—Giriş
—Temel Kavramlar
—Bilgi Güvenliği Hedefleri
—Kriptoloji
—KriptogtafiYöntemleri
—Steganografi
—Bilgi Güvenliği Teknolojileri
—Kişisel Verilerin Korunması
—Kötü Niyetli Yazılımlar
—Sosyal Mühendislik
—Ağ Güvenliği
—İşletim Sistemi Güvenliği

Gizlilik: Confidentiality
Bütünlük: Integrity
Erişilebilirlik: Availability

Şifre bilimi: Crytography
Bilgi gizleme: Steganography
Şifreli metin: Chipter Text
Sayısal İmza: Digital Signature

Tehdit: Threat
Saldırı: Hack Hacker
Sızma: Intrusion Intruder
Hizmet engelleme Saldırısı: Denial of the Service (DoS)
Dağıtık hizmet engelleme saldırısı: Disturbuted Denial of the Service (DDoS)
Saldırı Tespit Sistemleri: Intrusion Detection Systems
Saldırı Önleme Sistemleri: Intrusion Prevention Systems
Güvenlik Duvarı: Firewall

KVKK: Kişisel Verilerin Korunması Kanunu
VERBİS: Veri Sorumluları Sicil Bilgi Sistemi
Aydınlatma Metni
Açık Rıza
ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi: Bilgi güvenliği sorunlarının ele alınmasını ve yönetilmesini destekleyen bir yönetim sistemi standartıdır.

BS439_01, BS439_02_1 ve BS439_02_2

Veri (Data): Gözlem, araştırma, deney, ölçüm, sayım yoluyla elde edilmiş, birbiriyle bağlantısı henüz kurulmamış bilinenler olarak tanımlanabilir.

Bilgi (Information): Verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir.

"Bir konu ile ilgili belirsizliği azaltan kaynaktır bilgi."
Shannon - Information Theory

Güvenlik: İç veya dış kaynaklı, kasıtlı veya kasıtsız oluşabilecek tehditlerin kabul edilebilir seviyeye çekilmesidir.

Bilgi Güvenliği (Information Security): Bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme çabası.

YAZILIM DONANIM VERİ
DEPOLAMA AKTARIM İNSAN

Bilgi Güvenliği Alt Başlıkları
Bilgisayar, mobil cihaz, ağ, web, mobil işletim, işletim sistemi, veritabanı ve bulut güvenliği
Fiziksel ve siber güvenlik
Bilgi güvenliği, fiziksel güvenlik, ağ güvenliği, uç nokta güvenliği, veri işleme gibi birçok alanı kapsayan geniş bir alandır.

Siber güvenlik (Cyber Security), bilgi güvenliğinin bir alt kategorisidir. Teknolojiyle ilgili tehditleri, bunları önleyebilecek veya azaltabilecek uygulamalar ve araçlarla ele alır.
Siber güvenlik yalnızca dijital verileri korumayı amaçlarken, bilgi güvenliği tüm verileri korumayı amaçlar.

Neden Bilgi Güvenliği?
2020 dünya geneli doğal afetlerin toplam bedeli 268 Milyar $, 2015 Siber Saldırılar 3 Trilyon $
ABD, İngiltere ve Rusta tedbirler alıyor.
-Gizli ve hassas bilgiler açığa çıkabilir.
-Bilginin içeriğinde henüz yetkisiz kişilerce değişiklik yapılabilir
-Bilgiye erişim mümkün olmayabilir.
-İş sürekliliği zarar görebilir
-Ticari, teknolojik, adli bilgiler kötü niyetli kişikerin eline geçebilir
-Ulusal / kurumsal itibar kaybı yaşabilir.
-Müşteri mağduriyeti ve memnuniyetsizliğine neden olabilir
-Yasal yaptırımlar ve tazminatlar gibi olumsuz sonuçlarla karşılaşılabilir.

Bilgi Güvenliğine Yönelik Tehditler

İç Tehditler	Dış Tehditler
-Bilgisiz ve bilinçsiz kullanım	-Hedefe yönelik Saldırılar
-Kötü niyetli hareketler	-Hedef gözetmeyen saldırılar

Bilgi Güvenliği Nasıl Sağlanır?
1-Yöntemsel Önlemler
2-Teknoloji Uygulamaları
3-Eğitim ve Farkındalık

Bilgi Güvenliği ve İnsan
Eğer teknolojinin tek başına güvenlik probleminizi çözebileceğini düşünüyorsanız, güvenlik probleminiz ve güvenlik teknolojileri tam anlaşılmamış demektir.
Bruce Scheiner
-Güvenlik, teknoloji kadar insan ve o insanların teknolojiyi nasıl kullandığı ile ilgilidir.
-Sadece doğru teknolojinin kullanılması değil, doğru amaçla ve doğru şekilde kullanılmasıdır.

Tehditin Kaynağı: Hacker, cracker
Motivasyon: Meydan okuma, ego, para
Olası Sonuçlar: Hackleme , Sosyal mühendislik, izinsiz sistem erişimi, sistemin çökmesi

Tehditin Kaynağı: Bilişim suçu
Motivasyon: Yasadışı bilgi ifşası, parasal kazanç
Olası Sonuçlar: Bilişim suçları, Sisteme sızma Hileli işlemler

Tehditin Kaynağı: Terörist
Motivasyon: Şantaj, tahribat, intikam, siyasi kazanç
Olası Sonuçlar: Siber savaş, Sistem saldırısı, Sistemde izinsiz değişiklik

Tehditin Kaynağı: Çalışanlar
Motivasyon: Merak, intikam, parasal kazanç
Olası Sonuçlar: Şantaj, Sahte - bozulmuş veri, Sahtekarlık ve hırsızlık, İzinsiz sistem erişimi

Tehditin Kaynağı: Endüstriyel casusluk
Motivasyon: Rekabet avantajı, ekonomik casusluk
Olası Sonuçlar: Savunma avantajı, Ekonomik sömürü, Bilgi hırsızlığı, Sostal mühendislik

CISO (Chief Information Officer - Baş Bilgi Güvenliği Yöneticisi
Bir kuruluşun bilgilerinin yönetilmesinden ve korunmasından sorumlu kişilerdir.
-Yönetim: Tüm Güvenlik operasyonlarının sorunsuz çalıştığını doğrulama
-Güvenlik Operasyonları: Tehditlerin gerçek zamanlı izlenmesini, analizini ve önceliklerinin belirlenmesi
-Güvenlik Mimarisi: Donanım ve yazılımın edinilmesi, entegrasyonu ve çalıştırılmasına yönelik en iyi güvenlik uygulamalarının uygulanması
-Program Yönetimi: Denetimler ve yükseltmeler yoluyla donanım ve yazılımın proaktif bakımının sağlanması
-Kimlik ve erişim yönetimi: Kimlik doğrulama, yetkilendirme, ayrıcalık vermenin uygun şekilde kullanılmasını sağlama
-Veri kaybı ve dolandırıcılık önleme: İçeriden gelen tehditlere karşı izleme ve bunlara karşı koruma
-Siber risk ve siber istihbarat: Güvenlik tehditlerine ilişkin mevcut bilgilerin korunması ve risklerin olası etkileri hakkında yönetimi bilgilendirme
-Soruşturmalar ve adli tıp: Kanıt toplama, yetkililerle etkileşimde bulunma ve ölüm sonrası işlemlerin yapılmasını sağlama

BS439_03_1

Bilgi Güvenliği Hedefleri:
-Tehditlerin farkında olmak
-Bilginin geniş çaplı tehditlerden korunmasını sağlamak
-Kayıpları en aza indirmek
-İşlerin devamlılığını sağlamakcö
-İşlerde meydana gelebilecek aksaklıkları azaltmak
-Bilginin her koşulda gizliliğini, erişilebilirliğini ve bütünlüğünü korumak

Bilgi Güvenliği Unsurları

C	I	A
Confidentiality	Integrity	Availability
Gizlilik: İletilen bilginin içeriğinin gizli kalması	Bütünlük iletilen bilginin içeriğinin yolda değiştirilme veya yok edilmeye karşı korunması	Süreklilik: haberleşmenin kesintiye uğramadan yapılması

Kimlik Denetimi (Authentication) : Bilgiyi gönderen kişinin kimliğinin doğruluğundan emin olma
İnkar edilememezlik (Non-repudiation): Bilgi gönderen veya işleyen kişinin yaptığı işi, alıcının bilgi aldığını sonradan inkar edememesi
İzlenebilirlik(Accountability):Kullanıcı işlemlerinin takibinin yapılmasının sağlanması
Güvenilirlik (Reliability): Sistemin tutumlu davranması
Yetkilendirme(Authorization)

Gizlilik İhlali: Haberleşme kanalını dinleyen saldırgan gönderici ile alıcı arasındaki mesaj trafiğini dinleyebilir (dinleme ihlali) ve elde ettiği mesajları okuyarak bu haberleşmenin gizliliğini bozar. Bu tehdit dinleme tehdidi olarak bilinir.

Bütünlük İhlali: Haberleşmeye müdahele edip göndericinin mesajlarını değiştiren saldırgan, alıcıya giden mesajı istediği şekile sokabilir. Bu tehdit mesajın bütünlüğünü bozan değiştirme tehdididir.

Süreklilik İhlali: Saldırgan, haberleşen iki taraf arasındaki hattı veya haberleşme araçlarını kulanılamaz hale getirerek haberleşmenin sürekliliğini engellemeye çalışır.

Kimlik Denetimi İhlali: Saldırgan, alıcıya göndericinin kimliğini taklit ederek bir mesaj gönderebilir. Bu durumda eğer alıcı güvenilir bir kimlik doğrulaması yapmıyorsa yanlış mesajlarla kandırabilir.

İnkar Edilememezlik İhlali: Mesajı gönderen veya alan tarafın bu işi yaptığını inkar etmesi söz konusu olabilir. Bu kötü niyetli girişimi boşa çıkaracak mekanizmalara ihtiyaç vardır.

İzlenebilirlik İhlali: Tüm çalışanların şirekete ait bir bilgi altyapısına dışarıdan yazılım yüklemekten kaçınması gerektiğine dair bir politika var. Bilgi güvenliğinden sorumlu kişi, bu politikaya uyulduğundan nasıl emin olabilir?

Tanımlama -> Kimlik Denetimi -> Yetkilendirme -> Loglama -> HesapVerilebilirlik

Kimliklendirme(Identification): Kullanıcının sistemde bir kimliğe sahip olma süreci
Doğrulama(Authontication): Kullanıcı kimliğinin sistemdeki geçerliliğin doğrulanma süreci
Yetkilendirme(Authorization): Geçerliliği doğrulanan kullanıcının, kimliğinde sahip olduğu yetkilerin kullanıcıya atanması süreci

Bilgi Güvenliği Hedeflerine Nasıl Ulaşılır?
-Gizlilik: Simetrik şifreleme, Asimetrik şifreleme
-Bütünlük: Mesaj Kimlik doğrulama algoritmaları, Özetleme algoritmaları
-Süreklilik, Kimlik Denetimi: // , Özetleme algoritmaları, Sayısal imza
-İnkar edilememezlik: Sayısal imza, Asimetrik şifreleme, Özetleme algoritmaları

BS439_04_1 ve

Tanımlar
Kriptoloji (cryptology), kriptografi (şifreleme bilimi) ve kriptanaliz (şifre analizi) ile ilgili bir bilim dalıdır.

Kriptografi (cryptography), yunanca da gizli anlamına gelen "kriptos" ve yazı anlamına gelen "graphi" kelimelerinden türetilmiştir. Amacı ileti/bilgi güvenliğin sağlamaktır.

Kriptanaliz amacı, var olan şifreleri çözmektir. Kriptografik algoritmaların analizi ile ilgilenir.

