AĞ GÜVENLİĞİ

NURSEDA EKİCİ

Saldırı: Sistemin güvenliğini etkisiz hale getiren hücum.
Tehdit: Güvenlik fonksiyonlarını engelleyen potansiyel güvenlik bozucu
Saldırgan: Ağdaki bazı servislere erişip zarar veren kişi

Ağ güvenliği: Bilgisayar güvenliği + Haberleşme
↳ Verinin iletimi esnasında korunması kavramıdır.

Güvenlik açığı testleri:
→ Güvenlik Denetimleri
→ Güvenlik Açığı Taraması
→ Penetrasyon
→ Fiziksel girdi
→ Sinyal güvenlik saldırısı
→ Sayısal Mühendislik Saldırısı

Ağ güvenliği çözümleri:
→ Kriptografik
→ Sistem Tabanlı

Kriptografik çözüm mimarisi: (şifreleme)
→ Algoritma tasarımı
→ Algoritma ile gizli bilgi üretimi
→ Gizli bilginin dağıtımı paylaşımı
→ Protokol belirleme

Not: Hedefe varma sürecindeki veriye data denir. (iletişim durumdaki). Bilgisayarda saklanan veriye statik veri veya storage verisi denir.

Güvenlik mimarisi: Servis sağlayıcılarını, işletmelerin ve son kullanıcıların global güvenlik zorluklarını gidermek için oluşturulmuştur.

- Güvenlik boyutları
- Güvenlik katmanları
- Güvenlik Planları

8 Güvenlik Boyutu:
- Erişim kontrolü
- Kimlik doğrulama
- İnkar edememe
- Veri gizliliği
- İletişim gizliliği
- Veri bütünlüğü
- Kullanılabilirlik
- Gizlilik

Güvenlik mekanizmaları:

- Şifreleme mekanizmaları
- Sayısal imzalar
- Erişim kontrol mekanizmaları
- Veri bütünlüğü mekanizmaları
- Kimlik doğrulama mekanizmaları
- Trafik dolgu mekanizmaları
- Yönlendirme kontrol mekanizmaları

Saldırıların Sınıflandırılması:

1- Engelleme
2- Dinleme
3- Değiştirme
4- Oluşturma

Katmanlı Güvenlik Planı:

1- Engelleme
2- Saldırı saptama
3- Kurtarma

Virüs: Belleğe yerleşerek çalışan programlara kendisini ekleyebilen ve sürekli çoğalan zararlı programcıklar.

Trojan: Bulaştıkları bilgisayarlardaki şifreleri, dosyaları veya herhangi bir veriyi ele geçirmek üzere tasarlanmıştır. (casusluk)

Solucan: (worm) Sızma ve çoğalma mekanizmasıdır. İnternete bağlı bilgisayarların IP'lerine bakar paylaşıma açık dosyaları varsa kendini oraya eklar.

DOS Atakları:

1) **Dos atağı:** Tek kaynaktan tek hedefe (Aşırı paket yükleme)

2) **DDOS atağı:** Çok kaynaktan tek hedefe

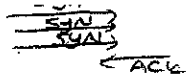
3) **DRDOS atağı:** DDos'tan farklı olarak ek ağ'lar kullanılır.

DOS Atağı Çeşitleri:

1) TCP/IP'yi istismar eden

- Ping-of-death → Doğru ora büyük paket gönderir.
- TearDrop → Bozuk paket gönderir.

2) TCP/IP zayıflıkları



- SYN flood → ACK gelmeden tekrar SYN gönderince buda taşma yapıyor.
- Land Atak → kaynak yerine hedef adres yazılınca hedef kendi kendine cevaplar.

3) Brute-force → Kaba kuvvet

- Smurf → ICMP paketleri hedefli kaynak adresi değiştirip zombilere yollar

4) IP spoofing (IP sahtekarlığı)

Instrusion Attacks (Sızma Atakları): Sistemde yetkisiz kullanım, kaynaklara izinsiz erişim, bilgi çalınması ...

Zombiler (iç atak): Sisteme yerleşir belirli porttan gelen DDos atakla-rını gerçekleştirir.

SQL atakları

DNS zehirlenmesi: Başka bir DNS'e yönlendirmesi

DNS: IP adreslerini kullanıcının anlayabileceği şekle dönüştürür.

Ağ güvenliğine katmanlı bakış:

1) Perimeter
2) Network
3) Host
4) Aplication
5) Data

Perimeter (Level 1):

Firewall: Güvenlik duvarı

→ Trafik kontrolü
→ NAT işlemi (Adres çevirimi)
→ VPN sonlandırma

DMZ: Bir kuruluşun dış servislerini içeren ve bu servisleri daha büyük güvensiz bir ağa maruz bırakan fiziksel veya mantıksal bir alt ağdır.

Ağ Tabanlı anti-virüs: Veri tabanındaki listeler ile gelen IP'leri karşılaştırır. (Eğer içine anti-virüs yüklüyse) alarm ağ içine almaz)

VPN Tüneli: DMZ içinde bir VPN etkin yönlendirici güvenlik yönlendirici yada sunucu üzerinden sona erdirilir. 2 cihaz, ağ, arasında özel bir köprü görevi vardır.

Network: (Level 2)

IDS → saldırı tespit sistemi
IPS → saldırı önleme sistemi

Ağ erişim kontrolü: Ağa başka bir ağın yada cihazın dışarıdan erişim kontrolü yada ağın sadece içerde kalmasını sağlamak. Yetkilendirme

Host (Level 3)

IDS, VA (Güvenlik Açığı Değerlendirilmesi), kimlik doğrulama, Antivirüs yazılımı, yetkilendirme

Application: (Level 4)

- Application Shield (Yazılımsal-Firewall)
- Yetkilendirme
- Giriş Doğrulama

Data (Veri güvenliği): (Level 5)

- Şifreleme (Encryption)
- Şifreleme (kriptografi)
- Erişim kontrolü

Sayısal imzanın Sağladıkları:

- Veri bütünlüğü
- Veri sınırsız
- İnkar edememe
- Gizlilik

OSI

MAC (fiziksel) Adres = Değişmez. 6 byte, 48 bit.

