Bilgi Güvenliği ve Kriptoloji

Temel Kavramlar

Veri (Data)?

- Latince "datum" (çoğul şekli "data" ve "vermeye cesaret etmek" fiilinin geçmiş zamanı, dolayısıyla "verilen şey")
- Dilimizde de verilen şey anlamında, "veri" olarak kullanılmaktadır.
- **Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış (işlenmemiş) bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.**
- **Ham veri** (raw data) düzenlenmemiş veri olarak ifade edilebilir. **Veri** (data) ise satır ve kolonlar bazında ifade edilmiş, bir formata sahip olan verileri ifade etmektedir.

Bilgi (Information)?

- **Bilgi, verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir.**
- Veri ve ilişkili olduğu konu, bilgi üretecek şekilde bir araya getirilir.
- **İşlenmiş veri** olarak da ifade edilebilecek bilgi, **bir konu hakkında var olan belirsizliği azaltan bir kaynaktır.**
- Veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmelerin) çıktısıdır.
- Örneğin, sorgu ve raporlama fonksiyonları sayesinde, veritabanındaki verinin çekilerek bilgiye dönüşümü sağlanır. (ürün, miktar ve fiyat toplamları, satılan ürünlerle bunların miktar ve hacimleri bilgiyi sağlar)

Nitelikli Bilgi (Knowledge)?

- **Nitelikli bilgi, veri madenciliği (data mining) teknolojisi içeren uygulamalar sayesinde, veri içerisindeki gizli eğilimlerin (trend) ve örüntülerin (patterns) belirlenmesi olarak düşünülebilir.** (Sınıflandırma (Classification), Regresyon (Regression), Kümeleme (Clustering))

  - Müşteri Memnuniyeti ve Profillerinin Belirlenmesi (Pazarlama)
  - Bölgeler arası gelişmişlik farklılıklarının azaltılması yönünde oluşturulacak strateji ve planların hazırlanması (Devlet Planlama Teşkilatı)
  - Kredi kartı harcamalarına göre müşteri gruplarının belirlenmesi,(Bankacılık)
  - Riskli müşteri örüntülerinin belirlenmesi. (Sigortacılık)

Güvenlik?

- Karşılaşılabilecek **tehditlere karşı önlem alma**
- Kişi ve kurumların Bilgi Teknolojilerini- BT (IT – Information Technology) kullanırken karşılaşabilecekleri **tehdit ve tehlikelerin daha önceden analizlerinin yapılarak gerekli önlemlerin alınmasını sağlama**
  - BT, bilgisayar tabanlı bilişim sistemlerinin, özellikle yazılım uygulamaları ve bilgisayar donanımının incelenmesi, tasarlanması, geliştirilmesi, yürütülmesi, yönetimi ve desteğine verilen addır.
  - **BT temel olarak bilgisayarlar ve yazılımlar aracılığıyla bilginin işlenmesi, dönüştürülmesi, saklanması, korunması, iletilmesi ve bu bilgiye güvenli bir biçimde erişilmesini sağlar.**

Bilgi Güvenliği

- **Bilginin değerli veya değersiz olduğunu belirlemek veya bilginin taşıdığı değeri ölçmek, en az bilginin kendisi kadar önemlidir.**

- Bilgiyi değerlendirirken bilginin kalitesini gösteren özelliklere bakılması gerekir.

- Doğruluk, güncellik, konuyla ilgili olma, bütünlük ve öz, gereksinimlere uyum gösterme, iyi sunulma ve fiziksel ve idrak yolu ile erişim gibi ölçütler **bilginin kalitesini belirleyen etmenlerden** bazılarıdır.

- **Bilginin çok önemli bir varlık olması,**
  - **ona sahip olma ile ilgili bazı konuların düzenlenmesini ve**
  - **yeni şartların getirdiği özelliklere göre ayarlanmasını**

  gerektirmektedir.

Bilgi Güvenliği

- Bilgi en basit benzetme ile para gibi bir metadır.
- Dünya gündeminde bir konudur.
- **Bilgi güvenliği**,
  - bilginin bir varlık olarak hasarlardan korunması
  - doğru teknolojinin doğru amaç ve şekilde kullanılmasıyla, her türlü ortamda bilginin istenmeyen kişiler veya sistemler tarafından elde edilmesini önleme

şeklinde ifade edilebilir.

