Genel Tanımlar
Güvenlik Gerekleri ve Korunacak Varlıklar
Bilgisayar Ağına Saldırı

Prof. Dr. Resul Daş

Ağ Güvenliği

- Internet'in gelişmesiyle birlikte bilgisayar ağları da doğal olarak gelişmiştir.
- Bu gelişmeye paralel olarak ağ kurulup işletmeye alındıktan sonra ağ yönetimi ve ağ güvenliği büyük önem kazanmış ve ağın güvenilir bir şekilde çalışması anahtar sözcük konumuna gelmiştir.

Ağ Güvenliği

- Bilgisayarlaşmanın artmasıyla birlikte, dosyaları ve bilgisayarda saklanan diğer bilgileri korumak gerekliliği açıktır.
- Özellikle zaman paylaşımlı ve halka açık iletişim sistemleri gibi paylaşılmış sistemlerde veri güvenliği daha da önemlidir.
- Veriyi korumak ve saldırganları engellemek amacıyla tasarlanmış olan sistem ve araçların genel adı Bilgisayar Güvenlik Sistemidir.

Ağ Güvenliği

- İkinci ana konu, dağıtık sistemler ve son kullanıcının terminali ile bilgisayar arasındaki veri taşıyan haberleşme olanaklarının güvenliğe etkileridir.
- Ağ güvenliği tedbirleri verinin iletimi sırasında onun korunmasını esas alır.
- Bütün iş yerleri, devlet ve akademik kuruluşlar birbirlerine ağlar ile bağlandığı için ortaya büyük bir ağ çıkmaktadır ve buna bağlı ağlar denilmektedir.
- Bu durumda koruma ağdaki bütün birimleri kapsamak durumundadır.

Ağ Güvenliği

- Komple bir ağ o günün teknolojisi ile en iyi biçimde projelendirilip kurulduktan sonra iş bitmemekte, ağın performanslı, güvenilir ve güvenliğinin sağlanmış olması gerekmektedir.
- Güvenilir ve güvenli kavramları birbirine karıştırılan fakat anlamları farklı olan kelimelerdir.

Güvenilir Sistem

- Güvenilir sistem güçlü sistem demektir.
- Yoğun trafikte bile tüm sistem kendinden beklenen performansı sergiler ve herhangi bir tıkanmaya, çökmeye sebep olmaz.
- Bunun için sistemde kullanılan aktif cihazların uygulamaya dönük dikkatli seçilmiş olması ve daha önemlisi konfigürasyonunun iyi ve bilinçli bir şekilde yapılmış olması gerekir.

Güvenli Sistem

- Güvenli sistem ise denetimli sistem demektir.
- Internet gibi genele açık bir ağa bağlanan kurumsal ağların aşağıdaki özelliklere sahip olmasını belirtir;
  - dışarıdan gelebilecek tehlikelere karşı korunması
  - Kurumun sahip olduğu bilgi ve verilere izin verildiği ölçüde erişilmesi
  - Kurumun kendi elemanları tarafından yapılacak iç ve dış erişimlerin denetlenmesi

