, rakiplerinin konumları, alandaki nüfus bilgileri ve detayında yaş, gelir, eğitim bilgileri, edinebilirlerse rakiplerinin ciroları, en önemlisi ortalama kira bilgisini bir araya getirerek, yeni bir market açmak için en uygun noktayı bulmayı analiz ediyor.

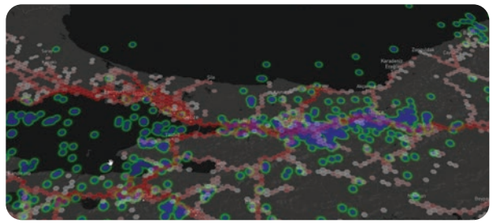
Batuta Kullanım Alanları

Batuta, temelde harita destekli bir analiz aracıdır. Kabiliyetleri, CBS araçları ile yapılabilen birçok iş ile kesişmektedir. Bu noktada harita ile karar alma sürecini yönetebilecek tüm sektör ve meslekler, Batuta'nın potansiyel kullanıcısı konumundadır.

Akıllı Şehir Uygulamaları

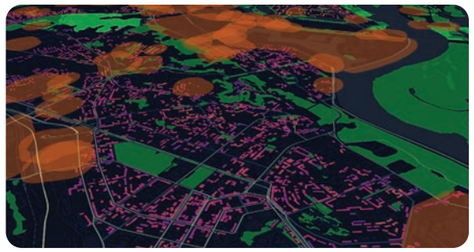
Kent yönetimi ve planlama süreci artık akıllı teknolojilerin sık kullanıldığı bir alan. Gerçek zamanlı veriler, uzun vadede altyapı masraflarını azaltırken karar alma sürecinde operasyonel verimliliği artırır.

Nüfus yoğunluğu planlama, yeni ulaşım ağları belirleme, sosyal medya analizi, trafik kontrolü, toplu taşıma istatistikleri ve kent yönetimi ile ilgili tüm sosyo ekonomik kararlarda kullanılabilecek büyük veri analizi, doğru karar almada bir altlık oluşturur.Tüm bu süreçlerde, büyük veri ile doğru karar alabilmek için Batuta'nın sağladığı görsel altyapıyı kullanmak, büyük fayda sağlar.



Şehir Planlama

Kent planları oluşturmak için birçok farklı alandan veri kullanmak gerekir. Kamu kurumları bu farklı verileri plan kararı almak için kullanmak zorundadır. Batuta tek bir harita üzerinde ortak bir proje analizi oluşturarak işleri kolaylaştırır. Planlama ve tahmin için daha tutarlı bir zemin elde etmek için trafik, geçmişe ve geleceğe dönük demografi, hane geliri, suç oranı gibi ek veri katmanları eklenir, uydu görüntüleri ya da hava fotoğrafları ile de analizler desteklenir.



Perakende Sektörü Kullanımı

Perakende sektöründe en sık konum verisi kullanımı satış, pazarlama ve gayrimenkul yönetiminde olmaktadır. Batuta ile perakende bayilerinde toplam satışların izlenmesi, kar ciro hesaplamaları, bu bilgi doğrultusunda pazarlama faaliyetlerinin nerelerde yoğunlukla gerçekleştirilebileceği kolayca analiz edilebilir. Ayrıca mevcut ve potansiyel gayrimenkul alanları, buna göre yeni açılabilecek bayilerin uygun konumlarının tespiti gibi analizler de yapılabilir.

Ulaşım ve Lojistik Sektörü Kullanımı

Mevcut ulaşım rotalarında taşınan insan ya da eşyaların analizleri Batuta ile yapılabilir. Bu şekilde toplu ulaşım planlamada ana eksenler ve sık kullanılan merkezler, istatistiki bilgilerle haritada gösterilir. Yeni ulaşım metotları, kapasite artırma ihtiyacı ve yeni rotalar konusunda öngörülerde bulunulabilir. Milyonlarca noktayı anlık gösterebilmesi sayesinde, kurum filolarından anlık edinilebilecek konum bilgileriyle, yoğun çalışma bölgeleri ve sık kullanılan rotalar hesaplanarak rutin işlerin daha verimli yapılabilmesi için analizler yapılabilir.

> **Harita ile karar alma sürecini yönetebilecek tüm sektör ve meslekler, Batuta'nın potansiyel kullanıcısı konumundadır.**

Afet Yönetimi

Batuta ile yüz binlerce bina, daha önce yaşanmış afet konumları, on binlerce deprem noktası, saniyeler içinde ısı haritaları, tematik renklendirme gibi tekniklerle sorgulanır ve herkes tarafından anlaşılır şekilde sunulabilir. Sel taşkın alanları ile mevcut yapılı çevre, aynı harita üzerinde gösterilir. Afet etki alanı, hasarlar, insan kayıpları veri tabanına işlendiği takdirde, kamu kurumlarının hızla müdahale edebileceği noktalar ve bölgeler kolaylıkla belirlenmiş olur.

Yerel Yönetimler

Batuta ile tüm mekansal veriler, hem kurum içinde kullanılabilir hem de vatandaşlar ile paylaşılabilir bir yapıya getirilebilir. İmar planları, kadastral planlar, yol ve bina rayiç bedelleri, planlanan yol yapım ve kazı yapılacak alt yapı çalışmaları izlenebilir. Mahalle nüfus yoğunluk verileri, tematik gösterimle zenginleştirilebilir.

Batuta Altyapısı

Batuta ile Docker altyapısında 3 farklı mikroservis çalışmaktadır. Ara yüz, veri tabanı ve rest kütüphaneden oluşan 3 farklı mikro servis dakikalar içinde kurulup, güncellenebilmektedir. İstenildiği durumda kurumlar diğer servisleri kendileri kodlamak şartıyla yalnız ara yüz ya da rest kütüphanesini kullanabilirler. Servislerin ayrı sunulduğu bu şekilde bir entegrasyon için, Java ve Spring Framework ile geliştirilen sunucu tarafı yazılımlar, Swagger kullanarak daha kodlama yaparken dokümante edilmiş olur. Geliştirilen tüm servislere arayüz geliştirmek isteyenler detaylı bir dokümantasyon ile ulaşabilirler.

Coğrafi veriler arayüze GeoJson küçültüp ziplenerek çağrıldığı için veritabanı bağımsız çalışır diyebiliriz. Mevcutta TÜBİTAK BİLGEM Yazılım Teknolojileri Enstitüsü (YTE) olarak da kullanımının artırılması konusunda destek verdiğimiz, "Dünyanın En Gelişmiş Açık Kaynak Kodlu Veritabanı; Postgresql" ve üzerinde coğrafi işlemler yapmaya olanak veren Postgis kullanılmaktadır. Proje başlangıcında NoSql çözümler ile çalışabilirlik test edilmiş, bu konuda Cassandra ve NoSql veritabanlarına coğrafi özellik kazandıran Geomesa teknolojisi ile çalışılabileceği konusu teyit edilmiştir.

Coğrafi zeka ile gerçekleştirilen uygulamalar konusunda Uber Firması'nın çözümlerinden bahsetmiştik. Uber, kendi analizlerinde kullandığı bir çok ürünü açık kaynak kod olarak tüm dünyaya da açmış durumda. Bunlardan en sık kullanılanlardan biri analiz haritaları oluşturmayı sağlayan KeplerGL. Webgl kullanarak milyonlarca coğrafi veriyi web ortamında gösterip, ısı haritaları, grid ve arı peteği gruplamalar, 3 boyutlu gösterimlerle görselleştirebiliyor.

Batuta'da hem hazır çözüm olan KeplerGL kullanıldı hem daha dinamik, değiştirilebilir, kurumların ihtiyaçlarına göre geliştirilebilir YTE Harita uygulaması oluşturuldu. Pie, bar, kolon, radar, gül, kelime bulutu, çizgi grafik konusunda Alibaba Firması'nın da geliştirmesinde destek oluğu AntV kütüphanesi kullanıldı.

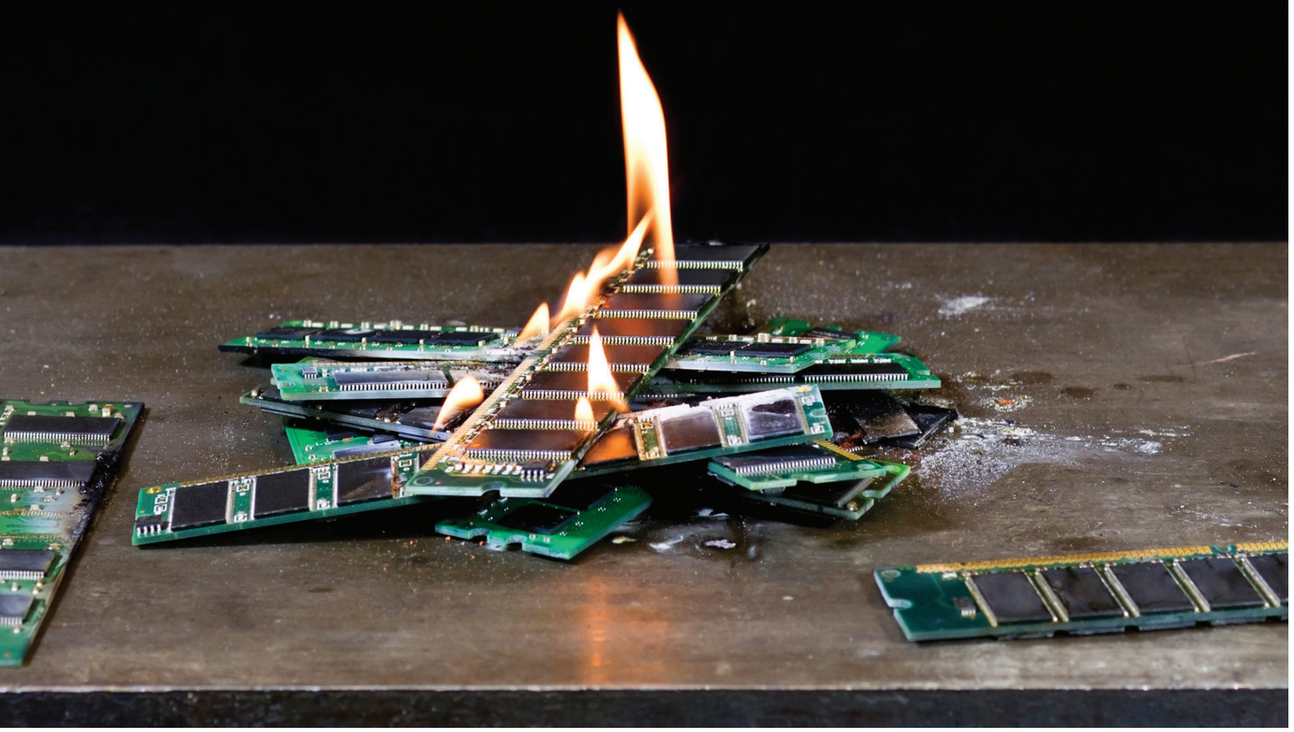
Tüm bu öğeler izleme ekranlarına, yerleri, boyutları değiştirilebilir ve kaydedilebilir şekilde birçok BI (iş analitiği) uygulaması, dashboard alanında sunulan özellikler gibi esnek ve isteğe göre tasarlanabilir şekilde geliştirilmiştir.

Kaynakça

• Will Cadell, 2019, "Geospatial Is Not GIS", Erişim Tarihi: 01.12.2020, https://www.forbes.com/sites/forbestech-council/2019/03/21/geospatial-is-not-gis

• Uber Open Summit 2018, Urban Computing with Advanced Visualization https://www.youtube.com/watch?v=yS-mqs6dXQxc

Yoğun Paketlenmiş Askeri Elektronik Cihazların Isıl Yönetimi



Yusuf Tekin - Araştırmacı, Hayrettin Özgür Keklikoğlu – Uzman Araştırmacı,
Sertaç Gürel - Başuzman Araştırmacı / BİLGEM İLTAREN

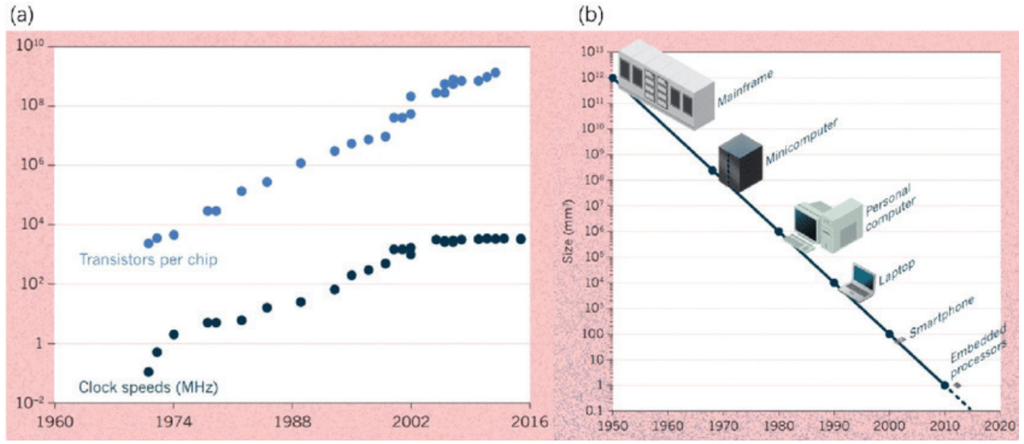
> İki sistem arasındaki sıcaklık farkının neden olduğu enerji aktarımı, ısı olarak tanımlanmaktadır.

Elektronik cihazlar birçok sektörde yaygın olarak kullanılmaktadır. Gelişen teknoloji ile elektronik cihazlar giderek küçülse de işlevsellik artmaktadır (Şekil 1). Elektronik cihazların küçülmesi, cihazın birim başına ürettiği ısı miktarında belirgin bir artışa neden olmaktadır. Yüksek güç tüketen bu gibi elektronik cihazlar, yeterli ısıl yönetime sahip olmadığı durumlarda içerisinde bulundurdukları elektronik kartlarda ani sıcaklık yükselimlerine neden olmaktadır.

Elektronik kartlara monte edilmiş entegre çipler silikon malzemeden yapıldıkları için sıcaklık değişimlerine karşı oldukça hassastır. Bu durum, elektronik kart üzerinde bulunan bileşenlerin çalışma performansını olumsuz etkilemekte ve kullanım ömrünü kısaltmaktadır. Elektronik cihazların hata oranı da sıcaklıkla orantılı olarak artmaktadır.

Bu gibi durumların önüne geçmek için elektronik cihazların mekanik tasarımları yapılırken hem modül bazında hem de kutu seviyesinde gerekli soğutmayı sağlayacak tasarımların gerçekleştirilmesi gerekmektedir. Ancak artan devre yoğunlukları ve bileşenlerin boyutlarındaki azalmalar, elektroniklerin termal kontrolünü daha karmaşık hale getirmekte ve bileşen sıcaklıklarını istenilen değerin altında tutabilmek zorlaşmaktadır.

Genel kullanılan bazı ısıl yönetim teknikleri, elektronik kartların daha düşük sıcaklıklarda ve daha az



Şekil 1 (a) Mikroişlemci yongası başına transistör sayısı ve saat hızları (b) Her 10 yılda bir makinelerin boyutu eğilimleri. [1]

termal döngüye maruz kalacakları ortamlar oluşturarak, istenilen performansta daha uzun süre çalışmasını sağlamaktadır. Bir elektronik cihazın ısıl yönetiminde temel amaç, ısı yayan bileşenler ile ısı emici ortam arasında en kısa termal yolu oluşturabilmektir.

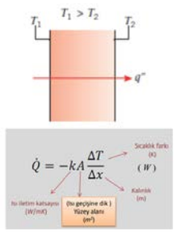
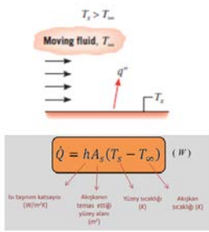
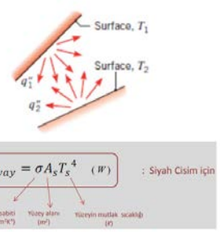
Genel Isıl Yönetim Teknikleri

İki sistem arasındaki sıcaklık farkının neden olduğu enerji aktarımı, ısı olarak tanımlanmaktadır. Isı transferi, sıcaklık farkından kaynaklanan enerji aktarımıdır. Enerjinin ısı olarak transferi, her zaman yüksek sıcaklıktaki bir ortamdan düşük sıcaklıktaki ortama doğrudur ve iki ortam aynı sıcaklığa eriştiğinde ısı transferi durur. Bir ortam içinde veya ortamlar arasında, sıcaklık farkı mevcut olan her durumda, ısı transferi her zaman gerçekleşir. Sıcaklık farkı ne kadar büyükse, ısı transfer hızı o kadar yüksek olur.

Isı transfer mekanizması 3 farklı yol ile gerçekleşmektedir. İletim (kondüksiyon), taşınım (konveksiyon) ve ışınım (radyasyon).

Modül Seviyesinde Soğutma Teknikleri

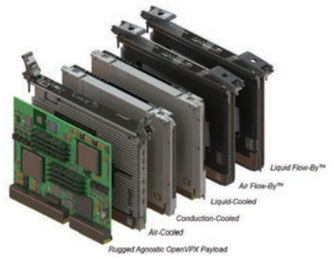
Elektronik elemanların termal kontrolü, ısı transferinin uygulanmasında başlıca alanlardan biri olmuştur. Elektronik elemanların soğutulması işleminde güvenilirlik derecesini sağlamak için sınırlanan maksimum ve minimum eleman sıcaklığına önem verilmesi gerekmektedir. Optimum performansı elde etmek için parçalar arası sıcaklık farkı en aza indirilmelidir. Elektronik elemanların ısıl direnci azaltılıp uygun soğutma koşulları sağlanmalıdır (Şekil 2).

İletim	Taşınım	Işınım
		
Bir katı veya durgun akışkan içerisinde, bir sıcaklık farkı olması durumunda, ısı transferi iletim ile gerçekleşir. Bir ortamda ısı iletim hızı ortam boyunca sıcaklık farkına, ortamın kalınlığına ve ısıl iletim katsayısına (k) bağlıdır.	Bir yüzey ile ona bitişik hareket halindeki bir akışkan farklı sıcaklıklarda ise, ısı transferi taşınım ile gerçekleşir. Bir ortamda taşınım ile ısı aktarımı, ısı taşınım katsayısına (h), akışkanın temas ettiği yüzey alanına ve ortamlar arası sıcaklık farkına bağlıdır.	Farklı sıcaklıklardaki iki yüzey arasında ısı transferi ışınım ile gerçekleşir. Bir ortamda ışınım ile ısı aktarımı, Stefan-Boltzman sabitine, yüzey alanına ve yüzeyin mutlak sıcaklığına bağlıdır.

Tablo 1. Isı Transfer Türleri

İletim ile elektronik kartların soğutulması

Elektronik kartların üzerinde bulunan bileşenle-



Şekil 2 Modül Seviyesinde Soğutma Teknikleri

ANSI/VITA Standart	Özet	Tanım
48.0	Temel Standart	
48.1	Direk Hava Soğutmalı	Doğrudan bileşen üzerinden hava ile soğutma
48.2	İletim ile Soğutmalı	Soğutucu kapak ile soğutma
48.4	Sıvı Soğutmalı	Modül içerisinden sıvı dolaştırma ile soğutma
48.8	Hava Soğutmalı	Modül içerisinden hava dolaştırma ile soğutma

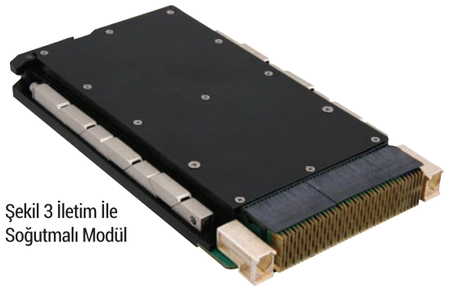
Tablo 2. ANSI/VITA 48.0 standardına göre en yaygın kullanılan soğutma teknikleri

rin sıcaklıklarının düşük tutulabilmesi için kalın bir soğutucu kapak kullanılması gerekmektedir. Kartın bileşenlerinde meydana gelen ısının, termal arayüz malzemeleri (termal ped, termal macun vs.) kullanılarak ilk olarak soğutucu kapağa aktarılması gerekmektedir. Soğutucu kapağa aktarılan ısı, metal gövde boyunca hareket ederek içerisinde bulunduğu ısı emici görevini üstlenen kutuya iletilir. Soğutucu kapak içerisinde devre kartındaki bileşenden, soğutucu kapağın kenarına kadar gerçekleşen ısı akışı, düşük dirençli yolu takip ederek gerçekleşecektir. Soğutucu kapak ne kadar kalın olursa, termal direnci de o kadar düşük olur. Böylelikle ısı daha hızlı aktarılacağı için soğutucu kapağın merkezi ile kenarları arasındaki sıcaklık farkı daha az olacaktır. Kullanılan termal ped kalınlığı ve cinsi, temas noktalarındaki yüzey kalitesi ve kapakların kutu içerisindeki kanallara sabitlenmesinde kullanılan kilitli kamalara uygulanacak tork miktarı termal direnci etkileyen diğer parametrelerdir.

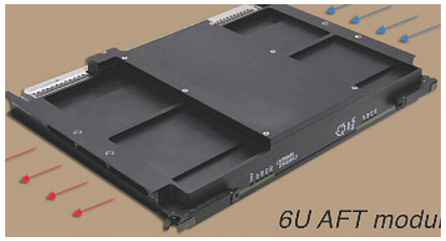
Yüksek güç yoğunluğuna sahip baskı devre kartlarında soğutucu kapak kullanılarak sağlanan iletim ile soğutma yetersiz kaldığında hava veya sıvı ile soğutmalı yöntemler tercih edilmektedir.

Hava ile elektronik kartların soğutulması

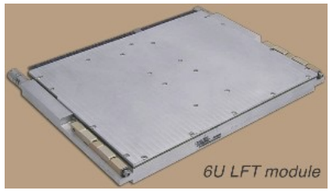
Isı üreten baskı devre kartını çevreleyen soğutucu kapak içerisine uygun sayıda kanatçık yerleştirilerek, soğutma havasının doğrudan bu kanatçıklar içerisinden geçmesi sağlanır. Bu işlem, kart üzerindeki bileşenin soğutma havası ile teması olmaksızın soğutulması işlemidir. Kilitli kama kullanımına gerek olmadığından ve kalın bir soğutucu kapağa ihtiyaç duyulmadığından ağırlığın önemli olduğu çalışmalarda tercih edilmektedir. Isı değiştiricisi ile ısı kaynağı arasındaki mesafe



Şekil 3 İletim İle Soğutmalı Modül

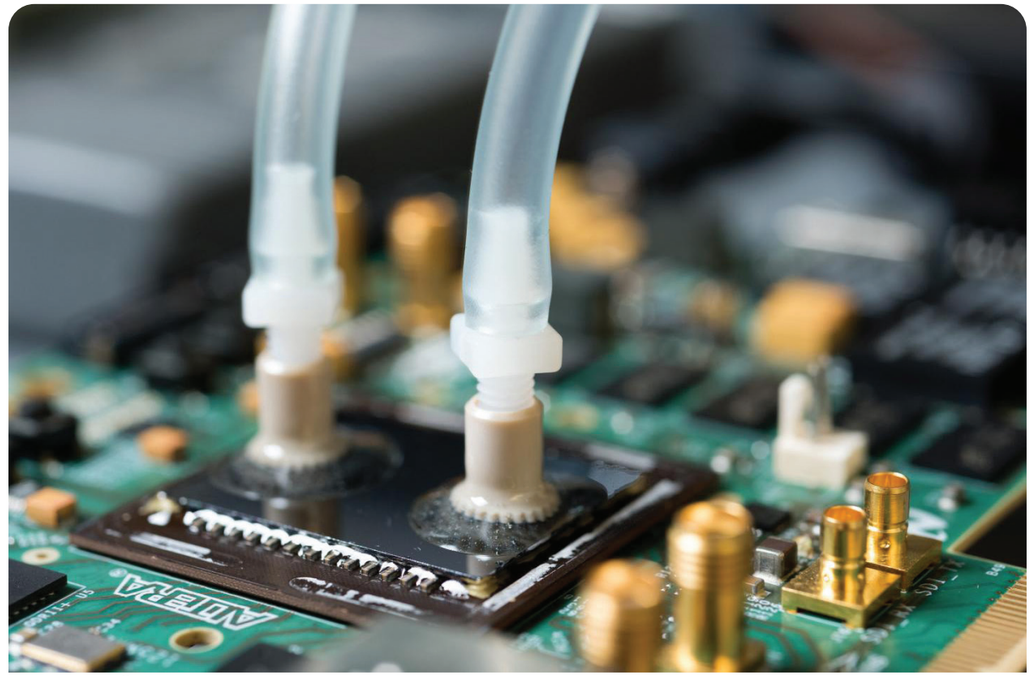


Şekil 4 Hava İle Soğutmalı Modül



Şekil 5 Sıvı Soğutmalı Modül

Şekil 6 Doğal Konveksiyon Soğutmalı Modül



Şekil 9 Bileşen Üzeri Sıvı Soğutma

çok yakın olduğu için modül başına ısı atımı da oldukça fazla olabilmektedir.