MAC spoofing: Switch tablolarını bir sürü MAC adresi ile doldurmak.

ARP: IP adreslerinin MAC karşılıklarını haritalar

ARP sorgusu: Verilen IP adresinin kime ait old. cevap verir.

ARP spoofing: IP-MAC eşleşmelerini kendine yönlendirir.

ARP Güvenlik Kusurları:

- Önbelleğin sınırlı olusu
- Kimlik doğrulama eksikliği
- Bu kimden geldi diye bakmaz.
- meşru ve gayrimeşru mesajları ayırt etmek için bir yöntem yok.

OSI katmanları:

Uygulama: Kullanıcının ağdan istediği hizmetlerin tarif edilmesi

* DATA

→ FTP, HTTP, Telnet, TFTP

Sunum: Veri formatlama, şifreleme, sıkıştırma

* DATA

→ JPEG, TIFF, ASCII, SMB, HTML

Oturum: İstenen hizmete uygun oturum açılması

* DATA

→ SQL, ASP, TLS, SSH, BSP

USTAUF

(ulaşım)
Taşıma: Uçtan uca akış kontrolü → TCP (Bağlantılı) → UDP (Bağlantısız)
Bağlantı ve soket no

* SEGMENT

Ağ: Mantıksal adresler (IP vb)
Yol belirleme
Ağlar arası paket gönderme
cihazları: → Routers (katman 3 switch)

* PAKET

Veri bağı: Bitleri Byte, byte çerçeveye dönüştürür.) LLC
(LLC, MAC) LAN Teknolojilerini tarif eder.

Pencereleme
Parity ve CRC kontrol işlemleri) MAC

cihazları: NIC, switch, bridge

* ÇERÇEVE

→ LAN Protokol, WAN protokol

Fiziksel: Bit düzeyinde hareket → cat5 RJ45 → modem Hubs multiplexer
Ağ topolojisi seçimi
kablo seçimi

* BİT

Fiziksel katmandaki Açıklar:
* Herkesin erişebileceği bir ağ alt yapısı
* Elektromanyetik ortam

HUB: Veri herkese broadcast yayınlanır

Veri bağı katmanı Açıkları:

LAN saldırıları: Bu saldırıların çoğunluğu iletişim sırasında kimlik doğrulama eksikliğine dayanır.

- CAM (Switch mac tablosu
- VLAN hopping
- ARP ön bellek zehirlenmesi
- Spanning Tree Protokol manipülasyonu
- DHCP istismarları

OSI'nin 4. katman açıkları (ulaşım)

TCP	UDP
- Güvenilir	- Güvenilmez
- Yavaş	- Hızlı
- Hata denetimi	- Hata denetimi yok
- Bağlantılı bağlantı	- Bağlantısız bağlantı
- Telefon Görüşmesi	- Video, ses vs. gönderimi
- Sıralı Paketler	- Sırasız paketler

TCP'nin zayıflıklarına yönelik Saldırılar

- SYN flooding
- Oturum ele geçirme

Port: Değişik bilgisayar aynı bilgisayar servislerini kullanabilmesi için servisleri tanımlayan adresleridir.

Soket No: 32 bit IP + 16 bit port no

SYN: istek
ACK: onay
FIN: kopatma isteği

SYN=1 ve ACK=0 bağlantı açma isteği
SYN=1 ve SYN=1 bağlantı açma onayı
SYN=0 ve ACK=1 veri paketi veya ACK paketi
} 3'lü el sıkışma

Bağlantı koparılması: SYN'a belirli bir süre ACK gelmediğinde bağlantı kopar. Saldırmak için FIN=1 olan segment gönderilir.

→ TCP portu açıksa gelen SYN'ye karşı ACK+SYN döner.

SYN otakları önlemeye yöntemleri:

- **SYN cookie:** SYN'ye dönecek cevapta ISN (sıra no SYN'nin içinde) özel olarak hesaplanır ve hedefe gönderilir. Hedeften ACK gelince ISN tekrar hesaplanır. ISN uygunsa bağlantı kurulur.
- **SYN cache:** Belirli bir değerin üstünde SYN alındığında SYN cookie'yi tetikler, sistem korumaya geçer.
- **SYN proxy:** Sistemlere gelecek tüm SYN paketlerini karşılar 3'lü el sıkışma tamamlandıktan sonra paketleri sisteme yönlendirir.
- TCP kimlik doğrulama

UDP portlarından Saldırılar:

echo servisi: Kendine gönderilen herşeyi tekrarlar
chorgen servisi: Sürekli bir veri akışı oluşturur.
Bir tarafa echo bir tarafta da chorgen olursa sonsuz bir trafik oluşur.
UDP flood Saldırıları: Saldırganın hedef sisteme rastgele bir portuna UDP paketi göndermesiyle olur.

VLAN:
Sanal LAN'dır. OSI'nin 2. katmanında çalışır. Aynı VLAN'daki bilgisayarlar haberleşebilir. Farklı VLAN'daktiler haberleşemez.

→ VLAN'ların içinde trafik sadece router ile kontrol edilir.

VLAN Haberleşmesi: VLAN arayüzü oluşturmak, bu arayüzlere birer IP no vermek sonrasındada VLAN'lar arasında yönlendirme yapmak gerekir. Yönlendirmeyi yönlendirici veya 3. katmandaki switch ile yapılır.

VLAN Oluşturma Tipleri?