Şifreleme (encryption), bir iletinin (açık/düz metin, plain text) içeriğini, uygun bilgi (anahtar,key) elde olmadan okunamayacak hale getirme işlemidir.

Şifrelemenin amacı, iletinin istenmeyen şahıslar tarafından okunmasını engellemektir.

Şifre çözümü (decryption, deşifre), şifrelemenin tam tersi, yani şifrelenmiş metnin (chiper text) düz metine çevrilmesi işlemidir.

İLETİM ORTAMI
Açık Metin -> Şifreleme -> Şifrelenmiş Metin -> Şifre Çözme -> Açık Metin
Plain Text ->Encryption-> Cipher Text -> Decryption -> Plain Text
Şifreleme anahtarı
Şifre Çözme anahtarı
Bir metnin şifrelenmesi ve şifrelenmiş metni çözülme aşamaları

Kriptoloji, kökü 4000 yıl öncesine dayanan en eski çalışmalardan birisidir.
M.Ö. 1900 Eski Mısırlılar - İlk yazılı kriptografik belgeler

Atbash şifreleme (M.Ö. 590), İbranice alfabesinin tersinin kullanılmasıyla gerçekleştirilmiştir.
ABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZ
ZYVÜUTŞSRPÖONMLKJİIHĞGFEDÇCBA

Ebced hesabında, her bir harfin sayısal değeri vardır. Bir kelimedeki harflerin ebced tablosundaki sayısal karşılıkların toplamı, anlatılmak istenen bir olayın tarihine denk getirilir.
Aherun (elif+gayn+ra+vav+nun) = 1+600+200+6+50=857
Hicri 857 (M. 1453) İstanbul'un Fetih Tarihi

Tarihçe
Skytale cihazı, ilk kriptografik cihazdır. Bir çubuğun etrafına bir mesajın sarılması ile elde edilen metin, şifreli metindir ve açık metindeki harflerin karışımıdır.
M.Ö. 487 Yunanlı Spartalılar - Skytale

-Kriptografinin tarihta görüldüğü ilk belirgin örnek olarak, Julius Caesar'ın devlet haberleşmesinde kullandığı yerine koyma şifresi (M.Ö. 60-50) gösterilir.
-Kriptografi tarihinin ilk yıllarından beri kullanılan en temel algoritmaları, yer değiştirme (transposition) ve yerine koyma (substitution) olarak bilinir.
-İlk kriptonanaliz çalışması -Abdurrahman el-Halil İbn-i Ahmed, "Kitab-ül Muamma" (M.S. 718) adlı eserinde Bizans imparatoru için Yunanca yazılmış bir şifreli mektubun çözümünü vermiştir.
-Kriptoplojide asıl ivmelenme, 2.Dünya savaşında ülkelerin bu bilime ilgi göstermesiyle gerçekleşmiştir.

BS439_05_1

KRİPTOGRAFİ YÖNTEMLERİ

Klasik Yöntemler:
-Yerine Koyma:
-Tek Alfabeli
-Çok Alfabeli
-Yer değiştirme

Modern Yöntemler:
-Simetrik:
-Blok Şifreleme:
-AES
-DES
-3DES
-Akış Şifreleme:
-RC4
-SEAL
-Asimetrik:
-RSA
-DSA
-Diffine-Heliman

KLASİK KRİPTOGRAFİ YÖNTEMLERİ

Sezar Şifreleme (Caesar Cipher, M.Ö. 58), harflerin alfabedeki 3 konum sonrasındaki karşılığı ile değiştirilmesi esasına dayanır.
Anahtar = ne kadar ötelenecek
Şifrelenen harfin alfabedeki sırası = (Şifrelenecek harfin alfabedeki sırası + Anahtar sayı)mod26

İngiliz Alfabesi 26 harf -> 26! farklı şifre tablosu , 25 farklı anahtar sayı

Frekans analizi ile sezar şifresi çözülebiliyor. En çok kullanılan harf ve kelimeler ile deşifre veya saldırılar yapılabiliyor.

Vernam Şifrelemede (Vernam Cipher, One Time Pad, 1917), rastgele verilerden oluşturulan tek kullanımlık bir şerit (pad) anahtar olarak kullanılır.
-Harfler ikili sisteme çevrilir, şeritte kendisine karşılık gelen ikili kod ile XOR işlemine tabi tutularak şifreli metin oluşturulur.
-Şifreli metin= (Açık metin) XOR (Anahtar)

Karakterleri ikili sisteme çevirmek için ASCII tablosu kullanılır
Açık metin = "ay"
ikili kodu: 01100001 01111001
Anahtar = 00011011 00001101
Şifrelenmiş kod = 01111010 01110100
Şifrelenmiş metin= "zt"

Açık metinde yer alan her karakter, şeritte karşısına denk gelen karakterle modüler toplama işlemine tabi tutularak şifrelenir.
Açık metin="nesibe", pad="yalçın"
n(17) + y(28) = m (45 mod(29))
e(6) + a(1) = f (7 mod(29))
s(22) + l(15) = g (37 mod(29))
i(12) + ç(4) =m (16 mod(29))
b(2) + ı(11) =j (13 mod(29))
e(6) + n(17) =ş (23 mod(29))
Şifreli metin="mfgmjş"
Deşifre için şifreli metindeki moddan anahtar olarak kullanılan metnin modları çıkartılır.

Enigma Şifreleme
Arthur Scherbius, 1920'li yıllarda elektromekanik bir şifre makinesi olan ünlü Enigma'yı icat etmiştir.
Enigma mekanizması sırasıyla klavye, elektrik bataryası, Enigma rotor kısmı ve karıştıcıdan oluşmaktadır.
Her harf karakterinin değiştirilmesi için rotor mekanizması geliştirilmiştir. Her karakter için izlenen yol böylece farklı olabilmektedir.
II.Dünya Savaşı sırasında Nazi Almanyası tarafından gizli mesajların şifrelenmesi ve tekrar çözülmesi amacı ile kullanılmıştır.
Makine, Alan Turing ve ekibi tarafından çözülmüştür.
Operatör hataları, prosedür açıkları ve ele geçen kod kitapları sayesinde çözümlenebildi.
Enigma şifreleme, Vigenere tablosunda kullanılan çoklu alfabe yöntemi kullanılır. Böylece tekrara düşmeden, aynı anahtar kullanılmaksızın mesajlar gönderilebilmektedir.
Harfin şifrelendikten sonraki halinin aynı harf olamaması, deşifre çalışmalarında çok sayıda olasılık denenmesini gerektirmektedir.

Hill Şifresi
Hill sistemi(1929), lineer cebire dayanmaktadır. Anahtar ve açık metin harflerinin sayısal değerlerinin olduğu eşitlikler kullanılır.
Hill şifresi ile açık metinde **m tane alfabetik karakter için m tane lineer kombinasyon** yapılarak m tane alfabetik karakter üretmektedir.

m=2 Açık metin, x=(x1,x2) şifrelenmiş metin, y=(y1,y2)
y1= 11x1+3x2
y2=8x1+7x2

(y1,y2) =(x1,x2) [11 8] Matris gösterimi
[3 7]
Açık metin, x, "AÇ" = {1,4} Anahtar,K= [2 4]
[3 5]

[1 4][2 4] = [14 24] -> y,{14,24} = "KT"
[3 5]

Şifrenin açılması için matrisin tersinin bulunması gerekir.
BS439_05_2

bkz:afin, playfair

MODERN KRİPTOGRAFİ YÖNTEMLERİ

-Claude Elwood Shannon'un 'Gizlilik Sistemlerinin İletişim Teorisi' isimli makalesi (1949), modern kriptografinin başlangıcı sayılır. Sonsuz uzunlukta, rastgele oluşturulmuş bir anahtar kullanan şifreleme sistemlerinin, anahtar olmaksızın kırılması mümkün değildir.
-Sonsuz uzunlukta bir anahtarın alıcıya güvenli yollardan iletilmesi…
-Whitfield Diffie ve Martin Hellman, 'Kriptografide Yeni Yönelimler' başlıklı makaleleri (1976) ile güvensiz bir iletişim hattı aracılığıyla iki tarafın aynı anahtarda nasıl anlaşacağı göstererek kriptografinin en temel sorunlarından biri olan anahtar alışverişi problemini çözdüler.
-Şifreleme için kullanılan anahtarın özellikleri ve çeşidine göre temel olarak iki çeşit şifreleme algoritması bulunmaktadır:
-Simetrik (gizli anahtarlı) şifreleme
. Blok şifreleme ve dizi/akan şifreleme algoritmaları
-Asimetrik (açık anahtarlı) şifreleme
-Anahtarsız algoritmalar

Simetrik Kriptografi
-Şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır. Şifreleme yapan ile şifrelemeyi çözecek kişiler arasında anlaşılmış ortak bir anahtardır.
-Gönderilecek gizli/şifreli metinle beraber üstünde anlaşılmış olan gizli anahtar da alıcıya gönderilir ve şifre çözme işlemi gerçekleştirilir.
-AES, RC4, DES, Blowfish, RC5 ve RC6 simetrik şifrelemeye örnektir.

Blok Şifreler
-Düz metin eşit uzunluktaki bitişik bloklara bölünür, her blok ayrı ayrı şifrelenerek şifreli metni oluşturur.
-Şifreleme işleminde, her blok için aynı anahtar kullanılır.

Akan Şifreler

-Metin bit bit işlenir. Düz metnin her bir karakteri (bit'i), düz metin ile aynı uzunluktaki anahtarın her karakteri (bit'i) ile ayrı ayrı, mod 2'ye göre toplama (XOR) yapılarak şifrelenir.
Şifreleme anahtarı, her bit için farklı olur.

Düz metin = m = m1,m2,…mn
Anahtar = k = k1,k2,….kn
Burada her i için ci = mi + ki
Şifreli metin c = c1,c2,……cn

Akan şifreler, herhangi bir blok şifresinden daha hızlı çalışır.

DES ve 3DES

Veri Şifrelem Standardı (Data Encryption Standard, DES) ilk simetrik şifreleme algoritmasıdır. (1974,IBM) Veriyi bloklara ayırarak şifreleme yapar.

-İşlemlerini, bitler (0 ve 1) üzerinden yapmaktadır.
-DES gizli anahtarı -56 bit uzunluğunda +8 bit parity (64 bit)
-2^56 olası anahtar

DES Algoritması

Dez avantajı avantaja çevirmek için geliştirilen 3DES algoritması Des şifrelemesinin 3 kere art arda yapılması şeklinde çalışır. Bu yüzden, DES'e göre 3 kat daha yavaştır.
3DES anahtar uzunluğu, 56x3 = 168-bit

AES

Gelişmiş Şifreleme Standardı (Advanced Encryption Standard, AES),

Rijndael (**RIJ**men a**N**d **DAE**men) algoritmasında bazı değişiklikler yapılarak oluşturulmuştur (2001).
-Aes içi şifreleme ve şifre çözme anahtarları aynıdır.
-AES-128, AES-192 ve AES-256; 128-bit blok uzunluğu ve 128, 192 ve 256 bit anahtar uzunluklarına sahiptir.
-Güvenlik açısından yüksek verimliliğe sahip simetrik-anahtarlı blok şifreleme yöntemidir.

Simetrik Kriptografi Kuvvetli Yönleri:

-Algoritmalar olabildiğince hızlıdır.
-Donanımla birlikte kullanılabilir.
-Güvenlidir.

Simetrik Kriptografi Zayıf Yönleri:

-Güvenli anahtar dağıtımı zordur.
-Kapasite sorunu vardır.
-Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

Asimetrik Kriptografi

-Amaç, anahtar dağıtım problemini çözmektir.
-Şifreleme algoritması gizli değildir ve iki tür (gizli ve açık) şifreleme anahtarı kullanılmaktadır. Açık anahtar kullanılarak metin şifrelenir ve gönderilir. Şifreli metnin çözülebilmesi gizli anahtara sahip olan kullanıcıya bağlıdır.
-Açık ve gizli anahtarlar arasında matematiksel ilişki olmalı ve açık anahtardan gizli anahtarı bulmak mümkün olmamalıdır.
-Kullanılan gizli anahtar başkalarından gizlidir ve sadece alıcıya aittir. Açık anahtar ise herkese verilir. Böylece herkes bilgisini şifreleyebilir ancak her şifreli bilgiyi okuyamaz.
-Tek yönlü bir mesajlaşma söz konusudur.