Sıvı ile elektronik kartların soğutulması

ısı üreten baskı devre kartını çevreleyen soğutucu kapak içerisinden, uygun bir soğutucu akışkanı dolaştırılarak modülün soğutulma işlemi gerçekleştirilmektedir. Sıvı soğutmalı sistemde, hava soğutmalı sistemde olduğu gibi, soğutucu akışkan soğutucu kapak içerisinde, bileşenlere doğrudan teması olmaksızın dolaştırılmaktadır. Ağırlığının fazla olması ve sıvı hattı bağlantı elemanlarının karmaşıklığı sebebiyle kullanımın alanları sınırlıdır.

Kutu Seviyesinde Soğutma Teknikleri

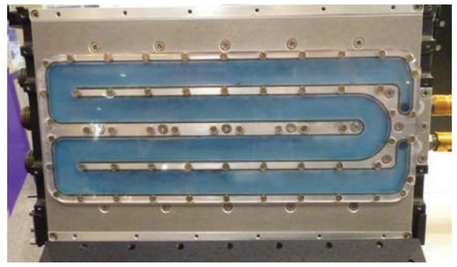
Modül seviyesinde bileşen üzerinden alınan ısının, ortamdan uzaklaştırılabilmesi için içerisinde bulundukları kutuların da soğutulması gerekmektedir. Kutu seviyesinde soğutma ile modül seviyesinde soğutma beraber düşünülmesi gereken konulardır.

Modül ve kasa, aynı soğutma tekniği ile soğutulabilecekleri gibi farklı soğutma teknikleri ile de soğutulabilirler. Örnek olarak, kutu seviyesinde sıvı soğutma yöntemi kullanılarak taşınım ile soğutma sağlanırken, modül seviyesinde iletim ile ısı aktarımı sağlanabilmektedir. Genel olarak kutu seviyesinde hava, sıvı ve doğal konveksiyon soğutmalı sistemler yaygın olarak kullanılmaktadır. [2]

Şekil 7 Hava Soğutmalı Kutu

Doğal konveksiyon yöntemi ile soğutma gerçekleştirilen kutular genel olarak düşük termal yüklerde ve az sayıda modül içeren sistemlerde kullanılırlar. Bu tarz kutuların dış yüzeylerinde, yüzey alanını arttıran ve ısı atımını kolaylaştıran kanatçıklar bulunmaktadır.

Hava soğutmalı kutular, doğal konveksiyonlu kutular ile benzer soğutma elemanları içermektedir. Isı transferini arttıran kanatçık yapıları her iki sistemde de kullanılmaktadır. Bu kutularda farklı olarak, havayı akışa zorlayacak elemanlar (fan vb.) kullanıldığından, kanatçıklar daha fazla hava ile temas edecek ve daha fazla soğutma sağlayacaklardır.



Şekil 8 Sıvı Soğutmalı Kutu

Soğutma için gerekli debiyi ve basıncı sağlayacak doğru fan türünü seçmek çok önemlidir. Fan kulla nımıyla ilgili en büyük endişe gürültü seviyesidir.

Soğutma sıvıları yüksek soğutma kapasitesine sahiptir. Örneğin; su ısıyı havaya kıyasla çok daha hızlı iletir. Bu nedenle sıvı soğutmalı kasalar yüksek güç tüketen elektronik kartların soğutulmasında sıklıkla tercih edilmektedir. Bu tarz kutuların duvarlarında uygulama gereksinimlerine göre optimize edilen sıvı kanalları bulunmaktadır. Isı bu sıvılara aktarılarak soğutma sağlanır.

Yeni Yöntemler

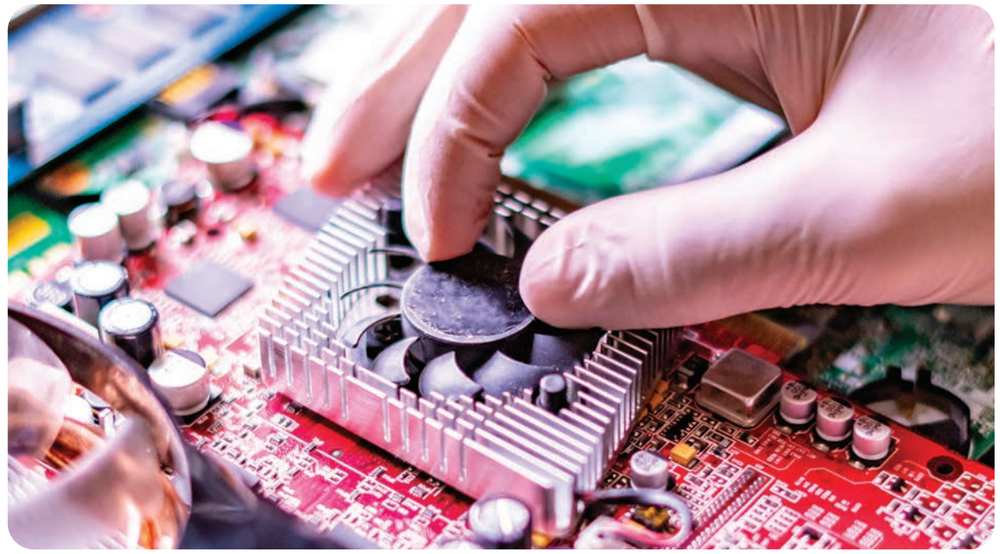
Modül ve kasa seviyelerinde, yukarıda anlatılan geleneksel yöntemlerin yanı sıra artan ısı yüklerinin önüne geçebilmek adına yeni soğutma teknolojileri geliştirilmektedir. Buradaki temel amaç; yüksek ısı üreten ve küçük yüzey alanına sahip elektronik bileşenlerin ürettiği ısıyı ortamdan hızlıca uzaklaştırarak istenilen çalışma sıcaklığına indirmektir. Bunun için ısıl borular, sprey soğutma, peltier ve bileşen üzeri sıvı soğutma teknolojileri gibi sistemler kullanılmaktadır. Bu gibi yöntemler soğutulan yüzey boyunca ısı bakımından homojenlik sağlayarak noktasal ısınmaların önüne geçmektedir.

Değerlendirme

Yüksek güçlü ve yüksek yoğunluklu elektronik sistemlerin termal yönetim gereksinimlerini başarılı bir şekilde ele almak, kullanılabilecek bütün soğutma yöntemlerini değerlendirerek uygun soğutma tekniğini seçmek ve sistemlerin görevlerini uzun vadede, sorunsuz ve güvenli şekilde yerine getirebilmesini sağlamak ısıl tasarım mühendisinin temel sorumluluklarıdır. Tasarım süreci, uygun soğutucu akışkanının seçilmesi, uygun fan/pompa kullanımı, debi ve basınç kayıplarının hesaplanması, çalışma sıcaklıklarının istenilen değerlerin altında tutulması gibi detaylı mühendislik çalışmalarını içermektedir.

Isıl tasarım gruplarının tasarım süreci, elektronik tasarım grupları ile bileşenlerin seçim aşamasından itibaren eşgüdümlü bir çalışma yürütmeyi gerektirmekte, hem projelerin ilerleyen aşamalarında karşılaşılması muhtemel sorunların önceden elimine edilmesi, hem de son ürünün toplam performansının iyileştirilmesi açısından önem arz etmektedir.

Kaynakça
[1] Zhibin Yan et al. «Droplet-Based Microfluidic Thermal Management Methods for High Performance Electronic Devices», Micromachines (Basel). 2019 Feb; 10(2): 89.
[2] «CHOOSING THE RIGHT COOLING METHODOLOGY,» [Çevrimiçi]. Available: https://www.atrenne.com/products/chassis-enclosures.

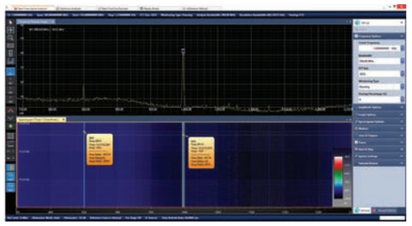


TÜBİTAK BİLGEM

Bu bir proje tanıtımıdır.

GERÇEK ZAMANLI SPEKTRUM GÖSTERİM SİSTEMİ (SPAR-R-26.5)

SPAR-R-26.5 analog sinyallerin geniş bantlı örneklenmesi, analizi ve kaydedilmesini sağlayan bir sistemdir. Sinyal analiz, pulse analiz, spektrum gösterim, I/Q veri kayıt, geri gösterim ve sayısal verilerin geri çalınması sistemin ana yetenekleri olarak tasarlanmıştır. Geliştirilen kullanıcı arayüz yazılımı ile analog ortamdan alınan sinyalin online analiz ve ölçümleri yapılabilmektedir.Dört adet kanallaştırıcı ile online pulse analizi yapılabilmektedir. Sinyallerin frekans-genlik, frekans-genlik-zaman, zaman-genlik ekranlarında kullanıcıya gösterimi yapılmaktadır. Ayarlanabilir sayısal ve RF donanım sayesinde geniş spektrum bandında ve güç seviyelerinde ölçüm ve analiz yapılabilmektedir. Askeri ve sivil uygulamalara uygun mekanik tasarıma sahip bir sistemdir.



www.bilgem.tubitak.gov.tr

Gerçek Zamanlı Spektrum Gözetleme Analiz ve Kayıt

> Radyo frekanslarının çok sık kullanımı ile günümüzde kullanılan bant genişlikleri, milli servet sayılması derecesinde önem kazanmıştır.

Muhammed Çalış - Uzman Araştırmacı, Enes Karav - Uzman Araştırmacı, Dr. Hüseyin Anıktar - Başuzman Araştırmacı, Hakan Yaren - Başuzman Araştırmacı, Dr. Dursun Baran - Başuzman Araştırmacı, Ahmet Can Bilgen - Araştırmacı / BİLGEM BTE

Elektromanyetik dalga kavramı, 1864 yılında İskoç matematiksel fizikçi James Clerk Maxwell tarafından elektromanyetik dalgaların elektrik dalgalarıyla aynı davranışı gösterdiği kuramıyla ortaya atılmıştır. Maxwell, 1867 yılında matematiksel çalışmalarıyla radyo dalgalarının varlığını tespit etti. Alman fizikçi Heinrich Hertz 1887'de Maxwell' in elektromanyetik dalgalarının varlığını laboratuvarında yaptığı deneylerle radyo dalgalarını üreterek gösterdi. Yaptığı deneyde laboratuvarının bir tarafındaki elektrik kıvılcımının yaymış olduğu manyetik dalganın bir tel halka tarafından hissedildiğini gözlemledi.

> Radarlar çok çeşitli ve modülasyon içeren darbe sinyalleri ile çalışmaktadır. Sinyallerin kayıpsız gösterimi ve kaydedilmesi için gerçek zamanlı çalışma prensibine uygun cihazlar gereklidir.

Bir radyo dalgasının hızının ışık hızı ile aynı olduğunun bulunmasından sonra, Hertz, radyo dalgalarının ışık dalgaları gibi yansıma, kırılma ve girişim yapabildiklerini gösterdi. Sonrasında saniye başına titreşim olarak tanımlanan Hertz onun ismiyle anıldı. Bu çalışmalar ışığında İtalyan mucit Guglielmo Marconi ilk radyo vericileri ve alıcılarını 1894-95 yılları arasında geliştirdi. 20. yüzyıldan itibaren ticari ve askeri bakımdan radyo iletişimi çok yaygın bir şekilde kullanılmaya başlandı.

Elektromanyetik dalgaların fiziki bir bağlantı kullanmadan atmosfer içerisinde veri taşıyabilmesi, kullanım alanlarının hızlıca gelişmesinin önünü açmıştır. Elektromanyetik sinyallerin hayatımızın her alanında kullanılmaya başlanması ile birlikte elektromanyetik spektrum kavramı ortaya çıkmıştır. Elektromanyetik spektrum, sinyallerin frekans ve dalga boylarına göre sınıflandırılması için kullanılan bir ölçüttür.

Elektromanyetik sinyallerin kullanımının askeri ve sivil alanda hızlıca yükselmesi ile birlikte elektromanyetik spektrum üzerinde kullanılacak alanların belirlenmesi için bant genişliği tanımı ortaya çıkmıştır. Radyo frekanslarının çok sık kullanımı ile günümüzde kullanılan bant genişlikleri milli servet sayılması derecesinde önem kazanmıştır. Bu gelişmeler sonucunda spektrum üzerindeki askeri ve sivil amaçla kullanılan sinyallerin tespit ve takip edilmesi çok önemli bir konuma gelmiştir.

Radyo frekansları sivil radyolar, telsizler, cep telefonları, uydu sistemleri ve radarlar gibi başlıca alanlarda kullanıldıkça sinyallerin tespit edilmesi, anlamlandırılması ve gerekli görüldüğünde kayıt edilebilmesi için gelişmiş yazılım ve donanım teknolojileri ortaya çıkmaya başlamıştır. Günümüzde bu tarz sistemler o kadar önem kazanmıştır ki ülkeler kendi teknolojilerinin ihraç edilmesine sınırlı oranlarda müsaade etmektedir. Bu durum, bu tarz teknolojilerin ülkemizde geliştirilebiliyor olmasının önemini ortaya koymaktadır.

Elektromanyetik sinyaller askeri amaçla TEMPEST (Telecommunications Electronics Material Protected From Emanating Spurious Transmissions) analiz, haberleşme, yön bulma, silah sistemleri gibi kritik önem arz eden alanlarda sıklıkla kullanılmaktadır. Bu alanlardan TEMPEST analiz ve ELINT uygulamalarından aşağıda detaylı bir şekilde bahsedilmiştir.

TEMPEST

Bilgi içeren elektronik cihazlardan, kontrol dışı elektromanyetik enerji yayılımlarının araştırılması, incelenmesi ve denetim altına alınması gereklidir. Bu yayılımlar kontrol altına alınmaz ise bilgilerin istenmeyen şekilde dış ortamdan toplanması mümkündür. TEMPEST kavramı bu kaçak yayınların toplanıp anlamlandırılmasının engellenmesini sağlamak amacıyla ortaya çıkmış bir kavramdır.

Askeri ve ticari amaçla üretilen cihazların her geçen gün daha karmaşıklaşması ile birlikte bir cihazın başka bir cihazla ve haberleşme sistemleri ile olan girişimleri de artmaktadır. Sistem saat oranlarının hızlanması da istenmeyen sinyallerin tespit edilmesini zorlaştırarak hatalı ölçüm sonuçlarında artışa sebep olmaktadır.

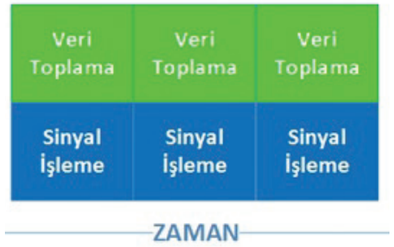
Geniş bantlı gerçek zamanlı spektrum analizörlerin uyumluluk testlerinde kullanımı istenmeyen sinyallerin ve harmonik sinyallerinin kayıp olmaksızın tespit edilmesine imkân tanır. İlgilenilen frekans aralığında hızlı ölçümler alınarak test süresinden tasarruf sağlanır.

ELINT- Electronic Intelligence (Elektronik İstihbarat)

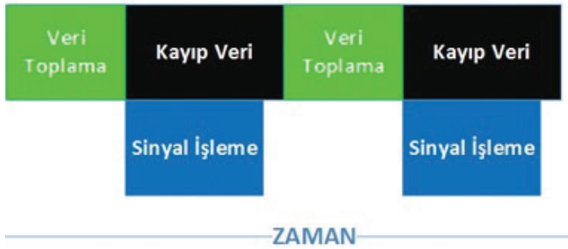
Elektromanyetik spektrumun takip edilmesi amacıyla yapılan işlemlere Elektronik Harp (EH) adı verilir. Bu kapsamda yapılan faaliyetler istihbarat amacıyla kullanılabilir. Sinyal istihbarat (SIGINT) sistemleri ile tespit edilen sinyaller, haberleşme istihbarat (COMINT) ve elektronik istihbarat (ELINT) olarak askeri amaçlarla değerlendirilir.

Radar istihbarat üst bant frekansı 40 GHz ve üstüne çıkan geniş bantlı ve gerçek zamanlı sinyal tespiti gerektirir. Çoğunlukla darbe sinyalleri tespiti amacıyla kullanılır. Radar varlığının tespit edilmesi cihazın temel görevidir. Radarlar çok çeşitli ve modülasyon içeren darbe sinyalleri ile ça-

Şekil 1. Gerçek Zamanlı Spektrum Analizör



Şekil 2. Klasik Spektrum Analizör



lışmaktadır. Sinyallerin kayıpsız gösterimi ve kaydedilmesi için gerçek zamanlı çalışma prensibine uygun cihazlar gereklidir. Bunun yanında tespit edilen radarın çalışma amacı, anlık görevi ve ne tür bir radar olduğu gibi bilgilerin tespit edilebilmesi için ürettiği sinyallerin frekans, genlik, darbe genişliği ve darbe tekrar sıklığı gibi parametreleri çıkarılabilmelidir. Gerçek zamanlı sistemler sayesinde radar çalışma parametreleri anlık ve en doğru şekilde çıkarılabilir. Aynı zamanda sinyaller kayıpsız kaydedilerek detaylı analiz yapılabilir.

Sinyallerin uygun bir şekilde sayısallaştırılıp ihtiyaç duyulan analiz, ölçüm ve gösterim algoritmalarının çalışabilmesi için antenden alınan işaretler RF koşullandırıcı birimleri üzerinden geçirildikten sonra RF almaç tarafından frekans düşürme işlemi ile sayısallaştırma biriminin algılayacağı IF frekans aralığına çevrilir. Geniş bantlı sinyal tespiti ve sayısallaştırılması kullanıcı kabiliyetlerinin artırılması ve tespit edilen sinyallerden daha fazla bilgi elde edilmesi için gerekli olan bir kabiliyettir. Sinyallerin sayısallaştırılmasının ardından, verilerin kayıpsız bir şekilde kaydedilmesi, geri gösterilmesi ve ihtiyaca göre tekrar analog olarak geri çalınması gibi özelliklerin kullanıcılar için sunulması daha detaylı analiz ve anlamlı bilgi edinilmesine imkân tanımaktadır.

Gerçek Zamanlı Spektrum Gösterimi

Bu gösterimde, sistemin çalışma analiz bant genişliğinde spektrum gözetleme noktasında herhangi bir kör zamanı bulunmamaktadır (Şekil 1). Sistem radyo frekansı (RF) spektrumunu zaman ekseninde örnekleyebilir ve Fast Fourier Transform (FFT) işlemini kullanarak bilgileri frekans alanına dönüştürebilir. Paralel çalışan FFT modülleri sayesinde veri aktarım ve spektrum gösterim esnasında herhangi bir bilgi kaybının oluşması engellenmektedir. Klasik spektrum analizörler belirli zamana ait spektrum bilgisini gösterebilmektedir. Bu tarama zamanları arasındaki ölü bölgeler veri kaybına neden olmaktadır (Şekil 2).

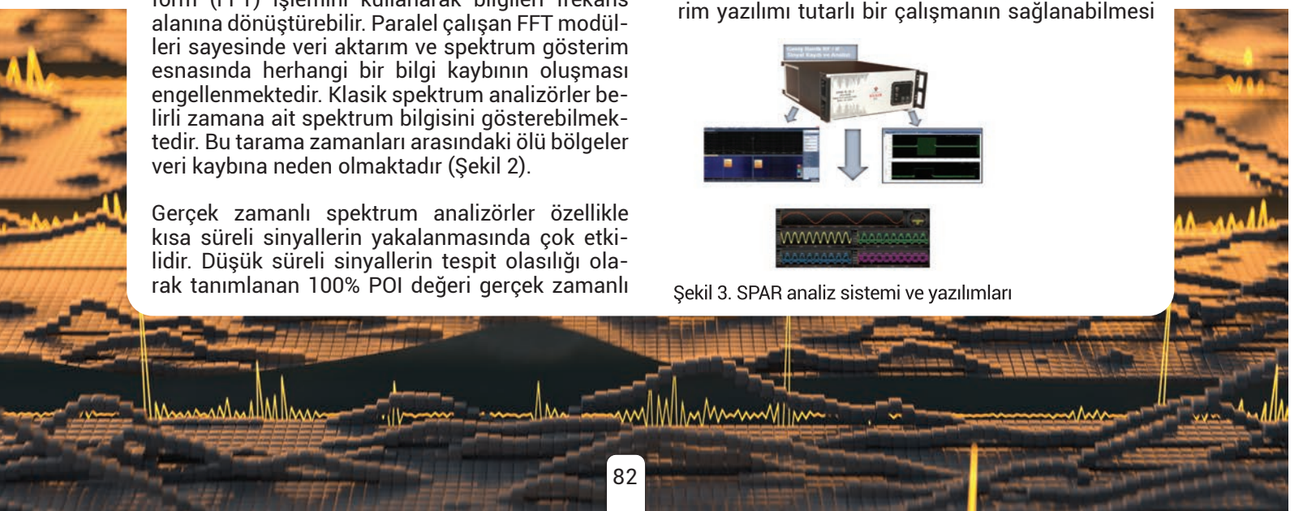
Gerçek zamanlı spektrum analizörler özellikle kısa süreli sinyallerin yakalanmasında çok etkilidir. Düşük süreli sinyallerin tespit olasılığı olarak tanımlanan 100% POI değeri gerçek zamanlı spektrum analizörlerin en önemli parametrelerinden biridir. Sistemde kullanılan FFT boyutuna ve örtüşme oranına bağlı olarak 100% POI değeri belirlenmektedir.
100%POI = (2-Örtüşme Oranı) x (FFT Nokta Sayısı) / (Örnekleme Frekansı)

Yazılım Tasarımı

Spektrum gösterim cihazları çeşitli sinyalleri tespit etmek ve operatöre analiz imkânı tanımak için ihtiyaca göre özelleşmiş gösterim ekranları ile ölçüm araçları içeren yazılımlardan oluşmaktadır. SPAR yazılımı "Gerçek Zamanlı Gösterim", "Gerçek Zamanlı Analiz", "Spektrum Tarama", "Osiloskop Gösterim" ve "Kayıttan Geri Oynatma" ekranlarından oluşmaktadır. Ekranlar genlik – frekans, 3 boyutlu genlik-zaman-frekans eksenlerinden oluşan dinamik bir şekilde değişen sinyallerin gösterimini kolaylaştıran, ayarlanabilen zaman eksenine sahip spektogram (şelale) grafiği, genlik - zaman grafiği ve sinyalin zarfının alınmasını ifade eden video - zaman grafiğini içermektedir (Şekil 3).