Statik

- İnsanlar portları kendisi konfigüre eder.
- Her bir port bir özel VLAN ile ilişkilendirilir.
- İnsanlar VLAN'a ve portlar arasındaki haritalamayı yapar.

Dinamik

- Portlar VLAN konfigürasyonu için dinamik rol oynar.
- VLAN haritalamasında MAC adreslerinin yazılımsal veri tabanı kullanılır.

VLAN Tipleri?

- Port tabanlı
- MAC adres
- Protokol Tabanlı

Access ve Trunk Bağlantıları?

Access port: Bir adet VLAN'a atanmış port.

Trunk port: Switch üzerinde yer alan tüm VLAN'lara üyedir. Farklı VLAN'lara üye portların birbiriyle iletişimini sağlar.

Ethernet teknolojisinde switch için bir VLAN'a ait çerçeveyi belirlemesi için iki yöntem kullanılır.

- ISL-INTERSWITCH (Cisco tescilli)
- IEEE 802.1Q (standartlara dayalı)

VLAN erişiminin sağlanması için "trunk port"ların aynı enkapsülasyon türüne sahip olması gerekir.

VTP (VLAN TRUNKING PROTOKOL)

VLAN bilgilerinin ağdaki diğer cihazlar ile paylaşımı amacı ile oluşturulan protokoldür.

VTP modları?

- Server
- Client (istemci)
- Transparent

VTP PRUNING:

Cihazlarda VLAN'a üye kullanıcı olmadığı sezimlenirse taşınmasına gerek yoktur buna denir.

VLAN atlamaması (hopping) otağı:

Saldırganın bağlı bulunduğu anahtardan farklı bir anahtar üzerinde kendi VLAN'ı, hariçindeki normalde erişemeyeceği gereken bir VLAN'a erişmesine denir.

a) anahtar sahtekarlığı (switch spoofing)

Cisco anahtarlarının portları access ve trunk porttur. Kendini trunk port olarak göstererek bütün VLAN'lara erişme yapar.

b) Çift etiketleme (Double Tagging)

Paketin istenilen VLAN'a ulaşabilmesi için porta giren çerçevelere iki adet header eklenir ve çerçeveyi ilk alan anahtarlayıcı tarafından birinci başlık çıkarılır. İkinci anahtarlayıcı ise başlıktaki VLAN bilgisini okuyarak paketi gitmesini istediği VLAN'e gönderir.

→ **kurtulmak için**

* Native VLAN'ı kullanıcılar için kullanmayın.
* Default VLAN'ı numarasına 1'den farklı bir değer verin ve bu VLAN'ı kullanıcılar için kullanmayın.
* Kullanılmayan portları kapat.

AĞ KATMANI

Farklı fiziksel segmentlerdeki PC'lerde arasındaki paketleri taşımak için yapılması gerekenleri tarif eder.

IP Routerlar: Ağ katmanı çalışır ve ağ adreslerine göre ağdaki paketleri yönlendirirler.

1- Aynı ağda doğrudan hedefe gönderir.
2- Farklı ağda hedefe gönder IP adres, maske, Gateway, IP

IP Paket yapısı:

- Her satır 32 sözcük
- Başlık uzunluğu 32 bit
- Sürüm
- Servis tipi
- Toplam uzunluk
- Parça No
- Yaşam süresi
- Protokol
- DF (Parçalanmamış 0 ise parça)
- MF (Parçalanmış 1 ise parça sonu)
- Tamamlayıcı
- Başlık sınama 16 bit

→ IP bağlantısız bir protokol old. için DOS saldırılarına açıktır.
→ IP protokol saldırıları için ICMP kullanılabilir.

IP Saldırıları:
1 Spoofing (Kimlik sahtekarlığı)
2 Fragmentation (Paçalara)
3 Port scanning (Port tarama)
4 Redirection (Yeniden yönlendirme)

Yerel spoofing: Saldırgan ve mağdur aynı alt ağda.
Blind spoofing: Saldırgan ve mağdur aynı alt ağda değil

IP spoofing: Ağ bağlı sisteminizle başka bir sisteme bağlanacaksanız bunu gizlemek istiyorsanız bağlantı sırasında kimliğinizi yanlış göstermedir.

Paketlerin Parçalanması (IP fragmentation)

MTU: En büyük olası bağlantı katmanı çerçevesi

- Paketlerin MTU (Maximum Transmission Unit)'yu geçmeyecek şekilde ağlar arasında iletimi sağlamak için boyutlandırılması işlemidir.
- IP başlığı parçaların bu paketin tekrar birleştirilmesi için gerekli bilgileri (parçaların herbirine aktarır.
- Parçalanmış paketlerde sadece ilk paket protokol bilgisini (TCP, UDP, ICMP vs) taşır.

Reassembly (Tekrar Birleştirme İşlemleri)

Birleştirme Sürecindeki Atak:
- Time out (zaman aşımı): Hedef host ve IDS'de farklı zaman aşımı uzunluklarının kullanılması saldırgana evasion atak gerçekleştirmesine izin verir.
- TCP header division (TCP başlık bölünmesi): Atak sayılmaz.

② Fragmentation:
MAC katmanındaki paketlerin göndereceği çerçeve boyutu belli old. için veriler parçalıyoruz. Paket birleştirme işlemi düzgün değilse saldırgan paket bölme araçlarını kullanarak ortamo sızar.

Atakları: Parçalanmış paketlerin üst üste gelmesi saldırganlara IDS, firewall ve routerlarda eski paketlerin kaydırılmasını sağlar. Saldırgan mesajı 3 parçaya böler.

Kaynak Rotalama Atakları: (Source Routing)

Saldırgan gönderici adresini aldatarak o paketi bir alt ağdan geliyormuş gibi gösterir.

Teardrop: IP paketlerinin tekrar birleştirilmesindeki zaafiyetlerden yararlanır.