Asimetrik Kriptografi Kuvvetli Yönleri:
-Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.
-Anahtarı kullanıcı belirleyebilir
Asimetrik Kriptografi Zayıf Yönleri:
-Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması
-Anahtar uzunlukları bazen sorun çıkarabiliyor olması

BS439_06_1

Diffie - Helman Anahtar Değişimi

-Diffie - Helman Anahtar Değişimi Algoritması (1976), kriptografik anahtarların değişiminde kullanılan özel bir yöntemdir. Haberleşecek tarafların ortaklaşa güvenli olmayan bir iletişim hattı üzerinden ortak bir gizli anahtar üretmelerine olanak sağlar.

-Alıcı ve göndericinin açık ve gizli iki anahtarı bulunur. Açık anahtarlar, büyük asal sayılar olarak seçilir.

Gönderici

1. a Rastsal sayısını üret.
2. A=g^a mod P hesapla ve Alıcıya gönder
3. Alıcıdan gelenle K=B^a mod P hesapla

Alıcı

1. b Rastsal sayısını üret.
2. B=g^b mod P hesapla ve Göndericiye gönder
3. Göndericiden gelenle K=A^b mod P hesapla

RSA

-RSA Algoritması (1978), Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman tarafından geliştirilmiştir.
-Çarpanlara ayırmanın zorluğunu temel alır.
-Anahtar uzunluğu 1024, 2048, 4096 bit şeklindedir.
-Yavaştır, çok işlem gücü gerektirmektedir.
-Şifreleme, anahtar değiştirme ve dijital imza oluşturma için kullanılır.

---**Anahtar oluşturma**:
-İki tane farklı, rastgele ve yaklaşık aynı uzunlukta olan p ve q asal sayıları seçer.
-n=pq ve t=(p-1)(q-1) değerlerini hesaplar.
- 1<e<t ve gcd(e,t)=1 olacak şekilde rastgele bir e sayısı seçer. Burada gcd en büyük ortak böleni ifade etmektedir.
- 1<d<t ve ed=1mod(t) koşulunu sağlayan d sayısını hesaplar.
-A'nın açık anahtarı (n,e) sayı çiftidir; A'nın gizli anahtarı ise d olur.

p=17, q=11 olsun.
n=pxq -> n = 17x11=187 ve t=(p-1)x(q-1) = 160

1<e<t ve EBOB(e,t) = 1 sağlayan e seçilir.
1<e=7 <160 ve OBEB(7,160)=1

Açık anahtar (n,e)=(187,7)
1<d<t ve e x d = 1 mod(t)
1<d<160, 7 x d = 1 mod(160) -> Gizli anahtar (n,d) = (187,23)
e x d = 1 + k x t
Gizli bilgiler p=17, q=11, d=23

---**Şifreleme**:
B kişisi A'ya bir m mesajı göndermek istesin. B kişisi, m metnini şifrelemek için şu yolları izler:
-Öncelikle A'nın açık anahtarını (n,e) alır.
-m metnini [0,n-1] aralığında yazar.
-Sonra c şifreli metnini hesaplar, yani c = m^e (mod n)
-Oluşan c şifresini A'ya gönderir.

Örn; Metin değeri:88 c= m^e (mod n) , m<n
Şifrelenmiş metnin değeri = 88^7(mod 187) = 11
---**Şifre çözme**:
Şifreli c metninden açık metni bulabilmek için A kişisi aşağıdaki işlemleri yapar
-d gizli anahtarını kullanarak ve m=c^d(mod n) işlemini uygulayarak m açık metne ulaşır.
m=c^-e(mod n)
Örn; m = c^d (mod n)
Metnin deşifrelenmesi -> 11^23 (mod 187) = 88

Anahtar: p=11, q=3
pq = 11 x 3 = 33
t = (p-1)(q-1) = 10 x 2 = 20
e = 3
ed = 1 mod(t)
d=7 (bu değeri bulana kadar işlem yapmak lazım)
Şifreleme: Metin: <<AY>> A=1, Y=28
c=m^e(mod n)
Şifrelenmiş metnin değeri = 1^3 (mod 33) = 1, 28^3(mod 33) = 7
Şifre Çözme: m= c^d(mod n)
Metnin deşifrelenmesi -> 1^7 (mod 33) = 1 ->'A'
7^7 (mod 33) = 28->'Y'

	AES	DES	ve	RSA
Özellikler	AES	DES		RSA
Anahtar Uzunluğu	128,192,256 bit	56 bit		>1024 bit
Blok Uzunluğu	128 bit	64 bit		En az 512 bit
Anahtar Tipi	Aynı	Aynı		Farklı
Türü	Simetrik	Simetrik		Asimetrik
Hızı	Hızlı	Orta		Yavaş
Güç tüketimi	Düşük	Düşük		Yüksek
Güvenilirliği	Güvenli	Yeterli değil		Güvenli
Devir Sayısı	10, 12, 14	16		1

BS439_06_2

Özet Fonksiyonlar

Özet Fonksiyon (hash function), girdi olarak bir mesajı alır ve matematiksel yollarla mesajın özetini/parmak izini çıkarır. Mesaj özeti, mesaj ile birlikte kimlik doğrulama için gönderilir.

-Özet uzunluğu, mesajın uzunluğundan bağımsız ve sabittir.
-Belli bir mesaj aynı özet fonksiyonu kullanıldığında, aynı mesaj özetini (message digest) verir.
-Farklı mesajlar için farklı özetler elde edilir.
-Özet fonksiyonu, geri dönüşü olmayan bir fonksiyondur, yani mesajın özetine bakarak mesajın kendisini elde etmek mümkün değildir.
-Özet fonksiyonu kullanarak, kimlik denetimi amacıyla özel anahtarlarla bütün mesajı şifrelemek zorunluluğu ortadan kalkar.
-Sistemde yalnız olarak kullanılmazlar. Sistemde bulunan simetrik ve asimetrik diğer algoritmalara yardımcı olmak için yapılmışlardır.
-En iyi bilinen özet fonksiyonları MD4 (128 bit), MD5 (128 bit) ve SHA-1 (160 bit)'dır.

Mesaj Kimlik Doğrulama Kodu

Mesaj Kimlik Doğrulama Kodu (Message Authentication Code, MAC) algoritması, bir gizli anahtar kullanır ve mesaj için küçük bir veri oluşturur. Bu veri, mesajın sonuna eklenir.

Sayısal İmza

Sayısal/Dijital imza, imzalayanın kimliğine dair en yüksek düzeyde güvence sağlayan belirli bir e-imza türüdür.

-Asimetrik kriptografi kullanılır. Gizli anahtarlarla imza atma işlemi ve açık anahtarlarla imza doğrulama işlemi yapılır.
-Mesajın sonuna eklenir.
-Mesajı alanın, mesajın göndericisinin kimliğinin doğrulamasını ve mesajın bütünlüğünün kontrolünü sağlar.
-İnkar edilememezlik hizmetini sağlar.

Orijinal İleti -> Hash ddeğerinin hesaplanması -> İleti özeti -> Özel anahtarla şifreleme ->İletinin imza bloğu

-Açık anahtar, elektronik sertifikanın içeriğinde tutulur.

Elektronik İmza & Sayısal İmza

-Gönderilmek istenen belgeye eklenen ve kimlik doğrulama amacıyla kullanılan elektronik veriye (elektronik imza (e-imza) adı verilir. Sanal ortamda ıslak imzanın yerine geçmektedir.
-Sayısal imza, imzalayanın kimliğini doğrulamak için sertifika tabanlı dijital kimlikler kullanır.
-Elektronik imza, sayısal imzaya göre güvenli bir kodlamaya ya da şifrelemeye sahip değildir.
-Hem elektronik hem de sayısal imzalar yasal olarak bağlayıcıdır.

İmza Tipleri

Electronic Signature: document, signature on canvas

Biometrik Signature: document, signature on canvas, X and Y values, Acceleration, Pressure, Speed, Delta Pressure

Digital Signature: document, digital signature block, sertificate

Advanced Biometric Signature using Digital Signature: document, digital signature block, signature on canvas, sertificate,X and Y values, Acceleration, Pressure, Speed, Delta Pressure

BS439_07_1

PGP

-1991 yılında Philip Zimmermann tarafından geliştirilen PGP (**Pretty Good Privacy**), hem şifreli e-postalar göndermek hem de hassas dosyları şifrelemek için kullanılan bir şifreleme sistemidir.

-PGP, hem simetrik şifreleme hemde asimetrik şifreleme kullanıldığından, hiç tanışmamış kullanıcıların özel şifreleme anahtarlarını değiştirmeden birbirilerine şifreli mesajlar göndermesine izin verir. Yavaş çalışır, zaman alır, işlem yükü çok ister ve uzun metinlerde kullanılmaz.

-OpenPGP, en yaygın e-posta şifreleme standardıdır.

Encryption Process

File -> Encrypt File with Public Key -> Encrypted File -> Email or FTP

(Kullanılan Gizli anahtarı alıcının açık anahtarı ile şifreliyor.)
(Ve şifrelenmiş anahtarla birlikte şifrelenmiş metni gönderiyor.)

Decryption Process

Email or FTP -> Enrypted File -> Decrypt File with Private Key -> File

(Alıcı şifrelenmiş olan anahtarı kişi kendi Gizli anahtarını kullanarak çözüyor.)
(Sonra şifresini çözdüğü anahtarlar şifrelenmiş metni deşifre ediyor.)

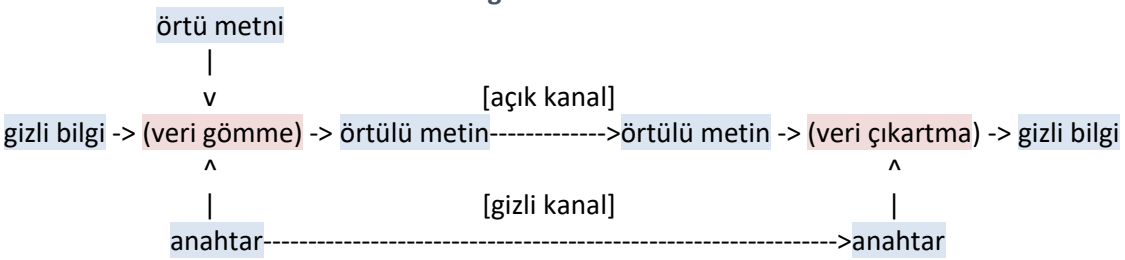
STEGANOGRAFİ

Stenografi (hızlı yazma) ile karıştırılır. Steganografi'nin amacı verinin yetkisiz kişiler tarafından erişilmesini önlemek. Steganography gizlenmiş yazı manasına gelir; yunanca'da steganos= "gizli, saklı" + grafi="çizim, yazım" kelimelerinin birleşiminden oluşmaktadır.
-İletilmek istenen bilginin varlığını gizleyip sadece anahtara (stego-key) sahip olan kişilerce algılanmasını sağlamak. Şifrelemenin alternatifi değil tamamlayıcısıdır.
-Ses, görüntü, video, metin dosyaları (**cover**) içerisine veri saklanabilir. Bu veri, metin olabiceği gibi, herhangi bir görüntü içerisine başka bir görüntüyü gizlemekte olabilir.
-İçerisinde gizli veri bulunduran taşıyıcıya **stego** adı verilir.