Bilgi Güvenliği?

- Bilgiye sürekli olarak **erişilebilirliğin** sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar **gizlilik** içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden **bütünlüğünün** sağlanması ve güvenli bir şekilde iletilmesi süreci

Bilgi Güvenliği nerede sağlanmalı ?

- –Üretim
- –Erişim
- –İşleme
- –Depolama
- –Aktarma
- –Yok etme

Siber Güvenliğin Temel Hedefi?

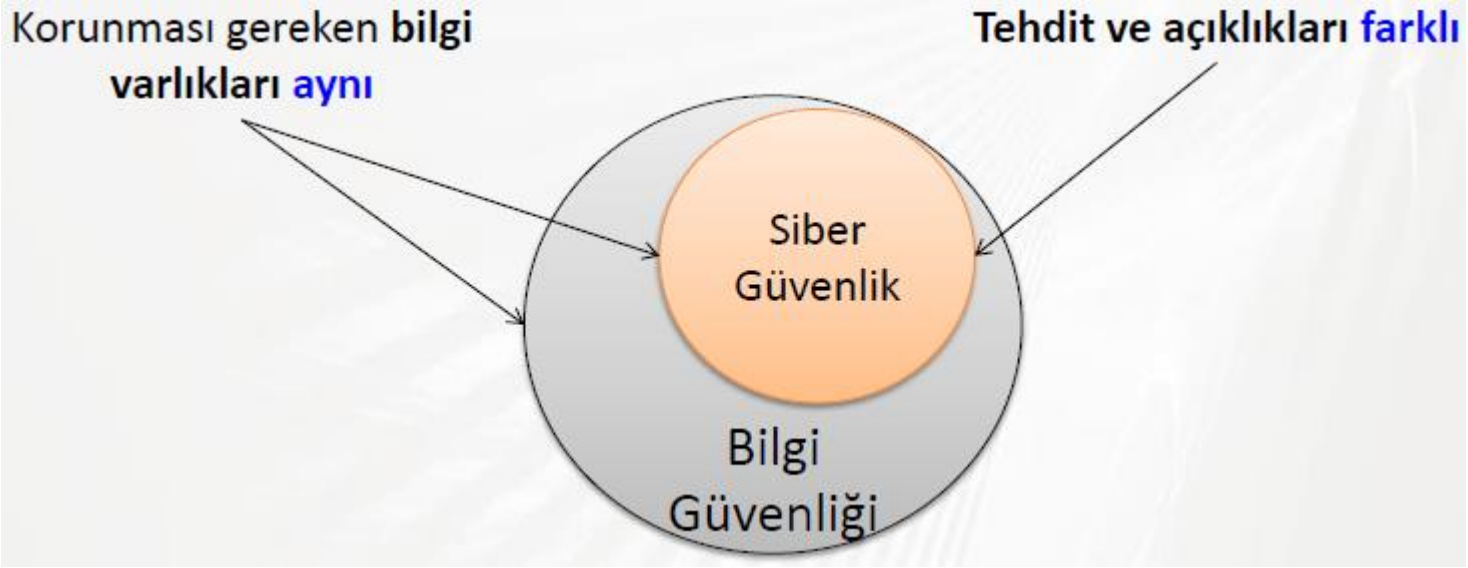
- İletişim halindeki bilgisayar ağlarından oluşan elektronik ortama Siber Uzay denir.

- Kurum ve kuruluşların veya en genel anlamda ulusların bilgi varlıkları ve kaynaklarını hedeflenen amaçlar doğrultusunda (organizasyon, insan, finans, teknik ve bilgi değerlerini dikkate alarak), başlarına **KÖTÜ BİR ŞEYLER GELMEDEN** korumaktır.