Ping of death: Sürekli gönderilen echo request mesajları 65.535 den büyük olduğu için buffer'ı taşırır.

IP Katmanın Genel Atak Tipleri:

- Evasion (Atlama) Ataği
- Insertion (Ekleme) Ataği: Sadece IDS'de geçerlidir.
- Dos Ataği

IP Datagramlarının yönlendirilmesi:

PC'lerin haberleşmesi için ağlar arasında datagramların yönlendirilmesi gerekir.

Dinamik ve Statik yönlendirme Tabloları:

↳ En uygun ve hızlı yolları belirler, tabloları oluşturur ve günceller.

Statik: Tablolar el ile girilir.

Datagram yönlendirme Protokolleri (IGP)/(EGP)

IGP kendi içindeki yönlendirme protokolleri

↳ En çok bilinen IGP'ler.

- RIP: yönlendirme bilgi değişim protokolü (UDP kullanır)
- OSPF: En kısa yolu seçer (IP datagramlarını kullanır)

EGP dışarıya yönlendirme protokolleri

↳ En çok EGP'ler

- BGP: Sınır geçit protokolü (TCP kullanır)

Routing Protokol Atakları:

Sahte RIP paketleri gönderir. Ağ geçitleri ve hostların rotalarını değiştirir ve bilgi sızdırır.

Router güvenliği:

- Fiziksel Güvenlik
- Yönlendiriciye erişim hakları
- Şifrelerin güvenliği
- Erişim Prot. güvenliği
- Gereksiz servisleri kapatmak
- İşletim sistemi

AĞI ROUTER İLE KORUMAK

Sadece küçük ağlarda veya iç yönlendiricilerde tercih edilmeli!

1) Risksiz portları kapatmak (sanal portları)

2) Bazı saldırı tekniklerine karşı önlemler

- IP spoofing
- Routing protokolde olan saldırılar
- Giriş ve giriş erişim listeleri
- reverse path kontrolü
- Smurf atakları

ICMP (İnternet kontrol mesaj Protokol)

- mantıksal hataları tehşis ve bildirim için kullanır
- Bağlantısız protokoldür
- Datagramların iletim ve teslimat sürecindeki hataları rapor ve kontrol bilgilerinin alışverişi için kullanılır.

- istekler
  - yanıtlar
    - Hata mesajı verir.

→ Sadece IP datagramla ilgili olaylarda ICMP mesajları üretilir.

TCP zayıflıkları ve Çözümleri

- Gizlilik
- Paket doğrulama (Paketin kaynak adresi değişmiş olabilir)
- İçerik bütünlüğü (Paket içeriği değişmiş olabilir)

ICMP Atakları

- **Echo Ataklar:** Ping (ICMP ile gerçekleşir) bombardımanı fazla ICMP yankı isteği paketlerini ağa yollayarak bant genişliği kullanıp ağ kaynaklarını tüketir.
- **Port scanning (tarama):** Hangi port açık ona bakar.
- **Nuke Ataklar:** Sahte adresler kullanarak 2 host arasında düzgün iletişimi veya mesajlarını her iki hosta göndererek hata varmış gibi gösterir.
- **Redirect Atağı: (Yeniden yönlendirme)**
  Mesajları göndererek hedef router'a yönlendirilmiş mesajları IP adresi saldırganın adresi olan bir hosta forword eder.

Önlem: Linux'ta kernelde değişiklik yaparak redirect mesajların alınmasını engeller.

ICMP flood: Bir ping broadcast fırtınası yaratarak hedef sistemi bunaltır.

Uygulama katmanı ve Protokolleri:

Görevleri:
- Çok değişik uç birimlerin tanınmasını sağlaması
- Uç birimler arasındaki dosya transferini sağlaması

Protokolleri:
- **SMTP:** e-mail alışveriş kurallarını düzenler.
- **SNMP:** ağ içerisindeki ağ aktif cihazlarının yönetimi için kullanır.
- **TELNET:** Sistemdeki kullanıcının başka bir sisteme bağlanarak o sistemi kullanmasını sağlar.
- **FTP:** Bilgisayarlar arası dosya aktarımını sağlayan protokol
- **HTTP:** Web sayfalarının alışverişini sağlar.
- **DNS:** İnternet isimlerini IP No'ya çevirir.

Uygulama mimarileri:
- Client-Server (İstemci-sunucu)
- Peer-to-Peer (Eş düzey)
- Hibrit

Uygulama Oluşturma Süreci

Proses: Host üzerinde çalışan program.

Proses iletişimi: Eğer aynı host üzerinde ise inter-proses-communication ile haberleştirler.
Farklı hostlarda iseler mesajla haberleştirler.

Soketler: Prosesler kendi soketleriyle mesaj gönderir veya alır.

Not: Host 32 bit IP adresine sahiptir.

API: Uygulama program arayüzü

ÖRN: Haberleşen süreçler (proses) birbirini nasıl tanır?

- IP adres: Basta süreçlerde çalıştırılabilen ana sistemin (host) IP adresi
- Port No: Ana sistemlere gelen mesajların hangi local süreçlere gönderilmesi gerektiğini belirlemesinde yardımcı olur.

→ **Proseslerin ulaşım servisi için**

- Bilgi kaybı
- Bant genişliği
- Zamanlama
- Diğer uygulamalar

} İhtiyacı vardır.

Not: Web'de HTTP protokolü kullanılır.

URL: Web sayfalarına ulaşmak için kullanılır.