Steganaliz

-**Steganaliz**, steganografik yöntemler kullanarak gizlenen verileri ortaya çıkartma bilimidir.
-Steganaliz yöntemleri: en basiti beyaz zemine beyaz yazı yazmak
-**Pasif Steganaliz**: Gizli verinin sadece varlığını tespit eden yöntemler
-**Aktif Steganaliz**: Gizli mesajın bir kısmını veya benzerini elde etmeyi sağlayan yöntemler

Stegosistem



BS439_07_2

Steganografi Örnekleri;

-Görünmez mürekkep
-Saçını sıfıra vurmuş bir askerin saçına mesajı kazıyıp saçı uzayınca göndermek
-Turuva atı
-Mikro noktalama (mercek yardımıyla bakılır)
-Gazete sayfalarına saklama
-Boş Şifreleme (Null Chiphering) örn: her kelimenin 1.2.3.1.2.3. sırasında harfi alınır

	Kriptografi	**&**	**Steganografi**
Amaç	İçeriği karartır		İletişimi gizler
Gizlilik	Şifreli Veri anlamsızdır		Gizli Veri görünmezdir
İletişim Güvenliği	Anahtarın Gizliliği		Veri Gömme Metodu
Sağlamlık Garantisi	Şifreleme Algoritması		İstatiksel ve Algısal Görünmezlik
Saldırılar	Bulmak kolay - Çıkartmak zor		Bulmak zor - Çıkartmak zor
Önlemler	Tersine Mühendislik		Veri Dinleme - İstatistik

Steganografi Yöntemleri

Steganografi (Steganography):
-Dilbilim Steganografi (Linguistic Steganography)
-Teknik Steganografi (Technical Steganography)

Metin, Ses , Görüntü, Video ve Ağ Steganografi gibi sınıflandırma da yapılabilir.

Metin Steganografi Yöntemleri

Format tabanlı yöntemler	Ayşe tatile çıksın (iki boşluk var)
Sözcük tabanlı yöntemler	Ayşe tatile gitsin
Söz dizimsel (sentaktik) yöntemler	Ayşe çıksın tatile
Anlamsal (semantik) yöntemler	Ayşe biraz dinlensin

LSB Ekleme Yöntemi

-En az değerlikli bitlerde (Least Significant Bit) mesajın gizlenmesidir
-RGB renk kodu kullanan görüntülerde daha çok veri gizlenebilir.

Ses Steganografi

-Gizli mesaj, dijital sesin içinde gömülüdür. Ses dosyalarının binary dizilerinin çok az değiştirilmesi ile yerleştirilir
-İnsan İşitme Sistemi (Human Auditory System - HAS) aralığı yüzünden, ses sinyalleri içierisine bilgi gizleme oldukça uğraş gerektiren bir konudur.
-LSB kodlaması, yankı veri gizlemesi, tayf yazılımı….

BS439_08_1

KİŞİSEL VERİLERİN KORUNMASI

Kişiyi belirlenebilir kılabilme özelliğine sahip verilerdir.
-Ad Soyad
-Telefon Numarası
-Sosyal Güvenlik Numarası
-Pasaport Numarası
-Motorlu Taşıt Plakası
-Özgeçmiş
-Resim
-Görüntü ve Ses Kayıtları
-Parmak İzleri…
Ek: Akım halinde "en sevdiğiniz hayvanın fotoğrafını paylaşma" gönderileriniz, güvenlik sorularınızın cevapları toplayan kötü niyetli kullanılabilir.

Özel (Hassas) Nitelikli Kişisel Veriler

Din - Mezhep - Kılık - Irk - Etnik Köken - Siyasi Düşünce - Felsefi İnanç

Biometrik - Genetik - Üyelik - Sağlık - İlişki - Ceza

Kişisel Verilerin İşlenmesi Kapsamı

Elde etme - Kaydetme - Depolama - Muhafaza Etme - Değiştirme - Yeniden Düzenleme

Açıklama - Aktarma - Devralma - Elde edilebilir hale getirme - Sınıflandırma - Engelleme

Kişisel Verilerin Korunması Kanunu
KVKK

6698 sayılı Kişisel Verilerin Korunması Kanunu, 24 Mart 2016 tarihinde TBMM'de yasalaşmış ve 7 Nisan 2016 tarihinde Resmi Gazete'de yayınlanarak yürürlüğe girmiştir.

-Kişisel verilerin işlenmesinde özel hayatın gizliliği başta olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek

Tanımlar;
-Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
-İlgili Kişi: Kişisel verisi işlenen gerçek kişi
-Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
-Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
-Açık Rıza: Belirli bir konuya ilişkin bilgilendirmeye dayanan ve özgür iradeyle açıklanan Açık Rıza Beyanı'nın yazılı alınma zorunluluğu yoktur. Elektronik ortam ve çağrı merkezi gibi yollarla alınması da mümkündür. İspat (inkar edilemezlik) yükümlülüğü, veri sorumlusuna aittir.

https://verbis.kvkk.gov.tr

Kişisel veriler, ilgili kişinin açık rızası olmaksızın işlenemez ve aktarılamaz.

-Aydınlatma metni: Veri sorumlusunun ve varsa temsilcisinin kimliği, verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, ilgili kişinin hakları konusunda bilgi içerir.
-Aydınlatma yükümlülüğü ve ispatı veri sorumlusuna aittir.
-Aydınlatma yöntemleri: Yazılı, sözlü, ses kaydı, çağrı merkezi, elektronik ortam

Kişisel Verilerin İşlenmesi

Genel İlkeler:
-Hukuka ve dürüstlük kurallarına uygun olma
-Doğru ve gerektiğinde güncel olma
-Belirli, açık ve meşru amaçlar için işlenme
-İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma
-İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etme

**Kişisel veriler, ilgili kişinin açık rızası olmaksızın işlenemez. Ancak kişinin açık rızası aranmaksızın kişisel verilerin işlenmesi;
-İlgili kişinin kendisi tarafından alenileştirilmiş olması
-Kanunlarda açıkça öngörülmesi
-Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması
-Fili imkansızlık nedeniyle rızasını açıklayamayac ak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması gibi durumlarda mümkündür.

**İlgili kişinin hakları;
-Kişisel veri işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgi talep etme
-Eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme
-Kişisel verilerin işlenme amacını ve amaca uygun kullanılıp kullanılmadığını öğrenme
-Kişisel verilerin kanunda öngörülen şartlar çerçevesinde silinmesini veya yok edilmesini isteme
-Yurt içinde/dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme ve kişisel verilere ilişkin düzeltme, silme işlemlerinin bu üçüncü kişilere bildirilmesini isteme
-Kişinin aleyhine bir sonucun ortaya çıkmasına itiraz etme
-Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme

Kişisel Verilerin Saklanması

-Veri sorumluları tarafından işlenen kişisel verilerin süresiz saklanması mümkün değildir
-Kişisel veriler işlenme süreleri bittikten sonra -ilk periyodik imha döneminde- imha edilmeli
-İlgili kişinin kişisel verilerinin işlenmesini istememesi ya da daha önce verdiği Açık Rıza Beyanı'nı çekmesi durumunda periyodik imha dönemi beklenmeksizin imha edilmelidir.

Veri Güvenliği

Veri sorumulusu,
-Kişisel verilerin muhafazasını sağlamak, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek için gerekli her türlü teknik ve idari tedbiri almak zorundadır.
-KVKK hükümlerinin uygulanmasını sağlamak için kendi kurum veya kuruluşunda gerekli denetimleri yapmak veya yaptırmak zorundadır.
-Kanun hükümlerine aykırı olarak öğrendikleri kişisel verileri başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük, görevden ayrılmalarından sonra da devam eder.

Yaptırım ve Cezalar

-Aydınlatma Yükümlülüğünün İhlali: En az 9.834₺ en fazla 196.686₺
-Veri Güvenliği Sağlama Yükümlülüğünün İhlali: En az 29.503₺ en fazla 1.966.862₺
-Kişisel Veri İhlali:
  -Hukuka aykırı olarak kişisel verileri kaydetme
  -Kişisel verileri hukuka aykırı olarak yayma, başkasına verme ve/veya ele geçirme

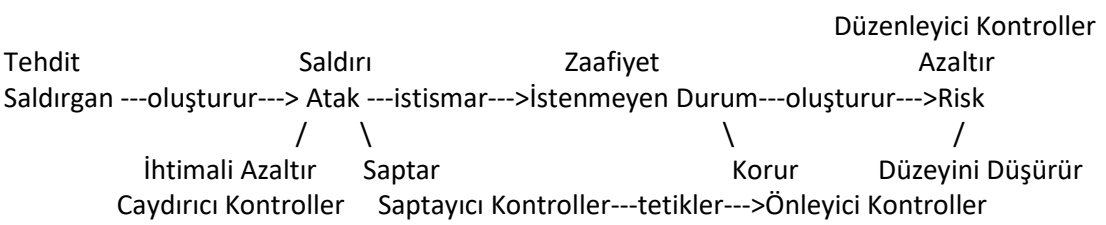
BS439_09_1

ZARARLI YAZILIMLAR

Bilgi Güvenliği Yaşam Döngüsü

-> Tehdit Analizi->Güvenlik Mekanizması---oluşturulur--->Sistem Tasarımı---uygulanır--->
İzle ve Yönet---sistem kontrolü--->Yeni Güvenlik Açığı---tespit edilir--->Tehdit Analizi ->

Sistem Güvenliği



Güvenlik Açıkları (Security Vulnerability)

Sistemin güvenlik politikasını ihlal etmek için kullanılabilecek zayıflıklardır.

-Zaafiyet örnekleri;

- -Donanım; yetersiz bakım, korumasız depolama..
- -Yazılım; eksik ya da yapılmamış yazılım testleri, karmaşık kullanıcı arayüzü..
- -Ağ; yetersiz ağ yönetimi, korumasız ziyaterçi ağ bağlantıları..
- -Çalışanlar; personel eksikliği, yetersiz güvenlik eğitimi..
- -Yapı; bina, kapılar, ve pencerelerin fiziksel koruma eksikliği, lokasyonun sele duyarlı olması
- -Organizasyon; düzenli denetim eksikliği

Tehdit(Threat)

Sistemde oluşabilecek olası bir olayın, sistemin ve/veya organizasyonun zarar görmesine neden olmasıdır (ISO 27005)

-Tehdit türleri;

- -Fiziksel hasar
- -Doğal olaylar
- -Temel hizmetlerde kayıp
- -Radyasyon nedeniyle rahatsızlık
- -Bilginin zaafiyeti
- -Teknik hatalar
- -İzinsiz Eylemler
- -Fonksiyonların zaafiyeti

-İnsan kaynaklı tehditler;
  -İç Kaynaklı;
    -Kaynaklara yetkisiz erişim
    -Bilgi hırsızlığı
    -Gizli bilgilerin ifşası
  -Dış Kaynaklı;
    -Virüs
    -Dağıtık hizmet engelleme saldırısı (DDoS)
    -Web sayfası manipülesi
    -Bilgilerin yok edilmesi
    -İş sürekliliğinin aksaması

Tehlike(Risk)
Belirli bir tehdidin sistemde bulunan bir güvenlik açığından yararlanarak sistemi zarara uğratma potansiyeli veya olasılığıdır.

Güvenlik açıklarından doğan güvenlik tehditleri, varlık üzerinde güvenlik riski oluşturur.

Tehdit * Güvenlik Açığı * Varlığın Değeri = Toplam Risk

Risk seviyesini belirlemek için, varlıklara yönelik tehditleri belirlemek ve sistemdeki güvenlik açıklarını bilmeniz gerekir.

Risk Yaşam Döngüsü
->Tehditler---faydalanır--->Güvenlik Açığı---nedeniyle--->Maruz Kalınır---oluşur--->
Tehlike---hafifletilir--->Güvenlik Önlemi---korur--->varlığı---tehlikeye sokan--->Tehditler->

Risk varlıkların, tehditlerin ve güvenlik açıklarının kesişmesidir.