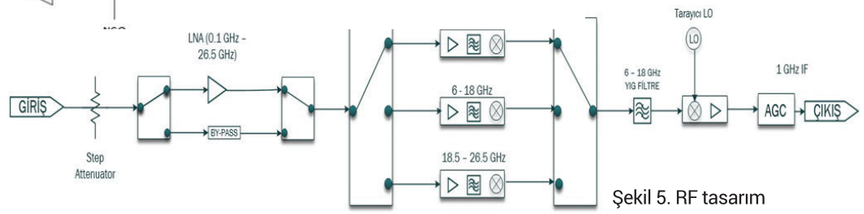
Sinyallerin kayıpsız bir şekilde kayıt edilebilmesi için 500 MHz analiz bant genişliğinde saniyede yaklaşık 3 GB veri kaydı yapılabilmektedir. Sayısallaştırma kartı üzerinden PCIe vasıtası ile alınan veriler RAID teknoloji ile SSD disklere paralel olarak yazılmaktadır. Bu kayıtların geri gösterimi için gerçek zamanlı gösterimde var olan grafik çeşitleri, çizim yöntemleri ve ölçüm araçlarının hepsi kullanılabilmektedir.

Birçok özelliğin bir arada bulunmasını gerektiren karmaşık bir kurguya sahip spektrum gösterim yazılımı tutarlı bir çalışmanın sağlanabilmesi için yazılım tasarımında gelişmiş teknolojilerin kullanılmasını zorunlu kılmaktadır. Katmanlı mimari ile kurgulanan yazılımda ön gösterim, sinyal işleme ve haberleşme işlemleri, veri tabanı erişimleri ve donanım ile olan işler birbirinden ayrılmıştır.

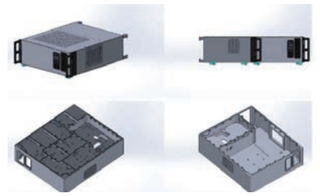


Şekil 3. SPAR analiz sistemi ve yazılımları

Şekil 4. FPGA Sinyal İşleme Blokları



Şekil 5. RF tasarım



Şekil 6. Mekanik Tasarım

Sayısal Tasarım

Geniş bantlı gerçek zamanlı spektrum analizörlerde yüksek hızlı veri işleme amacıyla yüksek örnekleme frekansına sahip ADC'ler ile kaynak miktarının fazla olduğu FPGA'ler kullanılmaktadır. Yüksek veri hızına sahip sinyallerin işlenebilmesi için paralel sinyal işleme yapıları kullanılmaktadır. FPGA'lerde bulunan yüksek hızlı DSP48 çarpıcılar ve hafıza elemanları karmaşık sinyal işleme algoritmalarının gerçekleştirilmesine olanak sağlamaktadır. Bu sayede sinyallere uygulanacak filtreleme, pencereleme, örtüştürme, FFT gibi işlemler veri kaybı olmadan yapılabilmektedir. Bu durumda spektrum gözetleme amacıyla hem sinyal işleme algoritmaları gerçekleştirilirken hem de veri kaydı ve gösterimi yapılabilmektedir. Sinyal işleme blokları Şekil 4'te gösterilmiştir.

FPGA'den PC'ye sinyal verilerinin kayıpsız aktarılabilmesi için PCIe'in meşgul olduğu zamanlarda verilerin tutulduğu büyük boyutlu RAM'ler kullanılmaktadır. PCIe'in verileri aktaramadığı durumda FPGA, verileri RAM'e yazarak ön depolama yapmaktadır. Ön depolama yapılan veriler PCIe'den ilk gönderilen veriler olmaktadır. Ön depolama verilerinin tamamı gönderildikten sonra FPGA verileri doğrudan PCIe üzerinden PC'ye aktarmaktadır.

RF Tasarım

0,1 – 26,5 GHz frekans aralığındaki 500 MHz bant genişliğinde RF sinyaller süperheterodin (superheterodyne) yapısı ile ADC'nin örnekleyebileceği frekans bandına dönüştürülmektedir. İstenmeyen sinyaller olan hayal sinyallerinin yok edilmesi için sistemde merkez frekansı ayarlanabilir 500 MHz bant genişliğine sahip YIG (Yttrium Iron Garnet) filtre kullanılmaktadır. Hayal frekanslarından temizlenmiş sinyaller, yüksek hızlı tarama yeteneğine sahip LO (Local Oscillator) yardımıyla yaklaşık 1 GHz (IF) bandına düşürülmektedir. IF sinyallerini kuvvetlendirmek veya zayıflatmak amacıyla IF katında kazanç bloğu kullanılmıştır. Ayrıca bant genişliğini değiştirebilmek için kazanç bloğunda filtre bankaları da yer almaktadır. RF tasarım blokları Şekil 5 üzerinde gösterilmiştir.

Mekanik Tasarım

Rack kabine monte edilebilir şekilde tasarlanmıştır. Mekanik boyutları 436 x 205 x 522 mm (yükseklik 2.5 RU, derinlik 522 mm) ve ağırlığı 32 kg'dır. TEMPEST geçirgenlik standartlarına uygun olarak tasarlanmış ve üretilmiştir. Bu standartlara uygun olmasını sağlamak amacıyla sistem içine hava giriş noktasına bal peteği (honeycomb) paneli monte edilirken, hava çıkış noktalarına duvar kalınlığının 1/3 oranında olacak şekilde delikler açılmıştır. Sistem içindeki sızdırmazlığı sağlamak amacıyla PCB ve RF kısmının arasına ve RF kısmında bulunan komponentlerin aralarına duvarlar örülmüştür. Dış ortamdan iç ortama, iç ortamdan dış ortama PCB-RF arası ve komponentler arası sızdırmazlığı sağlamak amacıyla iletken silikon conta için conta kanalları açılmıştır. Sistem 0 – 50°C aralığında tam performans ile çalışmaktadır. Sistem içinde bulunan SSD'ler dışarıdan takılabilir ve sökülebilir şekilde yerleştirilmiştir. Sistemin dış ortamlara dayanıklılığını arttırmak amacıyla mekanik parçalara kaplama ve boya yapılmıştır (Şekil 6).

Kaynakça

[1] https://interferencetechnology.com/2016-real-time-spectrum-analyzer-guide/
[2] "TEMPEST Bilgi Kaçaklarını Denetimi" , BILGEM Teknoloji Dergisi Sayı 10, Eylül 2020. https://bilgem.tubitak.gov.tr/sites/images/bilgem_teknoloji_dergisi-10.sayi_.pdf
[3] https://tr.wikipedia.org/wiki/Radyo_frekans
[4] Struan Reid, Patrica Fara, Bilim Adamları Tübitak Yayınları ISBN 9754031010

Yapay Zekâ ve Veri Mahremiyeti UYGULAMALARI

Mahmut Lutfullah Özbilen – Araştırmacı, Rabia Arkan – Araştırmacı, Emine Ahsen Akay – Araştırmacı,
Mehmet Haklıdır - Başuzman Araştırmacı / BİLGEM BTE

> **Saklanan kişisel veriler dışarı aktarılacağı veya uygulama ekranında gösterileceği zaman verinin tamamını kullanmak, hassas bilgilerin tehlikeye girmesine sebep olabilir.**

Gelişen teknoloji ve işlemci gücüyle akıllı sistemlerin kullanımının hızla arttığı günümüzde yapay zekâ; telekomünikasyondan havacılığa, tıptan savunma sektörüne kadar pek çok alanda yaygın olarak kullanılmaktadır. Ancak yapay zekâ uygulamalarının var olmasını sağlayan, günümüzün petrolü olan verinin mahremiyetini sağlama, halen üzerinde çalışılan önemli bir sorundur.

Bu zamana kadar geliştirilen yapay zekâ teknolojileri, veri mahremiyetini gözetecek şekilde tasarlanmamıştır. Ancak yasal düzenlemelerle de kişisel verilerin korunması bir zorunluluk haline gelince, geleneksel veri maskeleme ve anonimleştirme gibi yaklaşımların yanında federe öğrenme, homomorfik şifreleme gibi öncü ve umut verici teknikler ortaya çıkmıştır.

Veri Maskeleme ve Anonimleştirme

İnternet kullanımının son 20 yılda çok hızlı bir şekilde artmasıyla insanlar kişisel verilerini internet üzerinde birçok yerde paylaşmaktadırlar. İnternet üzerinde paylaşılmasa bile dijitalleşme ile birlikte okul kayıtlarında, alışverişlerde, hastanelerde kişisel veriler alınıp kurumların veri tabanlarında saklanmaktadırlar. Saklanan kişisel veriler dışarı aktarılacağı veya uygulama ekranında gösterileceği zaman verinin tamamını kullanmak hassas bilgilerin tehlikeye girmesine sebep olabilir. Örneğin banka üzerinde para transferi yaparken oluşturulan dekont üzerinde hesap numarasının bütün hanelerinin gösterilmesi dekontun üçüncü şahıslarla paylaşılmasına engel olacaktır.

Verilerin işlenmesi için başka bir ortama çıkarılacağı zaman da hassas verilerin gizlenmesi önem arz etmektedir. Mesela hastalıkların kişilerin yaşantısı ile ilgili makine öğrenmesi sınıflandırma çalışması yapılmasının istendiği zaman, hastaların kişisel verilerinden kimlik numaraları gibi bazı alanların çalışmayı yapacak ekiple paylaşılmasına gerek yoktur. Dolayısıyla bu verilerin korunması için veriyi saklamamız/gizlememiz/maskelememiz gerekmektedir.

Maskeleme işlemi verinin bir kısmının anlamsız (*, # vb.) ya da rastgele karakterlerle değiştirilmesi ile gerçekleştirilmektedir. Veri maskeleme ve anonimleştirme tablosunda(sayfa 84) örnek bir maskeleme işlemi görünmektedir. Hassas olan ID ve Telefon Numarası alanları ID alanı rastgele Telefon Numarası alanı da anlamsız karakterlerle değiştirilerek maskelenmiştir.

Hassas veriler maskelendiği zaman gizlenseler de hala kişisel verilerin kişilerle ilişkilendirilme tehlikesi vardır. Bir veride hassas alanlar maskelenmiş olsa da verinin diğer alanları kullanılarak o verinin kime ait olduğu ortaya çıkarılabilir. Verileri dış ortama aktarırken bu tehlikeden kaçınmak için verilerin anonimleştirilmesi gerekmektedir. Anonimleştirme, kişisel ve gizlilik içeren ham verinin kişiler ve kuruluşlarla ilişkilendirilemeyecek şekilde işlenmesidir. Maskelemeden farklı olarak hassas verinin gizliğinin yanı sıra anonim kalması da önemlidir. Anonimliği sağlamak için kulla-

> **Bir veride hassas alanlar maskelenmiş olsa da verinin diğer alanları kullanılarak o verinin kime ait olduğu ortaya çıkarılabilir.**

nılan en temel yöntem verilerin tekil kalmasının önüne geçmektir. Veri setinde bir satırın alanlarına bakılınca diğer satırlardan ayrılıyorsa bir şekilde verinin kime veya hangi kurumla ilişkili olduğunun ortaya çıkma tehlikesi vardır. Bu problemin önüne geçmek için kullanılan yöntemler aşağıda yer almaktadır.

Karakter Maskeleme: Anonimleştirmede kullanılan en temel yöntemlerden biri yazının başında bahsedilen maskeleme yöntemidir. Veri içeriğinin hepsi veya bir kısmı anlamsız veya rastgele karakterlerle değiştirilmektedir.

Genelleştirme: Verinin ifade ettiği anlamın daha geniş bir ifadeyle değiştirilme yöntemidir. Yaşı yaş aralığına çevirmek ya da adreslerde tam adres kullanmak yerine ilçe veya il adlarıyla değiştirmek örnek olarak verilebilir.

Değiştirme/Karıştırma: Veri setinin içindeki alanları birbirleriyle değiştirerek anonimleştirme sağlanır. Bu yöntem, alanların kendi içerisindeki ilişkiyi bozduğu için dikkatli kullanılmalıdır. Zira makine öğrenmesi gibi tekniklerde kullanılacaksa, modelin hatalı kalıplar öğrenmesine yol açabilir.

Veri Maskeleme ve Anonimleştirme

ID	İsim	Telefon Numarası
0000	Mahmut	5551234567
1111	Ahmet	5009876543
2222	Zeynep	5051112233

→

ID	İsim	Telefon Numarası
3842	Mahmut	55******67
2931	Ahmet	50******43
9201	Zeynep	50******33

Karakter Maskeleme:

ID	İsim	Telefon Numarası
0000	Mahmut	5551234567
1111	Ahmet	5559876543
2222	Zeynep	5551112233

→

ID	İsim	Telefon Numarası
3842	Mahmut	555*******
2931	Ahmet	555*******
9201	Zeynep	555*******

Genelleştirme:

İsim	Yaş	Adres
Mahmut	23	Mimar Sinan Mah
Ahmet	27	Cumhuriyet Mah
Zeynep	30	Mimar Sinan Mah

→

İsim	Yaş	Adres
Mahmut	21 - 25	İstanbul
Ahmet	26 - 30	İstanbul
Zeynep	26 - 30	İstanbul

Değiştirme/Karıştırma:

İsim	Yaş	Adres
Mahmut	23	Mimar Sinan Mah
Ahmet	27	Cumhuriyet Mah
Zeynep	30	Mimar Sinan Mah

→

İsim	Yaş	Adres
Zeynep	23	Cumhuriyet Mah
Ahmet	30	Mimar Sinan Mah
Mahmut	27	Mimar Sinan Mah

Federe Öğrenme

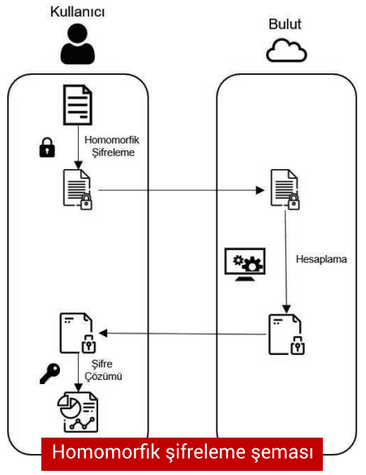
İlk olarak 2016 yılında yapılan bir çalışmada[3] karşımıza çıkan Federe öğrenme; merkezi makine öğrenmesi modellerinin yerel cihazlarda bulunan kişisel verileri görmediği ve modellerin yerel cihazlar arasında dağıtıldığı, işbirlikçi bir makine öğrenmesi yöntemidir. Federe öğrenme, verilerin tek bir merkezde toplandığı klasik makine öğrenimi yöntemlerinin aksine verileri modele getirmez, makine öğrenimi modellerini veri kaynaklarına getirir. Bu sayede, kişisel verilerin mahremiyeti ve güvenliği sağlanırken aynı zamanda model performansı için ihtiyaç duyulan büyük veriler de modellere kazandırılmaktadır. Ayrıca, klasik yöntemlerde verilerin merkezileştirilmesinden dolayı ortaya çıkan; verilerin yönetimi, işlenmesi, aktarımı gibi teknik zorluklardan da kaçınılmış olur.

Federe öğrenme yöntemi 4 temel süreç ile uygulanmaktadır;

- Merkezi sunucu, merkezi modeli ve başlangıç parametrelerini yerel cihazlara gönderir. Veriler, yerel cihazlarda bulunur ve bu verilerin yerel cihazlardan herhangi bir çıkışı olmaz.
- Yerel cihazlar, gelen merkezi modeli kendi veri kümesini kullanarak eğitir. Her yerel model, merkez sunucudan gelen en güncel parametrelerle ve yerel veri kümeleri kullanılarak eğitilir.
- Eğitilen yerel modellerin güncel parametreleri merkezi sunucuya geri aktarılır.
- Merkez sunucuda her yerel cihazdan gelen yeni parametreler, çeşitli yöntemler kullanılarak birleştirilir. Merkezi model, birleştirilen güncel parametreler kullanılarak yeniden eğitilir. Merkezi modelde optimum parametreler elde edilene kadar önceki adımlar tekrar edilir.

Federe öğrenmeye Google'ın Android cihazlardaki klavye uygulaması olan Gboard örnek verilebilir [4]. Bu uygulamada, kullanıcıya sunulan önerilerin geliştirilmesi için kullanıcıların kişisel sorgularına verilen önerilerin tıklanma durumları yerel cihazlarda depolanır. Bu verilere erişim olmadan Federe öğrenme ile Gboard'un sorgu öneri modelinin iyileştirilmesi sağlanır.

Federe öğrenmenin ilk örnekleri mobil cihazlar üzerinde yapılmış olsa da; Federe öğrenme, özellikle veri mahremiyetinin önemli olduğu Sağlık, Eğitim, Bankacılık gibi sektörlerde de kullanılmaktadır. Ayrıca literatürde, Federe öğrenme ile sağlanan mahremiyetin arttırılmasına yönelik çalışmalar da yapılmaktadır. Bu amaçla, merkezi ve yerel cihazlar arasında paylaşılan modelin ve parametrelerin gizliliğini sağlayan çeşitli güvenlik yöntemleri kullanılmaktadır.



Homomorfik şifreleme şeması

Homomorfik Şifrelemenin Makine Öğrenmesinde Kullanılması

Makine öğrenmesi, birçok sektörde kullanılmaya ve bir ihtiyaç haline gelmeye başladı. Ancak sağlık, finans gibi bazı sektörlerde verilerin özel ve hassas olması, makine öğrenmesi çözümlerinin uygulanmasına engel oluyordu. Aynı şekilde gelişen teknolojiyle birlikte veriler hızla büyümeye başlamış ve bu büyük verinin işlenmesi için daha güçlü makinelere, bulut ortamlarına ihtiyaç duyulmuştur. Kullanıcılar verilerini işlenmesi için başka ortamlara veya bulut ortamlarına aktarma ihtiyacı duymakta ve eğer verileri özelse bu veriyi bir şekilde şifrelemesi gerekmektedir. Geleneksel şifreleme yöntemleri maalesef bu soruna çözüm olamazken, homomorfik şifreleme metotları bu sorun için uygulanabilir bir çözüm sunmuştur.

Homomorfik şifreleme, şifrelenmiş veri üzerinde hesaplama yapmaya izin veren bir şifreleme yöntemidir. Şifrelenmiş veride matematiksel toplama ve çarpma işlemleri gerçekleştirilebilmektedir. Toplama ve çarpma işlemlerini yapabilmek polinom hesabı yapabileceğimiz anlamına gelmektedir. Bu sayede şifreli metin(ciphertext) çözülmeden düzyazı(plaintext) halindeki gibi işlenebilir ve analiz edilebilir olmuştur. m veriyi, E(m) ise verinin şifrelenmiş halini temsil edecek olursa:

$$E(m_1 + m_2) = E(m_1) \oplus E(m_2)$$

$$E(m_1 . m_2) = E(m_1) \otimes E(m_2)$$

Çeşitli homomorfik şifreleme yöntemleri vardır. Aralarındaki fark, şifrelenmiş veriler üzerinde gerçekleştirilebilecek matematiksel işlem türleri ve işlem sayısıdır. Bunlar Kısmen Homomorfik Şifreleme (Partially Homomorphic Encryption), Biraz Homomorfik Şifreleme (Somewhat Homomorphic Encryption) ve Tamamen Homomorfik Şifreleme(Fully Homomorphic Encryption)'dir.

Kısmen homomorfik şifreleme(PHE), sadece bir matematiksel işlemin sınırsız sayıda gerçekleştirilebildiği bir şifreleme yöntemidir. Rivest-Shamir-Adleman (RSA), ElGamal ve Paillier şifreleme metotları Kısmen Homomorfik Şifrelemeye örnek olarak verilebilir.

Biraz Homomorfik şifreleme(SHE) yönteminde ise matematiksel işlem türünden ziyade, bu işlemlerin gerçekleştirilme sayısı kısıtlıdır. Tamamen Homomorfik şifreleme (FHE) yöntemleri şifrelenmiş veriler üzerinde sınırsız sayıda hem toplama hem de çarpma işlemlerinin gerçekleştirilmesine olanak sağlar.

Homomorfik şifreleme şeması, Flaticon.com'dan alınan ücretsiz simgeler ile yapılmıştır. Eser Sahipleri: Freepik, Pixel perfect ve Smartline.

Homomorfik şifreleme ile şifrelenmiş veri üzerinde makine öğrenmesi teknikleri uygulanabilir olmuştur. İhtiyaca göre farklı kullanım senaryoları oluşturulabilmektedir. Kullanıcının önceden eğitilmiş bir makine öğrenmesi modeline veri gönderip sonuç almak istediği bir senaryoda kullanıcı, verisini şifreler ve şifrelenmiş verisini açık anahtar (public key) ile birlikte hesaplamanın yapılacağı ortama gönderir. Şifrelemede açık anahtar veriyi şifrelemek, gizli anahtar (private key) ise şifrelenmiş veriyi çözmek için kullanılır. Kullanılan şifreleme yöntemine göre modelin parametreleri açık anahtar ile şifrelenerek matematiksel işlemler gerçekleştirilir ve sonuç yine şifrelenmiş olarak elde edilir. Kullanıcı gizli anahtarı ile şifrelenmiş sonucu çözebilir. Aynı şekilde kullanıcı hazırda olan bir modeli kullanmak yerine elindeki veriyi şifreleyerek başka bir ortamda makine öğrenmesi modeli eğitebilir. Ancak veri her zaman tek bir kullanıcının elinde olmayabilir. Birden fazla kullanıcının veri sağladığı sistemlerde ise anahtar yönetimi Güvenli Çok Şahıslı Hesaplama (Secure Multi-party Computation) [5] veya Güvenilir Üçüncü Şahıs (Trusted Third Party) [6] ile yapılabilir.

Kaynakça

1. "What is Data Masking", DataSunrise. [Online]. Available: https://www.datasunrise.com/blog/professional-info/what-is-data-masking/ [Accessed: 14-Apr-2021]
2. "GUIDE TO BASIC DATA ANONYMISATION TECHNIQUES", Personal Data Protection Commission Singapore, 2018. Available:https://www.pdpc.gov.sg/help-and-resources/2018/01/guide-to-basic-data-anonymisation-techniques
3. McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." Artificial Intelligence and Statistics. PMLR, 2017.
4. https://ai.googleblog.com/2017/04/federated-learning-collaborative.html
5. Karthik A Jagadeesh, David J Wu, Johannes A Birgmeier, Dan Bonehand Gill Bejerano. Deriving genomic diagnoses without revealing patient
6. Runhua Xu, James B.D. Joshi, and Chao Li. CryptoNN: Training Neural Networks over Encrypted Data

2020 Yılı TÜBİTAK Fotoğraf Yarışması

Suyun Hayatımızdaki Yeri

Röportaj: Mehmet S.Ekinci – Başuzman / BİLGEM KKYBY

Fotoğraf sanatıyla ilgilenen TÜBİTAK çalışanlarını teşvik etmek, onları bir araya getirerek eserlerini sergilemelerini sağlamak, TÜBİTAK'a sanatsal canlılık kazandırmak amacıyla düzenlenen Fotoğraf Yarışması'nın 2020 Yılı konusu, 'Suyun Hayatımızdaki Yeri' idi.