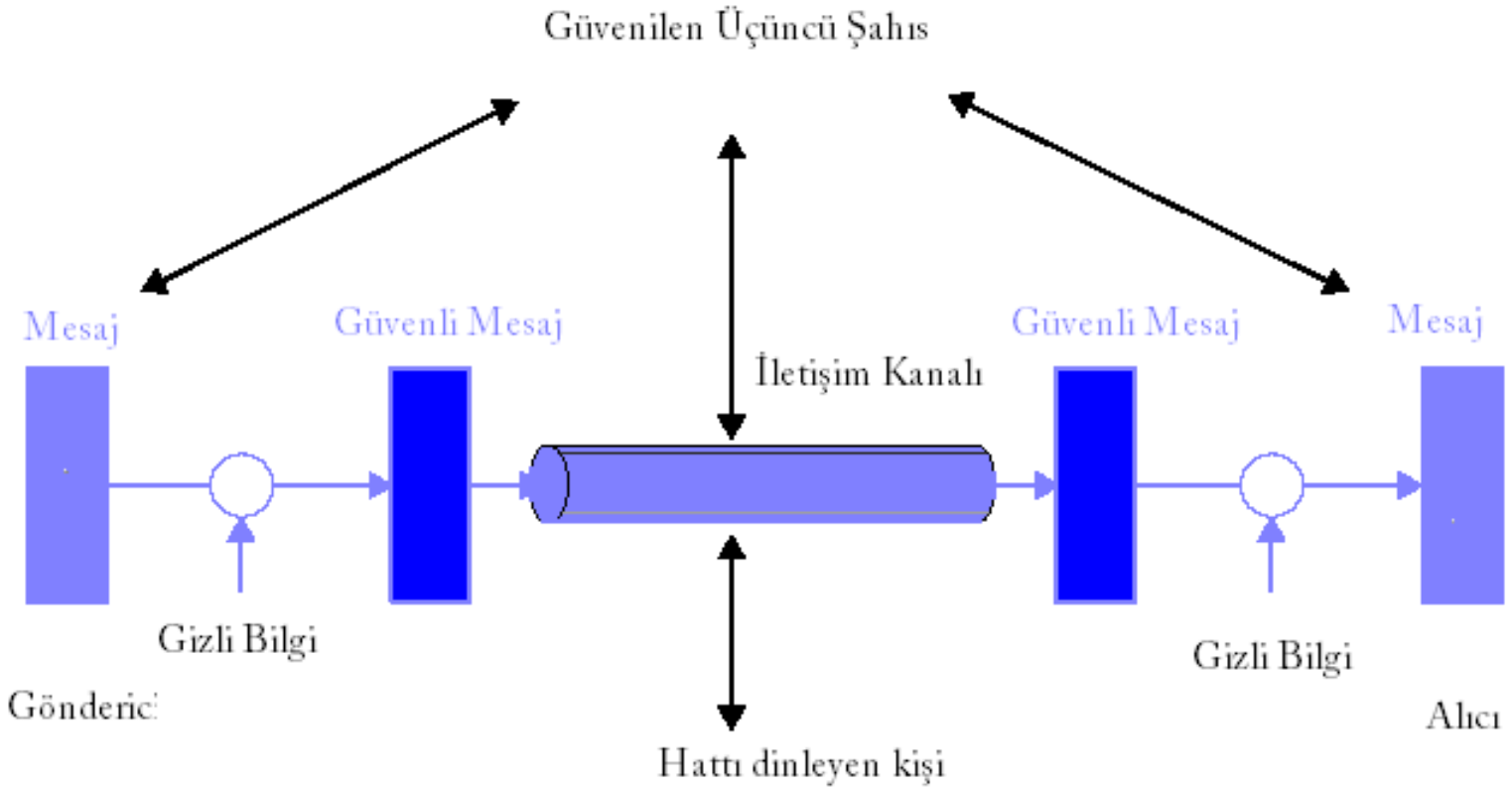
Ağ Güvenliği

- Ağ güvenliğini sağlayabilmek için hem ağdaki bilgisayarların hem de ağın güvenliği sağlanmak zorundadır.
  - Bilgisayar Güvenliği, veriyi korumak ve saldırganları (hacker) engellemek için alınacak tedbirlerin tümünü içerir.
  - Ağ Güvenliği ise iletişimin güvenliği ile ilgilenir.

Ağ Güvenliği

- Ağ güvenliği çözümlerini kriptografik ve 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 Güvenliği İçin Bir Model