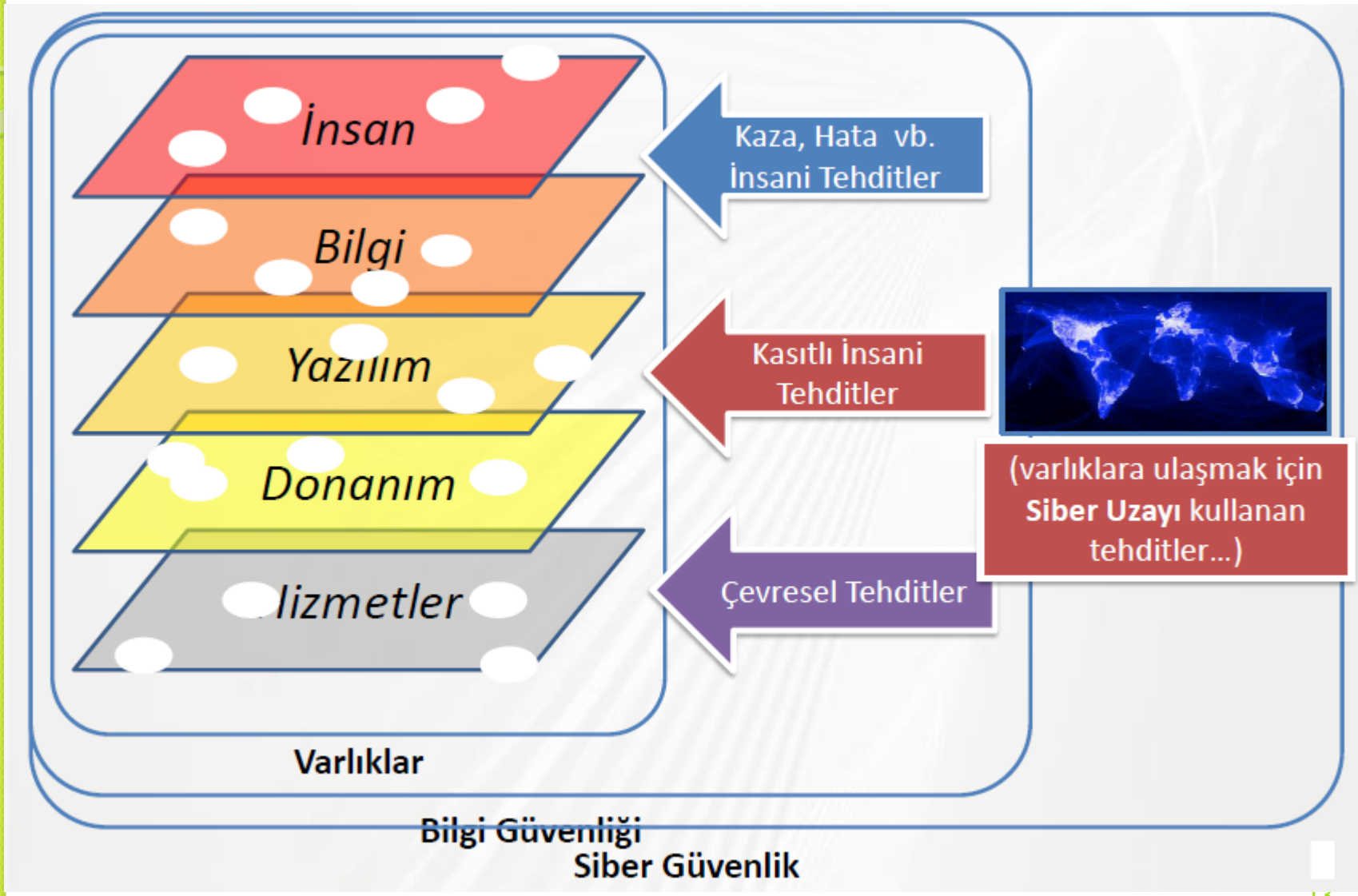
Siber Savunma İle İlgili Yanlış Düşünceler

- Antivirüs yazılımımız var, dolayısıyla güvendeyiz!
- Bilgimin kopyasını alıyorum, güvenlikten bana ne!
- Güvenlikten bilgi işlem sorumludur.
- Kurumumuz güvenlik duvarı (firewall) kullanıyor, dolayısıyla güvendeyiz!
- Bir çok güvenlik saldırısı kurum dışından geliyor!