Tehdit	**Zaafiyet**	**Risk**
Yangın	Yangın söndürme sistemi olmaması	Maddi Manevi Zarar
Hırsız	Fiziksel güvenliğin olmaması	Cihazların çalınması
Nem	Donanım dayanıksızlığı	Kurumsal bilgi kaybı
Sızma	Antivürüs kurulumu olmaması	Verilerin çalınması

Bilgisayar Korsanı (Hacker)
Ağlardaki ve bilgisayarlardaki açıklardan yararlanarak sistemlere izinsiz ve yetkisiz giren kişidir. Siyah, beyaz ve gri şapkalı hacker olarak tabir edilen 3 gruba ayrılır.

Tanımlar:
-Hacktivist: Kendilerine göre kötü veya yanlış olan toplumsal veya politik sorunları dile getirmek amacıyla belirli siteleri hack'leyerek mesajlarını yerleştirirler
-Phreaker: Telefon ağları üzerinde çalışan, telefon sistmelerini hackleyerek bedava görüşme yapmaya çalışırlar
-Cracker: Sistemleri ve özellikle de yazılımları kırarak kopyalarını dağıtırlar
-Script kiddie: Hacker olmamalarına rağmen az olan bilgileriyle tehlike arz ederler
-Lamer: Anlamsızca şeyler yapar ve hacker olmamasına rağmen kendini hacker olarak gösterir

Zararlı Yazılımlar (Malicious Software a.k.a. Malware)

Sistem güvenliğini tehdit eden, kullanıcı tarafından izin verilmeyen işlemler gerçekleştiren; bilgisayar sistemine zarar verme, kullanıcı verisini silme, engelleme, kopyalama, değiştirme, çalma, bilgisayar ve bilgisayar ağlarının performansını düşürme gibi zararlı amaçlar için programlanan yazılımlardır.

-**Bilgisayar Virüsü**

Bilgisayara zarar vermek için kendisini gizleyerek, kullanıcının izni veya bilgisi dışında sistemin çalışşma şeklini bozabilen ve verileri yok edebilen programlardır.

"**Brain**" adlı ilk kişisel bilgisayar virüsü, 1986 yılında geliştirildi. Dükkanlarından yazılım çalan müşterilerden bıkan iki kardeş, yazılım hırsızlarının disketlerinin önyükleme sektörünün etkilenmesi için virüsü tasarladıklarını öne sürdüler. Diskler kopyalandığında virüs de yayılıyordu.

-**Bilgisayar Solucanı (Worm)**

İlk olarak John Von Neuman tarafından kendini kopyalayabilen bilgisayar programı fikri ortaya atılmıştır. Kendilerini bir bilgisayardan diğerine otomatik olarak kopyalamak için tasarlanan, bilgisayarın çökmesine kadar etkilere yol açabilen programlardır.

Stuxnet, ABD ve İsrail'in İran'ın nükleer çalışmalarını sekteye uğratmak için kullandığı solucan yazılımdır. Endüstriyel kontrol sistemlerinin ve dış dünyaya kapalı sistemlerin de hedef olabileceğini göstermiştir. Stuxnet genellikle virüs bulaştırılmış bir USB flash sürücü aracılığıyla hedef ortama bulaştırılır. Stuxnet, üç bileşenden meydana gelmiştir:

-Saldırının main payload işlevi ile iligili tüm yordamları yürüten bir solucan
-Solucanın çoğaltılmış kopyalarını otomatik olarak çalıştıran bir bağlantı dosyası
-Tüm kötü amaçlı dosyaları ve süreçleri gizlemekten sorumlu bir rootkit bileşeni

-**Casus Yazılım (Spyware)**

Saldırgana kurban hakkında ilgili kişisel ve gizli bilgileri sisteme sızıp iletir.

Truva atı (Trojan) gerçek bir uygulama gibi gözükür. Ancak sistemde güvenlik açığı oluşturup zararlı yazılımların inmesi için zemin hazırlar. Saldırgan, truva atı kullanarak bilgisayarın ekran görüntülerinin alınmasını, sabit diskinin formatlanması, bilgisayar üzerindeki gizli dosyalara erişim gibi kötü niyetli işlemler gerçekleştirebilir

-**Spam**

Kişilere gönderilen genellikle reklam amaçlı maillerdir. Ancak birçoğu bilgisayara virüs, truva atı ya da bilgisayar solucanı bulaşmasına yol açar.

-Tuş Dinleyicisi (Keylogger)

Kullanıcıların klavye hareketlerini kaydetmek, bilgisayarındaki işlemleri kötü niyetli kullanıcılara iletmek için geliştirilmiştir.

-**Reklam Yazılımı (Adware)**

Arama isteklerinizi reklam web sitelerine yönlendirmek, pazarlama verilerini toplamak için tasarlanmışlardır.

-**Fidye Yazılımları (Ransomware)**

Bulaştığı bilişim sistemleri üzerindeki dosyalara erişimi engelleyen/kısıtlayan ve kullanıcılardan fidye talep eden zararlı yazılımlardır. Sahte olması ihtimal dahilindedir.

WannaCry saldırısı, dünya genelinde 230.000 bilgisayarı etkiledi. Dünya çapında 4 milyar dolarlık kayba yol açıldığı tahmin edilmektedir. Verilerin iade edileceğine dair bir garanti yoktur ve her yapılan ödeme suçluları ve suçu teşvik edip gelecekte de benzer saldırıların gerçekleşmesine neden olur.

-**Botnet**
Çok sayıda kullanıcının bilgisayar güvenliğini ihlal etmek, bilgisayarların kontrolünü ele geçirmek için bot'lar ile saldırı yapar. Bot'lar belirli eylemleri otomatik olarak gerçekleştirmek için tasarlanan programlardır.
Yayıncıların canlı sohbetlerine yorum atması için yazılabilen bot yazılımlar, her zaman yayıncının kendisi değil, "kötü niyetli biri tarafından bot atılıp yayıncının platform tarafından suçsuz yere ceza alması" halinde durduk yere zarara uğratılabiliniyor. Diğer durumda nedeni; yayıncı izleyici başına para kazanıyor olması ve platform'un kullanıcı sayısının artması uğruna bu tarz bilgisayar korsanlarına ödeme yapabileceği ihtimalinin yanısıra kullanıcı sürekliliği için süre bazlı verilen teşvik ödüllerinin botlar tarafından elde edilebiliyor olmasıdır.

-**DDoS (Distributed Denial of Service)**
Temel amaç bilgi sızdırmak ya da kar sağlamak değil, saldırı gerçekleştiren hedef sisteminlerin çalışamaz hale gelmesine neden olmaktır. Dağıtık haldeki çok sayıda bilgisayardan aynı anda yapılır. Güvenilirliği ve sürekliliği sağlamak adına bu tip ataklara 4 farklı kurumun 3 farklı cihazla sunduğu internet hizmetlerini yedek olarak tutarak önlem alınabilir.

-**Sosyal Mühendislik (Social Engineering)**
İnsan faktörünü kullanan saldırı tekniklerinden ya da kişiyi etkileme ve ikna yöntemlerinden faydalanarak normal koşullarda bireylerin gizlemeleri/paylaşmamaları gereken bilgileri bir şekilde ele geçirmesidir

Saldırı Türleri

Kaba Kuvvet (Brute Froce)
Kişilerin veya kurumların hesaplarına izinsiz erişim elde etmek için yapılan parola denemeleri

Dinleme (Eavesdropping)
Bilginin izinsiz bir şekilde ele geçirilmesi ve bir gözetleme biçimidir.

Ortadaki Adam (Man in The Middle)
Değişikliğe uğratma, aktif bir biçimde verileri değiştirerek sisteme saldırı gerçekleştirme

Sıfır Gün (Zero Day)
Bir programlama hatasından veya yanlış yapılandırmadan kaynaklanan ve henüz düzeltme eki bulunmayan yazılım veya donanım açığı kullanılarak gerçekleştirilir (bug abuse)

Rootkit
İşlemlerini işletim sisteminden ve sistem kayıtlarından gizlediği için tespit edilmesi zordur. Daha fazla gizli program yüklemek ve sisteme "arka kapılar (**backdoor**s)" oluşturmak için kullanılır.

SQL Enjeksiyon (SQL İnjection)
SQL güvenlik açıklarından faydalanılarak kurbanların veri tabanları kontorl altına alınır.

Dikkat

-Bilgisayar hızında düşüş
-Ekranda garip ve çok sayıda mesajların belirmesi (popup)
-Kullanılan programların çökmesi ya da çok yavaş çalışması (crash)
-Doküman ya da dosyaların isimlerinin, boyutlarının, kayıt tarihlerinin kendi kendine değişmesi
-İnternette dosya 'indirme' ve 'yükleme' hızının çok düşmesi
-Monitörde tuhaf hareketler olması
-Açılır reklamların normalden daha sık görünmesi

Korunma

-Anti-virüs, anti-malware yazılımlar kulllanılmalı. Koruma yazılımları güncel olmalıdır.
-Telefonun Bluetooth ve Wi-fi bağlantısı kullanılmadığı durumlarda kapalı olmalıdır.
-Ağ adının değiştirilmesi ve gizlenmesi
-Şifreleme yöntemi, dosya tarama
-Güvenlik Duvarı
-http adreslemesinin https olmasına bakılmalıdır. Sondaki s "secure"den gelir.

[Vize Sonrası] BS439_11_1

SOSYAL MÜHENDİSLİK

-İnsan faktörünü kullanan saldırı tekniklerinden ya da kişi etkileme ve ikna yöntemlerinden faydalanarak normal koşullarda bireylerin gizlemeleri / paylaşmamaları gereken bilgileri bir şekilde ele geçirme sanatıdır.

-Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir.

-Kullandığı en büyük silahı, insan zaafiyetleridir.

-Örneğin sosyal medya akımlarında, ingilizce bir şarkıda en sevdiğin hayvan kısmında videonun üstüne yazılan yazı ile güvenlik sorularından biri olan bir sorunun cevabı ele geçirilebilir.

İnsan Tabanlı Sosyal Mühendislik Teknikleri
Sosyal mühendislikte insanlarla doğrudan iletişime veya etkileşime geçilmesi durumudur.

https://www.youtube.com/watch?v=34h2Dk7R1lU

Bilgisayar Tabanlı Sosyal Mühendislik Teknikleri
Sosyal mühendislik süreçlerinde insan zaafiyetlerinin yanında sistem zaafiyetlerinin de kullanılması durumudur.

https://www.youtube.com/watch?v=XKeaqmO5wRg

-Bir web sitesinin veya mobil uygulamanın tasarım olarak benzerini yapıp bilgilere erişme
-Sahte mail
-Reklamlara tıkla para kazan siteleri
-Kendisini bir firmanın yetkili kişisi gibi tanıtıp bilgilere erişme (telefon görüşmeleri)
-Zincirleme mektup

https://news.bbc.co.uk/2/hi/technology/2320121.stm

Sosyal Mühendis
İnsanlardan önemli bilgileri öğrenmek için aldatıcı konuşmalar yapan veya diğer haberleşme ve ikna yöntemlerini kullanan kişidir.