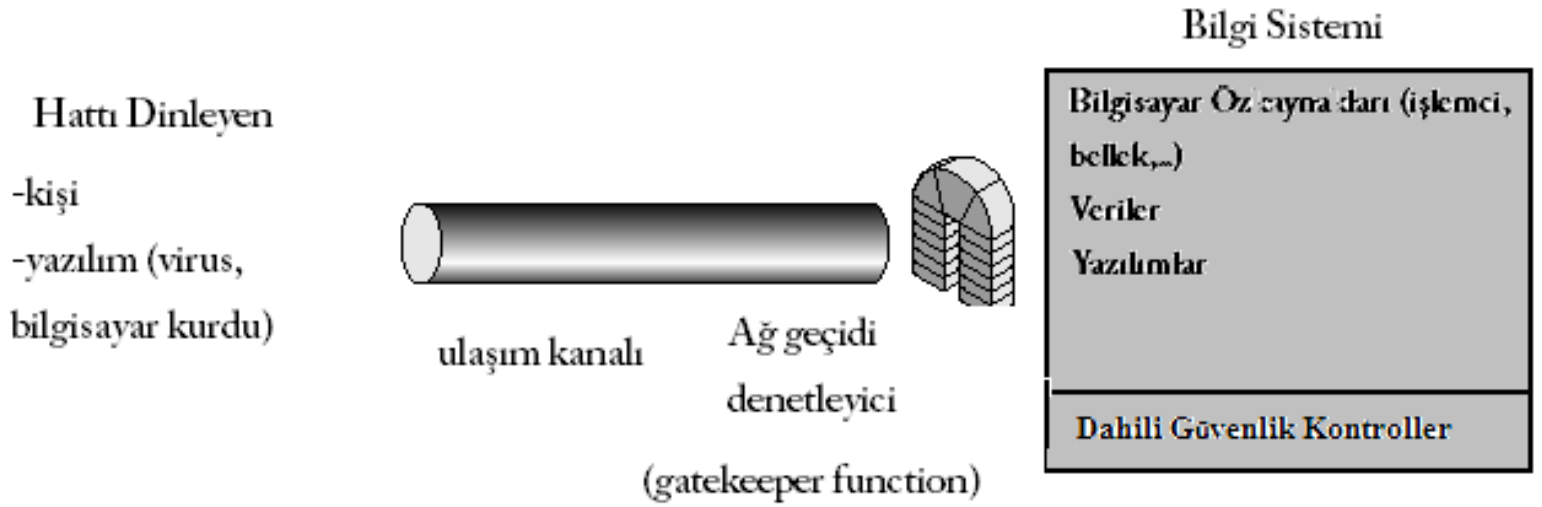


Gönderici ve alıcı mesajları gizli olarak iletirken, güvenli bir üçüncü şahıs gizli bilgilerin dağıtıcısı olarak hizmet vermekte, her iki taraf arasında noter görevi görmektedir.

Ağ Güvenliği İçin Bir Model

- 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

Bilgisayar Güvenliği İçin Bir Model



Bu modeli kullanmak için:

- Kullanıcıları tanıyan uygun bir ağ geçidi denetleyici seçmek
- Dahili Güvenlik Kontrolü uygulaması

Yapmak gereklidir.

Güvenlik Sisteminin Katmanları

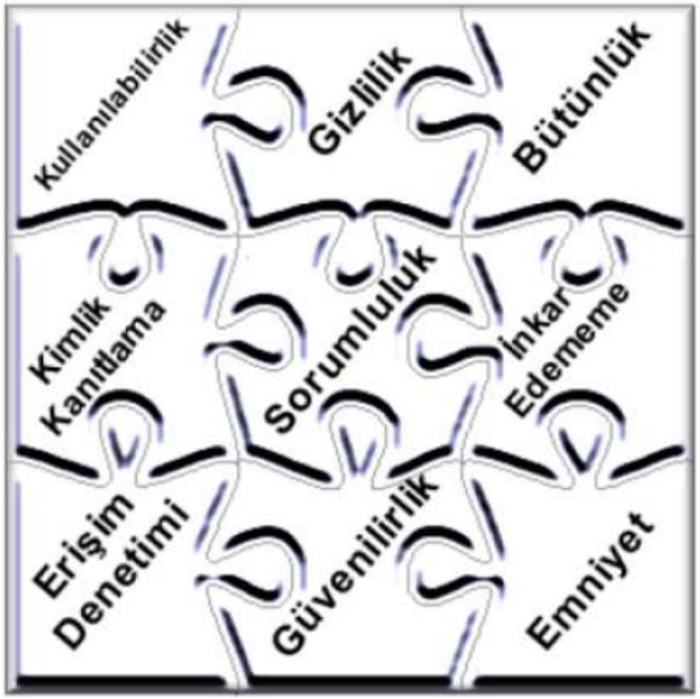
- Ağ güvenliğinde şifreleme yapıtaşı olarak kabul edilmektedir.
- Güvenlik protokolleri şifreleme algoritmalarını kullanarak bazı fonksiyonelliklerin kazanılmasını sağlar.
- Tüm sistemin güvenliği ise, yönetim politikası ve kişilerin eğitimi gibi konuları içerir.