Düzenlenen yarışmaya, TÜBİTAK çalışanları, sanatsal bir yaklaşımla farklı bakış açıları ve çekim teknikleri kullanarak ürettikleri fotoğraflarla katıldı. Seçici Kurul, 203 TÜBİTAK çalışanının gönderdiği toplam 484 fotoğrafı titizlikle inceledi. İlk üçe giren ve mansiyon alan fotoğraflar dâhil olmak üzere toplam 33 fotoğraf sergilemeye uygun bulundu.

TÜBİTAK Fotoğraf Yarışması'nda, Birincilik ödülü, İkincilik ödülü ve 3 mansiyon ödülü alan BİLGEM çalışanlarının 13 fotoğrafı, sergi için seçildi. Fotoğraflarının hikâyelerini ve fotoğraf çekmenin kendileri için ne anlama geldiğini çalışma arkadaşlarımıza sorduk...

"Rahmet'
Melih Kaya – Uzman / BİLGEM BTE

1 Birincilik Ödülü

Fotoğraf çekmek, bakmanın ötesinde görmenizi sağlar!

Melih Kaya

2020 Yılı TÜBİTAK Fotoğraf Yarışmasında ödül alan ve sergilenen fotoğraf(lar)ınızın hikayesini bizimle paylaşabilir misiniz?
Birincilik ile ödüllendirilen fotoğrafımı 2017 yılı Haziran ayında Sakarya'da bir ziyaret esnasında çektim. O gün hava kapalıydı ve zaman zaman yağmur çiseliyordu. Kısa bir yürüyüş sonrası eve dönüş esnasında buğday tarlalarının arasından geçerken gördüğüm manzara karşısında etkilendim. Yakından baktığımda ise detaylar daha çok ön plana çıktı. Beni etkileyen "O an"ı kalıcı bir anıya dönüştürdüm. Fotoğraf Yarışması konu başlığının "Suyun Hayatımızdaki Yeri" olduğunu öğrendiğim zaman yarışmaya bu fotoğrafımla katılmak istedim.

Fotoğraf çekmek sizin için ne ifade ediyor, size ne sağlıyor? Neden fotoğraf çekiyorsunuz?

> Fotoğraf çekmek, her gün 'baktığımız' çevremizdeki detayları 'görme' yetisi kazandırıyor.

Fotoğraf çekmek, her gün 'baktığımız' çevremizdeki detayları 'görme' yetisi kazandırıyor. Her gün biraz daha ayrıntıları görebilir hale geliyorsunuz. Bakmak ile görmek arasındaki farkın arasını açmaya çabalıyorsunuz. Bu çaba sizi gündelik hayatın telaşından koparıp aslında "O an"ın içinde bulunan güzel anıları biriktirmeye yönlendiriyor. Bazen kaydedemediğiniz bir görüntü, zihninizde uzun bir süre pişmanlığınız olarak kalabiliyor. Tam da bu noktada fotoğraf çekmenin kıymetini anlıyorsunuz.

Size göre iyi bir fotoğrafın olmazsa olmazları nelerdir?
İyi bir fotoğrafın olmazsa olmazı iyi bir kompozisyona sahip olmasıdır. Kompozisyon fotoğrafların etkileri ile ilgili önemli bir konudur, fotoğraf ile iletilmek istenen mesajın başarısını belirler. Fotoğrafta kompozisyon öğelerini kural olarak değil, gözün hoşlanacağı anları yakalamak konusunda birer rehber olarak görebiliriz. Bir fotoğraf kendisini ne kadar süre izlettiriyorsa o kadar başarılı bir kompozisyona sahiptir diyebiliriz.

"Susuzluk"
Oğuzhan Kireç – Teknisyen / BİLGEM UEKAE

M Mansiyon Ödülü

Fotoğraf roman gibidir, size anlatır.

Oğuzhan Kireç

2020 Yılı TÜBİTAK Fotoğraf Yarışmasında ödül alan ve sergilenen fotoğraf(lar)ınızın hikayesini bizimle paylaşabilir misiniz?
"Susuzluk" isimli fotoğrafımda susuzluğun en çok hissedildiği Emirli Baraji'nın üzücü halini kadrajıma aldım. Çünkü su kulesinin ben artık yokum dediğini duyar gibiydim. İnsanların buna aldırış etmeden balık tutmaya çalışması, beni farklı duygulara sevk etti. İşte bu duyguların bütün objelerini bu fotoğrafta anlatmaya çalıştım.

"Yağmura karşı mücadele" fotoğrafımda bir salyangozu fotoğrafladım. Su bize her ne kadar hayat ve kolaylık sağlasa da, sanırım bazılarımız için böyle olmuyor. Doğa yürüyüşü sırasında aniden bastıran yağmura karşı durmadan ilerlemeye çalışan bu küçük salyangoz gibi. İşte bu cümlelere kanıt olarak bu fotoğrafı çektim. Umarım ben yanılıyorumdur ve bu salyangoz durup yağmurun keyfini çıkarıyordur.

> Evrenin daha renkli, daha samimi ve sıcak olduğunu anlatmak için fotoğraf çekiyorum.

"Yağmura karşı mücadele"

Fotoğraf çekmek sizin için ne ifade ediyor, size ne sağlıyor? Neden fotoğraf çekiyorsunuz?
Bence fotoğraf çekmek roman gibidir, size her şeyi anlatır, dünyaya farklı bir bakış açısından bakmamızı sağlar. Evrenin daha renkli, daha samimi ve sıcak olduğunu anlatmak için fotoğraf çekiyorum.

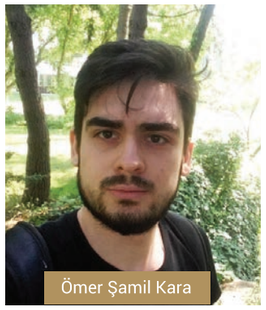
Size göre iyi bir fotoğrafın olmazsa olmazları nelerdir?
Bir fotoğrafın olmazsa olmazı bakıldığında daima heyecan verebilmesidir. Çünkü fotoğraf, geleceğimize somut bir mirastır. Bıraktığımız bu mirasa ne zaman bakarsak bakalım, ilk günkü heyecanı yakalamamız gerekir.

"Boğaza Düşen Hayat"

Ömer Şamil Kara – Araştırmacı / BİLGEM SGE

Mansiyon Ödülü

Fotoğraf, doğada zaten var olan bir kareyi kayıt altına almaktır.



Ömer Şamil Kara

2020 Yılı TÜBİTAK Fotoğraf Yarışmasında ödül alan ve sergilenen fotoğraf(lar)ınızın hikayesini bizimle paylaşabilir misiniz?

Fotoğraf yarışmasını duyduktan sonra çekebileceğim güzel fotoğraf fikirleri üzerinde düşünmeye başladım. Arabada giderken yağmur yağmaya başladığı bir sırada cep telefonu ile fotoğraf çekme fikri aklımıza geldi. Arabanın ön camına düşen yağmurlar eşliğinde bir köprü manzarası yakaladık ve güzel olduğunu düşündüğüm için bu fotoğraf ile yarışmaya katıldım.

Fotoğraf çekmek sizin için ne ifade ediyor, size ne sağlıyor? Neden fotoğraf çekiyorsunuz?

> Fotoğraf anı ölümsüzleştirdiği gibi, iyi çekildiği takdirde o ana, hiç bakılmamış yeni bir bakış açısı katabiliyor.

Fotoğraf anı ölümsüzleştirdiği gibi, iyi çekildiği takdirde o ana, hiç bakılmamış yeni bir bakış açısı katabiliyor. Belki defalarca aynı manzarayı gören insanlar bile değişik bir bakış açısıyla çekilmiş aynı manzara fotoğraflarına hayran kalabiliyor. Ben fotoğraf çekmekten keyif aldığım için fotoğraf çekiyorum.

Size göre iyi bir fotoğrafın olmazsa olmazları nelerdir?

İyi bir fotoğrafın sınırları olduğunu düşünmüyorum. Fotoğrafı iyi yapacak birçok farklı etken olabilir. Fotoğrafın aslında doğada zaten var olan bir kareyi kayıt altına almak olduğunu düşünüyorum. Fotoğrafçının görevi sadece o güzel/mükemmel kareyi arayıp bulmak, bulduktan sonra kaydetmektir.

"İparhan"

Özdemir Kavak – Başuzman Araştırmacı / BİLGEM BTE

Mansiyon Ödülü

İyi fotoğraf bir daha çekmeyi başaramayacağınız fotoğraftır!

Özdemir Kavak

2020 Yılı TÜBİTAK Fotoğraf Yarışmasında ödül alan ve sergilenen fotoğrafınızın hikâyesini bizimle paylaşabilir misiniz?

Fotoğraf çekmeye üniversite yıllarımda, abimin fotoğraf makinasıyla manzara fotoğrafları ile başladım. O zamanlar hep makro fotoğraf çekmek isterdim fakat makro lenslerin fiyatlarının yüksek olması sebebiyle bunu epey ertelemek zorunda kaldım. 2013 yılında ilk fotoğraf makinamı ve makro lensimi aldım.

> 2013 yılında ilk fotoğraf makinamı ve makro lensimi aldım. İlk çekimlerime de TÜBİTAK Gebze Kampüsü'nde başladım.

İlk çekimlerime de TÜBİTAK Gebze Kampüsü'nde başladım. Küçük canlıları çekmeye başladıkça çoğumuz için alt tarafı bir ot, çalı olan bitkilerde sayısız canlının yaşadığını fark ettim ve çekimlerim iyice bu alana kaydı. Bu küçük canlıların arasında ise renkli kanatlarıyla kelebeklerin yeri ayrıdır. Çektiğim kelebeklerin türünü merak etmeye başladım. Araştırmalarımla şimdi gönüllü yöneticisi olduğum trakel.org (Türkiye'nin Anonim Kelebekleri) adlı siteye ulaştım. Site aracılığıyla benim gibi fotoğraf çeken birçok insanla tanıştım. Artık kelebek fotoğrafçılığı benim için tutkuya dönüşmüştü. Sınırlı bir alana sahip olan Gebze kampüsümüzde 50'ye yakın kelebek, 4-5 tür orkide fotoğrafladım. Endemik türleri fotoğraflayabilmek için Isparta, Denizli, Antalya, Erzurum, Kars, Hakkâri, Van, Adana, Osmaniye'ye seyahatler yaptım; 200'ün üzerinde kelebek türü fotoğrafladım.

Fotoğraf yarışmasındaki fotoğrafı çekmek için sabah gün doğmadan yola çıkmıştım. Amacım Gebze'de bahar aylarında görülen çiğ damlalarını çekebilmekti. Arazide biraz gezindikten sonra iparhan (Melitaea cinxia) kelebeğini buldum. Kelebeği bulduğumda antenlerinde dahi çiğ damlaları mevcuttu fakat ışığın fotoğraf çekimine uygun olmasını bekleyene kadar bir kısmı kurudu. Sonuç olarak biraz uykusuz kalsam, ıslansam da amacıma ulaşmıştım.

Fotoğraf çekmek sizin için ne ifade ediyor, size ne sağlıyor? Neden fotoğraf çekiyorsunuz?

Boş zamanlarımda doğada olmak, fotoğraf çekmek fiziksel olarak yorucu olsa da mental olarak dinlenmemi sağlıyor.

Size göre iyi bir fotoğrafın olmazsa olmazları nelerdir?

Bana göre bir fotoğrafa yüklenen anlam ve kompozisyon önemlidir. İyi fotoğraf bir daha çekmeyi başaramayacağınız fotoğraftır. Işığınız bol olsun.

Atom Altı Parçacıkları Sayan Radyasyon Ölçer (SB)

Uğur Kılıç, Selen Akçelik, Prof. Dr. Melahat Bilge Demirköz / ODTÜ İVMER
Emre Sarı - Araştırmacı, Dr. Aziz Ulvi Çalışkan – Enst. Md. Yrd. / BİLGEM UEAKE

> Radyasyon Ölçer(SB), ROKETSAN yerleşkesinde yapılan çevresel testleri ve ODTÜ İVMER Laboratuvarı'nda çeşitli kalibrasyon kaynakları ile yapılan performans testlerini başarıyla geçmiştir.

2019'da kurulan Orta Doğu Teknik Üniversitesi Uzay ve Hızlandırıcı Teknolojiler Uygulama ve Araştırma Merkezi (İVMER) çalışmalarına, Kalkınma Bakanlığı'ndan 7,5 milyon TL'lik bütçe ile bir radyasyon test tesisi kurulumu için, 2015'te "Parçacık Radyasyonu Testleri Oluşturma Laboratuvarı" olarak projelendirilmesiyle başlamıştır. ODTÜ-SDH'nin (Saçılmalı Demet Hattı) kurulumu kapsamında, alt yapı desteği için Türkiye Enerji, Nükleer ve Maden Araştırma Kurumuyla (TENMAK), bilgi transferinin sağlanması için ise CERN ile işbirliği anlaşmaları imzalanmış ve bu imkânlar sağlandıktan sonra Savunma Sanayii Başkanlığı (SSB), Hava Savunma ve Uzay Dairesi ile imzalanan protokolle projeye müşteri kurum olmuştur.

Bu proje ile, uzayda kullanılacak elektronik ve yapısal malzemelerin Avrupa Uzay Ajansı'nın ESA ESCC 25100 standardına göre Tekil Olay Etkileri (Single Event Effect, SEE) testlerinin yapılması amacıyla ODTÜ SDH kurulmuş ve Savunma Sanayii Başkanlığınca kabulü yapılmıştır. ODTÜ SDH ile şu ana kadar 20 kurum ve kuruluşa test hizmeti verilmiştir.

Testlerde sunulan proton demeti; kinetik enerjisi 15 30 MeV aralığında, radyasyon alanı 15,40 cm × 21,55 cm (yaklaşık bir A4 kâğıdının boyutları) ve ±%10 homojenlikte ve proton akısı 106–1011 p/cm2/s aralığında olup, ESA ESCC 25100 standardına uygun olarak verilmektedir. Standart koşullarının sağlandığının test edilmesi için ODTÜ-SDH'de çeşitli dedektörler kullanılmaktadır.

Standart parametrelerinden biri olan demet homojenliği hakkında bilgi edinmeyi sağlamak için fiber sintilatörler ve bu sintilatörlerin altında da, çıkan fotonların algılanması için YİTAL'in ürettiği PIN Dedektör bulunmaktadır. Dört adet fiber sintilatör, okuma elektroniği kartında bulunan PIN dedektörün her bir kadranına denk gelecek biçimde üzerine yerleştirilmiştir. Düşük karanlık akımı ve hızlı tepki süresi sayesinde demet alanı X ve Y eksenlerinde yüksek doğruluk ile taranır. Fiber sintilatörlerin demet alanının içerisine girmesiyle parçacıklar sintilatörlere çarpar ve fotonlar oluşur. Oluşan bu fotonlar sintilatörlerin altında bulunan PIN dedektör'e iletilir ve okuma elektroniğinin girişinde proton akısıyla orantılı bir elektrik akımı elde edilir. PIN dedektörden elde edilen verilerle demetin homojenliği, konumu, boyutu ve akısı öğrenilir. Alınan bu veriler ODTÜ-SDH'nin Test ve Ölçüm Alt Sisteminde bulunan diğer dedektörler ile de doğrulanarak kullanılır.

ODTÜ İVMER'in çalışmalarının başarılı bir şekilde ilerlemesi ve uzay radyasyonu alanındaki deneyiminin artması ile SSB projeye, uydulardaki radyasyon miktarının ölçülmesi için kullanılacak Yerli Radyasyon Monitörü (YRM) geliştirilmesine yönelik ek iş paketleri tanımlamıştır. Bu iş paketleri kapsamındaki çalışmalarına devam eden ODTÜ İVMER, YRM'nin ilk prototipi olan Radyasyon Ölçer (SB)'i ROKETSAN işbirliği ile geliştirmiştir.

Radyasyon Ölçer (SB) YİTAL'in ürettiği iki silisyum (PIN) dedektör ile yapılmış bir parçacık teleskobuna ve bir Geiger Sayacı'na sahip radyasyon sayacıdır. Radyasyon Ölçer (SB), ROKETSAN yerleşkesinde yapılan çevresel testleri ve ODTÜ İVMER Laboratuvarı'nda çeşitli kalibrasyon kaynakları ile yapılan performans testlerini başarıyla geçmiştir.

Radyasyon Ölçer (SB), SSB tarafından başlatılan ve ROKETSAN'ın Mikro Uydu Fırlatma Sistemi Geliştirme Projesi (MUFS) ile geliştirilen SR-0.1 sonda roketinin ilk prototopine alt sistem seviyesinde entegre edilerek, katı-sıvı yakıtlı motor teknolojisiyle 26–29 Ekim 2020 tarihleri arasında başarıyla iki kez uzaya çıkmış (yaklaşık 130 km) ve geri dönmüştür.

Radyasyon Ölçer (SB) roketin ikinci aşamasının üstünde yer almış ve bilimsel yük bölmesi açıldığında doğrudan uzay ortamına maruz kalmıştır. ODTÜ İVMER ekibi uçuş öncesinde ROKETSAN ile birlikte çalışarak alt sistem seviyesinde entegrasyon yapılmasının yanında, Radyasyon Ölçer (SB)'den gelecek verilerin telemetrinin bir parçası olmasını sağlamıştır. İki uçuş için de telemetriden gelen veri ayrıştırılıp, süre-irtifa/parçacık sayısı şeklinde grafiklendirilmiş ve böylelikle uçuş kontrol odasında bulunan bir monitörden canlı olarak izlenebilmiştir.

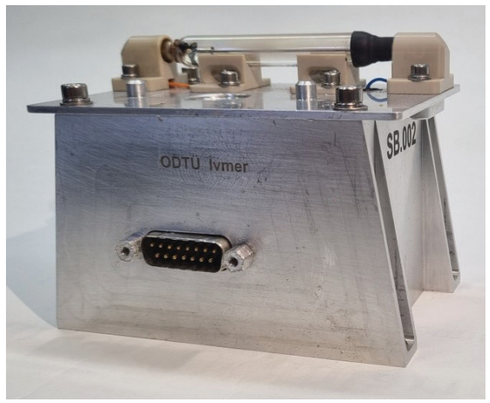
Bu başarılı uzay yolculuğu ile ODTÜ İVMER Radyasyon Ölçer (SB), atmosfer ve uzayda görev süresinin her saniyesinde radyasyon hızının ve parçacık miktarının belirlenmesini sağlamış ve böylelikle çakışık mantık prensibiyle çalışan parçacık teleskobu tasarımı doğrulanmıştır. Ayrıca anılan uçuş sayesinde "LEO'da Uzay Aracı için Uzay Radyasyon Monitörünün Tasarımı ve İlk Türk Sonda Roketinde Bir Prototip Uçuşunun Sonuçları" başlıklı bir yüksek lisans tezi yayımlanmıştır [1].

Radyasyon Ölçer (SB)'in duyarlığını geliştirmek amacıyla YİTAL ve ODTÜ İVMER çığ fotodedektörler (Avalanche PhotoDiode, APD) üzerine Ar-Ge çalışmalarına başlamıştır. Daha yüksek hassasiyetli ölçümler için çözümler sunması beklenen YİTAL'in CMOS üretim sürecine uyumlu çığ fotodiyotun tasarım özellikleri aşağıda tanıtılmıştır.

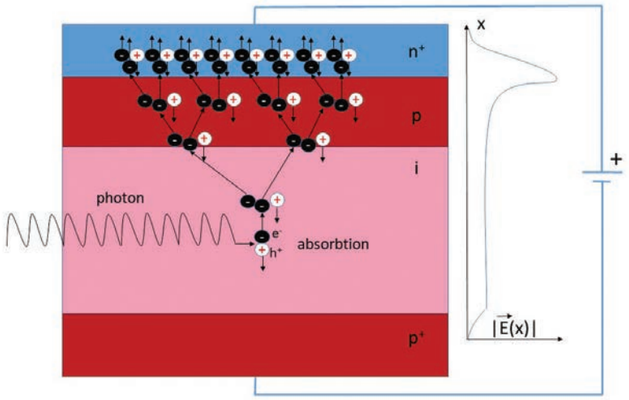
Çığ Fotodiyot

Son zamanlarda birçok sektörde teknolojik bir yarış içerisinde olan algılayıcılar gün geçtikçe gelişerek farklı uygulamalara ve özellikle otonom sistemlere yüksek duyarlıkta çözümler sunmaktadır. Gizemini -adından da anlaşılacağı üzere- çalışma yönteminden alan çığ fotodiyotlar, yüksek hassasiyetle hızlı tepki süresine sahip olarak otomotiv, uzay, askeri teknolojiler gibi birçok alanda söz sahibi olmuştur. Adını aldığı çığ bölgesi sayesinde yüksek akım kazancı sağlayarak, düşük güçteki sinyallerin algılanmasını kolaylaştırmıştır. Düşük güçlü fotonları algılayabilme özelliğiyle görüntüleme sistemlerinde, hızlı ve hassas uzaklık ölçümü yapan sistemlerde kullanılan çığ fotodiyotların yerli ve özgün bir teknolojiyle üretilmesi amacıyla ODTÜ İVMER ile birlikte YİTAL'de geliştirme çalışmalarına başlanmıştır.

Efektif bir çığ fotodiyot üretimindeki temel zorluk, yüksek kazanç ile düşük şiddetli fotonların algılanmasının hızlı bir şekilde yapılması sırasında düşük gürültüye sahip olmak ve ters belverme gerilimini sabit tutmaktır. Bu amaçla çığ bölgesi iyon konsantrasyonları ayarlanarak, oluşan elektron-delik



Radyasyon Ölçer



Şekil 1. Elektron-delik çifti üretimi ve çığ bölgesi etkisi

çiftini çoğaltma işlemi sonucunda yüksek kuantum verimliliğine sahip olunmaktadır. Saf bölgede oluşan elektron-delik çiftinin çığ bölgesine ulaştığında yüksek elektriksel alanla karşılaşması sonucu çarpışma iyonizasyonu etkisi ortaya çıkmaktadır. Bu etki sonucunda, elektronlar enerjilerini çarptığı elektronlara aktararak iletim durumuna geçirmektedir. Bu sayede düşük güçlere sahip bir sinyal dahi kazanç sayesinde algılanabilmektedir.

Işık enerjisini ve radyasyonu elektrik enerjisine çevirmede çığ fotodiyodu diğer algılayıcılardan ayıran en önemli parametre, şüphesiz çığ bölgesi tasarımı ve üretimidir. n+ tipi yarıiletken ile p tipi yarıiletken arasında oluşabilecek bir çığ bölgesinin 105–106 V/cm mertebelerinde elektriksel alana sahip olabilmesi için bu bölgenin silisyum katkı profili önem arz etmektedir. Ayrıca, katkılama miktarlarıyla bağlantılı olarak oluşacak tıkamada kutuplu p-n jonksiyonunun fakirleşme bölgesinin geniş olması nedeniyle, yüksek tıkama gerilimi altında düşük kapasite elde edilmesi, yüksek kesim frekansı düzeylerine ulaşmada önemli avantaj sağlamaktadır.

Pek çok uygulama için efektif bir spektral bölgeye sahip olan silisyum çığ fotodiyotlar 100-400V arası ters besleme gerilimlerine, 1 nA'in altında karanlık (gürültü) akımına, 2 ns altında tepki sürelerine sahip olmalarıyla geniş kullanım alanı bulmaktadır. 1,5 mm, 3 mm, 5 mm gibi küçük boyutlarıyla büyük işler başararak üzerine literatür çalışmalarının yapıldığı yarıiletken ailesinin bir parçası olan bu yapıların, gelecek teknolojilere şimdiden çözümler üreteceği aşikârdır.