- **Siber Güvenlik**, bilgi güvenliğinde söz konusu olan tehdit ve açıklıkların bir altkümesi ile ilgilenir.



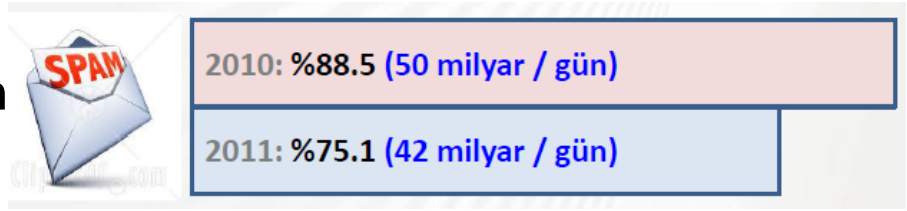
Bilgi Güvenliği ve Siber Güvenlik



Siber Tehditlerin Özellikleri

- Farklı coğrafi konumlardan saldırı şansı (Saldırganın konumu?)
- Düşük maliyet (Bilgisayar + Internet)
- Kötü yazılım (bilgisayar virüsleri, solucanlar, vs.)
- Servis dışı bırakma saldırıları ("DDoS- Distributed Denial of Service attack"- çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşur, bunlar genellikle bir veya birden fazla web sunucusudur)
- Yığın E-postalar

  Yığın e-postaların toplam e-posta trafiğine oranı:



- Parola balıkçılığı siteleri (("Phishing"-Password+fishing : şifre avcıları, genelde e-posta gibi yollarla kişilere ulaşır ve onların kredi kartı gibi ayrıntılarını sanki resmi bir kurummuş gibi ister)
- İçerik değiştirme / bilgiye yetkisiz erişim…

Siber Tehditlerin Hedefleri

- Bilgi sistemleri ve kritik ulusal altyapılar
  - Finans
  - Ulaştırma
  - Enerji v.b
- Değer ifade eden sektörler
- Ulusal güvenliğe ait kritik bilgiler
  - Sağlık verileri
  - Kritik ekonomik veriler
  - Savunma sanayi

Siber Tehditlerin Hedefleri

- BT sistemlerinin ve fiziksel mekanizmaların iç içe olduğu sistemleri hedefleyen sistemler
- Mobil uygulamalar ve gömülü sistemler
- Örnek uygulamalar
  - Uzaktan hasta takip sistemleri
  - Araç içi ağ sistemleri ve araçtan araca iletişim sistemleri