Güvenliğin Önemli Gereksinimleri

- Bilgi güvenliğinin en temel unsurları şunlardır:
  - Gizlilik (confidentiality),
  - Kullanılabilirlik (availability),
  - Kimlik kanıtlama (authentication)
  - Bütünlük (integrity),
  - İnkâr edememe (non-repudiation)
- Bunun dışında
  - Sorumluluk (accountability),
  - Erişim denetimi (access control),
  - Güvenilirlik (reliability) ve
  - Emniyet (safety)

  etkenleri de bilgi güvenliğini destekleyen unsurlardır.

Güvenliğin Önemli Gereksinimleri



- Bu unsurların tamamının gerçekleştirilmesiyle ancak bilgi güvenliği tam olarak sağlanabilecektir.
- Şekilden de görülebileceği gibi, bu unsurların bir veya birkaçının eksikliği, güvenlik boyutunda aksamalara sebebiyet verebilecektir.
- Bu unsurlar birbirini tamamlayıcı unsurlardır.

Güvenliğin Önemli Gereksinimleri

- Gizlilik (confidentiality);
  - Bilginin yalnızca yetkili kişilerin yada bilgiyi kullanan ve yaratan kişi tarafından bilinmesi anlamına gelir.
  - Bu özellik genellikle, şifreleme (encryption) ve anahtar dağıtımı (key distributing) ile ilgili teknikleri gerektirir.

Güvenliğin Önemli Gereksinimleri

- Kullanılabilirlik (availability),
  - Bilginin istenildiği zaman yetkili kişilerce kolayca erişilebilir ve kullanılabilir olmasıdır.
- Kimlik Kanıtlama (authentication),
  - Bilgiyi gönderen ve alan kişilerin gerçekten o kişiler olup olmamasıyla ilgilidir.
  - Bu özellik şifreleme tekniklerine dayanan kişi tanıma ve yetki verme teknikleriyle sağlanmaktadır.

Güvenliğin Önemli Gereksinimleri

- Bütünlük (integrity) ve İnkar Edememe (nonrepudiation),
  - Bütünlük bilginin içeriğinin kötü niyetle yada yanlışlıkla değiştirilip değiştirilmediğiyle ilgilidir.
  - İnkar edememe ise bilgiyi oluşturan yada kullanan kişinin daha sonradan bunu reddedememesidir.
  - Bu gereksinimler şifreleme teknikleri ile sağlanabilir.

Güvenliğin Önemli Gereksinimleri

- Sorumluluk (accountability);
  - Belirli bir eylemin yapılmasından, kimin veya neyin sorumlu olduğunu belirlenmesidir.
- Güvenilirlik (reliability);
  - Bir bilgisayarın, bir bilginin veya iletişim sisteminin şartnamesine, tasarım gereksinimlerine sürekli ve kesin bir şekilde uyarak çalışması ve bunu çok güvenli bir şekilde yapabilmesidir.

Güvenliğin Önemli Gereksinimleri

- Erişim Denetimi (access control);
  - Kaynaklara erişim haklarının tanımlanması, bilgiye yalnızca erişim hakkı olan kullanıcıların ulaşabilmesidir.
  - Bu özellik iyi tanımlanmış erişim hakları ile tanımlanır.
  - Bu işlem için de firewall (ateş duvarı) adı verilen yazılım ve donanımlar kullanılmaktadır.

Güvenliğin Önemli Gereksinimleri

- Emniyet (safety);
  - Bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gömülü olduğunda, kendisi veya gömülü olduğu ortam için istenmeyen potansiyel veya bilfiil tehlike oluşturacak etkinlik veya olayları önleme tedbirlerini içermektedir.

Güvenlik Protokolleri

- Ağ üzerinde iki bilgisayarın karşılıklı veri aktarabilmesi ve ortak süreçler yürütebilmesi için bilgisayarların karşılıklı çalışabilme yeteneğinin olması gerekir.
- Birlikte çalışabilme,verici ve alıcı arasında kullanılacak işaretler,veri formatları ve verinin değerlendirme yöntemi üzerinde anlaşma ile mümkün olur.
- Bunu sağlayan kurallar dizisi de protokol olarak adlandırılır.

Güvenlik Protokolleri

- Katmanlarına göre güvenlik protokolleri şu şekildedir.
  - Uygulama katmanındaki güvenlik protokolleri
    - Kerberos, S/MIME, PGP
  - Ulaşım katmanındaki güvenlik protokolleri
    - SSL, SSH, PCT, TLS
  - İnternet katmanı protokolü
    - IPSec, IKMP

Güvenlik Düzeyleri

- Güvenlik düzeyi, özel bilgilerin saklı olduğu yerde hangi düzeyde korunacağını belirtir.
- Bilgi çeşitli düzeylerde koruma altına alınabilir.

