AĞ GÜVENLİĞİ

GİRİŞ

18-19

"Eğer siz kendinizi ve düşmanınızı tanıyorsanız, yüzlerce savaştan galip çıkarsınız…..

Eğer kendinizi biliyorsanız fakat düşmanınızı tanımıyorsanız , her kazandığınız zafer için bir yenilgiye katlanırsınız….

Eğer siz kendinizi ve düşmanınızı tanımıyorsanız, devamlı olarak kaybedeceksiniz….."

Savaş Sanatı - Sun TZU

Ağ Güvenliği

- Bilgi güçtür, her zaman değerlidir. Sadece gerekli kişiler tarafından elde edilebilmeli, kullanılmalıdır…

- Özel bilgi yetkisiz kişilerin eline geçmemelidir, istenmeyen kişilerin eline geçmesi durumunda anlaşılabilir olmaması gerekir…

- Kısacası durağan haldeki (Örn. Hafızalanmış) veya işlenme sürecindeki veya seyahat halindeki (Örn.Ağ ortamında iletilen) *bilginin (data) güvenliği* önemlidir.

Görevler ve Tanımlamalar

Bilginin sayısal kodlanmış şekli Veri (Data)'dir. Bir sayısal cihazda hafızalanmış olan veya işlenen veya bir ağda seyahat eden veriler için;

- **Gizlilik (*Confidentiality*)**
- ***Bütünlük (İntegrity)***
- ***İnkar edememe (Non-repudiation)***
- ***Faydalanılabilirlik-kullanılabilirlik (Availability)***

özelliklerini garanti edilmiş, yani güvenliğinin sağlanmış olması gerekir.

Kısacası üzerinde çalışılan veya iletişim sürecindeki veya statik haldeki veri *(işlenebilir veya saklanabilir haldeki kaynak verisi- text, resim, hareketli resim, ses, online veriler, e-mail mesajı v.b)* sadece yetkili kişiler tarafından okunabilmeli ve üzerinde işlem yapılabilmelidir.

Güvenlik

Fiziksel güvenlik

İletişim güvenliği

Sinyal güvenliği

Bilgi Güvenliği

Bilgisayar Güvenliği

Ağ Güvenliği

Ağ Güvenliği = Bilgisayar Güvenliği + Haberleşme Güvenliği

Fiziksel Güvenlik

- Bilgi güçtür, çünkü bilgi kaybı genellikle, kritik varlıkların kaybı anlamına gelir.
- Taşa oyulmuş veya sonraki zamanlarda kağıda yazılmış bilgiler önemlidir.
- Mısırlılar M.Ö 2.000 'de kilitleri kullanırdı.
- Taşınabilir olmayan bilgileri fiziksel olarak korumak için Gardiyanlar, duvarlar, köpekler, güvenlik noktaları ve çitler kullanıldı.
- Bilgisayar sistem odalarına kartlı giriş veya giriş çıkış kontrolu da fizksel korumanın bir parçası olarak görülebilir.

İletişim güvenliği

- İletişim güvenliği için şifreleme keşfedildi.

-**Skytale** :Yunanlılar, M.Ö. 5-3. yüzyılda "Skytale" adlı Şifreleme aletini savaşta kullandı. Kalın bir sopaya deri şerit sarılırdı. Mesaj şeritin üzerine sopa boyunca yazılır ve şerit açık olarak yollanırdı. Karşı taraf, şeridi aynı kalınlıkta bir sopaya sarıp mesajı okurdu .

Yunanlılar'ın Skytale adlı şifre aleti

- **ATBASH** : İbrani peygamber ***Yeremya***, M.Ö. 600-500'lerde ATBASH şifresini kullandı. şifrede, alfabenin ilk harfi son harfle, ikinci harf sondan ikinci harfle yer değişir. Böylece alfabenin ilk yarısındaki harfler, ikinci yarıdaki uygun harfle yer değiştirmiş olur. AĞAÇ kelimesinin Şifrelenmiş hali "ZRZÜ" dür.

- Frekans analiziyle Şifre kırma tekniğini, Müslüman matematikçi **El Kindi (801-873)** buldu. Sezar şifresi ve benzerlerinin çözümünü anlatan eser, Süleymaniye Osmanlı Arşivi'ndedir.

- William Frederick Friedman; tüm zamanların en iyi kriptologu olarak tanınır. Japon şifreleme düzenlerini kırmaya yardım etti.

Almanlar'ın Şifresi Kırılamayan Makinesi: ENIGMA

ABD Başkanı Thomas Jefferson'un 1790'da geliştirdiği şifreleme diski

Sinyal güvenliği

- Telsiz telefonlar için hiçbir güvenlik söz konusu değildi. Bu konuşmayı izinsiz dinleme veya kesmek çok kolaydır.

  Spread Spectrum teknolojisi güvenlik ve güvenilirliği artırır.
  Doğrudan dizili Spread Spectrum (DSSS)
  Frekans atlamalı yaygın spektrum (FHSS)

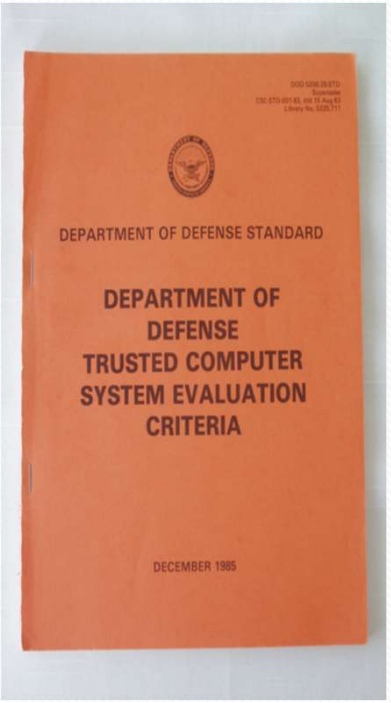
Bilgisayar Güvenliği

Bilgisayarların içerisindeki kaynakların, dosyaların, verilerin çalınmaya değiştirilmeye, izlenmeye, izinsiz kullanılmasına v.b karşı korunması önemli bir sorundur.

Bilgisayarlardaki kaynakları, dosyaları ve veriyi korumak ve saldırıları engellemek için tasarlanmış sistem ve araçlar bu konuda değerlendirilir.

Bilgisayar Güvenliği

- Orange Book" (DoD rainbow serisi) olarak bilinen, Trusted Computing System (Güvenilir Bilgisayar sistemi) Değerlendirme Kriterleri (TCSEC) aşağıdaki cetvellere göre bilgisayar sistemlerinin gizliliğini tanımlar:
- A(A1): Verified Protection **(Doğrulanmış-Onaylanmış Koruma)** : En yüksek güvenlik bölümlemesi.
- B(B1-B3): Mandatory Security (**Zorunlu Güvenlik**): Büyük ve güvenilir olması gereken Bilgi işlem merkezlerinin (**Trusted Computing base** –TCB) zorunlu olarak güvenliğidir.
- C(C1-C2): Discretionary Protection (**İsteğe Bağlı koruma):** Kurumlarda'larda isteğe bağlı korumadır.
- D: Minimal Protection (**Minumum düzeyde koruma**): A,B,C düzeylerinden herhangibirindeki başarısılık için güvenlik kontroludur.



Ağ güvenliği

- Ağ güvenliği kavramı, verinin iletimi esnasındaki korunması anlamındadır.

- Ancak Ağ güvenliği kavramı; resmi, özel, akademik, kişisel ağların biribiyle iletimde bulunması için oluşturulmuş ortak ağa bağlı tüm birimlerin de korumasını da kapsamaktadır.

Bilgi güvenliği

- Sadece fiziksel güvenlik, haberleşme güvenliği, sinyal güvenliği, bilgisayar güvenliği ve ağ güvenliği tüm güvenlik riskleri çözmek için yeterli değildir.
- Bilgi güvenliği açısından incelendiğinde, sadece biz tam bir güvenlik resmini oluşturmak için bunların hepsini kullanarak bilgi güvenliğini sağlamalıyız.
- Ayrıca bilgi güvenliği;

Üst yönetim desteği,
İyi güvenlik politikaları,
Risk yönetimi,
Personel eğitimi,
Güvenlik açığı testleri,
Yama yönetimi,
İyi bir kod tasarımı, ve benzeri

gibi işlevleri de gerektirir.

SALDIRI(ATTACK) , TEHDİT(Threat), SALDIRGAN (Hacker)?