İnsanların doğasında bulunan zaafiyetleri kullanarak sonuca ulaşırlar;
-Yardımcı olma isteği
-İnsanlara güvenme eğilimi
-Sorundan uzak durmaya çalışma çabası
-…

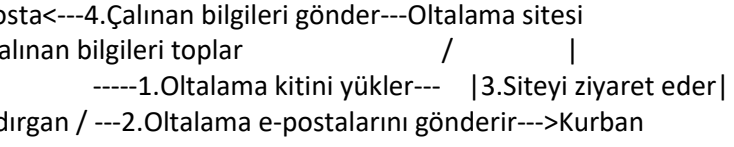
Sosyal mühendisin belirgin özellikleri
-Yardımsever görünürler
-İkna kabiliyetleri yüksektir
-Etkileyici, nazik ve sempatik kişilik sergilerler
-Genellikle iyi giyimli kişilerdir
-İnsanların güvenini kazanma eğilimi sergilerler
-Acındırma, suçluluk duygusu hissettirme ve sindirme en çok kullanılan üç psikolojik yöntemdir
-…

Sosyal mühnedislik saldırılarında kullanılan donanımlar
-Donanımsal keylogger
-Gizli kameralı araba anahtarı
-Gizli kameralı kalem
-Gizli kameralı gözlük

Sosyal Mühendislik Saldırıları
-Oltalama (Phishing)
-Omuz sörfü (Eavesdropping, Shoulder surfing)
-Kimlik hırsızlığı (Identity theft)
-Yardım masası (Help desk)
-Truva atları (Trojans)
-Çöp dalışı (Dumpster diving)
-Kimliğe bürünme (Impersonation)
-Üçüncü taraf (Third-party Authorization)
-Tersine sosyal mühendislik (Reverse Social Engineering, RSE)
-…

BS439_11_2

Oltalama (Phishing, Kimlik Avı, Çevirimiçi Dolandırıcılık)
İnternet kullanıcısın kandırarak, kullanıcıya ilişkin kredi kartı bilgileri, banka hesap numaraları, internet şifresi gibi birçok özel bilgiyi ele geçirmektir.



-**Sykipot**
2006 yılında Adobe Reader and Acrobat uygulamasının güvenlik açıkları kullanılarak sisteme erişim saldırısında çoğunlukla amerikan ve ingiliz savunma telekominikasyon firmaları hedef alınmıştır.

-**Ghostnet**
2009 yılında sistemlerin ses ve görüntü kayıt aygıtlarını kullanmak üzere enfekte edilmesini kapsayan bir saldırı genellikle büyükelçilikler gibi diplomatik temsilciliklere yönelik gerçekleştirilmiştir.

Cevap Verilirse
-Parolayı ele geçirenler tarafından, gönderilecek mesajın görünen ismin, sizin ismininz yerine genellikle başka bir isimle değiştirilir.
-Hesabınızda bulunan veya size sonradan gelecek olan mesajlar saldırgana yönlendirilir ve sizdeki kopyası silinir
-E-posta hesabınızda kayıtlı bulunan başka sitelerin parolaları ele geçirilir.
-Mesajın sonuna eklenecek olan imza metni değiştirilir.
-…

E-posta Güvenliği
-E-posta hesabınız için kullandığınız parola, diğer hesaplarınızda kullandığınız parolalardan farklı olmalıdır.
-Kişisel bilgilerinizi isteyen e-postalara yanıt vermeyin
-Şüpheli gördüğünüz e-postalardaki URL linklerine tıklamayın. (bit.ly, ow.ly, tinyurl.com, is.gd, goo.gl, tiny.cc, cli.gs…)

Telefon Oltalaması (Vishing)
Saldırı gerçekleştirmek için telefon görüşmeleri kullanılmasıdır. Korsan/Dolandırıcı sizi arar, kişisel ve finansal bilgilerinizi ele geçirmeye çalışır. Ses tonu; gerçekçi, tedirgin edici ve güven verici olabilir.

Ne Yapmalı?
-Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgilerinizi kimseye söylemeyin.
-Parola kişiye özel bilgidir, sistem yöneticinize bile telefonda veya e-posta ile parolanızı söylemeyin.
-Paylaştığın bilgileri seçerken dikkat edin.
-Kimlik bilgilerini sorgulayın.
-Kaynağın güvenilirliğini kontrol etmek için farklı iletişim kanalları kullanın.
-Cihazlarınızın güvenliğini yükseltin.
-…

Risk Alanları ve Mücadele Stratejileri
-Telefon (Yardım Masası) (Taktik: Taklit ve inandırma)
Mücadele Stratejisi : Çalışanların ve yardım masasının telefonla hiçbir şekilde şifre veya diğer gizli bilgilerin verilememesi için eğitilmesi

-Binaya giriş (Taktik: Yetkisiz fiziksel erişim)
Mücadele Stratejisi : Sıkı kimlik kartı güvenliği, çalışanların eğitilmesi ve güvenlik görevlilerinin çalıştırılması

-Ofis (Taktik: Omuz sörfü, Klavyeyi gözetleme)
Mücadele Stratejisi : Sizden başka birinin ortamda bulunduğu durumlarda şifrenizi girmeyin. Zaruri durumlarda hızlı bir şekilde tuşlara basınız veya uzaklaşmasını rica ediniz.

-Telefon, Ofis (Taktik : Yardım masası aramalarında taklit etme, Kimsenin olmadığı açık odalar bulabilmek için koridorlarda dolaşma)
Mücadele Stratejisi : Bütün çalışanlara yardım masası desteği alabilmesi için tekil bir PIN numarası atanması

-Posta odası, Makine odası, Santral (Taktik: Sahte notların sokulması, Erişmeye teşebbüs, cihazların kaldırılması ve gizli bilgileri elde edebilmek için bir protokol analizcisi eklenmesi)
Mücadele Stratejisi : Posta odasını kilitle ve izlmeye tabi tut. Santral, sunucu odaları vs. her zaman kilitli tut ve cihazların güncel envanterini tut

-Telefon ve PBX (Taktik: Telefon görüşme ücreti erişimi çalma)
Mücadele Stratejisi : Şehirlerarası, milletlerarası ve cep telefonu aramalarını kontrol et, konuşmaları izle, aktarmaları reddet

-İş yeri atık deposu (dumpster), Intranet, Internet (Taktik: Çöplük karıştırma, Şifre araklamak için Intranet veya Internet üzerinde sahte yazılımların oluşturulması ve konulması)
Mücadele Stratejisi : Bütün çöp kutularını güvenli ve izlenen alanlarda tut. Önemli belgeleri kesme makinesiyle yok et, manyetik ortamdaki verileri sil. Sistem ve ağ değişikliklerinden sürekli haberdar ol, şifre kullanımı eğitimi ver.

-Ofis (Taktik: Hassas belgelerin çalınması)
Mücadele Stratejisi : Belgelere gizlilik derecesi ver ve bu belgeleri kilitli yerlerde sakla

-Genel, Psikolojik (Taktik: Taklit ve ikna)
Mücadele Stratejisi : Bütün çalışanları sürekli uyanık tutarak ve eğitim programlarına tabi tutarak bilinçlendirme

https://kamusm.bilgem.tubitak.gov.tr/dokumanlar/belgeler/kitaplar/temel_kavramlar.jsp

BS439_12_1

Biyometrik Güvenlik Teknolojileri

Kimlik Doğrulama (authentication)
Kullanıcıların iddia ettikleri kişi olup olmadıklarını ispat etmek için kullanılır.

Teknolojik gelişmelerle birlikte, kullanıcıların kimliklerini sanal ortamlarda doğrulamak için;
-Sadece kullanıcının kendisi ve doğrulama otoritesinin bildiği bir parola,
-Tek kullanımlık parola üreten bir yazılım veya donanım,
-Biyometrik yöntemler kullanılmaktadır.

Kullanıcının kimlik bilgisi = kullanıcı adı + parola (akıllı kart veya parmak izi)

Kimlik doğrulama çeşitleri;
-Tek faktörlü kimlik doğrulama
-İki faktörlü kimlik doğrulama
-Çok faktörlü kimlik doğrulama

-En yaygın kullanılan kimlik doğrulama yöntemi, sadece kullanıcının kendisinin bildiği parola kullanımıdır. Zayıf yönleri, kötü niyetli kişiler tarafından çeşitli yollarla kolayca ele geçirilmesi ve bu nedenle sık aralıklarla değiştirilen parolaların unutulması

-Akıllı kart kulanımı ve biyometrik yöntemler, daha güvenlidir ancak kullanıcıya ek maliyet getirir.

Güçlü bir parola
-En az sekiz karakter uzunluğunda olmalı
-En az bir küçük harf, bir büyük harf, bir rakam, bir noktalama işareti içermeli
-Kişisel bilgiler (ad, soyad, doğum tarihi gibi) içermemeli
-Aynı parola birden çok kimlik doğrulama sisteminde kullanılmamalı
-Belirli zaman aralıklarında yenilenmemeli
-Önceden kullanılan perolalardan farklı olmalı
-…

Biyometrik teknolojiler
Kimlik doğrulama (authentication) = olduğunu söylediğin kişi misin?, doğrulama (verification) = seninle ilişkili veriler var mı? ve tanımlamayı (identification) = sen kimsin? birleştirmektedir. Parmak izleri, el geometrisi, kulak memesi geometrisi, retina ve iris desenleri, ses dalgaları, tuş vuruşu dinamikleri, DNA ve imzalar gibi bir veya daha fazla ayırt edici biyolojik özellik aracılığıyla bireylerin benzersiz bir şekilde tanımlanabileceği yollara dayanmaktadır.

İnternet bankacılığında kullanıcı tanımlama, Akıllı ev sistemleri, Yüksek güvenlik gerektiren binaların giriş çıkış işlemleri, Uzaktan eğitim sınav işlemleri, Havaalanları giriş çıkış işlemleri gibi birçok farklı alanda kullanılmaktadır.

Biyometrik Yöntemler

Fizyolojik (Physiological) Yöntemler : Kişinin fiziksel özellikleri analiz edilir.
-Yüz detayları, parmak izi, avuç izi, el geometrisi, iris desenleri, retina taraması, kan örneği veya ses tanıma,…

Davranışsal (Behavioral) Yöntemler : Kişinin neyi ve nasıl yaptığı analiz edilir.
-El yazısı (imzası) tanıma, klavye hareketlerini algılama,…

Biyometrik Yöntem	**Hata Oranı**
Retina Tarama (Işığı ileten damarlar)	1:10.000.000
İris Tarama (Göz rengini veren bölge)	1:131.000
Parmak İzi Tarama	1:500
El Geometrisi Tarama	1:500
İmza Tarama (Yazı)	1:50
Ses Tarama	1:50
Yüz Tarama	Veri yok
Vascular Patterns	Veri yok

Biyometrik Tanımlama
İki tür hata vardır:
-Hatalı Kabul (False Acceptance) yanlış kişiyi kaydetmek
-Hatalı Reddetme (False Rejection) gözlük takınca reddetmek

BS439_12_2

Parmak İzi Tanıma

Parmak izi okuyucu teknolojisi
Parmak izinin döngülerini, kıvrımlarını, parmak izinin sırt uçlarını ve diğer özelliklerini tarar ve bunları depolanan şablonlarla karşılaştırır. Bir eşleşme bulunduğunda erişim verilir.

El Geometrisi Tanıma

El geometrisi teknolojisi
Elin geometrisini değerlendirir
-Parmak uzunluğu
-Parmak genişliği
-El genişliği
-Eklemler arasındaki mesafe

Avuç içi / Parmak Damarı Tanıma

Avuç içi veya parmakların görüntülerinden damar desenlerini / modellerini analiz ederek kimlik doğrulamasını gerçekleştirir
Hitachi
Akıllı telefon kameralarını kullanarak yüksek hassasiyetli parmak damarı kimlik doğrulaması

Yüz Tanıma

Yüz tanıma teknolojisi
Arşivlenmiş bir görüntüye göre öznenin yüzünün geometrik özelliklerini analiz eder.
Kişinin gözlerinin merkezi konumlandırılmalı ve kesin konumlara yerleştirilmelidir.

İris Tanıma

İris, göz bebeğimizin etrafında yer alan renkli halkadır. İrisin biyometrik teknolojilerden biri olarak kullanılmasının sebepleri;
-Dünyada aynı irisin olma olasılığı 1/10^78 dir.
-Ömür boyu değişmeyen tek organdır.
-Tek yumurta ikizleri aynı DNA yapısına fakat farklı iris yapısına sahiptir.