Elektromanyetik tayfın morötesi, kızılötesi veya görünür ışık bölgelerinde çalışma olanağı sunan çığ fotodiyot, yüksek hassasiyetle ve düşük gürültüyle çalışma avantajıyla otonom sistemlere maliyet etkin özgün çözümler sunmaktadır. Gerek LIDAR teknolojilerine gerek askeri lazer mesafe ölçüm sistemlerine alternatif olma anlamında, çığ fotodiyot güçlü ve etkin bir adaydır. Otomotiv sektöründen askeri teknolojilere, uzay teknolojilerinden sağlık sektörüne kadar birçok alanda otonom kabiliyetlerin artması, algılayıcılara düşen görevleri daha da önemli kılmaktadır. Hata oranını düşürmek ve hızlı karar verebilmek adına, çığ fotodiyotlar gerek maliyet gerek teknolojik açıdan tercih edilmektedir.

> **YİTAL ve ODTÜ İVMER, Radyasyon Ölçer(SB)'in duyarlılığını geliştirmek amacıyla çığ fotodedektörler üzerine Ar-Ge çalışmalarına başlamıştır.**

Silisyum Çığ Fotodiyot Üretim Parametreleri

1100 nm dalga boyuna kadar yüksek kuantum verimliliğiyle algılama avantajı sunan silisyum 1,12 eV (300 K) yasak bant aralığına sahiptir. Bu enerji düzeyi ve üzerindeki elektromanyetik radyasyon silisyum çığ fotodiyot tarafından soğurulur (absorption). Belirli bir dalga boyunda soğurulan foton akısı (Q) yarıiletken içerisine nüfuz ederken soğurma katsayısına (α) bağlı olarak sönüme uğramaktadır [2]:

$$Q(x)=Q_0 . e^{-\alpha x}$$

Yarıiletken malzeme içerisinde üstel olarak sönen foton akısı elektron–delik çiftinin üretimini gerçekleştirmektedir. Optik olarak üretilmiş taşıyıcılar, yüksek tıkama gerilimi altında kırınıma uğrayıp terminallere (anot, katot) ulaşarak elektrik akımını oluşturur. Bu nedenle, dedektöre gelen fotonların elektron-delik çifti oluşturma yüzdesi olarak tanımlanan kuantum verimliliği (η) ve aygıtın giriş-çıkış arasındaki ilişkisini tanımlayan tepkiselliği (responsivity, S) etkin bir çığ fotodiyot üretimi için önem arz eden parametrelerdir:

$$\eta_e=(1-R_\lambda) . \eta_i$$

R_λ : *Yansıma katsayısı*

Çığ fotodiyot üzerine yasak bant aralığından yüksek enerjili ışık düşürüldüğünde elektronlar fotonların enerjisini soğurur ve iletim bandına geçer. İletime geçen elektronlar elektriksel alan altında ilerleyerek kontaklardan toplanır ve elektrik akımını oluşturur. Sonuç olarak, uygulanan birim optik güce karşı oluşan fotoakım olarak tanımlanan, tepkisellik parametresi ortaya çıkmaktadır:

$$S_{\lambda 0}=\eta(\lambda/1240) ,$$

λ : *Dalga boyu [nm]*

Çığ fotodiyodu diğer algılayıcılardan farklı kılan en önemli özelliği çığ bölgesi etkisidir. Optik güç karşısında oluşan elektron-delik çiftinin çığ bölgesinde yüksek elektriksel alanla karşılaşması sonucu çığ etkisi denilen multiplikasyon olayı gerçekleşmektedir. Elektronlar çarpışma iyonizasyonu etkisi sonucunda çarptığı elektronu iletim durumuna geçirerek akım kazancını sağlamaktadır. Çarpışma iyonizasyon katsayısına (α) bağlı olarak oluşan multiplikasyon faktörü (M), p-n jonksiyonu içerisinde yükselen elektriksel alanın bir fonksiyonudur:

$$M=I_m/I_p ,$$

I_m : *Multiplikasyon sonrası oluşan akım,*
I_p : *Gelen fotonun oluşturduğu akım*
$\alpha=1/(L_{int})av ,$
$(L_{int})av$: *İki çarpışma arası ortalama uzaklık*

Yüksek multiplikasyon katsayısına sahip olabilmek için çığ bölgesi kalınlığını ve bu bölgenin elektriksel alanını olabildiğince yüksek tutmak gerekir. Bu sayede akım kazancının yüksek olması mümkün olmakta, ancak, multiplikasyon katsayısına bağlı önemli bir parametre olan gürültü faktörü ortaya çıkmaktadır. PIN fotodiyotlara nazaran yüksek gürültülere sahip çığ fotodiyotlarda, çığ bölgesi nedeniyle oluşan gürültü, multiplikasyon katsayısına ve diyot üzerine gelen fotonların birincil olarak oluşturduğu elektron ve delik akımlarına bağlıdır. Çığ sürecinde çoğunluk taşıyıcıların elektronlar olduğu çığ fotodiyot tasarımlarının gürültü düzeyleri düşüktür. Ayrıca, elektron hareketliliğinin (mobilitesinin) deliğe göre yüksek olması nedeniyle çığ prosesinde çoğunluk taşıyıcı olarak elektronların baz alınması, yüksek hızlı tepki süresine sahip olmada ve gürültü akımının (I_N) düşük olmasında önemli bir parametredir [2], [3].

$$I^2=2qI_{p0} M^2 F$$

I_p0 : Fotoelektrik akımı
q : Elektron yükü
$F=I_e/(I_e+I_h)$
I_e : *Elektron akımı*
I_h : *Delik akımı*

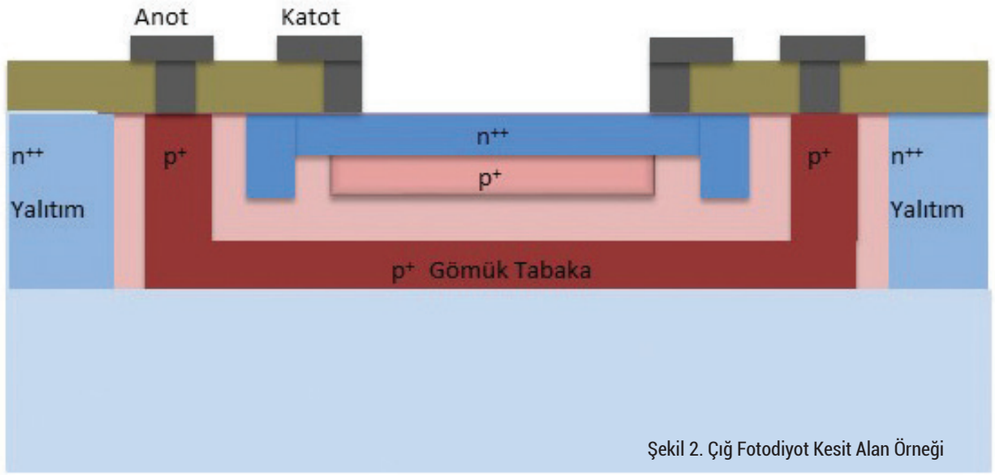
Sonuç olarak, yüksek hızlı tepki sürelerine sahip, yüksek hassasiyetli algılayıcıların gün geçtikçe öneminin arttığı teknoloji çağında, bahsedilen üretim parametreleri kullanıcı odaklı optimize edilerek üretilmiş yerli bir çığ fotodiyodun günümüzde ve gelecekte askeri ve sivil alanlarda birçok devreye etkin bir algılama avantajı sunacağı açık olarak görülmektedir.

Kaynakça

[1] A. Albarodi, "LEO'da uzay aracı için uzay radyasyon monitörünün tasarımı ve ilk Türk sonda roketinde bir prototip uçuşunun sonuçları," Yüksek Lisans Tezi, Orta Doğu Teknik Üniversitesi, Ankara, 2021. Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=9MiDp3x86xrwjpi5-14w-SHAhj4Ee55Y31X-teKIvhWbIilkj6uBemtxZrVfIY123

[2] I. Węgrzecka et al., "Design and properties of silicon avalanche photodiodes," Opto-Electron. Rev., vol. 12, no. 1, pp. 95 104, 2004.

[3] S. VK Arora, Proximity Fuzes: Theory and Techniques. New Delhi: Metcalfe House, 2010.



Şekil 2. Çığ Fotodiyot Kesit Alan Örneği

FOTAS Projesi: Fiber Optik Kablolarla Sismik Analiz

Mücahit Kavaklı - Araştırmacı, Hasan Yetik - Uzman Araştırmacı,
Dr. Umut Uludağ – Başuzman Araştırmacı / BİLGEM UEKAE

> TÜBİTAK BİLGEM'de 2016 yılında, DAS teknolojisi kullanılan Fiber Optik Tabanlı Akustik Sensör (FOTAS) Projesi'ne başlanmıştır.

Günümüzde fiber optik (FO) kablolar haberleşme sistemlerinde yaygın ve etkin olarak kullanılan iletim hatlarıdır. Özellikle 90'lı yıllardan günümüze internet kullanımının artmasıyla birlikte çok hızlı büyüme sağlamıştır. Bu nedenle ülkeler fiber optik altyapısını sürekli genişletmektedir. Günümüzde fiber hatların uzunluğu dünyada milyonlarca km ile ifade edilirken Türkiye'de 404 bin km'lik fiber hat mevcuttur [1].

Yapılan bilimsel çalışmalar neticesinde fiber optik kablolar sadece veri iletimi için değil bir sensör olarak sıcaklık, basınç, gerilme gibi fiziksel ölçümlerin algılanmasında da kullanılmaktadır. Son yıllarda ise noktasal sensörlerden kurulu klasik ağlara kıyasla uzun menzilli hatların tüm konumlarının gerçek zamanlı ve yüksek çözünürlüklü olarak gözlemlenmesinde kullanılmaya başlanmıştır. FO sensörler, üretimden yapı sağlığı izlemeye, çevre ve sınır güvenliğinden boru hatlarında sızıntı tespitine, savunma teknolojilerinden sivil erken uyarı sistemlerine kadar uzanan geniş bir yelpazede kullanım ve uygulama alanına sahiptir. Bu uygulamalarda FO sensörleri bir algılama dizini olarak kullanılmasına olanak sağlayan sistemlere literatürde Fiber Optik Dağıtık Akustik Algılama (DAS) denmektedir [2].

DAS, yeni ve benzer işi yapan sistemlere göre 100 km'yi aşabilen algılama menziline ve yüksek uzamsal çözünürlüğe sahip, uygun fiyatlı, nispeten daha az bakım gerektiren, düşük güç tüketimli, sahada enerji ihtiyacı olmayan bir teknolojidir. Ayrıca haberleşme amaçlı kullanılan sıradan fiber kablolar kullanılarak gerçeklenebilir. Bu sebeple kullanıma sunulacak birçok yerde hâlihazırda fiber optik kabloların bulunması nedeniyle sahaya kurulumu en hızlı sistemdir. Çoğu fiber haberleşme hattında, yedek olarak tutulan bir dizi kullanılmayan fiber optik kablo bulunur. Bu kablolarda herhangi bir veri iletişim yapılmaz ve literatürde karanlık fiber (Dark fiber) olarak anılır. Kullanım dışı olan bu fiberler DAS sisteminde sıklıkla kullanılmaktadır. Bu yönüyle ülke sınırları, deniz ve okyanus tabanı, petrol boru hatları, karayolları ve demir yolları gibi yer ve bölgelerde DAS sisteminin kurulumu kolaylıkla gerçekleştirilebilmektedir.

DAS sistemlerinin kullanım alanı, ilgili optik/elektronik tasarımın geliştirilmesi, parametre değişikleri ve teknolojik gelişmeler sayesinde sürekli genişlemektedir. Yeni bir alan olarak sismik hareketlerin DAS sistemi aracılığıyla tespit ve analiz edilmesinde potansiyel bir çözüm olarak karşımıza çıkmaktadır. Günümüzde yer kabuğunda meydana gelen sismik hareketleri algılamak, analiz etmek amacıyla dünyanın farklı yerlerine üç uzamsal boyutta yer hareketlerini algılayan ve kaydeden sismometreler yaygınlıkla kullanılmaktadır. Tek bir sismometre ile depremin oluşturduğu dalgaları tespit etmek mümkün iken deprem hareketlerini, depremin yerini, büyüklüğünü ve topografik haritalanmasını çıkarmak gibi amaçlar için çok sayıda sismik algılayıcı içeren ulusal ve ulaslararası boyutta sismik ağlar oluşturulmuştur. Ayrıca bu ağlardan gelen veriler analiz edilerek deprem/tsunami erken uyarı sistemleri geliştirilmek amacıyla Japonya, ABD, Türkiye gibi ülkelerde çalışmalar yapılmaktadır. Bu ve benzeri amaçlar için Türkiye'de sismik istasyonların kurulmasına 1970'lerde başlanmıştır. 2019 yılı Ekim ayı itibariyle Türkiye'deki toplam ivmeölçer ve hızölçer sayısı 1100 civarındadır [3]. Bu sismik ağların sayılarını arttırarak daha hassas ölçümler yapmak için önemli bir yatırım gerekmektedir.

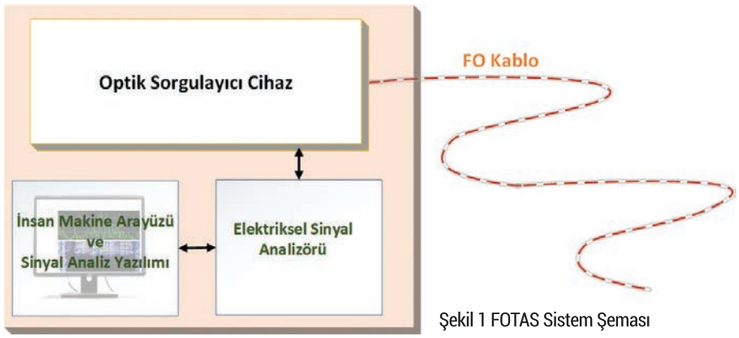
Sismometrelerin uygun yerlere yerleştirilmesi, uzun vadeli bakım maliyetleri, sismometreler arasındaki zaman sekronizasyonu, her sismometre için ayrı güç kaynağı ve veri iletim hattı gereksinimi önemli zorluklar olarak karşımıza çıkmaktadır [4]. Ayrıca nüfusu yoğun olan bölgeler ve deniz tabanı gibi yerlere fiziksel limitler dolayısıyla sınırlı sayıda sismograf yerleştirilebilmektedir. Bu noktada DAS sisteminin sismik araştırmalarda kullanılmasındaki önemli motivasyonlar olarak; fiber optik kabloların çoğu yerde mevcut olması, sahada fazladan güç gereksiniminin olmaması, tek bir merkezden yönetildiği için saat senkronizasyonunun basit olması, efektif olarak sensörler arası mesafenin çok yakın konumlandırılabilmesi, şehir içinde, deniz ve okyanus geçişlerindeki boş fiberlerin kullanılabilmesi sayılabilir.

Nasıl Çalışıyor?

FO kablo üzerinde meydana gelen gerilme, akustik etki, kırılma ve kopma gibi fiziksel etkilerin tespitinde OTDR (Optical Time Domain Reflectometry) ölçüm yöntemleri kullanılmaktadır. Bu yöntemler, FO hatta gönderilen lazer darbelerinin yansıyan veya çeşitli saçılma mekanizmaları (Rayleigh, Brillouin veya Raman) ile geri saçılan kısmının zamana, frekansa ve faza bağlı analizine dayanmaktadır. Bu sayede ölçüm zamanı ve fiziksel etkinin meydana geldiği konumu ilişkilendirilerek olaylar konumlarıyla birlikte tespit edilmektedir.

TÜBİTAK BİLGEM olarak geliştirdiğimiz sistem, DAS uygulamalarında sıklıkla kullanılan yaklaşımlardan biri olan ve genlik tabanlı eşevreli OTDR (C-OTDR) sistemiyle Rayleigh geri saçılımının analizine dayanmaktadır. Çalışma prensipleri klasik OTDR ile benzer olan bu teknolojide FO hatta iletilen lazer ışığı sebebiyle hat boyunca geri saçılan enerji hattın yakınındaki sismik aktivitelerden veya mekanik harekelerden etkilenmektedir.

Sistemin temelini oluşturan ana bileşenler Şekil 1'de gösterilmiştir.



Şekil 1 FOTAS Sistem Şeması

Optik Sorgulayıcı Cihaz (OSC): Lazer kaynağı, optik modülatör, optik kuplör, optik sirkülatör ve dengeli foto algılayıcı (DFA) gibi elemanlardan oluşan bileşendir.

Elektriksel Sinyal Analizörü (ESA): Foto algılayıcıdan gelen elektriksel sinyalin sayısallaştırıldığı, optik modülatörün darbe genişliği ve darbe tekrarlama sıklığı pa-

rametrelerinin ayarlandığı, gürültü giderimi, filtreleme gibi işlemlerin yapıldığı bileşendir.

Sinyal Analiz Yazılımı (SAY): ESA parametrelerinin belirlendiği, sinyal işleme algoritmalarının entegre edildiği ayrıca dosya kaydetme, silme gibi işlemlerinin yapıldığı bileşendir.

Lazer kaynağından çıkan ışığın bir kısmı istenilen uzamsal çözünürlük ve maksimum uzaklığa karşılık gelen darbe genişliğine ve darbe tekrarlama frekans değerine göre modüle edilir ve fiber hatta gönderilir, diğer kısmı optik yerel osilatör olarak kullanılır. Fiber optik hattan dönen Rayleigh saçılmaları ile optik yerel osilatörden gelen ışık çarpılır, sonrasında elde edilen ışık foto algılayıcının girişlerine verilerek optik sinyal elektriksel sinyale dönüştürülür. Elektriksel sinyal önce uygun filtrelemelerden sonra sayısallaştırıcıdan geçirilir. Son olarak sinyal işleme teknikleri uygulanarak hat üzerinde meydana gelen mekanik ve sismik etkiler tespit edilerek veri kütüphanesine kaydı yapılır.

Bu sistemde darbe genişliği, lazerin gücü, hattın uzunluğu ve darbe tekrarlama frekansı arasında önemli bir ilişki ve denge bulunmaktadır. Örneğin, gönderilen ışığın darbe genişliği arttırıldığında oluşturulan sanal sensörler arası mesafe artmakta ve sensör sayısı azalmaktadır, fakat bu sayede daha fazla lazer gücü fiber optik hatta verildiği için daha uzun mesafeleri algılama imkanı elde edilmektedir. Bu nedenle DAS teknolojisinin kullanım alanına göre sistemin tasarlanması, parametrelerinin belirlenmesi önem arz etmektedir. Daha ayrıntılı bilgi için [5] makalesine bakılabilir.

FOTAS, Depremleri Kayıt Altına Alıyor!

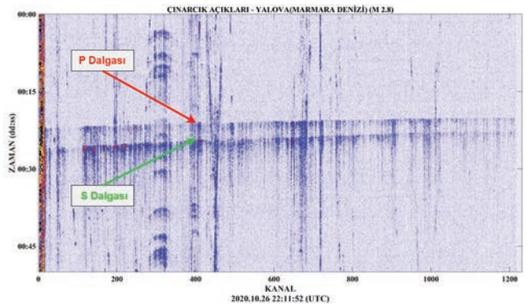
TÜBİTAK BİLGEM olarak 2016 yılından itibaren bu teknolojinin ülkemize kazandırılması ve hem sivil hem de askeri amaçlar doğrultusunda kullanılabilmesi amacıyla DAS teknolojisi kullanılan Fiber Optik Tabanlı Akustik Sensör (FOTAS) Projesi'ne başlanmıştır. Bu çalışmalar neticesinde 2019 yılında tehdit sezimi uygulaması olarak prototip tasarımı ve testleri tamamlanmıştır. Geliştirilen FOTAS sisteminin TÜBİTAK-Sanayi işbirliği çerçevesinde ürünün satışa hazır ticari bir ürün haline getirilmesi amacıyla Kocaeli'nde bulunan bir firmaya teknoloji transferi gerçekleştirilmiştir. Şu an itibariyle kullanıma hazır olan ürün ülkemizin farklı yerlerinde hizmet vermeye başlamıştır [6].

DAS teknolojisinin diğer uygulama alanlarında da ürün geliştirmeye yönelik olarak 2019 yılında deprem, patlama gibi sismik hareketlere neden olan olayların görece daha düşük maliyet ve kurulum ile tespit ve analiz edilmesi amacıyla çalışma başlatılmıştır. Bu kapsamda ilk etapta elimizde bulunan mevcut 3 km'lik fiber optik hatlarımız ile veri alımına başlanmıştır. Daha sonra, aldığımız umut vaadeden sonuçlar neticesinde biri Gebze (Kocaeli) yerleşkemiz ile İstanbul ili arası 30 km uzunluğunda, diğeri Gebze yerleşkesinden İzmit Körfezi'ni geçerek Yalova ili arası 25 km uzunluğunda olmak üzere iki uzun menzil fiber optik hattı çalışmalarımızda kullanılmaktadır. Bu hatlardan aralıksız olarak veri kayıt faaliyetlerine devam edilmektedir.

FOTAS sistemini sismik verileri algılama amaçlı kullanmaya başladığımız 2019 yılından itibaren, Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) [7] ve Boğaziçi Üniversitesi Kandilli Rasathanesi ve Deprem Araştırma Enstitüsü'nün (KRDAE) [8] verilerine göre büyüklüğü 1.8 ile 6.7, hattımıza uzaklığı ise 16 ile 867 km arasında değişen yüzün üstünde deprem sistemimiz tarafından algılandı ve veri kütüphanemize kaydedildi. Bu veriler arasında Denizli, İstanbul, Elazığ, İzmir, Konya gibi illerimizde meydana gelen depremlerin yanı sıra Yunanistan, Romanya gibi çevre ülkeler ile Akdeniz ve Ege'de meydana gelen belirli büyüklüklüğün üzerindeki depremler de bulunmaktadır.

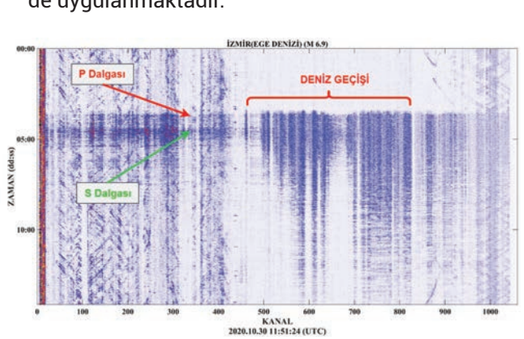
FOTAS sistemiyle alınan bu verilerde deprem sonucu sismik hareket meydana geldikten sonra oluşan ilksel (Primary wave) ve ikincil (Secondary wave) dalgaları tespit edilmektedir. P dalgası, S dalgasına göre daha hızlı ilerleyen ancak etkisi görece düşük bir sismik dalgadır. Deprem bilimciler bu iki dalga arasındaki ilişkiyi kullanarak depremin uzaklığı, konumu ve büyüklüğü hakkında bilgi elde etmektedirler. Ayrıca bu bilgi deprem ve tsunami erken uyarı sistemlerinde de kullanılmaktadır.

Şekil 2'de FOTAS sistemi ile 2020.10.26 - 22:11:52 tarih ve saatinde algılanan Çınarcık açıklarındaki depremin yaklaşık 30 km'lik fiber optik hattımız üzerindeki etkisi görülmektedir. Dikey eksen zamanı, yatay eksen ise 25 metre aralıklarla dizilmiş 1232 adet sanal sensörü ifade etmektedir. Bu sensör sayısı daha önce de ifade edildiği üzere ihtiyaca ve şartlara göre arttırılıp azaltılabilmektedir. İlk olarak P dalgasının, sonrasında da S dalgasının hattı etkilediği görülmektedir. Ayrıca sensörlerin konumları gereği deprem merkez üssüne uzaklıkları değişiklik gösterdiğinden dolayı dalganın farklı zamanlarda geldiği görülmektedir. Bu özellikle sismometrelerin çok uzak kaldığı veya olmadığı karada veya denizdeki lokasyonlarda depremlerin tespitinde öncü rol oynayabilme potansiyelini içermektedir. Ayrıca bu şekilde FOTAS sisteminin algıladığı çevresel gürültü de görülmektedir.