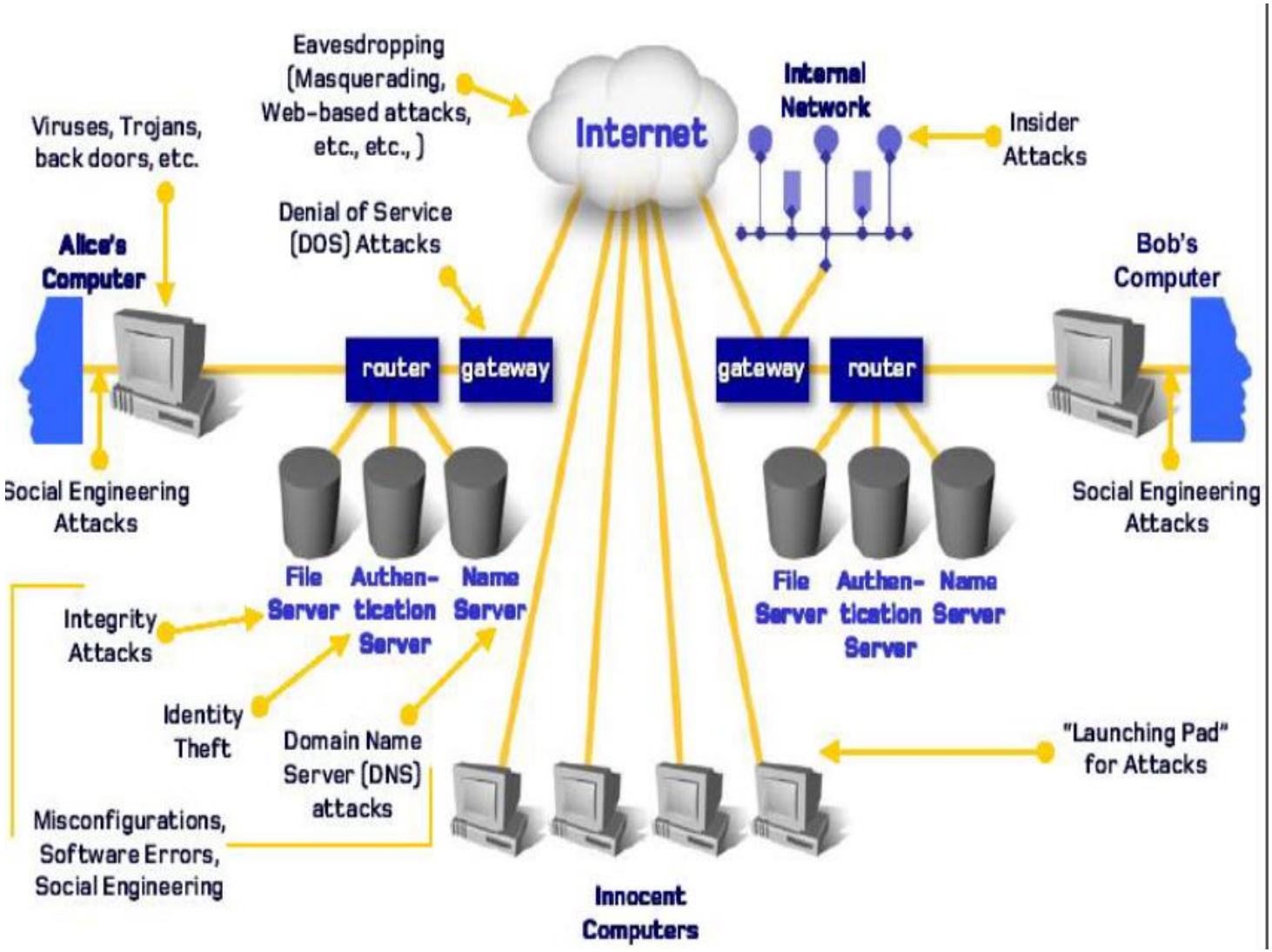
Siber Savaşlar

- Casusluk
- Manipülasyon
- Propaganda
- İletişim
- Sistem bozma
- Bilgi kirliliği
- Sistem kilitleme
- Dolandırıcılık
- Sisteme yetkisiz erişim
- Sistemin bozulması
- Hizmetlerin engellenmesi
- Bilgilerin
  - Değiştirilmesi
  - Yok edilmesi
  - İfşa edilmesi
  - Çalınması

Siber silahlar

- Hizmetin engellenmesi saldırıları (DoS, DDoS)
- Bilgisayar virüsleri
- Kurtçuklar (worm)
- Truva atı (trojan)
- Klavye izleme (key logger) yazılımları
- İstem dışı ticari tanıtım (adware) yazılımları
- Casus / köstebek (spyware) yazılımlar
- Yemleme/Sazan avlama (phishing)
- İstem dışı elektronik posta (spam)
- Ağ trafiğinin dinlenmesi (sniffing ve monitoring)

İnterneti Anlamak



- **Social Engineering Attacks (sosyal mühendislik atakları):** Kişileri gizli bilgi vermeleri ya da erişim sağlamaları için aldatma süreci

- **Virüs:** Bilgisayar virüsü, kullanıcının izni ya da bilgisi dahilinde olmadan bilgisayarın çalışma şeklini değiştiren ve kendini diğer dosyaların içerisinde gizlemeye çalışan aslında bir tür bilgisayar programıdır. Kendini çoğaltmalı Kendini çalıştırmalı (yürütmeli) tahrip edici bir tür bileşeni bünyelerinde barındırırlar

- **Worm:** Solucan da, virüs gibi, kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır ancak bunu otomatik olarak yapar. İlk olarak, bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirir. Solucan bir kez sisteminize girdikten sonra kendi başına ilerleyebilir.