İris tanıma sistemi
İrisin dijital görüntüsü alınır. Çekilen resimden iris ayırt edilerek kalan kısımlar çıkartılır. Demodulasyon adı verilen bir işlem ile iris resminden DNA çizgisine benzer bir kod(IrisCode) üretilir.
-Canlılık testi yapabilen yegane biyometrik teknolojidir.
-Doğrudan temas olmadığı için hijyeniktir.
-Sistemin hata kabul olasılığı 1/10^42 dir.

Ses Tanıma

Ses tanımlama sistemleri
Konuşmacının ağız ve boğaz şeklinin yarattığı özellikler dayanır. Kullanıcıya şifre niteliğinde kullanılan belirli bir kelime grubu okutularak elde edilen ses verisi, spektral analizler kullanılarak dijitalleştirilir ve veritabanına kaydedilir. Sonrasında, kullanıcı aynı kelime grubunu okuyarak sisteme erişebilir.

Engelleyici faktörler
-Ses dosyasının çok fazla yer kaplaması
-Hastalık veya başka dış etkenlerden etkilenmesi
-Parazit oluşturan dış ortamdan gelen gürültüler
-Geçiş/erişim hakkına sahip bir kişinin ses kaydı kullanılarak kolayca aldatılabilir olması

Yürüyüş Tanıma

Kişinin yürüyüşüyle kimlik tespiti yapmaya dayanır.

Southampton Üniversitesi'nden profesör Mark Nixon tarafından tasarlanan bir kimlik tanımlayıcı oda, yürüme biçimlerindeki detaylarla kişileri hafızasına kaydetmekte ve sonrasında içerisinden kimin geçtiğini tanımlayabilmekte. (Yürüyüş Tüneli, 2008)

Avantajları
-Klasik yöntemlerden çok daha iyi doğruluk sunabilir olması
-Biyometrinin çalınması, kaybedilmesi veya ödünç verilmesi çok daha zor olması
-Herhangi bir parolayı ezberleme zorunluluğu olmaması
-Kişinin özellikleriyle ilişkili olduğundan, o kişinin bu erişim yeteneğini unutması, yanlış hatırlaması veya kaybetmesi daha zor olması
-Biyometrik okuyucular, en güvenilir yöntemlerden olması
-Çalınan parolalar ve kimlik sahtekarlığı (spoofing) gibi tehditlere karşı dayanıklı olması
-…

Dezavantajları
-Biyometrik yöntemlerin en pahalı kimlik doğrulama yöntemleri olması
-Biyometrik tarayıcıların tipik olarak diğer okuyucular kadar hızlı olmaması
-Biyometrik kimlik doğrulama yapan sistemlerin bazılarının, düzgün çalışması için kullanıcı tarafında beceri gerektirmesi (kullanıcı hata payının yüksek olması)
-Bazı biyometrik sistemlerin çeşitli nedenlerden dolayı yönetim tarafında kabul edilemez olarak algılanması (yönetmesi riskli, tecrübeli uzman sayısı az)
-…

BS439_13_1

Ağ Güvenliği

Günümüzde dijitalleşmenin etkisinde birçok kurum verilerini ağlara taşısa da, çok büyük öneme sahip özel ve kurumsal bilgilerin internet gibi global ve güvensiz bir ortamda dolaşması güvenlik kaygılarının artmasına sebep olmaktadır.

Nitekim 2021 yılı Ocak ve Haizran ayları arasında Türkiye'de her gün 1.611, her saat 67 ve her dakika 1 adet kötü amaçlı yazılım saldırısı gerçekleşti. Ayrıca 31.613 adet ağ güvenliği saldırısı yaşandı ve bu saldırıların büyük bir çoğunluğu "Web Brute Force Login" olarak gerçekleşti.
(WatchGuard, 2021)

Ağ güvenliği (Network Security)
Ağ trafiğini de kapsayan dijital varlıkları korurken, izinsiz ağ saldırılarını izleme, önleme ve bunlara yanıt verme için tasarlanmış araçları, taktikleri ve güvenlik politikalarını tanımlar.

Her kuruluşun bir ağa sahip olduğu varsayılırsa;
-Kendi yerel ağını korumak
-Diğer ağlarla olan iletişimi korumak

Temel alanları:
-**İletişim Güvenliği (Communication Security)**
Kuruluşlar ve son kullanıcılar arasında ağlar üzerinden iletilen verilerin korunması

-**Çevre Güvenliği (Perimeter Security)**
Bir kuruluşun ağının yetkisiz erişimler karşı korunması

Ağ Güvenliğinin Önemi

Kaynaklara yetkisiz ve illegal sebeplerle kötü amaçlı erişimleri engellemek ve verinin dolaşımı sırasında gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak ağ güvenliği kapsamında yapılmaktadır.

Ağın önemli ve hassas bilgiler barındırması sebebiyle içerdeki verilerin ve hizmetlerin korunması önemlidir. Her ağa, güvenlik açıkları nedeniyle içeriden ya da dışarıdan izinsiz erişimler olabilmektedir. Önemli verilerin sadece iç ağdaki kullanıcılara değil aynı zamanda dışarıdan girebilecek kişilere karşı da korunması gerekir.

Ağ protokolleri, yazılım ve konfigürasyondaki açıklar ve problemlerden kaynaklanan uzaktan erişim zayıflıkları, saldırganların yetki alarak dışarıdan sisteme girişlerini kolaylaştırmaktadır.

Ağ Tabanlı Saldırılar

DoS ve DDoS (Denial of Service - Hizmet Dışı Bırakma ve Distributed DoS)
Amaç hedef sunucu, uygulama ve servisin hizmet dışı kalmasını sağlamaktır. DoS tek bir kaynaktan hedefe yönelik trafik üretirirken, DDoS birden fazla kaynaktan hedefe doğru trafik üretir. Bilgi güvenliğinin temel unsurlarından erişilebilirliği tehdit eder.

Sniffing (Paket Dinleme)
Ağ üzerinde yer alan veri akışını dinleyerek çözümler ve veriyi ele geçirmeyi amaçlar

İyi niyetli kullanım
-Sistem problemlerini ve performansını anlam
-Uygulama operasyonlarının testi
-Saldırıların tespiti

Kötü niyetli kullanım
-Protokoller üzerinde pasif olarak veri toplama
-Hedef ağın trafiğini ve örüntüsünü keşif
-Ağ içerisine dahil olarak arka kapı bırakma

Spoofing (Aldatma, sahtecilik)
Güvenli olarak görünen kaynaktan paket gönderilerek alıcıyı aldatmak amaçlanır.
-URL spoofing : Saldırgan hedefinde olduğu kişiye benzer bir URL linki gönderir.

IP spoofing (IP sahtekarlığı)
Saldırgan veri paketlerini gönderirken farklı bir IP adresi ile değiştirerek gönderir, böylece saldırı yapılan bilgisayar gerçek kaynağı göremez.
Saldırganlar, korumalı ağa kötü amaçlı yazılımlar ve botlar göndermek, DoS saldırıları yürütmek veya yetkisiz erişim elde etmek için IP sahtekarlığını kullanır.

ARP spoofing (Adres Çözümleme Protokolü sahtekarlığı)
Saldırgan yerel ağı sahte ARP paketleri ile doldurur. Tüm trafik, hedeflenen varış yerine ulaşmadan önce saldırganın bilgisayarına yönlendirilir. Bu aşamada saldırgan isterse verileri bozabilir ya da değiştirebilir.

ARP (Address Resolution Protocol)
İki bilgisayarın haberleşmesi için gerekli fiziksel adreslerin tespit edilmesini sağlar. DNS mantığı ile çalışır.

Man-in-the-Middle, Session Hijacking, Denial of Service (DoS)

Ağ Güvenliği Çözümleri

-Güvenlik Duvarı	-Bulut Güvenliği	-Kablosuz Ağ Güvenliği	-Uygulama Güvenliği
-Ağ Erişim Kontrolü	-Antivirüs ve Antimalware	-VPN	-Mobil Güvenlik

Kablosuz Ağ Güvenliği
Kablosuz ağlar; kolay kurulum, fiziksel bir konuma bağlı olmama ve hareket etme yeteneği ve ölçeklenebilirlik sunar.

Bir kablosuz ağı yetkisiz ve kötü niyetli erişim girişimlerinden korur ve varsayılan olarak tüm kablosuz iletişimi şifreleyen ve güvence altına alan kablosuz cihazlar (genellikle bir kablosuz router / switch) aracılığıyla sağlanır.

Kablosuz ağ güvenliğini sağlamaya yönelik yaygın kullanılan algoritma ve standartlar; WEP (Wired Equivalent Policy - Kabloluya Eşdeğer Gizlilik), WPA (Wireless Protected Access - Kablosuz Korumalı Erişim)

Mobil Cihaz Güvenliği
Mobil cihazlarda saklanan bilgilerin ve servislerin koruma altına alınması olarak değerlendirilebilir.

Önümüzdeki üç yıl içinde BT kuruluşlarının yüzde 90'ı kurumsal uygulamaları kişisel mobil cihazlarda destekleyebilir. Bu durumda, ağa hangi cihazların erişebileceğini kontrol etmek ve ağ trafiğini gizli tutmak için bağlantıları yapılandırmak gerekecektir.

BS439_13_2

Bulut Bilişim
Bilgi işlem hizmetlerinin (sunucu, depolama, veritabanı, ağ, yazılım, analiz ve makine zekası dahil) İnternet ("bulut") üzerinden sağlanmasıdır. Bulut sunucuları, dünya çapında birçok veri merkezinde bulunduğundan, kullanıcılar ve işletmeler, fiziksel sunucuları işletmek veya kendi cihazlarında yazılım programları çalıştırmak zorunda değildir.

Bulut Güvenliği
Genel, özel ve hibrit bulut olmak üzere üç tür bulut ortamı vardır.
-Genel Bulut: Amazon, Microsoft Azure, Dropbox gibi üçüncü taraf sağlayıcılar tarafından sunulur. Genel halk tarafından kullanılabilir.
-Özel Bulut: Tek bir şirket tarafından kullanılabilen bir bulut hizmetidir.
-Hibrit Bulut: Hem özel hem de genel bulutların özelliklerini birleştirir.

Bulut Bilişim Güvenliği
Bulut tabanlı veri, altyapı ve sistemlerde tehdit koruması sağlamak için bir dizi teknoloji, politika ve prosedür içerir.
Bulut güvenliği, merkezi koruma, tahsisli donanım olmaması nedeniyle maliyetin düşürülmesi, idari personel ihtiyacının azaltılması, mininmum kesinti süresi, verilere her yerden kolay erişim ve kolay ölçeklenebilirlik gibi birçok avantaj sunar.

Uygulama Güvenliği
Herhangi bir uygulama, saldırganların ağınıza sızmak için kullanabileceği delikler veya güvenlik açıkları içerebilir. Uygulama güvenliği, bu açıkları kapatmak için kullanılan donanım, yazılım ve süreçleri kapsar.

Web Güvenliği
Esas olarak web sitelerinin, web servislerinin ve uygulamaların güvenliğine odaklanır.
Bir web güvenlik çözümü, çalışanların web kullanımını kontrol edecek, web tabanlı tehditleri engelleyecek ve kötü amaçlı web sitelerine erişimi engelleyecektir.