Güvenlik Düzeyleri

- En alt düzeyi veri kaydı alanları düzeyinde koruma altına almaktır
  - Örneğin bir veritabanına ait veri kaydının belirli alanları şifrelenerek o bilgilere erişilmesi denetim altına alınabilir.
  - Böylece koruma altına alınmış olan alanlara yalnızca erişim hakkı olan yada oraya erişmek için şifre anahtarına sahip olan kullanıcılar erişebilir.
- Bu koruma düzeyinin bir üstü veri kaydının bir kısmının değil tamamının korunmasıdır.
- Daha sonra diğer güvenlik düzeyleri gelmektedir.

Güvenlik Düzeyleri

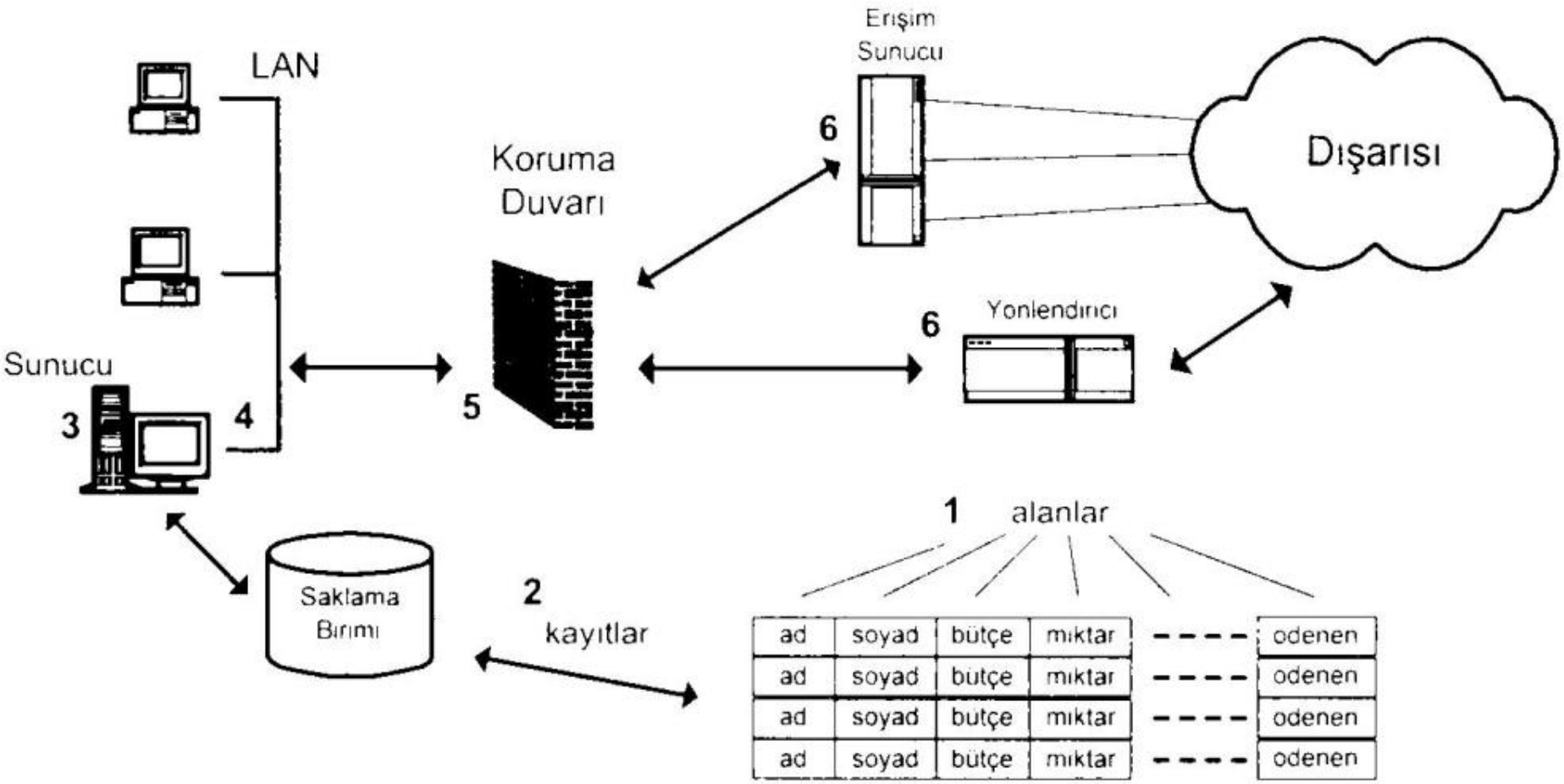
- Güvenlik düzeyleri 6'ya ayrılabilir.Bunlar:
  1. **Kayıt alanı düzeyinde koruma**
  2. **Veri kayıdı düzeyinde koruma**
  3. **Uygulama programı düzeyinde sorgulama/koruma**
  4. **Bilgisayara bağlanmayı sorgulama**
  5. **Ağ kaynaklarını hizmet türleri açısından koruma**
  6. **Ağa girişi sorgulama/koruma**