ÖRN: http://www.mbe.com.tr/mbe/yapi.html

Kullan protokol = HTTP
Tam domain adı = www.mbe.com.tr
dizin = mbe
Alınacak metin = yapi.html

BİLGİSAYAR SİSTEMLERİ GÜVENLİĞİ

→ **Sağlanabilmesi için:**

- Firewall: Ağ ile dış ağlar arası bir geçit
- Özel sanal ağlar: (VPN)
- Proxy: Bağlantı uygulamasında araya giren ve bağlantıyı istemci için kendisi gerçekleştiren sistem
- Anti-virüs çözümleri: Trafiği üzerinden geçirerek virüs taraması yapar.
- İçerik süzme (content filtering)
- VLAN

Firewall Teknolojileri:

- **Paket Filtreleme:** Paketlerin sadece başlık bilgilerine göre değerlendirilmesi
  - Statik paket filtreleme
  - Dinamik " "
- **İçerik Filtreleme:** Paketlerin uygulama içeriğinde bakılır.
- **Uygulama Seviyesi (Proxy):** Bağlantının sonlandırıldığı ve paketlerin içeriğinin denetlendiği teknolojiler.

Firewall Topolojileri:

- Basit Dual-Homed Firewall
- Bütünüyle serbest olan DMZ içeren 2 bacaklı network
- 3 bacaklı Firewall

DMZ Bölgesi:

Firewall tarafından daha az korunan daha fazla erişime izin verilen bölge

NAT:

Gerçek IP adresiyle sadece internete çıkmak için geliştirilmiştir.

NAT Tablosu:

Dahili ağdan harici ağa olan her türlü iletişim izlenir ve tüm ara birimlerdeki paketlerin ne yapılacağı konusunda yardımcı olan tablodur.

Port Yönlendirme:

Erişim sağlamak istenen sunucuya iletilen gerçek IP adresi güvenlik duvarının dış dünyaya açılan IP adresi olarak belirlenir.

VPN: (Virtual Private Networks): Sanal Özel Ağ

İnternet üzerinde şifreli ve güvenli veri iletişimini sağlamak için düşünülmüş teknoloji

1) Remote access VPN
2) Site to site VPN

Görevleri:

- Kimlik doğrulama
- Erişim kontrol
- Gizlilik
- Veri bütünlüğü

VPN Tünelleme:

Bir genel ağ üzerinde sanal bir noktadan noktaya bağlantı oluşturmak

Tünelleme Protokolleri:

1) Taşıyıcı Protokoller
2) Enkapsüle " = PPTP, L2TP, IPSEC
3) İletim " = PPP, SLIP

VPN Gerçekleştirme Tipleri:

1) Donanım = VPN desteği olan routerlar
2) Firewall
3) Yazılım

Hibrid Sistemler ve Şifreleme Yöntemleri

Şifreleme: açık metni şifreleme algoritmasıyla anlaşılmaz hale getirme

Şifreleme Algoritmaları:

1) Simetrik şifreleme: Şifreleme ve deşifreleme için 1 tane gizli anahtar kullanır.

Kuvvetli yönleri:

- hızlıdır.
- Donanım olarak uygulanır.
- Bit sayısı çok daha küçük
- Güvenlidir.

Zayıf yönleri:

- Güvenli anahtar dağıtımı zordur.
- Elmilik doğrulama ve bütünlük güvenli bir şekilde gerçekleştirmez zordur.

Simetrik şifreleme yöntemleri:

•Karakter tabanlı şifreleme yöntemi:

- Basit şifreleyiciler
- Ötelemeli şifreler (sezar)
- tek alfabede yerine koyma şifreler
- çok alfabede "
- Tek kullanımlık şifreler
- Gümüşde kullanılan simetrik şifreler → Çok kriptolama

Simetrik şifreleme Algoritmaları (DES)

DES;

-Açık metni paralara bölerek her parçayı bağımsız olarak şifreler.
-Şifrelenmiş metni açmak içinde aynı işlemi yapar.
-Parçaların uzunluğu 64 bit

Triple-DES
TWOFISH
İRON
İDEA
AES
RC4
MD5
SHA

} Simetrik şifreleme Algoritmaları

Asimetrik şifreleme

2 anahtara dayalı şifreleme sistemidir. Şifreleme için public key deşifreleme için private key kullanılır.

Kuvvetli yönleri:

- Bütünlük, kimlik doğrulama, Gizlilik güvenli bir şekilde sağlanır.
- Anahtarı kullanıcı belirleyebilir.

Zayıf yönleri:

- Şifrelerin uzunluğundan dolayı algoritmanın yavaş çalışması
- Anahtar uzunluklarının sorun çıkarması

Asimetrik şifreleme Algoritmaları:

- Diffie-Helman
- RSA
- DSA
- ECC

GÜVENLİK PROTOKOLLERİ:

- Uygulama katmanı = SSH, S-MIME, PGP, Kerberos
- Taşıma katmanı = TLS, [SSL]
- Ağ katmanı = IPSec
- Veri bağı katmanı = [PPTP, L2TP], IEEE 802.1X, WPA2
- Fiziksel katman = Quantum communication

Not: N-katmandaki koruma protokolü n. ve daha üst katmanları korur.

II. katman PPP Protokolü (WAN Protokolü)

Orijinal olarak çevirmeli veya xDSL internet ve ağ erişim sunucusu arasında kullanılacak protokoldür.

Mekanizması;

Kapsülleme, Link kontrol protokolü (LCP), Ağ kontrol protokolü (NCP)

PPTP Protokolü: Tünellere için kullanılır.
L2TP Protokolü: (katman 2 tünel protokolü)

L2TP	PPTP
- UDP (veri aktarımını UDP ile yapar)	UDP
- UDP (Tünel kurulumu)	TCP
- Aynı anda 2 nokta arasında 1 den fazla tünel açabilir.	Açamaz.