- **TEHDİT:** Belirli durum veya olayın oluştuğu anlarda, güvenlik fonksiyonunun yerine getirilmesini engellemeye hazır, potansiyel bir güvenlik bozucusudur (virüs, truva atı v.b).

- **SALDIRI:** Sistemin güvenlik servislerini etkisiz hale getirmeyi amaçlayan, akıllı bir tehditten oluşturulan ani bir hucum (Attack)'tır.

- **SALDIRGAN:** Saldırgan , ağ üzerinde ki genelde bazı servisler veren makinalara; hiçbir hakkı olmadan erişip zarar veren kişidir. Bilgi hırsızı olarak ta tarif edilir.

Güvenlik Açığı TESTLERİ (Vulnerabilty testing)

Güvenlik açığı testi süreci, bir kuruluşun ağını, güvenlik politikalarını ve güvenlik kontrollerini sistematik olarak incelemektedir. Amaç, güvenlik önlemlerinin yeterliliğini belirlemek, güvenlik eksikliklerini tespit etmek, potansiyel güvenlik önlemlerinin etkililiğini önceden tahmin etmek için veri sağlamak ve onaylamaktır.

- **Security Audits (Güvenlik Denetimleri):** Belirlenmiş güvenlik politikalarına uyulup uyulmadığını test eder.
- **Vulnerability Scanning (Güvenlik Açığı Taraması):** Hostlarda veya aktif cihazlarda güvenlik açıklarının aranmasıdır. Nessus v.b aryazılım araçlarıyla
- **Ethical Hacks (Penetration Testing) :** Etik Hackleme (Nufuz etme deneyi) Kurum ağına her seviyede yapılabilecek atakları simüle eder ve dener
- **Stolen Equipment Attack(Çalıntı Ekipman Saldırı):**Fiziksel ve iletişim güvenliği
- **Physical Entry(Fiziksel Girdi):**Kurumun fiziksel olarak kontrolu , kapılar CCTV
- **Signal Security Attack(Sinyal Güvenlik Saldırı):** Özellikle Wireless erişim için
- **Social Engineering Attack(Sosyal Mühendislik Saldırı):** Organizasyon işleyişini öğrenmek için yapılan saldırıların öğrenilmesi için...

- Yukarıda açıklanan testler farklı metodlar ile yapılabilir. En çok bilinenen metodoloji: Açık Kaynak Güvenlik Testi Metodolojisi Kılavuzu (**Open Source Security Testing Methodology Manual** -OSSTMM) güvenliği altı temel kısma böler.

- Fiziksel Güvenlik
- Internet güvenliği
- Bilgi Güvenliği
- Kablosuz Güvenlik
- İletişim Güvenliği
- Sosyal Mühendislik

Ağ güvenliği nedir?

- *Ağ güvenliğinin* amacı, insanların kendi hak ve çıkarlarını zedeleme korkusu olmadan bilgisayar ağlarından, serbestçe yararlanmasının sağlanabilmesidir.

- Ağ güvenliği; ağa bağlı bilgisayar sistemlerini ve ağdaki bilgisayarlarda saklanan veya ağ üzerinde iletilen elektronik verileri korumak içindir. Not:İnternet(public network)'in kullandığı IPV.4 TCP/IP protokolu güvensiz bir protokol topluluğudur. Niye?

- Internet üzerindeki (public network) veriler, routerdan router'a **store-end forward** anahtarlamaya göre geçerek hedefe ulaşmaktadırlar. İnsanlar tarafından yönetilen Routerlarda, bu veriler korumasız şekildedir. **Örneğin bu verileri Routerı konfigüre eden birisi kolaylıkla ele geçirebilir.**

- Veya network trafiğini dinleme programlarından birisini kullanarak, iletişim halindeki verilerin algılanması rahatlıkla yapılabilir. V.s.....V.s...

- **Dolayısıyla bir ağ üzerindeki bir kişi veya bir şirket, bir saldırgan (Attacker), bir hedef veya her ikisi konumundada olabilir.**

- Buna göre network güvenliğinde amac, ilk olarak saldırganları ve saldırı tiplerin tanıyabilmek ve onlara hedef olmamak için gerekli işlemleri yapmak olmalıdır.

- Bilgisayar Güvenliği, bilgisayar içerisindeki kaynakları, veriyi korumak ve saldırganları (hacker) engellemek için alınacak tedbirlerin tümünü içerir. Bunları sağlayan sistemler Bilgisayar Güvenlik Sistemleri'dir.

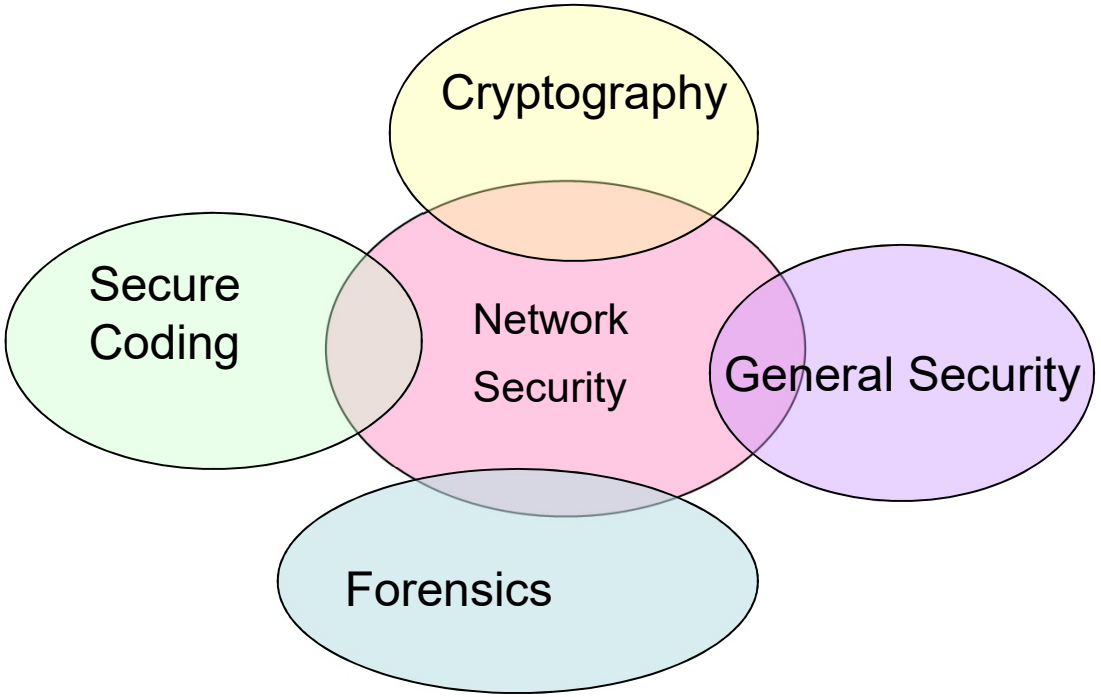
- Ağ güvenliği hem ağdaki bilgisayarların hem de ağın güvenliğinin (İletişim sürecindeki veri, ağ aktif cihazları) sağlanmasını gerektir.

- Biz; ağ güvenliği anlamında, daha çok ağın güvenliğini (İletim halindeki veriler ve aktif cihazların güvenliği) ön plana çıkaracağız.