- **Trojan:** Truva atı zararlı program barındıran veya yükleyen programdır. Truva atlarının zararlılığı da kullanıcının hareketlerine bağlıdır. Truva atları kendilerini kopyalayıp dağıtsalar bile her kurbanın programı (Truvayı) çalıştırması gerekir. Bu yüzden Truva atlarının zararlılığı bilgisayar sistem açıklarına veya ayarlarına değil toplum mühendisliğinin başarılı uygulamalarına bağlıdır.

- **Integrity Attacks (Bütünlük atakları):**

- **Identitiy Theft (kimlik çalma):**

- **DNS atağı: DNS (spoofing)** zehirleme kullanıcıları bir siteden saldırganın seçtiği başka bir siteye yönlendirmek için kullanılabilir Örneğin, bir saldırgan verilen bir DNS sunucusundaki bir hedef websitesi için IP adresi DNS girdilerini onun kontrolündeki sunucunun IP adresiyle değiştirerek zehirler. Sonra hedef sunucusundaki isimlerle eşleşen onun kontrolündeki sunucuda dosyalar oluşturur. Bu dosyalar bilgisayar solucanı veya virüs gibi zararlı içerikler içerebilir. Zehirlenmiş DNS sunucusuna referans edilmiş bilgisayara sahip bir kullanıcı güvenilir olmayan bir sunucudan gelen içeriği kabul ederek kandırılmış olacak ve farkında olmadan zararlı içeriği indirmiş olacaktır.

- DOS (Denial of Service) Atağı: Sisteme düzenli ve sürekli olarak saldırılması sonucu sistemin hizmet veremez hale gelir. Ayrıca DoS saldırılarıyla hedef sisteme ait kaynakların tüketilmesi de amaçlanır. Bu saldırı çok önemli sunucuların hizmet dışı kalması gibi sorunlara yol açabilir. Eğer saldırganlar saldırıyı tek bir ana bilgisayardan düzenlerse bu bir dos saldrısı olarak sınıflandırılır. Diğer taraftan, bir saldırgan aynı anda uzaktaki bir bilgisayara yönelik saldırılar için birçok sistem kullanıyorsa, bu bir Ddos saldırısı olarak sınıflandırılır.

- Ddos kullanan saldırganlar için başlıca avantajlar şunlardır: çoklu makineler bir makineye göre daha fazla saldırı trafiği oluşturabilir, çoklu saldırı makinelerini kapatmak tek bir saldırı makinesini kapatmaya göre daha zordur, çoklu saldırı makinelerinde her saldırı makinesinin davranışını izlemek zordur. Bu saldırgan avantajları savunma mekanizmaları için zorluklara neden olur.

- **IP spoofing** veya **IP sahteciliği**, sahte kaynak IP adresi ile Internet Protokolü (IP) paketlerinin oluşturulmasıdır. IP spoofing en sık DoS(Denial of Service)saldırılarında kullanılır.Bu tür saldırılarda amaç, hedef bilgisayarın sorgu trafiğini aşırı miktarda artırmaktır, saldırgan saldırı paketlerine yanıt almayı önemsemez.Sahte adres kullanarak paket göndermek bu yüzden uygundur.Bu amaçlı saldırılar için ip spoofing'in ek avantajları vardır-Her sahte paket farklı bir adresten geliyormuş gibi görünür bu sebeple filtrelemek daha zordur,ve saldırının gerçek kaynağı gizlenir.

- **Eavesdroping** özel konuşmaları gizlice dinlemek anlamına gelir. Gizlice dinleme ayrıca telefon dinlenerek, e-mail, kısa mesaj ve diğer özel kabul edilen iletişim cihazlarının izlenilmesiyle de yapılır Gizlilik güvenliği servisleri kullanılarak mesajlar gizlice dinlenmekten korunabilir.Bu güvenlik servisi genellile verinin şifrelenmesi yöntemiyle çalışır.

- **Masquerading (Yerine Geçme):** başka bir ağa atak yapan kullanıcının kendisini atak yaptığı sistemin yetkili bir üyesi olarak göstermesi, Bu atakta sistemin açığındanda faydalanarak kendisini yetkili bir kişi gibi göstererek gerekli izinleri alıp yetkili biri olduktan sonra verileri kopyalayabilir,silebilir ,değiştirebilir.