IPSec: Ağ ve ulaşım katmanı arasında yer alır.

alt protokolleri:
- IKE / ISAKMP
- ESP
- AH

modları:
- Taşıma modu
- Tünel modu

Secure Socket Layer (SSL):
Güvenli olmayan iletişim ortamında verinin güvenli bir şekilde iletilmesi sağlanmak için sayısal imza ve herkese açık anahtar ve özel anahtar şifrelemesini aynı anda kullanan yapı.
Veri iletiminde hashing'i kullanır.

SSL'de kullanılan şifreleme sistemleri:
a) Hash teknigi
b) Anahtar değişim Teknigi (RSA, Diffie-Hellman)
c) Simetrik veri şifreleme

Transport Layer Security (TLS):
Güvenli bir oturum açarak 2 nokta arasında güvenli bir veri transferi yapar.

Handshake: El sıkışma

Uygulama katmanı Güvenliği

Avantaj:
- Çok esnek
- Kimlik bilgilerine erişim kolay
- Verilere tam erişim
- Uygulama tabanlı güvenlik sağlar.

Dezavantaj:
- Pahalı
- Hata olasılığı yüksek
- Her uygulama için farklı
- Son kullanıcı PC'lerinde gerçekleştirilir.

PGP (Pretty Good Privacy)

- e-mail güvenliğini sağlayan protokol
- e-imza ve şifre göndermesi yapar. Çok güvenlidir.

S/MIME → İnternette güvenli mail yollamak için kullanılır.

Çift (Açık) Anahtarlı algoritmalar:

- Özel anahtarlar
- Açık anahtarlar
- Üretilen her anahtar çiftli essizdir.
  - RSA
  - DH
  - DSA
  - Eliptik Eğri Algoritmaları

VPN Ağları kullanım alanlarına göre

① Access VPN } Bireysel kullanım (gerçek kişiler)

② Intranet VPN } kurumlar şirketler kullanılır. (tüzel kişiler)

③ Extranet VPN }

VPN'le 3 güvenlik tekniği sağlanır.

1- Kapsülleme
2- Kimlik sorgulaması
3- Kriptolama

kriptografi: Belgelerin şifrelenmesi ve şifrelerinin çözülmesi için kullanılan yöntemler

kriptoanaliz: Kriptografik sist. kurduğun mekanizmaları inceler ve çözmeye çalışır.

Basit şifreleyiciler:

1- metni ters çevirmek ABİ - İBA

2- Geometrik yönt. AL BA yada ALBA

3- Yol Değiştirme

Sütun Yer Değiştirme

(1) Ör: SHIP EQUIPMENT On the FOURTH OF JULY

c=5 ve yörge şifresi için

① → orjinal 5 sütunu dönüşüm

1	2	3	4	5
S	U	T	F	O
H	I	O	O	F
I	P	N	U	J
P	M	T	R	U
E	E	H	T	L
Q	N	E	H	Y

YÖRGE

54132 → alfabetik sırada

1	2	3	4	5
S	U	T	F	O
H	I	O	O	F
I	P	N	U	J
P	M	T	R	U
E	E	H	T	L
Q	N	E	H	Y

Şifrelenmiş metin

TOFUSOFOIHNJUPITURMPHLTEEEYHNQ

→ deşifre edilmesi

1	2	3	4	5
T	O	F	U	S
O	F	O	I	H
N	J	U	P	I
T	U	R	M	P
H	L	T	E	E
E	Y	H	N	Q
Y	O	B	G	E
5	4	1	3	2

5	4	1	3	2
S	U	T	F	O
H	I	O	O	F
I	P	N	U	J
P	M	T	R	U
E	E	H	T	L
Q	N	E	H	Y

4) Dikey Değiştirme

Düz metin 4 sütun şeklinde

1	2	3	4
N	N	E	T
E	S	N	I
G	S	D	O
O	T	I	N
T	A	N	S
I	L	S	T
A	L	T	O
T	E	R	D

5- Gifte Dikey Değiştirme

4	2	1	3	→ obrek düzenlenir
T	N	N	E	
I	S	E	N	
O	S	G	D	
N	T	O	I	
S	A	T	N	
T	L	I	S	
O	L	A	T	
D	E	T	R	
A	D	I	U	
Y	S	O	C	

6) Öteleneli şifreleme (sezar) $s(x+k) \bmod(29)$

$e_k(x) = (x+k) \bmod (26)$

$d_k(x) = (y-k) \bmod (26)$

ÖRN: $s = x+3 \bmod(29)$

A B C D E F - - - - - - V Y Z

0 1 2 3 4 5 - - - - - - 26 27 28

Her harf kendinden sonraki 3. Harf ile şifrelidir

TÜRKİYE

VZTNLBG

7) Tek Alfabede yer değiştirme

$P = C = Z_{26}$ K, 26 sembolün 0, 1, 2 ... 25 tüm mümkün permütasyonlarını içerir. Her permütasyon;

$\pi \in K$ için

$e_\pi(x) = \pi(x) \rightarrow$ Şifreleme

$d_\pi(x) = \pi^{-1}(x) \rightarrow$ Deşifreleme

Burada π^{-1}, π'nin ters permütasyonu

$A = \{A, B \text{ - - - } Y, Z\}$ açık metin alfabesi

$B = \{m, cek \text{ - - - } GUSU\}$ şifreli metin alfabesi

→ TURKİYE G, Ğ, Ö, G, E, J, A

⑧ Çok Alfabeli Yerine Koyma

Ana alfabede → ADA

$A = \{A, B, C, Ç, D\}$

$B_1 = \{M, C, R, Z, K\}$

$B_2 = \{B, K, T, L, E\}$

$B_3 = \{K, S, P, M, O\}$

A için B_1'de 1. sıradan
M

D için B_2'den 5. sıradan
F

A için B_3'te 1. sıradan
K

<u>Note</u> En yaygın çok alfabeli yerine koyma şifresi Vigenere'dir.