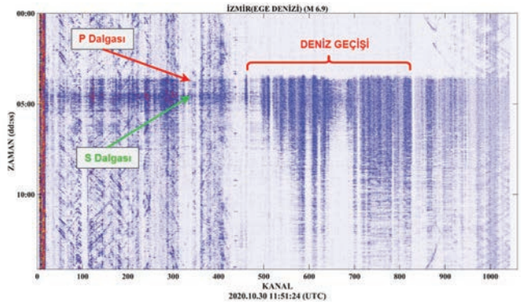
Şekil 2 Çınarcık Açıkları (M 2.8) Depremi:
FOTAS Sistemi ile Algılanan Sinyal

Marmara bölgesindeki fay hatlarını belli noktalarda kesen yaklaşık 25 km'lik diğer hattımız deniz geçişini de içermesi nedeniyle çevresel gürültüye daha az maruz kalmaktadır. Şekil 3'te İzmir açıklarında 2020.10.30 – 11:51:24 tarih ve saatinde meydana gelen 6.9 büyüklüğündeki depremin FOTAS sistemi ile algılandığı görülmektedir. Hattımıza uzaklığı yaklaşık 400 km olan deprem hemen hemen tüm sanal sensörlerimiz tarafından algılanmıştır. Şekilde deniz altından geçen fiber optik kabloda çevresel gürültü çok az iken şehir içinde kalan kısımda çevresel etkinin yüksek olduğu görülmektedir. Sistemizdeki bu istenmeyen çevresel etkileri azaltmak veya gidermek için filtreleme, gürültü giderimi gibi sinyal işleme tekniklerinin yanında farklı teknikler de uygulanmaktadır.



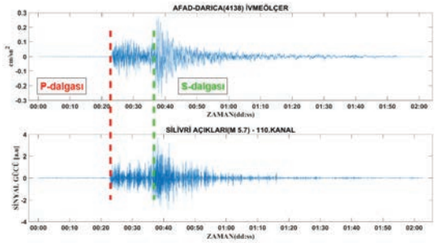
Şekil 3 İzmir Açıkları (M 6.9) Depremi: FOTAS Sistemi ile Algılanan Sinyal

Şekil 4'te 2019.09.26 – 10:59:24 tarih ve saatinde Silivri (İstanbul) açıklarında meydana gelen 5.7 büyüklüğündeki depremin yerleşkemiz içerisinde bulunan yaklaşık 3 km'lik hattımıza etkisi görülmektedir.



Şekil 4 Silivri Açıkları (M 5.7) Depremi:
FOTAS Sistemi ile Algılanan Sinyal

FOTAS sisteminde her sanal sensör ayrı ayrı ya da sensör dizisi olarak incelenebilmektedir. Şekil 5'te yerleşkemize yakın konumdaki AFAD'a ait Darıca'ya (Kocaeli) konumlandırılmış 4138 istasyon numaralı ivmeölçer ile FOTAS sisteminin sanal sensörü arasındaki ilişki görülmektedir. Sensör ve jeofonun birbirine yakın olması nedeniyle P ve S dalgalarının geliş zamanları arasında büyük oranda benzerlik bulunmaktadır.



Şekil 5 AFAD Kaydı ve FOTAS Sistemi 110. Kanal Karşılaştırması

Yukarıda açıklanan bağlamda fiber optik sistemlerin en belirgin özelliği maliyet etkin bir sensör dizisi olarak kullanılabilmesidir. Bu durum sismik hareketler hakkında hem uzamda hem de zamanda bilgi vererek birbirine uzak konumlandırılmış sismometrelerin sağlayamadığı uzamsal çözünürlüğü elde etmemizi sağlayacaktır. Bu sayede deprem hakkında daha fazla bilgi elde edileceği öngörülmektedir. Bu sistemin sismik araştırmalarda nispeten yakın zamanda kullanılmaya başlanmasına rağmen sistemin sürekli geliştirilmesi ve yeni sinyal işleme tekniklerinin uygulanmasıyla ilerleyen zamanlarda sismoloji alanında önemli etkileri olacağı düşünülebilir.

Sonuç olarak bu aşamada sürekli ve gerçek zamanlı meydana gelen sismik hareketlerin izlenmesi ve depremlerin tespiti noktasında geleneksel sismik algılama sistemlerini tamamlayıcı potansiyeli olduğu gözükmektedir. TÜBİTAK BİLGEM bu alandaki çalışmalarına sanayi ve akademi paydaşlarıyla birlikte devam edecektir.

Kaynakça
[1] Bilgi Teknolojileri ve İletişim Kurumu. (2020, Haziran). Türkiye Elektronik Haberleşme Sektörü Üç Aylık Pazar Verileri Raporu 2020-Q2. BTK: http://eng.btk.gov.tr/pazar-verileri
[2] Hartog, A. H. (2018). An Introduction to Distributed Optical Fibre Sensors. Boca Raton: Taylor and Francis Group.
[3] Afet ve Acil Durum Yönetimi Başkanlığı. (2021). AFAD. Türkiye Deprem Gözlem Sistemleri Çalışma Grubu: https://deprem.afad.gov.tr/icerik?id=4&menuId=91
[4] M. R. Fernández-Ruiz, M. A.-L.-H. (2020). Distributed acoustic sensing for seismic activity monitoring. APL Photon.
[5] Özkan, E., Erkorkmaz, T., Cesur, B., Yetik, H., Uludag, U., & Ölçer, İ. (2020). FOTAS (Fiber Optic Based Acoustic Sensing System): requirements, design, implementation, tests and results. SPIE Future Sensing Technologies. SPIE : https://spie.org/Publications/Proceedings/Paper/10.101117/12.2581713?SSO=1
[6] SAMM TEKNOLOJİ. (2021). FOTAS. Samm: http://www.samm.com/fiber-optic-akustik-algilama
[7] AFAD. (2021). Son Depremler. AFAD: http://deprem.afad.gov.tr/sondepremler
[8] KRDAE. (2021). Bölgesel Deprem-Tsunami İzleme ve Değerlendirme Merkezi. KOERİ: http://www.udim.koeri.boun.edu.tr/zeqmap/osmap.asp

TÜBİTAK BİLGEM

Bu bir proje tanıtımıdır.

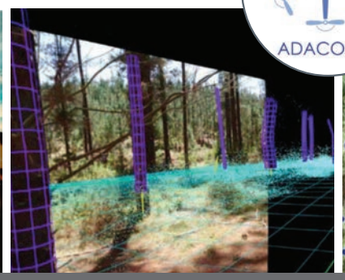
ADACORSA

Esnek Sistem Mimarileri Üzerinde Havadan Veri Toplama

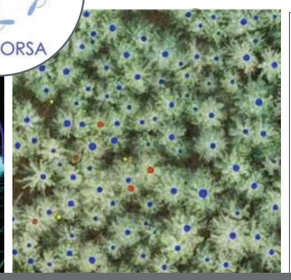
- TÜBİTAK BİLGEM, 12 farklı ülkeden 49 kuruluşu bir araya getiren HORİZON 2020 Çağrısı kapsamında yer alan ADACORSA Projesi'nde ülkemizi temsil eden taraflardan biridir.
- Şantiye içerisinde otonom çalışan insansız inşaat araçlarının dron ile koordineli çalışmasını sağlamak için, içerisinde yapay zekâ teknikleri ile çok-ajanlı yol planlama, araç görev planlama ve zamanlama modüllerini içeren bir algoritma tasarlanacaktır.
- Elektro-Optik ve multispektral (MSI / HSI) kameralarla donatılmış insansız hava araçları kullanımıyla ağaç türlerini belirlemek, yaşlı / ölü ağaçları tespit etmek, orman envanteri ve kereste hacim tahmini yapmak için uzaktan algılama, görüntü işleme analiz teknikleri ve teknolojilerinin yardımıyla derin öğrenme modelleri ve algoritmalarının geliştirilmesi planlanmaktadır.

ADACORSA

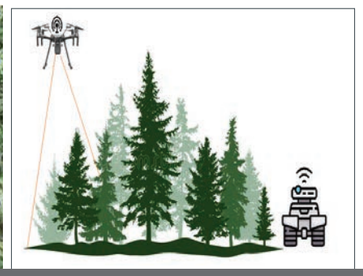
İnşaat alanı içinde otonom çalışan iş makineleri



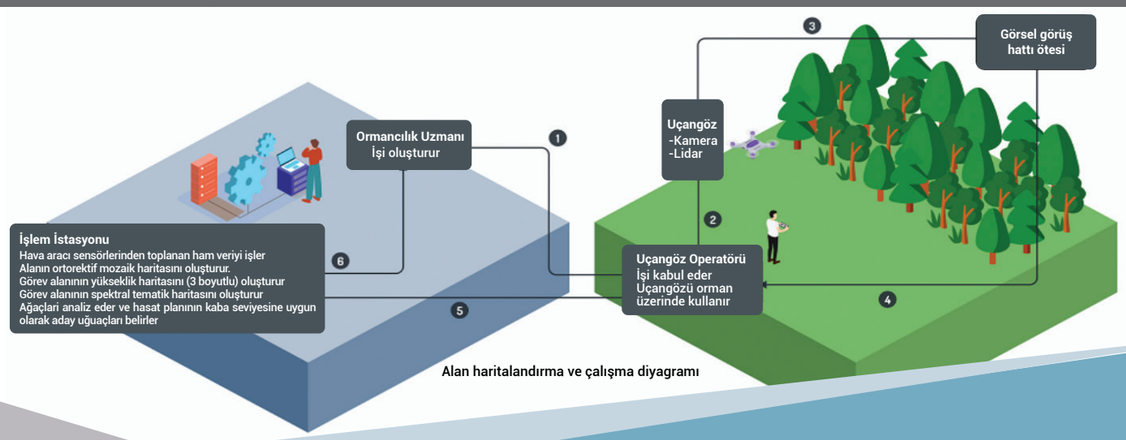
Ağaç çapı tespiti



Alanların yükseklik haritalarının çıkarılması



Drone taraması



Alan haritalandırma ve çalışma diyagramı

www.bilgem.tubitak.gov.tr

Dr. Süleyman Temel Yalçın Anısına…

Bu sayımızda, 15 Aralık 2020'de vefat eden, TÜBİTAK çatısı altında önemli hizmetlerde bulunmuş, UEKAE ve TÜBİTAK UME eski yöneticilerinden Dr. S. Temel Yalçın'ı anmak ve genç kuşaklara tanıtmak istedik. Kendisiyle birlikte çalışmış, isimlere 'Dr. S. Temel Yalçın'ı sorduk. Ortaya çıkan portre, çalışma hayatında gerçekten örnek ve model alınacak seviyede.

Bu vesileyle Hocamıza bir kez daha Allah'tan rahmet dileriz…

Temel Yalçın ve TÜBİTAK

> Temel Yalçın, 1 Şubat 1979 tarihinde TÜBİTAK MAM Uygulamalı Fizik Bölümü'nde araştırmacı olarak çalışmaya başladı.

Doç. Dr. Fatih Üstüner - Öğretim Üyesi / istanbul Ticaret Üniversitesi

Rahmetli Temel Yalçın Bey'le 1 Nisan 1996'da TÜBİTAK'ta işe girişimle beraber tanıştım. UME'de görevlendirildiği 2004 yılına kadar, onun biriminde çalışan bir personel olarak ortak mesaimiz devam etti. Bu dönem Temel Beyin, TÜBİTAK'taki ikinci çalışma dönemiydi. Daha önce 1992 yılında kurumdan emekli olmuş, 1994 yılında tekrar kuruma geri dönmüştü. 1996 sonrasında şahit olduğum döneme ait hatıralara geçmeden önce kısaca Temel Beyin özgeçmişinden bahsetmek isterim.

Özgeçmişi

1942 yılında dünyaya gelen Süleyman Temel Yalçın Bey, 1964 yılında Ankara Üniversitesi Fen Fakültesi Fizik Bölümü'nü bitirdi. Aynı bölümde yüksek lisans yapan Temel Bey, 1967 yılında Milli Eğitim Bakanlığı'nın bursunu kazanarak doktora öğrenimi için İngiltere'ye gitti. 1973 yılında Nottingham Üniversitesi Fizik Bölümü'nde Doktorasını tamamladıktan sonra yurda döndü ve önce Ankara Üniversitesi Fizik Bölümü'nde daha sonra aynı üniversitenin Tıp Fakültesi'nde araştırma görevlisi olarak çalıştı.

1 Şubat 1979 tarihinde TÜBİTAK Marmara Araştırma Merkezi Uygulamalı Fizik Bölümü'nde araştırmacı olarak çalışmaya başladı. 1985-1992 yılları arasında bugünkü Ulusal Metroloji Enstitüsü'nün temelini oluşturan, o zamanki adıyla "Milli Fizik ve Teknik Ölçme Standartları Merkezi"-nin, Dr. Birol Altan liderliğinde yürütülen kuruluş çalışmalarında yer aldı. Bu merkezin önde gelen araştırmacılarından biri olarak ilk laboratuvarların kurulumunda görev yaptı. Temel Bey bu dönemde özellikle akusto-optik, foto-akustik, ultrasonik ve sualtı akustiği alanlarında yoğun olarak çalıştı. Bu döneme ait ve Temel Bey'in bir konu üzerinde odaklanıp nasıl yoğun emek sarf ettiğini gösteren güzel bir örneği, emektar teknisyenlerimizden Sefa Ogan'ın bir hatırasını paylaşarak aktarmak isterim.

Sefa Ogan anlatıyor: "1986 yılında Deniz Kuvvetleri Komutanlığı'ndan bir grup subayımız Gebze'de çalıştığımız Uygulamalı Fizik Bölümü'nü ziyaret ettiler ve Temel Bey'le görüştüler. Amerika Birleşik Devletleri'nden alınan denizaltının sonar transduserinin çalışmadığını, ABD'den de gerekli yedek parçaları alamadıklarını yana yakıla anlattılar ve çözüm aradıklarını söylediler. Temel Bey, subayların ilettiği sonar transduserine ait kritik performans parametrelerini not aldıktan sonra uzun bir literatür araştırmasına girişti. Eşi Engin Yalçın Hanım bana 'bu adama ne oldu, dünyayla irtibatını kesti, gece gündüz durmadan çalışıyor' diyordu. Sonunda Temel Bey hesaplamalarını bitirdi, mükemmel empedans uyumu için uygun piezo-elektrik seramik malzemeyi ve boyutlarını belirledi. Tasarladığı piezo-elektrik seramik yapıyı Malzeme Enstitüsü'nde ürettirerek paketledi, testlerini gerçekleştirdi ve Deniz Kuvvetlerine teslim etti. Deniz Kuvvetleri, sonarı bu üretilen transduserle çalıştırmayı başardı".

UEKAE Yılları

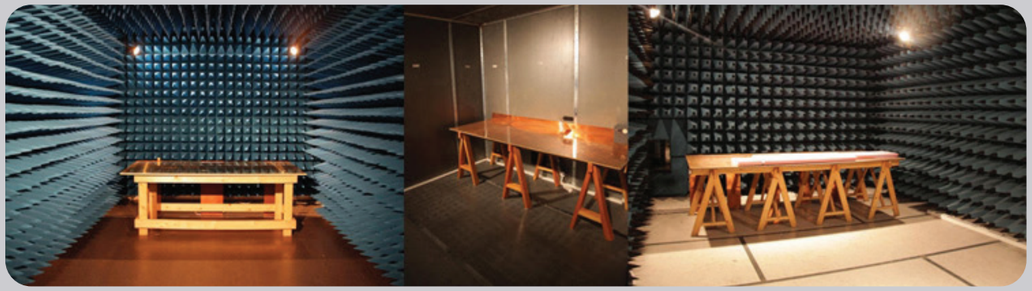
Temel Bey, 1992 yılında aldığı ani bir kararla TÜBİTAK'tan emekli oldu. İki yıl sonra Önder Yetiş Bey'in daveti üzerine TÜBİTAK MAM UEKAE'de Enstitü Müdür Yardımcısı olarak tekrar TÜBİTAK'ta çalışmaya başladı.

Bugünkü BİLGEM'in temelini oluşturan UEKAE enstitümüz 1994 yılında Marmara Araştırma Merkezi'ne bağlı olarak faaliyetlerini sürdürüyordu. Enstitü Müdürlüğüne, o dönemde özelleştirme kapsamında kapısına kilit vurulan TELETAŞ Ar-Ge'nin eski müdürü Önder Yetiş Bey henüz yeni gelmiş ve hızlı bir şekilde UEKAE Enstitüsünü kriptoloji alanında millileşme çabalarının odak noktası olması yönünde adımlar atmaya başlamıştı. Bu noktada, bu kutlu millileşme çabasının başta gelen kahramanları olan o zamanki müdürümüz Önder Yetiş Bey ve Genelkurmay MEBS Emniyet Şube'de kripto projelerinden sorumlu olarak görev yapan proje subayımız Rahmetli Mehmet Camalan'ı saygıyla anmak isterim.

TEMPEST Projesi

Çalışma hayatının bu ikinci döneminde Temel Bey, millileşme çabasının bir ayağını oluşturma görevini kendisine misyon edindi. Bu kapsamda gizlilik dereceli bilgi işleyen cihazlardan elektromanyetik ışıma yoluyla kaynaklanan bilgi kaçaklarını tespit etme ve incelemeyi konu edinen TEMPEST projesini hayata geçirmek için kolları sıvadı ve yoğun bir çalışma dönemine girdi. Tek başına TEMPEST projesiyle ilgili tüm ön araştırmaları yaptı ve kapsamlı bir teknik rapor hazırlayarak bu projenin yerli beyin gücüyle hayata geçirilebileceği fikrini ortaya koydu. Proje, nitelik olarak o zamanki UEKAE'nin personel yetkinlik profiline uzak bir projeydi. Projenin başladığı 1995 yılında UEKAE'nin henüz 50 kişi civarında bir personel mevcudu vardı ve bu personelin hemen hepsi, sayısal elektronik alanında uzmanlaşmış kişilerden oluşuyordu. UEKAE'de, elektromanyetik alanda çalışan bir kişi veya ekip mevcut değildi.

Bu koşullar altında Temel Bey, bir fizikçi olarak taşın altına tek başına elini koymuş ve ağırlıklı olarak henüz yeni mezun olmuş genç mühendislerden oluşan bir ekip oluşturmaya başlamıştı. ASELSAN'da edindiğim üç yıl RF tasarım mühendisliği tecrübesiyle, UEKAE Enstitü Müdür Yardımcılığı'nın yanı sıra Ar-Ge 951 TEMPEST Projesinin yürütücülüğünü de yapan Temel Bey'in ekibine 1 Nisan 1996 yılında dâhil oldum. Temel Bey o sırada 54 yaşında idi, projedeki diğer herkes 20'li yaşlarındaydı. Temel Bey bizim öğretmenimiz, biz de onun bir anlamda talebeleriydik.



Projenin iki önemli ayağı vardı: Elektromanyetik ışımanın algılanması ve algılanan işaretin işlenmesi. Projenin her iki kısmının da kendi içlerinde yeni açılımları barındıran nitelikleri vardı. Her günümüz yeni şeyler öğrenmekle ve uygulamakla geçiyordu. Temel Bey her sabah hepimizin odalarını ziyaret edip heyecanla, yeni açılım alanlarına ilişkin edindiği teknik bilgileri paylaşıyordu. Bu teknik bilgileri anlatırken bizim mühendis kökenli oluşumuzu zaman zaman unutuyor, bazı güncel konuları teorik fizik konularıyla irtibat kurarak heyecan içinde anlatırken bazen konudan tamamen koptuğumuz anlar da oluyordu.

Bu arada kurulumu devam eden EMC TEMPEST laboratuvarının, ilerleyen zamanda finansal olarak kendi ayakları üzerinde durması, ancak belirli bir düzenin kurulmasıyla mümkündü. 2001 yılında Türk Akreditasyon Kurumu'nun laboratuvar akreditasyon faaliyetlerine başlaması, ihtiyaç duyduğumuz düzenin kurulması anlamında bir çıkış yolu olarak gözüktü. Temel Bey, metroloji geçmişiyle akreditasyon sürecini bizzat yönetti ve EMC TEMPEST Test Merkezi (ETTM) olarak, Nisan 2003'de Türkiye'nin ilk akredite test laboratuvarı olma başarısını gösterdik. O dönemde ülkenin en kapsamlı test laboratuvarlarına sahip bir kuruluş olarak akreditasyon kavramına doğal olarak aşina olan TSE, bizden sonra, Aralık 2003'de akredite oldu.

Temel Bey, sayısal elektronikle iştigal eden arkadaşlarımıza TEMPEST konusunu anlatırken "her bit ışır" derdi. Bununla kastettiği fiziksel fenomen, sayısal devrelerde anahtarlama sırasında çekilen anlık akımın, devre yollarını birer anten gibi kullanarak elektromanyetik ışımaya yol açmasıydı. Bu ifade tarzı, onun anlaşılması zor konuları basitleştiren ama bilimsel çizgiden taviz vermeyen fizikçi kimliğini göstermesi açısından güzel bir örnektir.

Anı

Temel Bey'le birçok anımız var. Hatırımda yer eden önemli bir anı onunla birlikte platform seviyesinde elektromanyetik ortam etkileri konusunda yaptığımız öncü çalışmalardı. Bu konuda 1997 yılında yayınlanan MIL-STD-464 dokümanını birlikte Türkçeye çevirip Türkiye'deki farkındalığın artması için çeşitli sempozyum ve toplantılarda konuya ilişkin sunumlar yaptık. Genelkurmay Başkanlığı için Elektromanyetik Ortam Etkileri dokümanını hazırladık ve 1999 yılında Genelkurmay Başkanlığı'nda yüksek seviyede düzenlenen bir toplantıda sunumunu gerçekleştirdik.

O zaman gündemde olan ilk ATAK projesi kapsamında, TAI'ye platform seviyesi elektromanyetik ortam etkileri testlerinin yapılabileceği devasa büyüklükte bir test laboratuvarı için fizibilite çalışması yaptık. Yüksek güçlü mikrodalga silahları konusunda ilk bilgileri toparlamaya başladık. Birlikte yaptığımız bu çalışmalar esnasında onun sorgulayıcı bilimsel yaklaşımı, beni derinden etkilemiştir. Temel Bey'le çalışırken edindiğim bu bilimsel yaklaşımın, daha sonra TÜBİTAK bünyesinde yürüttüğüm Enstitü Müdürlüğü görevlerinde karşılaştığım çok farklı disiplinlerde teknik olarak doğru kararları almada bana çok yardımcı olduğunu özellikle belirtmek isterim.

Temel Bey bizlere öncülük yaptı. TEMPEST projesinde Temel Bey'in ekibinde görev yapan arkadaşlar zaman içinde kurumda o dönem nüvesi atılan yeni alanlarda çalışmalarına devam ettiler. Bugün faaliyetlerine devam eden UEKAE Elektronik İstihbarat Birimi, BTE Sensör ve Anten Sistemleri Birimi, TDBY EMI/EMC Test Değerlendirme Birimi ve TEMPEST Test ve Değerlendirme Birimi ortaya çıktı. Bu birimler, Temel Bey'in ülkemize yaptığı katkıları gösteren yaşayan örneklerdir. Temel Bey 15.12.2020 tarihinde vefat etti. Ruhu şad olsun.