Güvenlik Düzeyleri

- **1** ve **2** numaralı düzeyler en sıkı korumayı sağlar, iyi bir şifreleme ve şifre anahtarı üretme algoritması kullanılmalıdır.
- **3** ve **4** numaralı düzeyler birbirine benzemektedir. Biri ilgili uygulama programına girişi, diğeri bilgisayar sistemine girişi denetler.

Güvenlik Düzeyleri

- **5** ve **6** numaralı düzeyler genel olarak ağa dışarıdan bağlanmayı ve ağ üzerinde sunulan hizmetlere erişimi denetler, bu güvenlik düzeyleri genel olarak koruma duvarları (firewall) tarafından sağlanır.
  - Örneğin internete eklenen bir LAN'ın **6, 5** ve **4** numaralı düzeylerde korunması için bir güvenlik duvarı kurulabilir.



Güvenlik Düzeyleri

Güvenlik Gerekleri ve Korunacak Varlıklar

- Bilgisayar ağları, insanların bilgiye kolay ulaşımı, dolayısıyla çalışmalarındaki verimin artmasını sağlayan büyük bilgi ağlarıdır.
- Bilgiye kolay ulaşım için sunulan hizmetler (servisler, http, ftp, vs) aynı zamanda zarar verebilme riski de taşımaktadır.
- Bilgisayar ağlarının sunduğu imkanlardan faydalanmak, fakat gelebilecek zararları da en aza indirmek gerekmektedir.
- Ancak bu tedbir bazı şeylerden ödün vermemizi gerektirir.
- Güvenliği ön plana almak hızı da aynı oranda azaltmak anlamına gelmektedir.

Korunacak Varlıklar

- Bir ağda güvenlik ile ilgili bir çalışma yapılmaya başlandığında ilk karar verilmesi gereken nelerin korunması gerektiğidir.
- Korunması gereken varlıklar üç ayrı başlık altında toplanabilir
  - Veriler
  - Kaynaklar
  - Saygınlık

Korunacak Varlıklar - Veriler

- Veriler güvenlik ile ilgili olarak üç özelliğe sahip olmalıdır.
  - Gizlilik: Verilerin başkaları tarafından öğrenilmesi istenmeyebilir.
  - Bütünlük: Sahip olunan verilerin başkası tarafından değiştirilmemesi istenebilir.
  - Kullanıma Hazırlık: Verilerin istendiği zaman ulaşılabilir olup kullanıma hazır olması istenir.

Korunacak Varlıklar - Veriler

- Daha çok gizlilik ile ilgili güvenlik üzerinde durulmaktadır.
- Gerçekten de bu konuda risk çoktur.
- Bazı kişi yada kuruluşlar bilgisayarlarında bulunan gizli bilgilerin güvenliğini sağlamak amacıyla bilgisayarların internet bağlantılarını kaldırmaktadırlar.
- Ama bu durumda da kolay ulaşılabilirlik ortadan kalkmış olacaktır.

Korunacak Varlıklar - Kaynaklar

- Halka açık olan ağlara (internet) bağlanmak ile riske atılacak ikinci şey bilgisayar kaynaklarıdır.
- Başka insanların bir kuruluşa ait sabit diskte yer alan boş alanlarının yada diğer sistem kaynaklarının (işlemci, bellek vb…) başkaları tarafından kullanılması kabul edilebilir değildir.