"Ağ Güvenliği Sistemleri "

Ağ Güvenliği = Bilgisayar Güvenlik sistemi + İletişim Güvenliği

Ağ ve genel Güvenlik



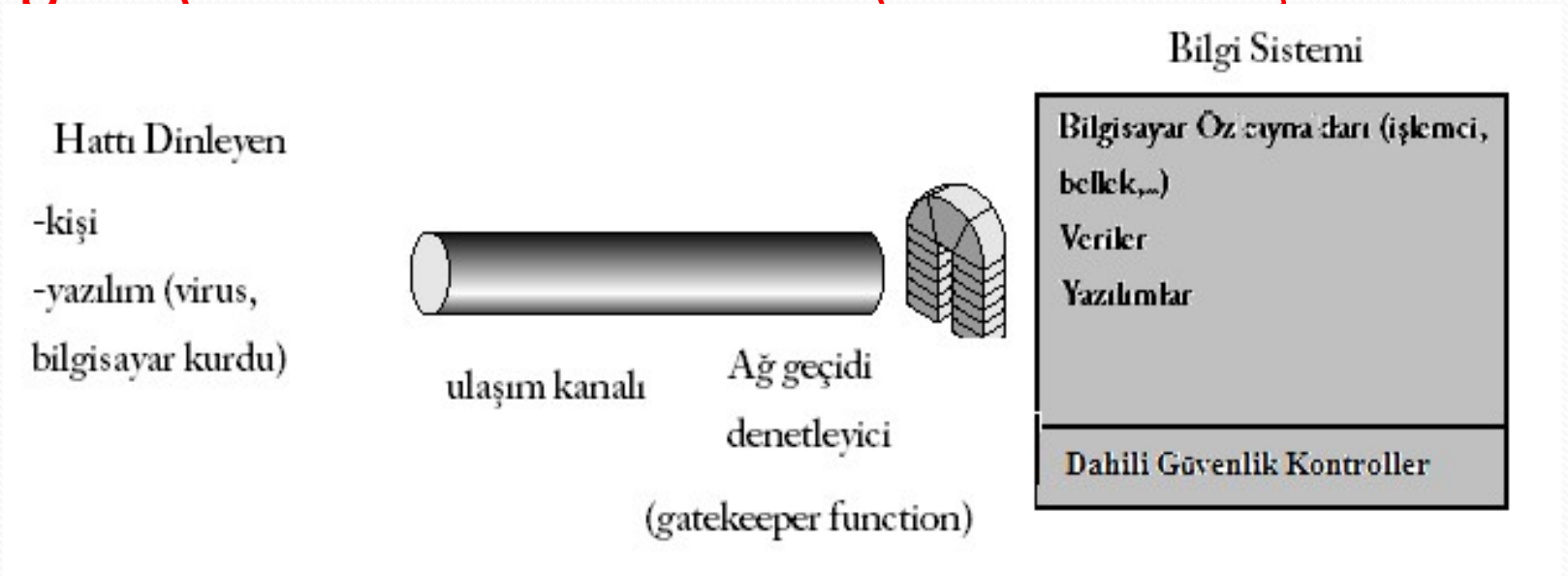
Ağ Güvenliği

- Ağ güvenliği çözümlerini;
  - Kriptografik
    - Sistem tabanlı

  çözümler olarak ikiye ayırmak mümkündür.

- Sistem tabanlı çözümler kriptografik işlemler içermeyen, sistem bilgilerini kullanarak güvenliği sağlamaya çalışan çözümlerdir.
- Bunlara örnek olarak yerel ağı dışarıdan gelecek saldırılardan korumayı amaçlayan güvenlik duvarları ve olası başarılı saldırıları anlamaya yönelik sızma denetim sistemleri verilebilir.

Ağ Erişim Güvenlik Modeli (Sistem Tabanlı Çözüme Örnek)



Bilgi sistemlerine (ağlara, Bilgisayarlara, Server'lara v.b) istenmeyen erişimin engellenmesi işlemidir.

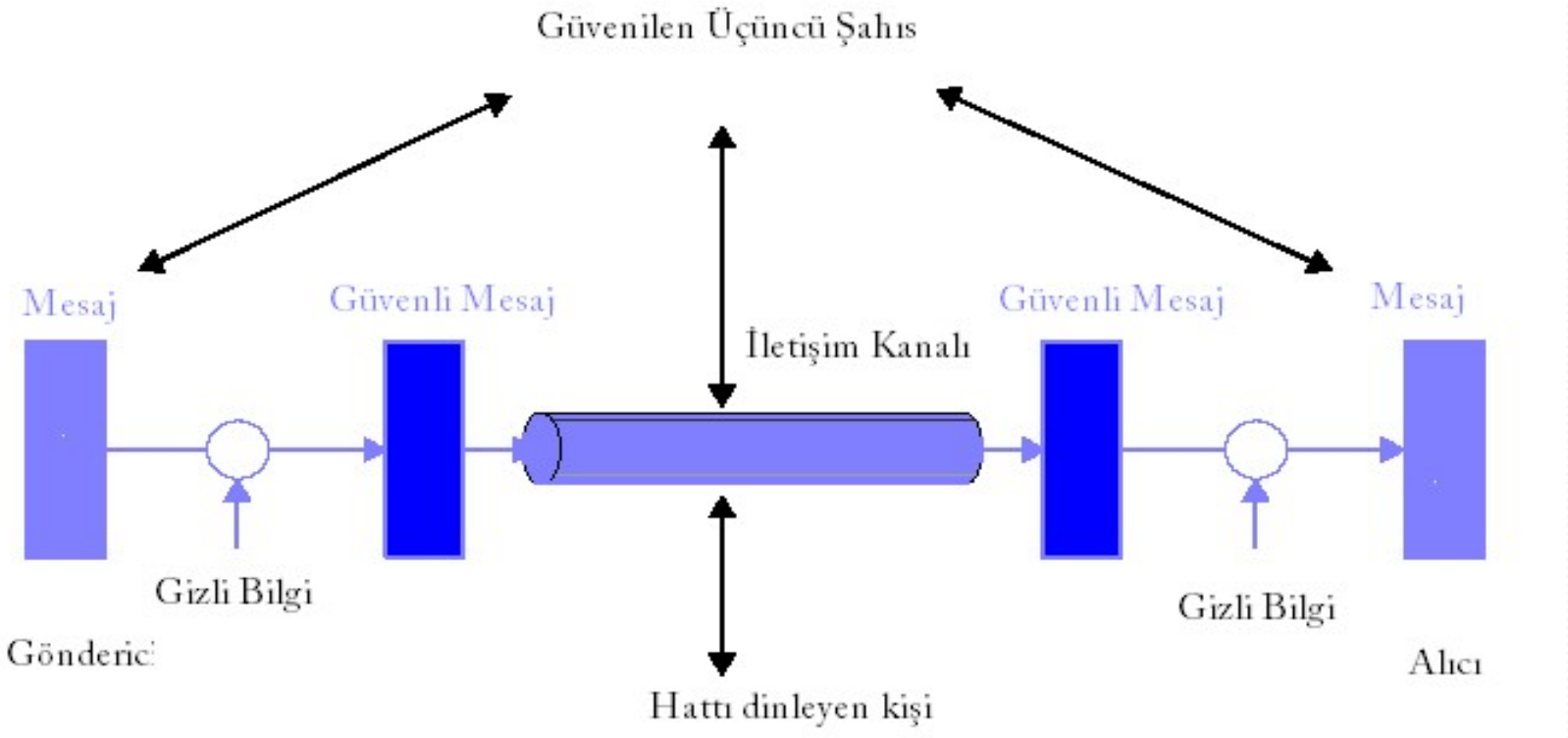
Bu modeli için:

- Kullanıcıları tanıyan uygun bir ağ geçidi denetleyici seçmek (pasword temelli erişim, erişim yetkisi ve seviyesi belirleme)
- Dahili Güvenlik Kontrolü uygulaması (Sistemi devamlı izleyerek anormal olayları sezmek ve tehditleri önceden belirleyebilmek- STS v.b)

Kriptografik Çözüm mimarisi

- Bu genel güvenlik mimarisi güvenlik servislerinin tasarımında dört temel işi göstermektedir.
  - Güvenlik ilişkili dönüşümler için bir algoritma tasarımı
  - Algoritma ile kullanılacak gizli bilginin üretimi
  - Gizli bilginin dağıtımı ve paylaşımı için yöntem geliştirme
  - Güvenlik algoritmasını ve güvenlik servisini sağlayacak gizli bilginin kullanımını sağlayacak protokol belirleme

Bir Ağ Güvenliği Modeli (Kriptografik tabanlı Güvenlik)



Gönderici ve alıcı mesajları gizli olarak iletirken, güvenli bir üçüncü şahıs gizli bilgilerin dağıtıcısı olarak hizmet vermekte, her iki taraf arasında noter görevi görmektedir.

Bir networkte, bir hedefe varma sürecindeki veriye , *iletişim durumundaki veri,* data denir. Bir storage'da veya bir lokal bilgisayarda saklanan veriye ise *statik veri* veya *storage verisi* denir.

Buna göre verinin, gizliliği ve bütünlüğünün anlamı;

1- İletişim halindeki verinin gizililiğinden kasıt, yetkisiz kişiler tarafından okunamamlıdır. İletişim halindeki verinin bütünlüğünden kasıt iletişim sürecinde, yetkisiz kişiler tarafından değiştirilememeli, üretilememelidir.