Vigenere şifresi:

Açık metin: DONT

Anahtar: CIPH

Şifreli metin: FWCA

A → A, B, C, D ---- Z → D için şifreden
→C → C, D, E, (F) --- B   F yazıyoruz
I → I, J, K ------ H
P → P, Q, R ------ O
H → H, J, K ------ G

Tek kullanımlık karakter Dizisi (Venom)

→ şifre ⇒ $C = (P + K) \bmod (29)$ şifre

Deşifre ⇒ (şifreli karakter − rastgele sayı) mod(29) + 29

$= (1 - 16) + 29 = 14$ (K)

- Bu yöntemin güvenliği rastgele üretilen dizinin güvenliğine bağlıdır. ÖRN: teletyp cihazı

Günümüzde kullanılan simetrik şifrelemeler

- Blok kriptolama:
  Veri kriptolama Standartı (DES)

- TWOFISH:
- Simetrik blok şifreleme algoritmasıdır.
- DES gibi Feistel yapısını kullanır. DES'ten farklı oluşturulan değişkenin S-box'lara sahip olmasıdır.

- IRON:
- 64 bitlik veri bloklarını 128 bitlik anahtarlarla şifrelemede kullanılır.
- Döngü sayısı 32 ile 16 arasındadır.
- Avantajı bitler yerine hex sayıları kullanmasıdır.
- Dezavantajı yazılım için tasarlanmıştır.

- AES:
- 4x4 'lük matrisler üzerinde yayılmış metin parçalarını satırlarına uygulanan kaydırma işlemleridir. 4 dönüşüm kullanılır. (subbytes, shiftrow, mix colums, addroundkey)

- IDEA:
- Alt anahtar üretim algoritması dairesel kaydırma üzerinedir.

- RC4:
- Şifrelenecek veriyi akan bir bit dizisi olarak algılar.
- Şifreleme hızı yüksektir.

- MD5:
- En ufak bit değişikliği bile çıktının tamamen değişmesine sebep olur.
- Veri bütünlüğünü test etmek için kullanılan bir şifreleme algoritmasıdır.

SHA (Secure Hash Algoritm – Güvenli Özetleme Algoritması)

MD5 ile benzer, uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanıp 160 bitlik mesajları özetli verir. Bu işlem sırasında mesajları 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar.
Çakışmalara karşı 80 bitlik güvenlik sağlar.

ASİMETRİK ŞİFRELEME ALGORİTMALARI

Diffie Helman: Sadece ortak gizli anahtarı belirlemede kullanılır.

ÖRN: 2 tarafta $p=23$ $g=5$ sayıların karşılıştırıyor.

Ali özel anahtar olarak $a=6$ ve borsa gönderir.

$5^6 \bmod 23 = 8 \rightarrow g^a \bmod p$

Borsa özel anahtar olarak $b=15$ seçip aliye gönderir.

$5^{15} \bmod 23 = 19 \rightarrow g^b \bmod p$

Ali: $(g^b \bmod p) \bmod p$ dert. hesaplanır. $19^6 \bmod 23 = 2$

Borsa $(g^a \bmod p)$ " " " $8^{15} \bmod 23 = 2$

→ Sonuç olarak gidip gelen bilgi 8 ve 19 olmaktadır.

RSA

Anahtarlar 2 büyük asal sayıdan üretilir. Bu rodan algoritmanın güvenliği büyük sayı üretme problemine dayalıdır.

ÖRN: $p=7$ $q=17$ bunların çarpımı $= 7*17 \rightarrow N=119$

$6*16 \rightarrow \phi(N)=96$

1'den büyük $\phi(N)(96)$'dan küçük $E=5$ seçilir. Bunun mod 96 tersi alınır. sonuç $D=77$ $\bmod(96)=1$ eşitliğini sağlayan 0-96

$E=5$ $N=119$ genel anahtar $D=77$ ve $N=119$ tam sayı ise özel anahtarları oluşturur.

DSA:

- Sayısal imza standardıdır.
- RSA'dan farklı şifreleme yapamaz sadece imzalama amaçlı kullanılır.

ECC: (Eliptik Eğri Algoritması).

- Diğerlerinden farkı güvenliği daha düşük anahtar değeri ile sağlayabilmesidir.
- Kablosuz ağlarda kullanılması uygundur.

AĞ GÜVENLİĞİ TEST VE DENETİM ARAÇLARI

İletilen bilginin veya bilgiyi ileten sistemin gerekli güvenlik öz. sağlayıp sağlamadığını test etmek ve denetlemek için kullanılır.

Sistem Güvenliği Araç genel Sınıflandırılması

① Bilgi Toplama Araçları

- Who Is
- DNS sorguları
- Google
- Sosyal mühendislik

② Paket Dinleyiciler

- Wireshark
- Windump
- Ettercap

③ Açıklık Tarayıcılar

- Nessus
- Iss
- NetIp
- BackTrack

④ Port Tarayıcılar

- Nmap
- superscan

⑤ Paket üreteçleri

TCP, UDP, ICMP, ARP vb. paketlerini gönderebilme

- Nemesis
- Colosoft
- TCPreplay

⑥ Topoloji Çıkarım Araçları

- Ping
- Tracert
- Firewalk

⑦ İşletim Sis. Tespit Araçları

- Xprobe2
- PoF

⑧ Şifre kırma Araçları

- medusa
- Cain and Abel
- Brutus

⑨ kablosuz Ağ araçları

- Tespit ve Analiz araçları
- Denetleme araçları
- Saldırı araçları

⑩ VPN Cihazı Test Araçları

- ipsecscan
- ike-scan
- ike probe

(11) Web uygulaması test araçları

- Paros
- Fire By
- Acunetix

(12) Veri tabanı test araçları

- ISS. Database Scanner
- App Detective
- Brute Force script

Sistem Güvenliği

Güvenliğin sağlanabilmesi için

- Güvenlik duvarı
- Özel sanal ağlar
- Saldırı tespit sis.
- Proxy
- Anti-virüs çözümleri
- İçerik süzme
- VLAN

Paket Filtreleme (Ağ katmanı Firewalları)

IP başlığındaki kaynak adres, hedef adres ve port numarası bilgilerine bakılarak gelen veri analiz edilir ve ona göre geçirilir veya atılır veya göndericiye bir mesaj gönderilir.