Bir Bilim İnsanının Ardından…

Ar-Ge 951 Projesiyle, Türkiye'nin ilk akredite EMC laboratuvarının kurulması, askeri testleri yapma kabiliyetinin kazanılması ve TEMPEST çalışmalarının başlatılması hedeflenmişti.

Prof. Dr. Bahattin Türetken - Öğretim Üyesi / Kocaeli Üniversitesi

Çıraklar ustalarını, öğrenciler hocalarını, araştırmacılar da proje liderlerini anlatırken 'ne öğrendiysem ondan öğrendim' cümlesini nadir kurar. Bilimi hayat felsefesi haline getirmiş, berrak bir hayatı düstur edinmiş bir bilim insanın arkasından başka ne denebilir ki… Evet, genç bir akademisyen iken tanıdığım Temel Bey'i anlatırken 'ne öğrendiysem ondan öğrendim' cümlesini rahatlıkla kurabilirim.

Ağustos 1998 yılı, saat 14:30. Plansız bir iş görüşmesi için odasına girdim. Plansız diyorum, çünkü o gün hasbelkader TÜBİTAK'tayım. Aslında iş görüşmesi demek doğru değil, tanışma diyelim. Hızlı, pratik, matematiksel ve bir o kadar da fiziksel bir konuşma. Şaşırmıştım. Daha önce gördüklerim gibi değil. Daha tanışırken aramızda şöyle bir konuşma geçti:
- Elektriksel yük 'vektörel' midir?
- Hayır, efendim, skalerdir.
- Peki ya akım?
- Akım yoğunluğu (J) vektörel, akım (I) skalerdir efendim.
- Peki, zamana bağlılık yoksa elektrik alan manyetik alana bağlı olabilir mi?
- Olabilir efendim. Eğer ortamda iletkenlik varsa olur. Ama bu bir dalga hareketi oluşturmaz.

Hızlı hareketlerle, gözlüklerini takıp telefona yöneldi. Bir numara çevirdi:
- Emine, Önder Bey orda mı?
- Odasında efendim. Telefonu meşgul. Bitince bağlıyayım.
- Önder Bey, sana bahsetmiştim bir teorisyen almayı düşünüyorum gruba diye… Onu buldum.
Sonra telefonu kapatıp bana döndü ve
- Seni işe aldım.
- Efendim ben bugün başka bir Enstitü ile görüşmek için davet edildim,
desem de beni Emine Hanıma yönlendirdi. Ve ertesi gün, hayatımın 15 yılını paylaşacağım, babacan, duygusal, zeki, çalışkan, hızlı, tatlı-sinirli bir yöneticimle iş hayatımın ilk günüydü. Yeni enstitü kurulmuş, teknolojik bağımsızlığımızı özellikle savunma sanayiinde sağlamak için gece gündüz çalışmaların başladığı ilk yıllardı…

Ar-Ge 951 Projesi devam etmekteydi. Bu proje ile Türkiye'nin ilk akredite EMC laboratuvarının kurulması, askeri testleri yapma kabiliyetinin kazanılması ve TEMPEST çalışmalarının başlatılması hedeflenmişti. Temel Bey, proje dokümanını tek başına, gelecek yılları görürcesine hazırlamış, bu proje ve daha sonraki bir çok projenin başarıyla yürütülmesine öncülük etmişti.

Kişiliği

Temel Bey çok merhametli, dirayetli, ahlaklı ve bilgiliydi. Olaylar arasında muhteşem bağlantılar kurar, problemlere farklı açıdan bakardı. Çalışanları arasında oldukça 'adaletli' bir duruş sergilerdi. Asla kin gütmez, kızgın ve sinirli olduğu anda kalp kırdığını düşünse o gün onu tamir ederdi. Gönül rahatlığıyla söyleyebilirim ki, asla kendisine kırıldığım bir an olmamıştır. Sesini yükseltse bile, merhametli ve önyargısız duruşu, bir an bile kendisine olan sevgimizi ve saygımızı eksiltmemiştir.

Berrak bir zihne sahipti. En zor problemleri bile hatırlar, çözer, yorumlardı. Görmediği, rastlamadığı konu pek azdı. Yeni popüler konular ilgisini çeker, onunla ilgili kitapları kütüphaneden alır ve sabaha kadar bitirir, ertesi gün öğrenmiş bir şekilde gelirdi. O tarihlerde ben de kütüphaneyi yoğun kullanırdım. Aldığım her kitabın arkasında, bir önceki kitabı alan kişi olarak onun adına rastlardım.

Koruyan kollayan, sahip çıkan bir proje lideriydi. Proje toplantıları veya sunumlarına onunla gidersek kendimizi oldukça rahat hissederdik. Çünkü o gelen her türlü soru, eleştiri gibi olumsuzlukları göğüslerdi.

Bilmediği, anlamadığı, özümsemediği hiçbir şeyi 'duymuş' gibi aktarmazdı. Yaptığı işlerde asla bir baştan savma olamazdı. Yazılan dokümanlar, dil, terminoloji oldukça hassas bir süzgeçten geçerdi.

Hassas ve zihni oldukça açık bir bilim insanıydı. Yaptığı her işi hakkıyla yapmayı severdi. TEMPEST'in temelini oluşturan Van Eck deneyini kendi tasarımıyla gerçekleştirmişti. Bu çalışmasını, yıllarca soyut olarak anlatmakta zorlandığımız TEMPEST' i kavratmak için 'demo' olarak yapardık.

Anı

Bir gün, Ankara MUBILDESKOM' da yapmış olduğumuz bir projenin tamamlanma ve kabul işlemi var. Üst rütbeli generaller de kabul işlemine gelecek. Temel Bey'in tasarımı olan demoyu da yapmamız gerekiyor. Düzenek kuruldu. Anten konumlandırıldı. Paşalar gelmeden önce demo yapıldı. Beklendiği gibi sistem başarı ile çalışıyor. Temel Bey sistemden az uzaklaşıp tekrar geri geldiğinde görüntü kayboluyor. Tekrar uğraşıyor. Tekrar çalıştırıyoruz. Bekleme anında biraz uzaklaşınca tekrar bozulma oluyor. Dolayısıyla stres oldukça fazla. Ya paşalar gelince çalışmazsa. Temel bey çok sinirli. Derken sistemi çalıştırdı. Başından ayrılmıyoruz. Neyse ki vakit geldi. Generaller geliyor haberini alınca Temel Bey bana döndü ve "Sakın buradan ayrılma... Biri ayarları değiştiriyor" dedi:) İçimden gülümsedim. Ama "tamam efendim" dedim.

Evet, gerçekten de sonradan orda bulunanlardan birisi itiraf etti. Temel Bey uzaklaşınca düğmeleri karıştırıp bakalım yapabilecek mi? Görüntü gerçek mi diye kendi çapında zorluk çıkarmaya çalışıyormuş... Oldukça başarılı bir sunum yapmıştı. Asla bir heyecanı olmaz, en yüksek mertebeden insanlara bile öğrencilere anlatır gibi berrak anlatım yapardı.

Öngörülü biriydi. Olaylar arasında bağlantı kurar, inovasyonları tetiklerdi. Ondan öğrendiğim şu iki cümle bugünümüze ışık tutar cinstendir:

• Her bit ışır. (bilgiyi işarete çevirdiğiniz zaman kontrolden çıktı demektir)

• Yazılım biter, üniversiteler kapanır. (Günümüzde bilgiye ulaşım teknikleri değiştiğinden üniversiteler değişime uğrayacak gibi. Yazılımın bitmesini ise her şeyin 'gömülü' olacağı anlamını taşıdığını ifade etmek isterim.)

Sonsöz

Evet, gönül rahatlığıyla tekrar yineliyorum. Ne öğrendiysek senden öğrendik. Çalışmayı, başarmayı, adaleti, merhameti... Ve öğrenmeye çalıştık, yapılan kötülükleri de affedecek kadar engin bir yürek taşımayı...

Ruhun şad olsun Kıymetli Hocam. Rahat uyu. İnandığın değerler uğruna ömrünü verecek ekip arkadaşların var.

Rahmetli Süleyman Temel Yalçın Bey

Temel Bey birbirinden farklı konularda, hatta uzmanlık alanlarının dışında bile çok detaylı bilgilere sahipti. Astronomiden balıkçılığa, arabalardaki ateşleme sistemlerinden bitkilere kadar pek çok farklı alanda, adeta o alanların uzmanı gibi konuları bize anlatırdı.

Bilal Kılıç- Başuzman Araştırmacı / BİLGEM TDBY

Rahmetli Süleyman Temel Yalçın Bey ile uzun yıllar birlikte çalıştık. Kendisi bilgili, deneyimli, çabuk parlayan ama kin tutmayan, hoşgörülü ve iyi niyetli bir yöneticimiz idi. Kızdığı zaman yüzümüze doğrudan söylerdi. Ama arkadan bizi sürekli savunur ve kollardı. Kendisini çok severdik. Rahat ve huzurlu bir çalışma ortamımız vardı. Sicil notlarımız her zaman çok yüksek olurdu. Kendisi ile yakın çalıştık ve birçok güzel hatıramız oldu.

Temel Bey ile 2000 yılında tanıştım. O tarihte ASELSAN'da çalışıyor idim. Temel Bey ve Fatih Bey ASELSAN'a gelmişlerdi. Orada tanıştım. Daha sonra ASELSAN'dan ayrılıp o zamanki adı UEKAE olan şimdiki adı BİLGEM olan bu kuruma geçmek istedim. Bunun için Gebze'ye iş görüşmesine gelmem gerekiyordu. Çalıştığım kurumdan izin alabilmem için izin nedenini yöneticimize söylememiz gerekiyordu. Ben de yöneticimize iş değişikliği için izin alacağım diyemediğim için Temel Bey'e Gebze'ye iş görüşmesi için gelemediğimi, mümkünse bu görüşmeyi kendisi Ankara'ya görevli geldiği zaman Ankara'da yapmak istediğimi söyledim. Sağ olsun bu talebimi kabul etti. Ankara'ya iş için geldiği bir zamanda konakladığı otelin lobisinde akşam saatlerinde iş görüşmesini yaptık.

Temel Bey bizlerle teknik konuları sık konuşurdu. Birbirinden farklı konularda, hatta uzmanlık alanlarının dışında bile çok detaylı bilgilere sahipti. Astronomiden balıkçılığa, arabalardaki ateşleme sistemlerinden bitkilere kadar pek çok farklı alanda, adeta o alanların uzmanı gibi konuları bize anlatırdı. Bu çok az insanda bulunan bir özelliktir. Bunu yapabilmek için öncelikle çok fazla okumak, okuduğunu anlamak, anladığını akılda tutmak, unutmamak ve bu birbirinden farklı birçok konuyu derli toplu anlatabilmek gerekir. Bende biraz eski bir kitap vardı. Zannediyorum elektromekanik ile ilgili idi. Yalnız kitap oldukça ağdalı bir İngilizce ile yazılmıştı. İngilizcede pek kullanılmayan kelimeler, ifadeler vardı. Cümle yapısı da uzun ve karmaşıktı. Yani kitap zor ve sıkıcı idi. Bir akşam mesai bitiminde biraz da muziplik olsun diye kitabı Temel beye verdim ve okumasını önerdim. Şundan emindim. Temel Bey o kitabı zor ve sıkıcı diye bırakmayacak mutlaka okuyacak, anlayacak ve anlatacaktı. Kitabı okuma işinin bir iki hafta kadar süreceğini zannediyordum. Temel Bey ertesi sabah geldi. Selamlaştık, konuşmaya başladı. Kitabı bana baştan sona anlattı. Yüzüne baktım gözleri uykusuzluktan kızarmıştı. Anladım ki gece boyunca kitapla uğraşmış ve kitabı bitirmişti. Bu kitabı, İngilizceyi ve ilgili konuyu çok iyi bilen birisinin bir iki haftadan önce okuması ve kavraması pek mümkün değildi. Belli etmedim ama hayretler içerisinde kaldım.

Temel Bey, kontrol etme ve yönetme hususunda baskın biri değildi. Bizi serbest bırakır, bizlere alan açardı. Bu bize daha fazla konfor ve özgüven verdi. Arkadaşlarla zaman zaman çatışma içerisine de girerdik. Ama bölümdeki bütün arkadaşlar belirli alanlarda uzmanlaştı. İlerleyen yıllarda kimisi akademisyen, kimisi iş insanı, kimisi yönetici, kimisi araştırmacı oldu. Birimdeki arkadaşlar hem teknik, hem idari hem de akademik alanda belirli yerlere geldiler.

Bir gün ofiste bir araştırmacı arkadaşımız ve bir güvenlikçi personelimiz sigara içiyordu. Her zaman böyle yapmazlardı ama o gün biraz rahat davranmışlardı. Temel Bey, sigara içen arkadaşlarımızı uzaktan gördü. Müthiş bir şekilde kızdı hatta biraz da kovaladı. Arkadaşlar hızlıca tabanları yağladılar. Temel Bey'in kızgınlığı en fazla bir gün sürerdi. Ertesi gün her şey normale dönmüş olurdu.

Kendisi ile ve birimdeki arkadaşlarla sık sık Ankara'ya genellikle günü birlik görevlere giderdik. Genelkurmay ve bağlı birliklerde toplantılara katılır, çalışmalar yapardık. Sabah güneş doğmadan yola koyulur ve aynı gün gece geç saatlerde İstanbul'a dönerdik. Allah rahmet eylesin. Mekânı cennet olsun.

Temel Bey Çalışanına Güvenirdi!

Temel Bey bir taraftan otoriterdi, diğer taraftan çalışanları işlerinde oldukça özgür bırakırdı, ancak çalışmaları da çok iyi takip ederdi.

Dr. Hamza Özer – Enstitü Müdür Yardımcısı / BİLGEM BTE

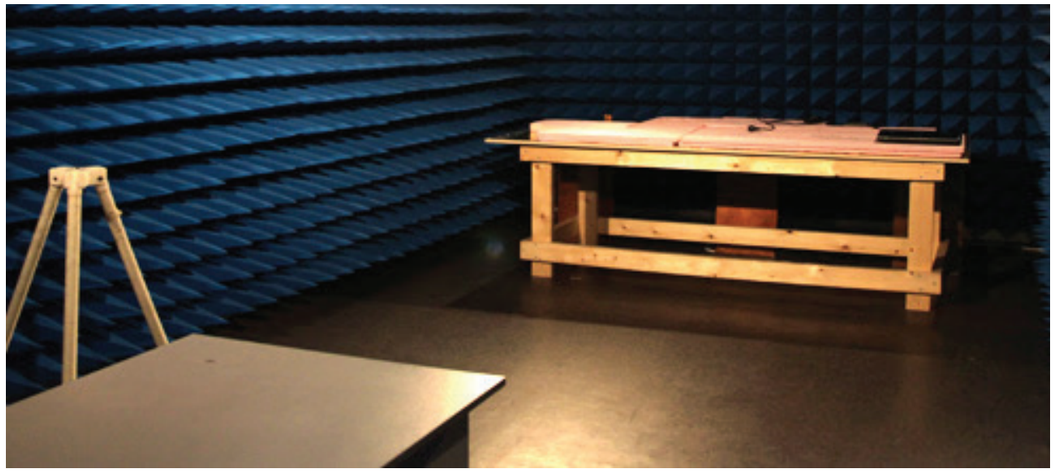
Temel Bey'i ilk defa, ben Üniversite'de asistanken, TÜBİTAK Başkanlık'ta bir proje toplantısında tanıdım. Konularına çok hâkim olduğunu gördüm, bunun yanında toplantıya ve çevresine de o kadar hâkimdi ki içimden "bu kim acaba, galiba TÜBİTAK Başkanı" diye geçirmiştim. Aradan bir süre geçti, TÜBİTAK UEKAE'de işe girdim ve kendimi Temel Bey'in laboratuvarında buldum. Başlangıçta tereddütlerim olsa da zaman geçtikçe orada, Temel Bey'in yanında çalışmaktan çok memnun oldum.

Temel Bey bir taraftan otoriterdi, diğer taraftan çalışanları işlerinde oldukça özgür bırakırdı, ancak çalışmaları da çok iyi takip ederdi. Çalışanına güvenir, çalışmalarına saygı duyar ve bunu da gösterirdi. Çok zeki, hızlı kavrayan, yeniliklere açık bir yapısı vardı. Çabuk sinirlenen biriydi, ama biz bilirdik ki siniri uzun sürmeyecekti ve yaptığı şey tamamen bizim ve kurumun iyiliği içindi. Kısacası çalışanlarını evladı gibi görürdü, sinirlenip kızması bile onların daha iyiye doğru gitmesi içindi. Kesinlikle kin tutmaz, yanlış yapana kızsa da oldukça toleranslı davranırdı. Bilirdik ki bize anlık olarak kızsa da aynı zamanda bizi koruyup kollardı. Özlük hakları gibi konularda yanına bir şey istemek için hiç gitmezdik, çünkü bu konularda herkesin hakkını zaten vereceğinden emindik.

Temel Bey'le ilgili çok anımız var, ama ilk aklıma geleni anlatmak istiyorum. Bir gün laboratuvarımızdaki en önemli cihaz olan TEMPEST alıcısı ile bir ölçüm yapıyorduk. Cihazın girişine, koruma amaçlı 'transient limiter' aygıtını takmadığımız için cihazın giriş kartını yaktık. Tamir ücreti 30 bin dolar civarındaydı. Büyük bir korku içinde Temel Bey bize ne yapacak diye düşünmeye başladık. Temel Bey geldi, durumu inceledi, bunun bir tecrübe eksikliğinden olduğunu anladı ve bize uzun bir nutuk çekti (aslında uzun bir ders verdi). Hiç uçak uçurmaya çalışmazsanız, hiç uçak düşürmezsiniz; ama hiçbir zaman da uçak uçuramazsınız dedi ve gitti. Bizi hayret ve hayranlık içinde bırakan bu hareketini hiç unutmuyorum.

Yeniliklere açıktı, çok hızlı okur, okuduğunu ve dinlediğini hızlı kavrardı. Bilmediğini veya az bildiğini çok rahatlıkla bilmiyorum der, kesinlikle ahkâm kesmeye çalışmazdı. Bunun yanında bildiği konularda kendinden çok emindi. Dinleyici olarak bulunduğumuz konferans/seminer gibi etkinliklerde, konuşmacıların bir yanlış veya eksiğini gördüğünde karşısındakinin unvanına bakmaksızın müdahale ettiğini çok gördüm.

Temel Bey ile ilgili anlatacak çok şey var. Dergi yazısının bir bölümü olmasından dolayı şimdilik burada keserek, kendisini saygı, sevgi, minnet ve rahmetle anıyorum. O artık gitti ama yaptıkları, bıraktıkları ve yetiştirdiği bizler varız. Ve bu sayede aslında yapmaya devam ediyor...



Temel Yalçın Güzel Bir İnsandı!

Alparslan Babaoğlu – Eski Enstitü Müdür Yardımcısı / BİLGEM UEKAE

Temel Bey'le 1993 senesinde, TELETAŞ'tan TÜBİTAK MAM'a bağlı Elektronik Araştırma Ünitesi'ne geçtiğimizde tanıştım. Bende bıraktığı ilk izlenim, çabuk sinirlenen, bilimsel doğrularından asla taviz vermeyen ve inandığı doğrular için sonuna kadar mücadele eden birisi şeklindeydi. Herkesle kolay samimi olmayan, özel hayatı konusunda fazla konuşmayan bir yapısı vardı.

Zamanla dost olduk. O senelerde hepimiz, kendi alanımızla ilgili devletin güvenliğinin sağlanması için üzerimize düşeni yapmak ve bilgi güvenliği konusunda TÜBİTAK'ı bir mükemmeliyet merkezi haline dönüştürmek için elimizden geleni yapma gayreti içindeydik.

Ben kripto konusuna odaklandım ve TSK'dan kullandıkları kripto algoritmalarının güvenlik düzeylerinin belirlenmesi amacıyla bir Kriptoanaliz Merkezi teşkil edilmesi için önemli bir proje aldım. Temel Ağabey de askerî yetkilileri TEMPEST konusunda ikna edip bir TEMPEST Test Merkezi kurmayı çok istiyordu; ancak elle tutulur gözle görülür somut bir konu olmadığı için yetkililer bir türlü ikna olmuyordu.

Bir gün küçük bir TV alıcısı aradığını söyledi. Benim bekarlıktan kalma kullanmadığım siyah beyaz bir küçük televizyonum vardı onu teklif ettim ve işyerine getirdim. Televizyon üzerinde şimdi hatırlamadığım bazı tasarım düzenlemeleri yaptı, bir almaç ve anten kullanarak düzeneği test edip gizlilik dereceli bilgi işleyen bir bilgisayarın ekranındaki bilgileri, uzaktan anten ve almaç vasıtasıyla televizyonun ekranında göstermeyi başardı.

Hemen askeri yetkililerden randevu aldık ve birlikte Ankara'da gösterim yapacağımız birliğe gittik. Nöbetçi Amir ile görüşüp konferans salonunda gizlilik dereceli bir toplantının yapıldığı binanın dışına düzeneği kurduk. Temel Ağabey biraz uğraşıp ayar yaptıktan sonra içerdeki bilgisayarın ekran görüntüsünü bizim televizyonun ekranına çıkartmayı başardı. Hemen toplantıdaki komutanlara haber gönderip bahçeye davet ettik. Komutanlar gördüklerine inanamamıştı ama Temel Ağabey, yaptığı gösteri sayesinde onları ikna edip kısa süre içinde çok arzu ettiği TEMPEST Test Merkezini kurmak için yanlış hatırlamıyorsam 5 Milyon TL'lik bir proje almayı başarmıştı.

Daha sonraki yıllarda bu merkez ülkenin bilgi güvenliği için çok önemli işlere imza attı, sayısız yetenekli mühendisin yetişmesine aracı oldu. Enstitü'ye her gelen ziyaretçinin mutlaka ziyaret edip bilgi aldığı ve Temel Ağabey ya da ekibinin yaptığı gösterilerle "yok canım daha neler, toprak hattından ya da kalorifer borusundan da bilgi sızar mı?" diye dehşete düştükleri ve TEMPEST konusunda bilinçlendikleri bir yer haline geldi.

İnandığı doğruların peşinden giden, ülkeye çok önemli hizmetleri olmuş bir güzel insandı. Allah rahmet eylesin, nûr içinde yatsın inşaallah .

Dr. Umut Uludağ: Gerçek, insan olarak hep aradığımız yegâne şeydir.

Röportaj: Mehmet S.Ekinci – Başuzman / BİLGEM KKYBY

Bu sayıda BİLGEM UEKAE'de Başuzman Araştırmacı olarak çalışan Sayın Dr. Umut Uludağ ile bir röportaj gerçekleştirdik. Umut Hocamız hayata, sanata, şiire-dair önemli ve özgün şeyler anlattı, gençlere nelere odaklanmalarıyla ilgili tavsiyelerini iletti…

BİLGEM UEKAE'de araştırmacı olarak çalışıyorsunuz. Akademide dersler veriyorsunuz. Şiir yazıyorsunuz. Yoğun zihin jimnastiği yaptıran kriptoloji soruları hazırlıyorsunuz. Karikatür çiziyorsunuz… Bu yaptıklarınız sizin için ne ifade ediyor? Ya da şöyle sorayım bunların her birinden devşirdiğiniz öz nedir?

Profesyonel ve akademik çalışmalarım dışındakiler, ara sıra karşılaştığım ve beni hayli rahatsız eden, bu çalışmalar dışındaki zamanımı boşa harcadığım hissine karşı geliştirebildiğim savunma mekanizmaları belki de. Elimden gelenleri şimdilik belirttiğiniz bu mecralarda sunabiliyorum, ama kesinlikle "iyi" veya bahsettiğim hissi uzaklaştırmada "çok başarılı" olduklarını iddia etmiyorum. Bu bağlamda bir müzik aleti çalabilmek, resim yapabilmek (ortaokulda düşük not aldığım tek ders idi), profesyonel şekilde spor yapabilmek de isterdim mesela, umarım ileride mümkün olur.