2- Statik haldeki datanın giziliğinden kasıt, bir lokal cihazda saklanan verinin yetkisiz kişiler tarafından okunamamasıdır. Statik heldeki verinin bütünlüğünden kasıt ise, yetkisiz kişiler tarafından değiştirilememesi, üretilememesidir.

- İletişim halindeki veya statik haldeki verilerin inkar-edememe özelliği ise, kendisine ait olan veriyi kişinin *benim değil* diye inkar edememesidir.

- Verinin kullanılabilirliği ise, yasal kullanıcıların Ağa bağlı bir bilgisayarın mevcut kaynaklar ve hizmetlerinden yararlanabilmesinin saldırganlar tarafından engellenmesine mani olmaktır. Örneğin, virüs bulaşmış bir bilgisayar sistemi üzerinden çok kısa zamanda virüsü tespit etmek ve dezenfekte etmektir. Veya DoS saldırısına uğramış sunucunun, hala kullanıcılara hizmet sunabilmesi işlemidir.

- İletişim Protokol özelliklerinden dolayı, protokolun yürütülmesi sürecinde, veya diğer yazılımların istenmeyen özelliklerinden yararlanarak saldırganlar saldırılarını yapabilirler. Bunlar iletişim protokollarının veya işletim yazılımlarının boşlukları, *kusurları, zayflıkları* olarak isimlendirilir.

- Ağ güvenliği prensipleri, bir pasif savunma işlevidir. Çünklü ağdaki kurban (mağdur-victim) bilgisayar saldırıya uğramadan önce, saldırıyı kimin yaptığını, nereden yapıldığının bilemez.

- Ağ güvenliğinde Derin bir katmanlı savunma sistemi oluşturmak, mümkün olan en iyi savunma taktiğidir.

- Savunma sistemi, çoklu katmanlı yapısıyla mümkün saldırılara karşı korumayı yapabilmelidir.

- Ağ güvenliği bilgi güvenliğinin (information security) önemli bir parçasıdır.
- Ağ güvenliğine ek olarak, Bilgi güvenliği;

Güvenlik politikaları,
Güvenlik denetimi,
Güvenlik değerlendirmesi,
Güvenilir işletim sistemleri,
Veritabanı güvenliği,
Güvenli kod,
Acil müdahale,
Adli bilişim, adli tıp,
Felaket kurtarma ve Güvenlik eğitimi

dahil olmak üzere diğer birçok güvenlik sorunları ile ilgili konuları da kapsar.

OSI Güvenlik Mimarisi X.800

- Veri güvenliğinde sistematik bir yaklaşım olarak; ITU-T (İnternational Telecomunication Union - Telecommunication Standardization Sector) kuruluşunun X.800 olarak adlandırdığı standartlara uyulur.

- X.800 Aynı zamanda yedi katmanlı OSI Temel Referans Modelinde güvenlik hizmetlerinin uygulanması içinde uygundur.

X.805 Standartı

- ITU-T ‘nin X.805 standartı ise,

“Uçtan uca haberleşme hizmeti sağlayan iletişim sistemleri için güvenlik mimari yapısını”

tarif eder.

- Güvenlik mimarisi, servis sağlayıcıların, işletmelerin ve son kullanıcıların global güvenlik zorluklarını gidermek için oluşturulmuştur.

- Kablosuz, optik ve kablolu ses, veri ve hibrit ağlar için geçerlidir. Bu güvenlik mimarisi, ağ altyapısının, servislerinin ve uygulamalarının yönetimi, denetimi ve kullanımı ile ilgili güvenlik kaygılarını giderir.

- Güvenlik mimarisi, karmaşık bir yapı olan 'uçtan-uca güvenlik ' problemini katmanlara (mantıksal bileşenlere) böler.
- Uçtan uca güvenliğin çok karmaşık yapısı, katmanlara paylaştırılarak karmaşıklık azaltılır ve katmanlara, yeni görev atamaları yapılabilir. Böylece uçtan uca güvenlik için çok karmaşık yapı daha basit şekilde katmanlarda çözülür ve biribinden soyutlanabilir.

Güvenlik mimarisi uçtan uca güvenlikle ilgili üç temel soruyu ele alır;

1) Ne tür bir korumaya ihtiyaç duyuluyor ve hangi tehditlere karşı gerekli?

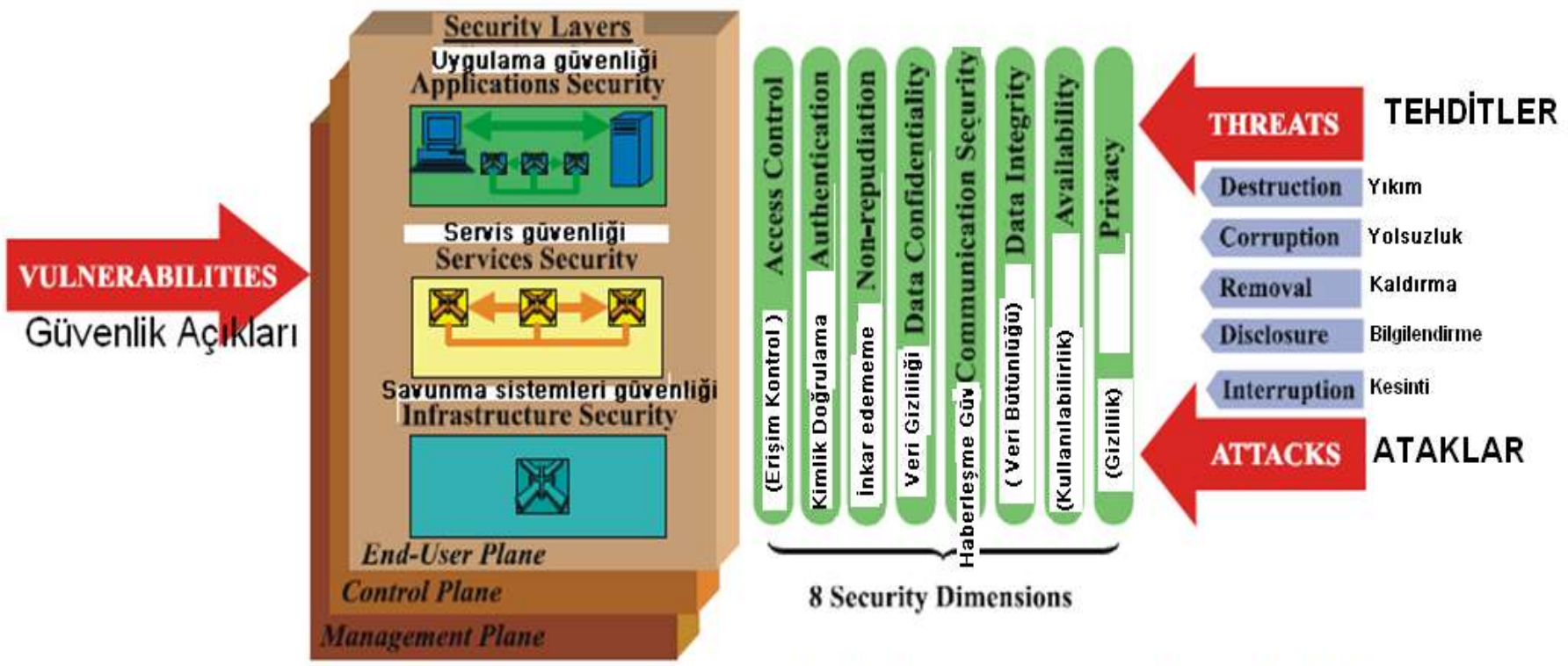
2) Korunması gereken farklı ağ teçhizatı türleri ve tesis grupları nelerdir?

3) Korunması gereken farklı ağ faaliyetleri türleri nelerdir?

- Bu sorular güvenlik boyutları (security dimensions), güvenlik katmanları (security layers) ve güvenlik düzlemleri (security planes) olmak üzere üç mimari bileşen tarafından ele alınmaktadır.
- Güvenlik mimarisi tarafından açıklanan ilkeler, ağın teknolojisi veya protokol yığını içindeki konumundan bağımsız olarak çok çeşitli ağlara uygulanabilir.

Uçtan-Uca İletişim Sistemleri için Güvenlik Mimarisi X.805

- Bu güvenlik mimarisi iki temel kavram üzerine kurulmuştur. **Katmanlar (Layers)** ve **Düzlemler(Plains)**.
- Bir güvenlik düzleminde (Plane), üç güvenlik katmanı da kullanılır.