- **Ağ geçidi** (İng. *gateway)*, farklı ağ iletişim kurallarını kullanan iki bilgisayar ağı arasında veri çerçevelerinin iletimini sağlayan ağ donanımıdır. Bir başka deyişle aynı dili konuşamayan iki ağ arasında tercüman vazifesi görür.

- **Yönlendirici** (İngilizce: *router*), aynı ağ iletişim kurallarını kullanan iki bilgisayar ağı arasında veri çerçevelerinin iletimini sağlayan ağ donanımıdır. Yönlendirme için OSI yedi katman modelinin üçüncüsü olan ağ katmanı kullanılır. Genellikle bu iş için özel üretilmiş donanımlar varsa da birden çok arayüzü olan bilgisayarlar da yazılım desteğiyle yöneltici olarak çalışabilirler.

- **DNS** (İngilizce: ***D**omain **N**ame **S**ystem*, Türkçe: **Alan Adı Sistemi**), internet uzayını bölümlemeye, bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan, bilgisayar, servis, internet veya özel bir ağa bağlı herhangi bir kaynak için hiyerarşik dağıtılmış bir adlandırma sistemidir.
- İnternet ağını oluşturan her birim sadece kendine ait bir IP adresine sahiptir. Bu IP adresleri kullanıcıların kullanımı için www.site_ismi.com gibi kolay hatırlanır adreslere karşılık düşürülür. DNS sunucuları, internet adreslerinin IP adresi karşılığını kayıtlı tutmaktadır.

- **Kimlik Doğrulama Sunucusu (Authentication Server)**
- Kimlik doğrulama, izin verme ve hesap tutma işlemlerini yapar. İstemcinin kimliğine bakarak servislere erişip erişmeyeceğini kontrol eder ve onaylar.

- **Gömülü sistem**, bilgisayarın kendisini kontrol eden cihaz tarafından içerildiği özel amaçlı bir sistemdir. Genel maksatlı, örneğin kişisel bilgisayar gibi bir bilgisayardan farklı olarak, **gömülü** bir **sistem** kendisi için önceden özel olarak tanımlanmış görevleri yerine getirir. Gömülü bir sistemin çekirdeğini, belirli bir sayıda görevi yerine getirmek için programlanan mikroişlemciler ya da mikrodenetleyiciler oluşturur.

Faydalar

- Zamandan bağımsızlık
- Mekandan bağımsızlık
- Hız
- Verimlilik
- Gelişim/Değişim
- Hayatı kolaylaştırıyor
- Yönetmeyi kolaylaştırıyor
- Denetlemeyi kolaylaştırıyor

Zararlar

- Bilmeyenler için kontrolü zor..
- Açıklarını bilenleri öne çıkarıyor..
- Kötülere çok yardımcı oluyor..
- Bilmeyenlere hayatı dar ediyor..
- Bağımlılık yapıyor..
- Kişisel gelişimi kısmen olumsuz etkiliyor..
- Gelişmemiş toplumları köleleştiriyor..

60 saniyede neler oluyor?

- 168 milyon e-posta gönderiliyor.
- 1500'den fazla blog iletisi yayımlanıyor.
- 70'den fazla domain adı alınıyor.
- Flicker üzerinden en az 6600 fotograf paylaşılıyor.
- Skype üzerinden 370000 dakika konuşuluyor
- Scribd üzerinden en az 1600 okuma gerçekleşiyor.
- Pandora'da 13000 saatten fazla müzik akıyor.
- 13 000 IPhone uygulaması indiriliyor..

Facebook

- En az 695000 Facebook durum güncellemesi yapılıyor.
- 79364 duvar iletisi yazılıyor.
- 510040 yorum yapılıyor.

Twitter

- 320 Twitter hesabı açılıyor
- En az 98000 Tweet atılıyor.
- 13000 fazla iPhone uygulaması indiriliyor.

Youtube

- 600000'den fazla yeni görüntü yayımlanıyor.
- Dünya genelinde YouTube'de kalma süresi 25 saatten fazla.

Yahoo

- en az 100 soru ve 40 cevap Yahoo'da akıyor.

LinkedIn

- LinkedIn'e 100'den fazla profil ekleniyor.