Korunacak Varlıklar - Saygınlık

- Her kişi yada kurumun saygınlığını ağ üzerinde de koruması önemlidir.
- Meydana gelebilecek güvenlik problemleri kişi ve kurumların doğrudan aleyhine olup kötü reklam olacaktır.
- Ağ üzerinde işlemler yapan bir kişinin başka bir kişinin adını kullandığı düşünülürse herhangi bir zarar verme durumunda adı kullanılan kişi zor durumda kalacaktır ve saygınlığını kaybedecektir.

Korunacak Varlıklar - Saygınlık

- Halka açık ağlara açılmayı düşünen kurumların eğitim ya da güvenlik politikası içinde saygınlığını koruması için kişilere düşen güvenlik tedbirlerinin anlatılması gereklidir.
- Ayrıca periyodik olarak takibinin yapılması şarttır.

Bilgisayar Ağına Saldırı

- İnternetin ve teknolojinin gelişmesiyle birlikte kişilerin önemli bilgilerini kötü niyetli kişilerden korumaları gerekmektedir.
- Kişilerin ve kurumların çeşitli güvenlik mekanizmaları ile bunu sağlamaları gerekmektedir.

Saldırganlar

- Saldırgan (Hacker), ağ üzerinde genelde bazı servisler veren makinelere hiçbir hakkı yokken erişip zarar veren kişi olarak tanımlanmaktadır.
- Genellikle sistemin bilinen açıklarından ve sistem yöneticisinin bilgisizliğinden faydalanarak bilgi hırsızlığı yapmaktadırlar.

Saldırganlar

- İstatistiki raporlara göre saldırıların çoğunun firma içerisinden yapıldığı tespit edilmiştir.
- İçeriden gelen saldırı sistem sadece dışarıdan korumalıysa çok zarar verici olabilmektedir.
- Saldırılar genellikle eğlence, kendini göstermek ya da sisteme zarar vermek amacıyla yapılmaktadır.
- Saldırganlar kötü niyetli saldırganlar ve kötü niyetli olmayan saldırganlar olmak üzere ikiye ayrılırlar.

Saldırganlar

- Kötü niyetli saldırganlar sisteme gerçekten zarar vermek amacıyla girerler. Açığını buldukları sisteme verebilecekleri en büyük zararı verirler. Genellikle ekip halinde çalışırlar. Bilgisayar korsanları, casuslar, teröristler ve profesyonel suçlular bu gruba girmektedir.
- Kötü niyetli olmayan saldırganlar ise genelde meraklı olarak adlandırılırlar ve eğlence amacıyla saldırıda bulunurlar.

Saldırganlar

Saldırganlar	Araçlar	Erişim	Sonuç	Amaç
Bilgisayar korsanları	Kullanıcı komutları	Gerçekleme zayıflıkları	Bilgi bozma	Finansal kazanç
Casuslar	Komut dosyası veya Program	Tasarım zayıflıkları	Bilgi çalma ya da açığa bilgi çıkartma	Politik kazanç
Teröristler	Araç takımı	Yapılandırma zayıflıkları	Hizmet çalma	Sosyal statüye meydan okuma
Meraklılar	Dağıtık araçlar	İzinsiz erişim	Hizmet önleme	Zevk için
Profesyonel suçlular	Veri dinleyici sistemler			