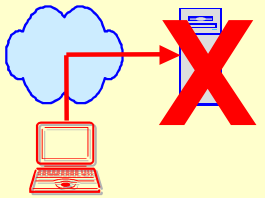


Security Architectural Elements in ITU-T Recommendation X.805

ITU-T X.800 ile tarif edilmiş Threat (Tehdit) Modeli

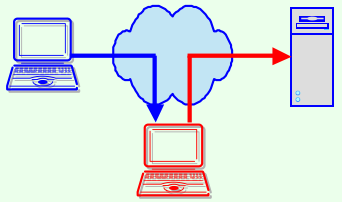
1 – Destruction (Yoketme-İmha) (Kullanılabilirliğe karşı yapılan atak):

– Bilgi ve/veya ağ kaynaklarının imha edilmesi.



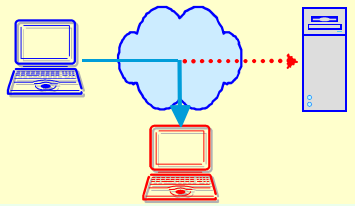
2 – Corruption (Bozma- yolsuzluk) (Bütünlük üzerine yapılan atak)

– Yetkisiz biri tarafından tahrif etme.



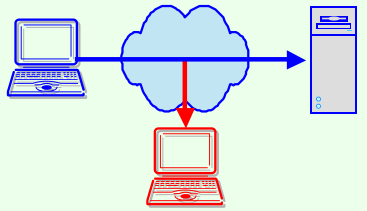
3 – Removal (Giderme- Kaldırma) (Kullanılabilirliğe karşı yapılan atak):

– Bilgi ve/veya kaynakların kaldırılması veya kaybedilmesi hırsızlığıdır.



4 – Disclosure (Açığa vurma, ifşa) (Bütünlük üzerine yapılan atak):

– Bir varlığa yetkisiz erişim.



5 - Interruption (Kesintiye uğratma) (Kullanılabilirliğe karşı yapılan atak):

– Hizmetlerin kesintiye uğramasıyla. Ağın kullanılamıyor veya kullanılamaz hale getirilmesi.

8 adet Güvenlik Boyutu, Ağın güvenlik açıklarının bütününü kapsar. 8 adet Güvenlik boyutunun herbiri ağ saldırılarının belirli bir kısmının önlenmesi için gereken önlemleri açıklar.

Sekiz güvenlik boyutu, herbir güvenlik perspektifine (Katmanlar ve düzlemlere) uygulanır.

- Ağ elemanlarına, servislere, uygulamalara erişimin limitlenmesi ve kontrolu. Yetkisiz erişimleri önlemek için.

Örnek:password, ACL, firewall

Access Control (Erişim Kontrolu)

Authentication (Kimlik Doğrulama)

İletişim kuracak varlıkların biribirlerinin kimliklerini doğrulamaları içindir.

Örnek: Paylaşılan gizli kod dizisi, PKI (Public Key İnfrastructure), digital imza, digital sertifika.

- Ağda oluşan tüm aktivitelerin inkar edilememesinin sağlanması.

Örnek: sistem log'ları, digital imzalar.

Non-repudiation (İnkar edememe)

Data Confidentiality (Veri gizliliği)

Verilerin gizliliğinin sağlanması. Veri içeriğinin yetkisiz kişiler tarafından anlaşılmamasını sağlar.Örn:Kriptolama

- Verilerin, sadece kaynaktan hedefe aktığından emin olunması.
- Örnek.: VPN, MPLS, L2TP

Communication Security (İletişim Gizliliği)

Data Integrity (Veri Bütünlüğü)

- Datanın gönderildiği veya saklandığı şekliyle alındığında emin olunması.
- Örnek: MD5, digital imza, anti-virus yazılımları.

Meşru kullanıcıların, anormal işletme şartlarında bile ağ elemanlarını, servisleri, uygulamaları kullanabilme yetkisinin belirlenmesi.

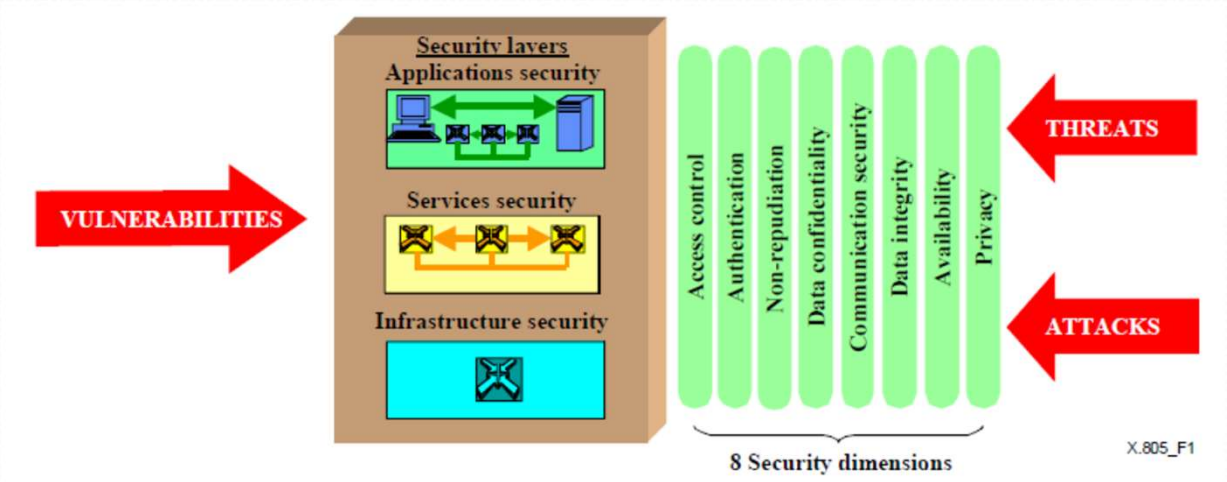
Örn: IDS/IPS, network redundancy, BC/DR (İş sürekliliği/Felaket kurtarma)

Availability (Kullanılabilirlik)

Privacy (Gizlilik)

Kimlik Tanımlamanın ve ağ kullanımının gizli tutulduğundan emin olunması.

- Örnek: NAT, Kriptolama



Her düzlemdeki Güvenlik katmanları, güvenli ağ çözümleri için bir dizi etkinleştiricidir. Altyapı katmanı (Infrastructure), Hizmetler (services) katmanına hizmet sağlar. Hizmetler katmanı, Uygulama (Application) katmanını etkinleştirir.

Altyapı güvenlik katmanı, ağ iletim elemanları ve belirli güvenlik boyutlarıyla korunan bireysel şebeke elemanlarından (router,switch, server v.b) oluşur.

Hizmetler güvenlik katmanı, servis sağlayıcıların müşterilerine sağladığı hizmetlerin güvenliğini sağlar. İnternet Servis Sağlayıcıların sunmuş olduğu hizmetler ve bu hizmetlerden yararlanan müşteriler, güvenlik tehditlerinin potansiyel hedefleridir. Bu güvenlik katmanı hizmet sağlayıcıları ve müşterilerini korumak için kullanılır.

Uygulamalar güvenlik katmanı, servis sağlayıcı müşterileri tarafından erişilen ağ tabanlı uygulamaların güvenliğine odaklanır. Bu uygulamalar ağ servisleri tarafından etkinleştirilir ve temel dosya aktarımını (örneğin FTP) ve web tarama uygulamalarını, ağ tabanlı sesli mesajlaşma ve e-posta gibi temel uygulamalar v.b olabilir. Veya 3. parti uygulamalar olabilir.

Güvenlik düzlemi, güvenlik boyutlarıyla korunan belirli bir ağ etkinliği türüdür.

Yönetim güvenlik düzlemi, ağ elemanlarının, iletim tesislerinin, arka ofis sistemlerinin (operasyon destek sistemleri, iş destek sistemleri, müşteri bakım sistemleri, vb.) ve veri merkezlerinin korunmasıyla ilgilenmektedir. Yönetim düzlemi hata, kapasite, yönetim, sağlama ve güvenlik (FCAPS) işlevlerini destekler.