Ağ Güvenliği İçin

-Kurum bünyesinde "Güvenlik Politikası" oluşturulmalı
-Ağ güvenliği için tek başına bir Güvenlik Duvarı yeterli değildir
-Önemli ve kritik bilgiler mutlaka şifrelenerek gönderilmeli
-Ağa bağlı her elemanın güvenliği belirli seviyelerde sağlanmalı ve sistem devamlı kontrol altında tutulmalı
-Uç noktaların internet altyapısı üzerinden birbirine bağlanmasında VPN çözümleri
-Çalışanlar, politikalar ve uygulamalar konusunda eğitilmeli
-…

Sanal Özel Ağ (Virtual Private Network - VPN)

Birden falza sistem veya ağın güvensiz ağlar üzerinden güvenli iletişimini sağlayan ağ bileşenidir.
-Ağ bağlantısını gizleyerek bulunulan IP adresini gizlemeyi sağlar
-Veri trafiğini şifreleyerek internet üzerinde bilgilerin güvenliğini sağlar
-Güvenli olmayan ağlara bağlanırken kimlik gizlemeyi sağlar
-Kullanılan yerel ağa ve sunucularına uzaktan güvenli bir şekilde erişim sağlar
-İnternet üzerinden farklı DNS servislerine güvenli bir şekilde bağlanabilmeyi sağlar
-…

Sanal Yerel Alan Ağları (Virtual Local Area Network, VLAN)

Farklı coğrafi konumlardaki donanım sistemleri bile aynı sanal yerel alan ağın bir parçası olabilir. Yetki veya kullanım ihtiyaçlarına göre bilgisayarlar, çeşitli sanal ağlara dağıtılır. Bir bilgisayar ancak kendi sanal ağındaki bilgisayarlar ile güvenli iletişimde olabilir, diğer ağlara izni dahilinde erişebilir veya hiç erişemez.

BS439_14_1

Bilgi Güvenliği Teknolojileri

Bilgi güvenliği, bilgilerin korunmasıdır ve bilgilerin yetkisiz taraflara ifşa edilmesi riskini en aza indirir. Teknoloji, insanların ihtiyaç ve isteklerini karşılamak üzere hedefe ulaşmak için kullanılan bilgi, beceri, yöntem ve süreçlerin tamamı. Bilgi güvenliği teknolojileri, dijital güvenlik için gerekli araçları sağlar.

Bilgi Güvenliği

Proaktif			**Reaktif**		
Ağ	**Bilgisayar**	**Uygulama**	**Ağ**	**Bilgisayar**	**Uygulama**
Donanım	Donanım	Anti-virus	Erişim	Erişim	Erişim Kontrolü
VPN	Anti-virus	SDKs	Biyometrik	Biyometrik	Biyometrik
Protokol	Protokol	Kripto	Loglama ve Şifreler	Loglama	Loglama
SDKs	SDKs	Dijital İmza	Güvenlik Duvarı	G.D. ve S.T.	Şifreler
Kripto	G. Açığı Saptama	Sertifika	Saldırı Tespit	Uzaktan Erişim	

Bilgi Güvenliği Teknolojileri;
-Antivirüs (Antivirus)
-Güvenlik Duvarı (Firewall)
-Saldırı Tespit Sistemleri (Intrusion Detection System, IDS)
-Veri Kaybı Önleme (Data Loss Prevention, DLP)
-Güvenlik Bilgileri ve Olay Yönetimi (Security Information and Event Management, SIEM)
-Kullanıcı Davranış Analizi (User Behavioral Analytics, UBA)
-Uç Nokta Tehdit Algılama ve Yanıt (Endpoint Detection and Response, EDR)

Antivirüs

Sistemi virüslerden korur.
Dosyanın bir virüs olup olmadığını tespit etmek için antivürüs, o antivirüsün veritabanında bulunan imzaları kullanılır.
Ağa bağlı tüm cihazlarda, kendilerini virüs saldırılarından korumak için bir antivirüs kurulu olabilir.

Güvenlik Duvarı

Kontrollü bir bağlantı kurmak, güvenlik ve denetimin uygulanabileceği tek bir darboğaz noktası oluşturmak için ağ ve internet arasına bir güvenlik duvarı (firewall) yerleştirilir. İç ağları dış ağlardan gelen saldırılara karşı koruyan bir kontrol noktasıdır. Kontrol noktası, kurallara göre hangi trafiğin girip çıkabileceğine karar verir.

Güvenlik Duvarı Teknolojisi Türleri
-Paket Filtreleri
-Durum Bilgili Paket Filtreleri
-Uygulama Seviyesi Ağ Geçidi / Yeni Nesil Güvenlik Duvarı

Güvenlik duvarının amaçları;
-İçeriden dışarıya tüm trafik güvenlik duvarından geçmelidir.
-Yalnızca yetkili trafiğin geçmesine izin verilecektir.
-Güvenlik duvarının kendisi penetrasyona karşı bağışıktır.

Güvenlik duvarlarının erişimi kontrol etmek ve güvenlik politikalarını uygulamak için kullandığı teknikler;
-Hizmet kontrolü
-Yön kontrolü
-Kullanıcı kontrolü
-Davranış kontrolü

Güvenlik Duvarı;
-Yetkisiz kullanıcıları, korumalı ağdan uzak tutar.
-Güvenlik duvarları genellikler dış saldırılara karşı ilk savunma hattıdır, ancak tek savunma olmamalıdır.
-Potansiyel olarak savunmasız hizmetlerin ağa girmesini veya ağdan ayrılmasını yasaklar.,
-Güvenlikle ilgili olayları izlemek iin bir konum sağlar.
-Güvenlikle ilgili olmayan çeşitli İnternet işlevleri için uygun bir platformdur.
-…

Saldırı Tespit Sistemleri

Saldırı (Intrusion): Bir hedef ağın güvenliğini (kaynakların gizliliğini, bütünlüğünü, sürekliliğini) tehlikeye atmayı amaçlayan eylemlerdir.

Saldırı Tespit Sistemleri (Intrusion Detection System - IDS): Bilgisayar sistemine ve ağ kaynaklarına olan saldırıları tespit etmeyi, sistemi izleyip anormal olan durumları saptamayı ve bunlara karşı gerekli önlemleri almayı amaçlayan güvenlik sistemleridir. Ağdaki saldırıları bulmada ve engellemede en büyük yardımcılardır. Saldırı Tespit Sistemleri, şüpheli etkinliği tespit eden otomatik sistemlerdir.

Saldırı Tespit Hataları
-False negatives: "saldırının algılanmaması"
-False positives: "zararsız davranışın saldırı olarak algılanması"

Kullandığı teknikler açısından;
-**İmza (Signature) tabanlı IDS**: Bilinen saldırı kalıplarını kullanarak saldırıları kolayca tespit edebilir. İlk kez yapılan saldırıların tespit edilmesi mümkün değil.
-**Anomali (Anomaly) tabanlı IDS**: Normal sistem davranışı modelini baz alarak sapmaları ve anormallikleri tespit etmeye çalışır. Olaylar arasındaki ilişkilerin yakalanması mümkün değil.

Tespit ettiği yerler açısından;
-**Ağ Tabanlı (NIDS)**: Bir bilgisayar ağının tamamını yada belirli bir kısmını izler. Ağdaki her bir harici güvenlik duvarının arkasında, harici güvenlik duvarının dışına, büyük ağ omurgası ve kritik alt ağların trafiğini izleme için yerleştirilebilir.

-**Bilgisayar (Host) Tabanlı (HIDS)**: Belli bir bilgisayarı izlerler

Saldırı Önleme Sistemleri

Saldırı Önleme Sistemleri (Intrusion Prevention System - IPS): Temel işlevleri, ağ veya sistem faaliyetlerini kötü niyetli etkinlikler için izlemek, kötü amaçlı etkinliği saptamak, bu etkinlikle ilgili bilgileri günlüğe kaydetmek, raporlamak ve bunları engellemek veya durdurmaktır. IDS, saldırıları sadece tespit edip raporlarken IPS, tespit edilen saldırıları aktif bir şekilde önleme/engelleme yeteneğine sahiptir.

Kullandığı çeşitli yanıt teknikleri;
-Alarm gönderme,
-Saldırıyı durdurma,
-Bağlantıyı sıfırlama,
-Trafik akışını rahatsız edici IP adresini engelleme
-Güvenlik ortamını değiştirme (bir güvenlik duvarını yeniden yapılandırma)

SNORT (Network Intrusion Detection & Prevention System)
-1998 yılında Martin Roesch tarafından geliştirilmiştir.
-Açık kaynak kodlu bir saldırı tespit ve önleme yazılımıdır.
-Hem kişisel hem de kurumsal kullanım için indirilebilir ve yapılandırılabilir
-Gerçek zamanlı ağ trafiği analizi ve veri paketi günlüğü (logging) sağlar
-Olası kötü amaçlı aktiviteleri tespit etmek için anormallik, kalıp eşleştirme (signature) ve protokol inceleme yöntemlerini birleştiren kural tabanlı bir dil kullanır.

(Wireshark)

BS439_14_2

Saldırı Önleme Sistemleri

Veri Kaybı Önleme (Data Loss Prevention - DLP): Değerli verilerin yetkisiz kişilerin eline geçmesini engellemek üzere tasarlanmış bir güvenlik teknolojisidir. Kurumsal cihazlarda veri envanterini tutan bir teknolojidir. Verilerin ne zaman taşındığını izler ve verilerin harici disk sürücüsü, bulut sunucusu veya e-posta alıcısı gibi yetkisiz konumlara taşınmasını önlemek için kuralları uygular. Kuruluşlar, çalışanların hassas bilgileri ağ dışına göndermediğinden emin olmalıdır. DLP teknolojileri, kişilerin kritik bilgileri güvenli olmayan bir şekilde karşıya yüklemesini , iletmesini ve hatta yazdırmasını engelleyebilir. Yöneticileri bilgilendirir.

Veriler	Temel kullanım amaçları
-Veri tabanı sunucuları	-Kişisel veri güvenliği
-Dosya sunucuları	-Veri koruması
-E-posta sunucuları	-Veri görünürlüğü
-Kişisel bilgisayarlar	
-FTP sunucuları	

Güvenlik Bilgiveri ve Olay Yönetimi (Seurity Information and Event Management - SIEM): Tespit edilen herhangi bir aktivite veya ihlalin toplandığı merkezdir. Cihazların ve uygulamaların ürettiği olay verilerinin gerçek zamanlı olarak toplanmasını ve analiz edilmesini sağlayarak olaylar arasındaki ilişkileri hesaplar (Anomali Tabanlı IDS'in yapamadığı şeyi yapar) ve kötü niyetli davranışların iç yüzünü ve yapısını ortaya çıkarmaya yardımcı olur.

Çalışma adımları;
-Çeşitli sistemlerin ve uç kullanıcıların ürettiği logların toplanması
-Farklı sistemlerden toplanan farklı formatlardaki logların tek bir formata dönüştürülmesi
-Logların ilişkilendirilmesi ve bağlantısının oluşturulması
-Olayların birden fazla sayıda kaydı tutulmuşsa bunları tek bir kayda indirgeyerek analiz edilecek verinin hacminin düşürülmesi ve işlemlerin hızlandırılması

Avantajları:

-Log Yönetimi	-Raporlama	-Bildirim ve uyarı verebilme
-Olay Yönetimi	-Yönetim kolaylığı	-Güvenlik ürünleri ile entegre edilebilme
-Gerçek zamanlı izleme	-Gelişmiş tehdit algılama	

En çok kullanılan SIEM ürünleri:
-IBM Qradar, Splunk, FortiSIEM, Logsign, McAfee

Open Source SIEM ürünleri:
-Elastic SIEM, Fluentd, Wazuh, Graylog, Octopussy

Kullanıcı Davranışı ve Analizi

Kullanıcı Davranış Analizi (User Behavioral Analytics - UBA): Kullanıcıların her gün oluşturduğu ağ olayları hakkında bilgi toplama sürecidir. Hem normal hem kötü amaçlı kullanıcı davranışlarından kaynaklanan trafik modellerini belirlemek için günlük log yönetimi ve SIEM sistemlerinde toplanan ve depolonan ağ ve kimlik doğrulama günlükleri dahil geçmiş veri günlüklerini analiz eder.