Statik Paket Filtreleme Tekniği

Gelen ve giden paketleri sadece gidileceği yer, erişmek istediği port numarası, protokolü gibi değerleri inceler.

Zayıflığı: Paketleri ilk gösteren sisteme yani oturumu ilk başlatanı saptayamıyor olması.

Dinamik Paket Filtreleme Teknolojisi

Firewalların statik paket filtrelemenin yani sıra oturumu takip etme özelliği vardır.

Zayıflığı: Paket içeriğini kontrol edememesi.

Uygulama katmanı Firewallları

- En sıkı koruma yapan firewall teknolojisidir.
- Aracı olarak proxy (vekil) sistem kullanır.
- Oturum başlatan ve hedef arasındaki paketler firewall'dan geçerek birbirine iletilir.

Aracı kullandığı için veri trafiğini hızı olumsuz etkilenir.

Ağ katmanı Firewallları vs Uygulama katmanı Firewallları

- Ağ katmanı Firewallarında kuralları aşmak diğerine göre daha kolaydır.
- Uygulama da daha iyi kayıtlama (log) ve etkinlik raporları tutmak mümkündür.
- Uygulamada sunucu makine işlemleriyle ilgilendiği için saldırılara açık halde
- Ağ'da daha kolay konfigüre edilir.

Firewall Topolojileri

① Basit - Dual - Homed Firewall

En basit ve en temel yolu

② Bütünüyle serbest olan DMZ içeren 2 bacaklı Network

- Router bir HUB ve SWITCH'e bağlıdır.
- DMZ bölgesi korumasız olarak internete açıktır.
- DMZ " için sınırlı bir koruma bir router ve bir çoklu IP adresi kalemlerine bağlıdır.

3 bacaklı Firewall

- DMZ böl. için koruma sağlamak için 2. çözümdür.
- karmaşıktır.

STATİK NAT

- Bir özel ağdaki tüm bilgisayarların internete kendi gerçek IP'si ile çıkmak istenesi durumudur.
- DMZ alanlarında kullanılır
- Bu diyagramda 1. firewall'a 3 ağ bağlıdır;
  a) İnternet
  b) DMZ alanı
  c) İki firewall arasındaki küçük özel ağ

DİNAMİK NAT

- İle özel IP adreslerimizi gerçek IP adreslerine statik olmayan bir yolla dönüştürüz.
- Dinamik dönüşümler NAT tablosundan silindikten sonra ağdaki diğer hostlar tarafından kullanılmak için bir timeout periyodu tutarlar.

Linux Netfilter ile NAT örnekleri

- Maskeleme
- Source NAT
- Destination NAT

Port adres yönlendirme (PAT)

- Statik ağ adres çevirmine alternatiftir
- erişim sağlanarak istenen sunucuya ilişkin gerçek IP adresi güvenlik duvarının dış dünyaya açılan IP adresi olarak kullanılır.
- İç ağdaki çok sayıda özel IP'yi tek bir reel IP ile local ağa çıkmak için kullanılır.

Saldırı önleme mekanizması

- Bu özellik genellikle uygulama tabanlı güvenlik duvarlarında bulunur. Tespit edilip engellenen saldırılara ilişkin kayıtlar tutulabilmektedir.

Transport katmanındaki Güvenlik

Web iletişimi için en önemli ve en alt seviye koruma taşıma katmanı koruma seviyesidir.

Secure Socket layer (SSL) ve Transport Layer (TLS)

Verinin internette bir yerden bir yere taşınması sorununa bir çözüm olması için SSL, TLS protokolleri ortaya atılmıştır. SSL ve TLS iki nokta arasında iletilen verinin bütünlüğü, gizliliği ve 2 uç noktanın doğrulanması için bir çözüm yöntemleridir. (TCP katmanı ile uygulama katmanı arasında çalışır.)

- SSL sayısal imza ve public-private key şifrelemesini aynı anda kullanılan bir yapıda tasarlanmıştır.

En yaygın kullanımı sunucu ile tarayıcı arasındaki iletişim şifrelenmesidir.

SSL fonksiyonları:

- Oturum için gerekli anahtarların oluşturulması
- mesajların şifrelenmesi ve deşifrelenmesindeki güvenliği ve gizliliği sağlar.
- Mesaj gönderen ve alanı doğrular.
- SSL veri iletimi esnasında hashing kullanılır.

Handshake Sertifikaları

Sertifika; kişinin açık anahtarının yetkili bir sertifika otoritesi tarafından imzalanmış halidir.

SSL 40, 56, 128 bitlik veriyi destekler.

EL sıkışma Aşamaları:

① İstemci sunucuya ilk ulaştığında el sıkış. başlar. Her iki taraf kullanacağı şifreleme fonk. üzerinde anlaşır.

② İstemci, sunucunun kimliğini doğrular.

③ İstemci, sunucudan aldığı dijital imzadan bir anahtar oluşturur ve bunu sunucuya yollar

④ Sunucu bu anahtarı alır, kontrol eder.

⑤ İsterse sunucu da istemciden kimlik denetimi istiyebilir.

SSL'de kullanılan şifreleme teknikleri

- Hash
- Anahtar Değişim (RSA, Diffie-Helmon)
- Simetrik veri şifreleme (RC2, RC4)

SSL mimarisi

- Handshake protokolü
- chipper spec değişim
- Uyarı protokolü