Kontrol güvenlik düzlemi, bilgi, servis ve uygulamaların ağ üzerinden verimli bir şekilde iletilmesini sağlayan faaliyetlerin korunmasıyla ilgilidir. Genellikle makinelerin (örneğin, anahtarlar veya yönlendiriciler) temel aktarım ağı üzerinden trafiği en iyi nasıl yönlendireceğini veya değiştirdiğini belirlemesine olanak tanıyan bilgilerin makinadan-makineye iletilmesini içerir.

Son kullanıcı güvenlik düzlemi, servis sağlayıcı ağının müşterilerin erişim ve kullanım güvenliğini ele alır. Bu düzlem, aynı zamanda gerçek son kullanıcı veri akışlarını da temsil eder. Son kullanıcılar yalnızca bağlantı sağlayan bir ağ kullanabilir, bunu VPN'ler gibi katma değerli hizmetler için kullanabilir veya ağ tabanlı uygulamalara erişmek için kullanabilirler.

Güvenlik Boyutları ve Tehdidlerin kapsanması

Security Dimension (Güvenlik Boyutu)	X.800 Security Threats				
	Destruction (Yok etme)	Corruption (Bozma)	Removal (Kaldırma, giderme)	Disclosure (Açığa vurma, ifşa)	Interruption (Kesinti)
Access Control (Erişim Kontrol)	✓	✓	✓	✓	
Authentication (Kimlik Doğrulama)			✓	✓	
Non-Repudiation (İnkar edememe)	✓	✓	✓	✓	✓
Data Confidentiality (Ver Gizliliği)			✓	✓	
Communication Security (İletişim Güvenliği)			✓	✓	
Data Integrity (Veri Bütünlüğü)	✓	✓			
Availability (Kullanılabilirlik)	✓				✓
Privacy (Gizlilik)				✓	

Güvenlik Mekanizmaları

- Güvenliğe karşı yapılan Atakların, anlaşılması, bu atağa karşı korunma veya tahribatını onarmak için kullanılan yöntemlerdir.

- **Şifreleme Mekanizmaları(Encipherment Mechanisms)**
  - veri gizliliği hizmet verirler.
  - Asimetrik / Simetrik algoritmalar

- **Sayısal İmzalar (Digital Signatures)**
  - Islak imzanının, elektronik ortamdaki sayısal eşdeğeridir.
  - Genellikle asimetrik şifreleme uygulayanır.

- **Erişim Kontrol Mekanizmaları (Access Control Mechanisms)**
  - Doğrulanmış kimlik bilgilerini kullanarak , bir varlığa veya varlıkla ilgili bilgilere erişim kontrol hizmetlerinin sağlanması.

- **Veri Bütünlüğü Mekanizmaları (Data Integrity Mechanisms):**
  • Veri bütünlüğünün sağlandığını kanıtlamak için, değişik ispat algoritmalarını kullanmak.
  • Mesaj kimlik doğrulama kodları (MAC), dijital imzalar v.b

- **Kimlik doğrulama mekanizmaları (Authentication Mechanisms):**
  • Temel bir kimlik temini, kimlik doğrulama hizmetleri sağlanması.
  • Ortak anahtar altyapısı (PKI - public key infrastructure) gibi şifreleme teknikleri ve güven altyapısı dayanarak.

- **Trafik-Dolgu Mekanizmaları (Traffic-Padding Mechanisms)**
  • Trafik analizi saldırılarına karşı koruma sağlama

- **Yönlendirme Kontrol Mekanizması(Routing Control Mechanisms)**
  • Belirlenmiş yollardan dinamik veya statik olarak, iletişim veri için belirli bir güzergah seçimi izini.

Saldırıların Sınıflandırılması

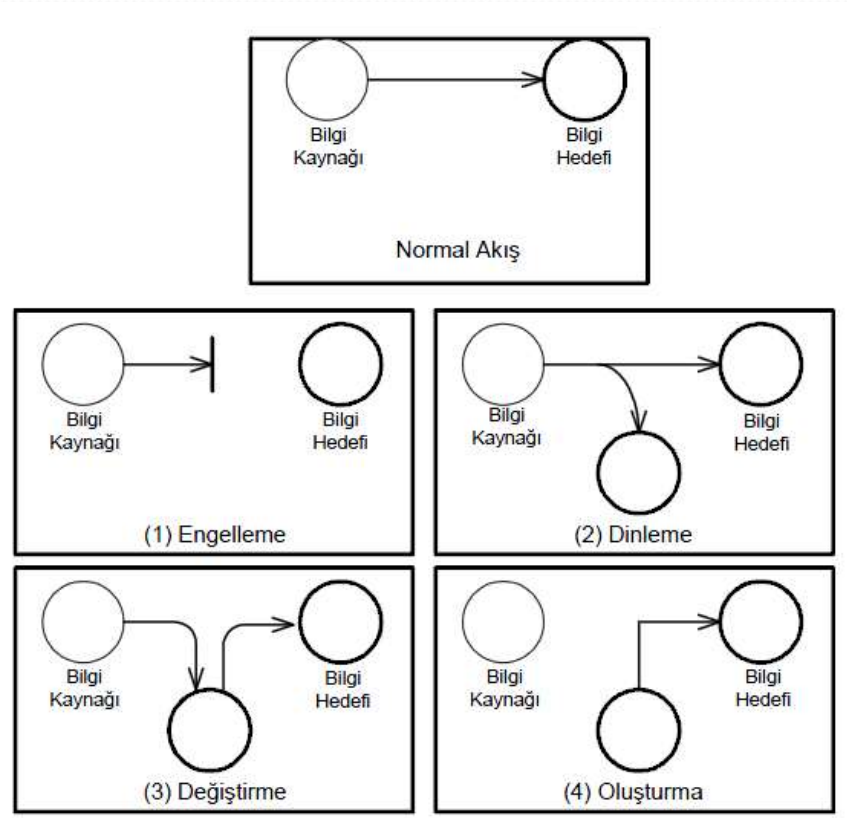
Bir kuruluşun bilişim sistemlerine karşı yapılan saldırılar aşağıdaki 4 kategoride incelenir.