> **Anlatılmak isteneni en kısa şekilde anlatabilmenin yolu bence şiirdir. Ki insan belli sınırlar içinde anlatmadan yapamıyor.**

Şiirde biraz daha duralım isterseniz… Sizce şiir nedir? Diğer edebi veya bilimsel ürünlerden farkı nelerdir?

Anlatılmak isteneni (ki insan belli sınırlar içinde anlatmadan yapamıyor bazı şeyleri başka bir kişiye, evcil hayvana, bitkiye, kağıda, sevdiği bir semte veya kendi kendine) en kısa şekilde anlatabilmenin yolu bence şiir. Diğer edebi türler, hikâye, roman gibi anlatılacakları çok daha geniş, detaylı bir şekilde aktarabiliyorlar ve bu hem yazar hem de okuyucu için çok değerli. Ama şiirde, anlatılanın belki de fevkinde anlatılmayan, anlatılamayanların nüvesi var diye düşünüyorum. Sanki mısralar gerçeğin çevresindeki, onun şeklini almış bir çeper gibi, gerçek de insan olarak hep aradığımız, aramak zorunda olduğumuz yegâne şey.

Kariyerinizle ilgili biraz bilgi verebilir misiniz? Planladığınız doğrultuda mı gelişti? Önemli dönüm noktaları nelerdi?

Kariyerlerimizi ne yazık ki tam anlamıyla yeteneklerimiz, isteklerimiz, olanaklarımız çerçevesinde gerçekleştiremiyoruz her zaman. Bu genel problem, bütün dünyada kaynakların (zaman, yer, materyal, ekonomik güç, bilgi vb.) kısıtlı olması, hızlı nüfus artışı gibi sebeplere dayanıyor. Sonuçta hayatlarımıza, büyük oranda merkezi sınav diye adlandırdığımız, zorunlu ama üzerinde düşünülmesi gereken bir yöntemle yön vermek durumunda kalıyoruz. Ben bu bağlamda, nispeten şanslı olduğumu ve istediğime yakın bir şekilde ilerleyebildiğimi düşünüyorum. İstanbul Atatürk Fen Lisesi ve Boğaziçi Üniversitesi'ndeki eğitimim, profesyonel-akademik hayatta ihtiyaç duyacağım yetenekleri bana kazandırdı. Bu vesileyle ilgili eğitmenlerime tüm emekleri için kalbî şükranlarımı sunmak istiyorum.

Dr.Umut Uludağ

1977'de İzmir'de doğdu, 1999 ve 2001 yıllarında Boğaziçi Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü'nden lisans ve yüksek lisans derecelerini aldı. 2006 yılında, doktora eğitimini biyometrik sistemler üzerine yaptığı çalışmalarla Michigan State Üniversitesi'nde (ABD) tamamladı. 2009'dan bu yana TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde başuzman araştırmacı olarak çalışıyor.

Araştırma ilgileri arasında biyometri, örüntü tanıma, imge&sinyal işleme ve kriptoloji bulunmaktadır. 2013-2020 yılları arasında üniversitelerde misafir öğretim üyesi olarak biyometri dersleri verdi.

TÜBİTAK BİLGEM ağ sayfasında 2010'dan beri "Ödüllü Kriptoloji Soruları", TÜBİTAK Bilim Genç ağ sayfasında ise 2020'den bu yana "Ayın Şifrebilim Sorusu" etkinlikleri için sorular hazırlıyor. "Kayıp Hattat" isimli şiir kitapçıklarını 2015'den beri kişisel ağ sayfasında (umutuludag.com) yayınlıyor.

Eğitim süreci sonrasında 1999 yılında çalışmaya başladığım TÜBİTAK, biyometri alanındaki doktora eğitimim için yurt dışına gitmeden önce teori-pratik, çalışma-sonuç alma, bilme-öğrenme sınırlarımı keşfetmemde bir yuva oldu. Doktora ve sonrasındaki çalışmalarımın ardından 2009 yılında yine aynı yuvaya döndüm.

> **1999 yılında çalışmaya başladığım TÜBİTAK, biyometri alanındaki doktora eğitimim için yurt dışına gitmeden önce teori-pratik, çalışma-sonuç alma, bilme-öğrenme sınırlarımı keşfetmemde bir yuva oldu.**

TÜBİTAK ilk iş yeriniz sanırım. Uzun yıllardır Kurumumuzda çalışıyorsunuz. Devinimin yüksek olduğu bir iş alanında, burada kalmayı tercih etmenizin arka planını paylaşabilir misiniz?

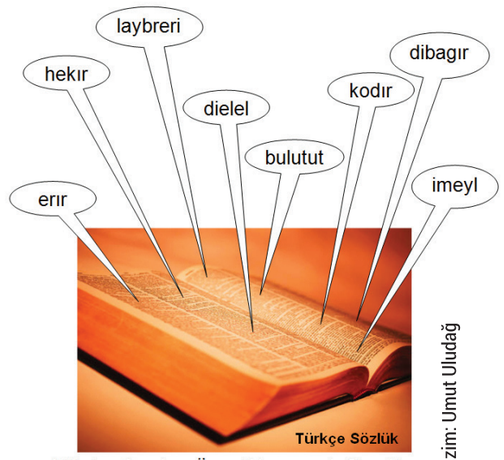
Evet, kısa süreli stajlar, üniversitelerdeki görevlerim vb haricinde Türkiye'de çalıştığım tek yer TÜBİTAK. ABD'de sektör, büyüklük, lokasyon düzlemlerinde birbirinden hayli farklı şirket ve eğitim-araştırma kurumlarda çalıştım ve bunun faydasını da gördüm. Türkiye'de ise, TÜBİTAK'da bunların kesişim kümesinde bir çalışma çerçevesi bulabildiğim için mutluyum diyebilirim.

Dergimizin hedef kitlesi arasında üniversite öğrencileri önde geliyor. Gençlere kariyer yolu ve genel olarak hayat yolculuğu ile ilgili neler tavsiye edersiniz?

Hakkıyla, emek vererek yaptıkları/içinde bulundukları her şeyin (sanat, spor, eğitim, geçinme gailesi) değerli olduğunu bilmelerini isterim öncelikle. Üniversiteden bir öğrencimin "Hocam, yayınladığınız bu şiirlerinizden bazılarının dünyanın en kötü şiirleri seçilebilme olasılığı sizi rahatsız etmiyor mu?" diye sorduğunu hatırlıyorum yıllar önce. Cevabım "Hayır" idi. Etik kurallar çerçevesindeki tüm üretkenlik, emek içeren iş sadece bunlara sahip olması sebebiyle bile önemli.

Çevresel koşullar her ne olursa olsun, ellerinden gelen güzelliği, iyileştirmeyi, çalışmayı dünyaya sunmaktan imtina etmemelerini salık veririm. Zamanın, dünyamızın, coğrafyamızın, ülkemizin aldıkları ve verdikleri hep bir düşünce konusu olacak. Bu insanlık tarihi boyunca da böyleydi, gelecekte de farklı düzlemlerde devam edecek.

Bu süreçte, gençlerimizin –ki, düşünceleri gerçeğe yaklaştırabilecek tek kaynağımız onlar– umutla eğitimlerine, çalışmalarına devam etmelerini, kendilerinin bugünlerini sadece kendilerinin dünleriyle karşılaştırmalarını, bu karşılaştırma sonucunda doğru yönde gelişmeyi görmelerinin de -her şey için olmasa bile- anlamı olan çoğu şey için yeterli olduğuna inanmalarını öneririm. Umarım yolları hep açık, hep güneşli, hep umutlu olsun.



- Dilimize Gereken Önemi Vermezsek Olacaklar - Çizim: Umut Uludağ

İsrafa Dair

"Türkiye'de günlük olarak üretilen 123 milyon adet ekmeğin 6,1 milyonu israf ediliyor. Ekmek israfının yıllık bilançosu 2,24 milyar adet ve bugünkü fiyatlar üzerinden değeri yaklaşık 3,4 milyar TL!"

Abdullah Alpaydın – Başuzman / TÜBİTAK RUTE

Modern zamanların en büyük toplumsal ve ekonomik sorunlarının başında geliyor israf. Bir tüketim canavarına dönüşen insan, bir o kadar da israf ediyor doğal olarak...

Özellikle endüstri ve teknoloji sahasındaki gelişmelerle birlikte konforu ve imkânları sürekli artarak zenginleşen insanoğlunun hırsı, doymazlığı, sahip olma ve tüketme arzusu da bir o kadar arttı. Kapitalist sistem de şu basit mantık üzerine kurulu: Daha fazla üret, daha fazla tüket! İhtiyacınızdan fazlasını satın aldığınızda israf da kaçınılmaz hale geliyor. Gereksiz yere harcanan para mali kaynak israfıyken; alıp kullanmadığımız yiyecek, giyecek ve diğer eşyalar da maddi kaynak israfına dönüşüyor haliyle. Burada acı olan, birçok şeyi tüketmeye fırsatımız olmadan çöpe atıyor oluşumuz. Toplumsal dayanışma eskisine göre çok zayıfladığı ve paylaşım azaldığı için, israfın boyutu her geçen gün inanılmaz rakamlara ulaşıyor. Diğer yandan, tabii kaynaklar da sorumsuzca tüketilip israf edildiği için insanlığın geleceği, başta açlık ve susuzluk olmak üzere birçok tehlikeyle yüz yüze.

"Dünyada açlığın ana sebebi yoksulluk, yoksulluğun başlıca sebebi de adaletsiz gelir dağılımıdır."

Ekmek İsrafı

Ülkemizden örnek verecek olursak, israf denince ilk akla gelen ve en çok göze batan her zaman ekmek olmuştur. Toprak Mahsulleri Ofisi (TMO) tarafından 2019 yılında yaptırılan bir araştırma, ekmek israfının korkunç ekonomik boyutunu gözler önüne sermekte. Bu araştırmaya göre Türkiye'de günlük olarak üretilen 123 milyon adet ekmeğin 6,1 milyon adedi israf ediliyor. Bir başka ifadeyle ürettiğimiz ekmeğin % 5'ini israf ediyoruz. 1 günde israf edilen 6,1 milyon adet ekmek, 4 milyon kişinin 1 günlük ekmek ihtiyacını karşılamaktadır. Bu durumda ekmek israfının yıllık bilançosu 2,24 milyar adet ve bugünkü fiyatlar üzerinden değeri yaklaşık 3,4 milyar TL!

Rakamlar oldukça çarpıcı. Sadece ekmek israfının ülke ekonomisine zararı bu düzeydeyken, her gün tüketmekte olduğumuz binlerce ürüne bağlı israfın maddi karşılığını varın siz hesap edin!

Tasarruftan Tüketime

İsrafı sadece ekonomik bir olgu olarak değerlendiremeyiz. Çok eskilere gitmeye gerek yok; hatırlayabildiğimiz yakın geçmişe (70-80'li yıllar) kadar insanımızın büyük çoğunluğu, tasarruf ve tutumluluk odaklı bir zihin yapısına sahipti. Halkımızın büyük kısmı son derece mütevazı şartlarda yaşamaktayken, israf da sınırlı boyuttaydı. Sadece gıda maddelerinin değil, giyeceklerin kullanımında da ölçülü hareket edilir, biri tamamen eskiyip kullanılmaz hale gelmeden yenisi alınmazdı. Eskiler bile atılmayarak bir şekilde farklı amaçlarla değerlendirilmesine gayret edilirdi.

Ev eşyaları bugün olduğu gibi modaya göre değiştirilmez, yıllarca kullanıldıktan sonra gerekirse tamir edilerek kullanılmaya devam edilir veya ihtiyaç sahiplerine verilirdi. Beyaz eşya ve elekt-

rikli ev aletleri zaten çok az evde bulunur, onlar da ömrünü tamamlayana kadar kullanılırdı. Maddi imkânları daha geniş olan varlıklı aileler bile mümkün olduğunca zenginliklerini ulu orta sergilemez, harcamalarını komşularının gözlerinin içine sokarak yapmamaya dikkat ederlerdi. Yani toplumsal dengenin korunmasına özen gösterilirdi.

Bugün, bırakın ihtiyacımız olan eşya ve aletleri, hiç ihtiyacımız olmayanlara bile kişi başına binlerce lira harcayıp, kısa zamanda da yenileriyle değiştiriyoruz. Eskimeden atılan eşyaların, giyeceklerin haddi hesabı yok. Evdeki mobilyaları 3-5 yılda bir yenilemek, beyaz eşyaları ve elektronik aletleri en yenisi ve en gelişmişiyle değiştirmek, evin dekorasyonunu yenilemek sıradan ve yadırganmayan bir işe dönüştü. İnsanlar maddi güçlerinin ötesinde borçlanarak bu gereksiz harcamaları yapıyor ve israf çılgınlığına katılıyor.

Dünyada Yoksulluk

Madalyonun bir yüzünde kontrolsüz tüketim ve sonucunda büyük kaynak israfı varken diğer yüzünde açlık, sefalet ve yokluk yer alıyor. Aşağıdaki rakamlar durumun vahametini gözler önüne seriyor.

- Dünya üzerindeki 7,9 milyar insandan 700 milyonu "aşırı yoksulluk"la pençeleşiyor. Bir diğer ifadeyle kişi başı günlük 1.90 USD sınırının altında (Dünya Bankası tarafından belirlenen) bir gelirle yaşamaya çalışıyor.
- Aşırı yoksulların % 75'i Sahra Altı Afrika ve Asya'da yaşıyor.
- Şehirlerde yaşayan nüfusun üçte biri "slum" olarak tabir edilen gecekondularda barınıyor.
- Doğan her 1000 çocuktan 39'u 5 yaşına gelmeden sıtma, ishal ve zatürre sebebiyle ölüyor. Bu hastalıkların başlıca sebepleri; yetersiz beslenme, kirli su ve yetersiz hijyen.
- Açlığa bağlı sebeplerle günde 25,000 (10,000'i çocuk), yılda 9 milyonun üzerinde insan ölüyor. Karşılaştırma yapabilmek için, Kovid-19'dan dolayı bugüne kadar ölenlerin sayısının tüm dünyada 4,5 milyon civarında olduğunu belirtmiş olalım.
- Dünya nüfusunun 2,2 milyarlık kısmı güvenilir içme suyu hizmeti alamazken, 785 milyonu ise temel içme suyu imkânından tamamen yoksun (2017 yılı itibariyle).
- Kırsalda yaşayanların kirli su içiyor olma ihtimali şehirlerde yaşayanların 7 katı.
- Kirlenmiş içme suyu tüketimine bağlı gelişen hastalıklardan dolayı her yıl 485,000 kişinin öldüğü tahmin ediliyor.
- 2016 yılı verilerine göre dünyada 6-11 yaş arası 63 milyon çocuk okula gidemiyor. 17 yaş altında bu sayı 263 milyona çıkıyor. Bu da her 5 çocuktan birinin okuldan mahrum kaldığını gösteriyor.

Açlığın ana sebebi yoksulluk, yoksulluğun başlıca sebebi de adaletsiz gelir dağılımı. Gelir dağılımında yaşanan eşitsizlik/adaletsizlik geçmişten günümüze ciddi bir sorun olmaya devam ediyor ve maalesef kaynaklara bir şekilde hükmeden güçlü azınlığın pastadan aslan payını aldığı, yüz milyonlarca insanın da açlık ve yoklukla baş başa olduğu gerçeği değişmiyor. İstatistikler gerek dünyada gerekse ülkemizde gelir paylaşımı adaletsizliğinde dişe dokunur bir iyileşme olmadığını hatta birçok ülkede kötüye gittiğini gösteriyor.

Zaman ve Sağlık İsrafı

İsraf demişken, zaman israfından bahsetmeden olmaz. Zaman, insanoğlunun sahip olduğu şeyler arasında kıymetini en az bildiği değerlerden biri. Saatlerini televizyon, internet ve cep telefonlarında harcayan, birbirleriyle sağlıklı sosyal etkileşim kurmaktan uzak yığınla insan var etrafımızda. Buralarda harcanan zamanın verimli kullanıldığından bahsetmemiz mümkün değil. Elle tutulur bir şey olmadığı için çok azımız zaman israfını önemsiyoruz ama şöyle bir gerçek var: Maddi bir şeyi tekrar elde edip yerine koyabiliriz fakat boşa harcanan zamanı geri getirmek mümkün değil.

Sahip olduğumuz nimetlerden kıymetini bilmediğimiz, dolayısıyla israf ettiğimiz bir diğeri de sağlıktır. Kötü beslenerek ve kötü yaşayarak sağlığımızı bozar sonra da geri kazanmak için para harcarız. Şu paradoksa bakın ki, insanların bir kısmı yeterli beslenemediği, diğer bir kısmı ise gereğinden fazla beslendiği ve tükettiği için hastalanmakta ve ölmekte. Dünyanın düzeni ne garip değil mi?

Kaynakça
- www.tmo.gov.tr
- www.worldbank.org
- www.who.int
- www.un.org

TÜBİTAK BİLGEM

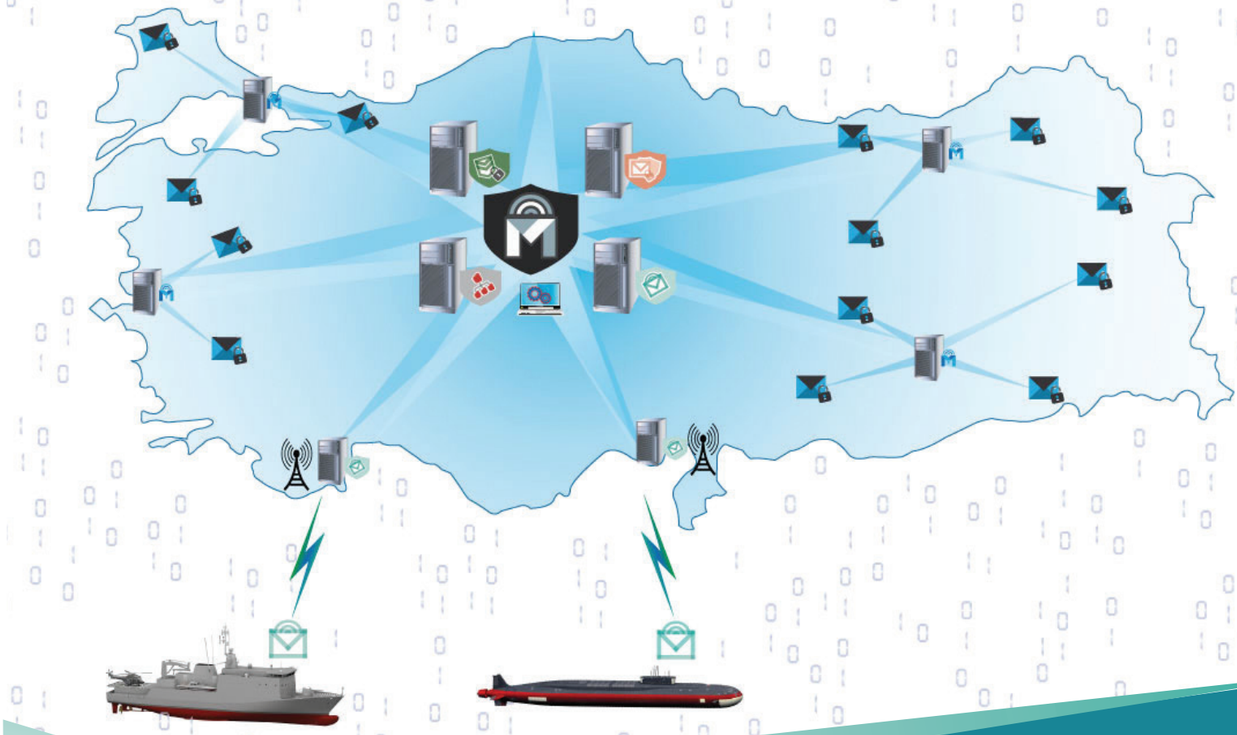
Bu bir proje tanıtımıdır.

Mesaj ve Evrak Dağıtım Sistemi
MEDAS-3

MEDAS-3 Projesi'nin amacı, MEDAS'ın tesisi ve işletimi sırasında elde edilen tecrübeler kapsamında; teknolojik gelişmelerle ortaya çıkan yeni ihtiyaçları karşılamak ve halihazırda TSK'da kullanılmakta olan MEDAS içindeki yabancı kaynaklı hazır ticari ürünleri, NATO ve uluslararası standartlar dikkate alınarak millileştirebilmek maksadıyla gerçekleştirilen Milli Askeri Mesajlaşma Sistemi (MAMSİS) Projesi ile kazanılan milli yeteneklerin sisteme dahil edilerek sistemin geliştirilmesi ve millileştirilmesidir.

Projenin çıktıları, uluslararası standartlara uygun ve ulusal ihtiyaçlar gözetilerek milli olarak geliştirilmiş olan mesajlaşma sistemi ve dizin sistemi yazılımları olacaktır.

Proje kapsamında mevcut dış sistemlerle (taktik ve stratejik sahada) entegrasyon sağlanacaktır.



www.bilgem.tubitak.gov.tr

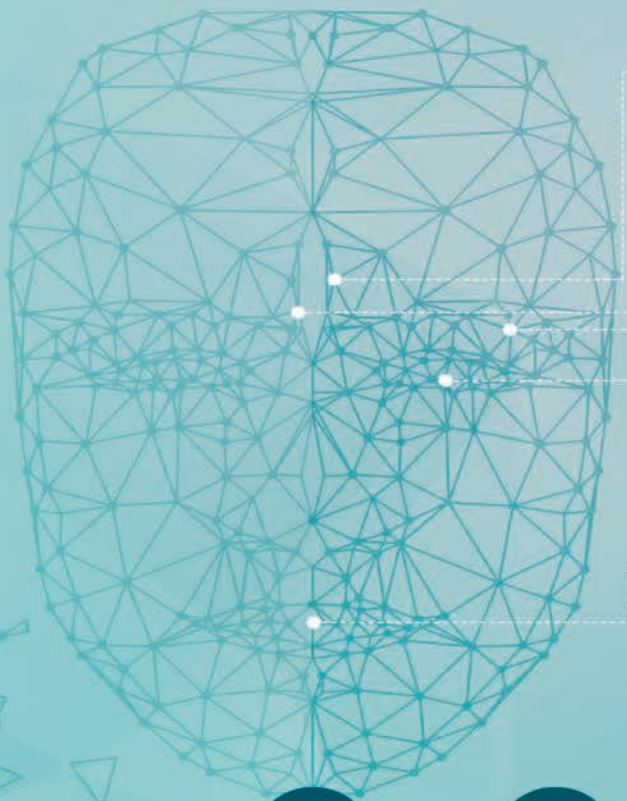
TÜBİTAK BİLGEM

DerinGÖRÜ

CognitiveServices

DerinGÖRÜ

TÜBİTAK BİLGEM'den Kurumsal Geliştiriciler için Ücretsiz Yapay Zeka Destekli Yüz Tanıma ve Görüntü/Video Analizi Platformu



- **Biyometrik Yüz Saptama/Tanıma**
- **Büyük Veri Kümelerinde** Biyometrik Yüz Tanıma
- **Duygu Durumu** Tanıma
- **Bakış Açısı** Kestirimi
- **Cinsiyet Tanıma,** Yaş ve Yaş Aralığı Kestirimi

- Kişi Sayımı ve Temel Aktivite Kestirimi
- Konuşma Yazılandırma
- El Parmak Hareketleri Saptama
- OCR (Optik Karakter Tanıma)

www.bilgem.tubitak.gov.tr