1-Engelleme

2-Dinleme

3-Değiştirme

4-Oluşturma



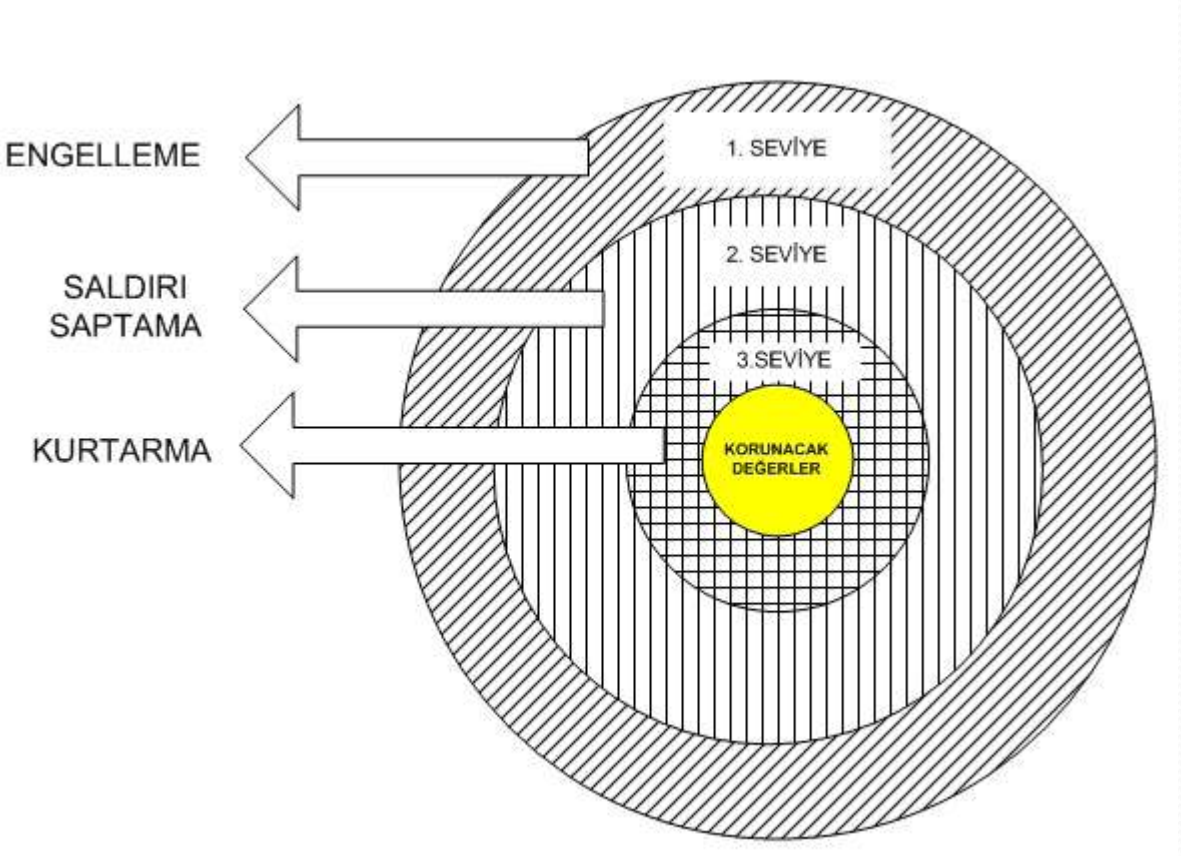
Ağ Güvenlik politikası

- Kurumların kendi kurmuş oldukları ve İnternet'e uyarladıkları ağlar ve bu ağlar üzerindeki kaynakların kullanılması ile ilgili kuralların genel hatlar içerisinde belirlenerek yazılı hale getirilmesi ile ağ güvenlik politikaları oluşturulur.
- Güvenlik politikasının en önemli özelliği yazılı olmasıdır ve kullanıcıdan yöneticiye kurum genelinde tüm çalışanların, kurumun sahip olduğu teknoloji ve bilgi değerlerini nasıl kullanacaklarını kesin hatlarıyla anlatmasıdır.

- Ağ güvenlik politikaları, kurumların yapılarına ve gereksinimlerine göre değiştiğinden bir şablondan söz etmek mümkün değildir. Ağ güvenliğinin sağlanması için gerekli olan temel politikalar aşağıda sıralanmıştır :

- 1. Kabul edilebilir kullanım (acceptable use) politikası
- 2. Erişim politikası
- 3. Ağ güvenlik duvarı (firewall) politikası
- 4. İnternet politikası
- 5. Şifre yönetimi politikası
- 6. Fiziksel güvenlik politikası
- 7. Sosyal mühendislik politikası

Katmanlı güvenlik planı

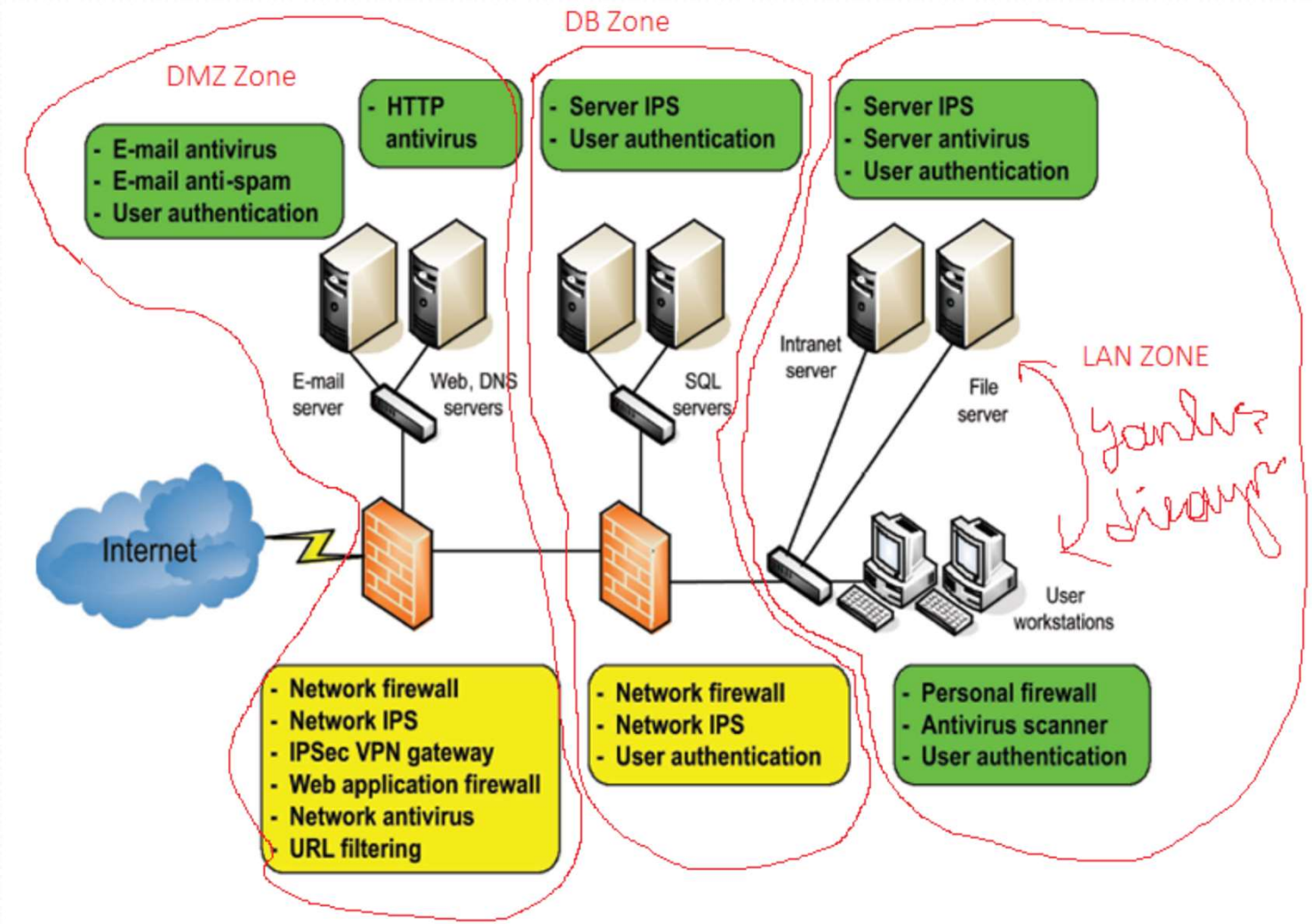


Bölümlenmiş güvenlik kavramı

- Farklı hassasiyet seviyesindeki IT sistem kaynaklarının (örneğin, farklı risk tolerans değerleri ve tehdit yatkınlık), farklı güvenlik bölgelerinde yer alması gerekir. Bu durum Şekil 'de gösterilmiştir.

- Bu kuralın bir uzantısı "bilgi gizleme"dir. Sadece bu işi yürütmek le görevlendirilmiş IT sistemleri bu işi yapar. (örneğin, İnternette resmi kayıtlı DNS sunucuları sorgulaması için kullanılan public DNS sunucuları sadece bu hizmeti sağlamak içindir)

Bilgi Bölümlendirme: IT sistem kaynakları ve bilgi farklı hassasiyet seviyelerinde farklı güvenlik bölgelerinde yer almalıdır.



Anlatılacaklar

- Bilgisayar ağlarında güvenlik konusu, ağa bağlı aktif cihazlara ve iletişim halindeki veriye, illegal olarak erişme, değiştirme, okuma, bütünlüğünü bozma, inkar etme v.b saldırıların öğrenilmesi ve önlenmesidir.
- Bu saldırılar, iletişim protokollarının açıklarından, ağ cihazlarına erişimin engellenmemesinden, güvenlik politikalarının iyi oluşturulamamasından kaynaklanmaktadır.
- Özellikle TCP/IP Version 4 iletişim protokol kümesiyle çalışan internet gibi dinlenmeye çok müsait ağ yapılarında seyahat eden verilerin her türlü saldırıya açık olduğu bilinmektedir.
- Ağ güvenliği (Sistematik ağ güvenliği) konusu üç farklı segment'te incelenecektir.

  1- İletişim protokolları açıklarından yararlanarak yapılan saldırılar ve tedbirler.

  2- Güvenlik protokollarının uygulanması

  3- TCP/IP protokol verilerinin Clear text olmasının getirdiği dezavantajlar ve tedbirler.
- Bu derste TCP/IP ve OSI katmanlı ağ modeli ve ilgili katman protokolları ve bunların zayıflıkları üzerinde durulacaktır. Bu zayıflıklardan yararlanılarak yapılacak saldırılar ve tedbirleri nelerdir? Tartışılacaktır….
- İlgili ağ cihazlarının korunması ve cihazların uygun konfigürasyonları ile ağ güvenlik açıklarının azaltılması, sistematik ağ güvenliği üzerinde durulacaktır.

Figure 1.2 Stack Attacks and Vulnerabilities

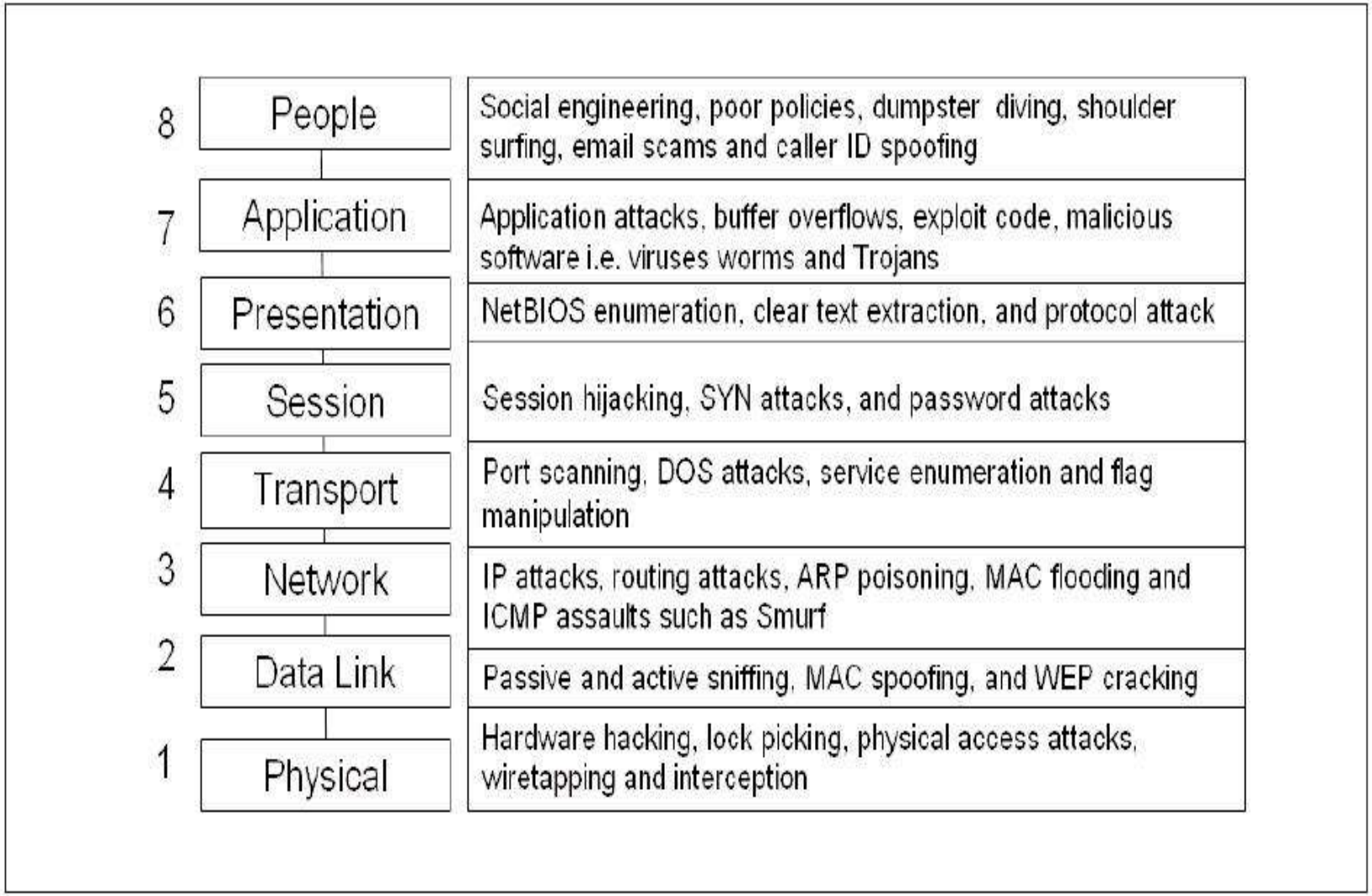
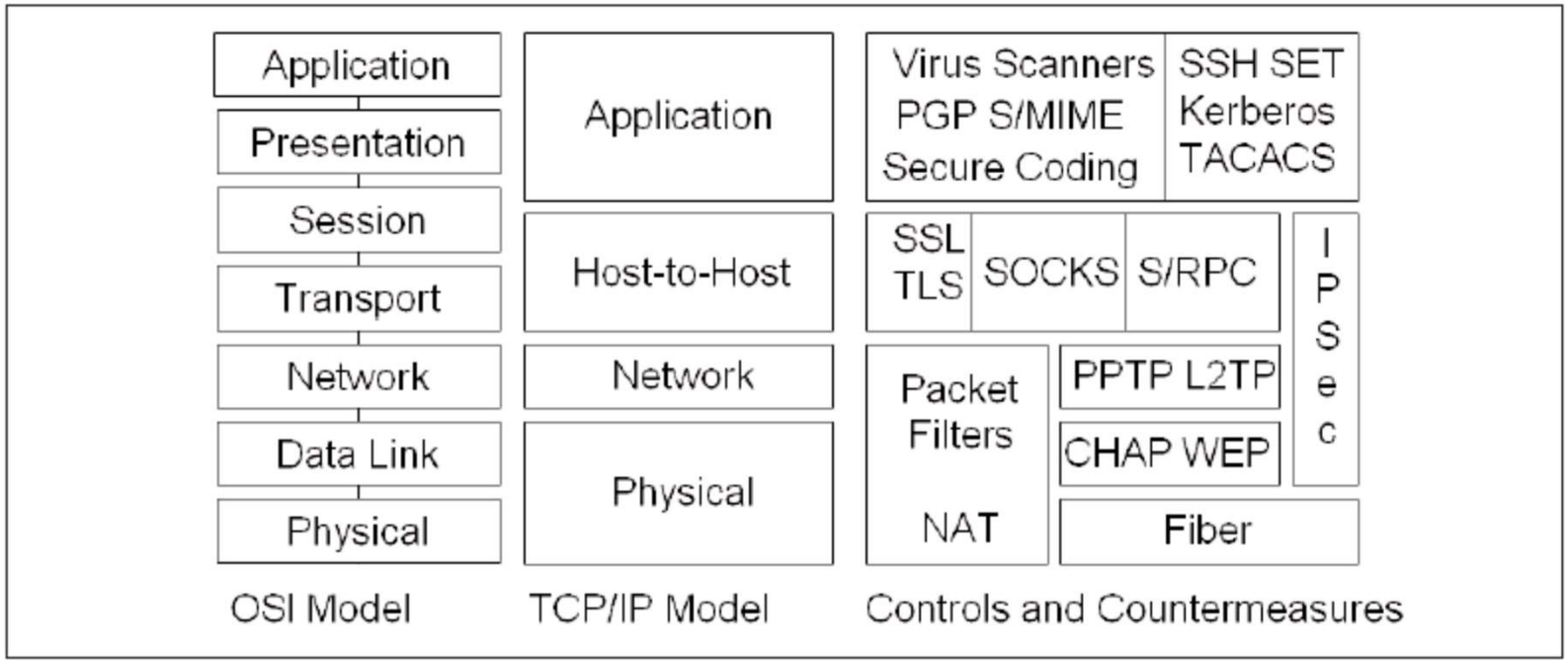


Figure 1.3 The OSI Model, TCP/IP Model, and Common Countermeasures



Derste anlatılacaklar….

- OSI/TCP-IP ağ modelinin kısa özeti
- Ağ modeli katmanı protokollarının incelenmesi açıkları, saldırı tipleri, önlemleri.
- Ağ aktif cihazlarında alınması gereken önlemler.
- Ağ güvenlik protokollarının açıklanması.
- Güvenlik duvarları, İç Ağ/Dış ağ koruması
- Şifreleme, e-imza konularına genel bakış.
- Penetrasyon (Nüfuz etme-sızma) Testleri

Konular işlenirken sanal ortamda gerekli uygulamalar ve projeler ile desteklenecektir. Bunun için kullanılacak yardımcı yazılım araçlar;

-GNS3 sanal ağ emülatör yazılımı

-Ağ güvenlik yazılım araçları ()Wireshark, NMAp v.b)

-Penetrasyon testleri için Kalli yazılım aracı

Vize ve Final Notu:Konu sonlarında verilecek projelerin değerlendirilmesinden oluşacaktır.