Saldırganlar ve amaçları

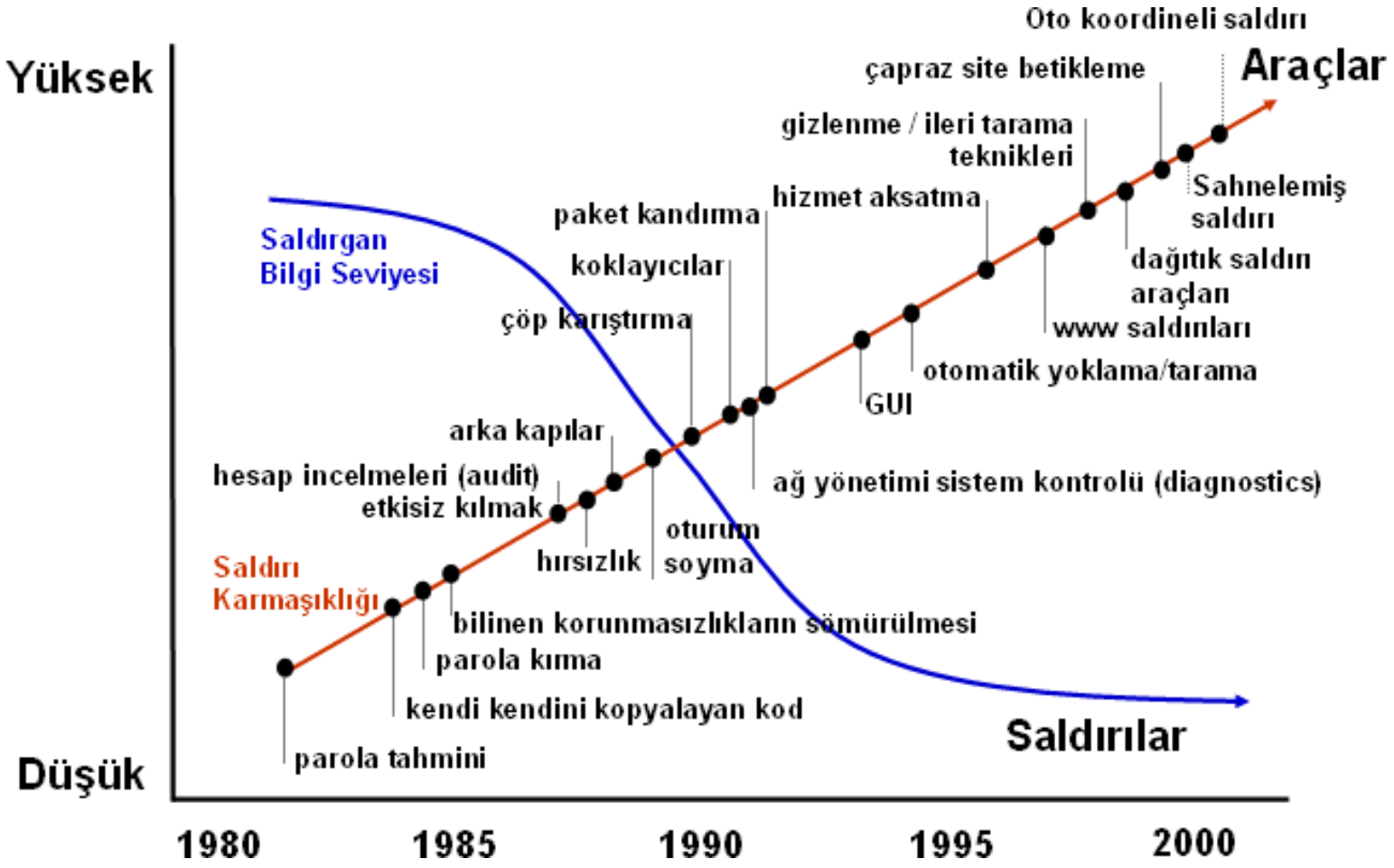
Saldırganlar

- Saldırganların sahip olduğu veya olması gereken teknik bilgi seviyesi ve yaptıkları saldırıların boyutları da zamanla değişim göstermektedir.
- Saldırılar zamanla ve gelişen teknoloji ile oldukça farklılıklar göstermektedir.

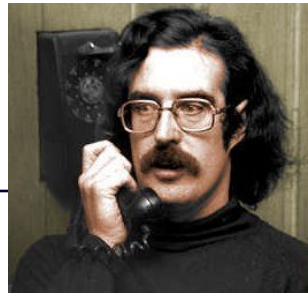
Saldırganlar

- Parola tahmin etme ya da işyerlerinde kağıt notların atıldığı çöpleri karıştırma gibi basit saldırılar, günümüzde artık yerini daha kapsamlı olan çapraz site betikleme (cross site scripting), oto koordineli (auto coordinated), dağıtık (distributed) ve sahnelenmiş (staged) saldırılara bırakmıştır.
- Saldırılar veya saldırılarda kullanılan araçlar teknik açıdan gittikçe karmaşıklaşırken, saldırıları yürütecek saldırganın ihtiyaç duyduğu bilginin seviyesi de gittikçe azalmaktadır.
- Bu durum saldırı ve saldırgan sayısını, saldırılar sonucunda oluşacak zararları artırırken, saldırıyı önlemek için yapılması gerekenleri de zorlaştırmaktadır.

Saldırı karmaşıklığı ve Saldırganın Teknik Bilgisi

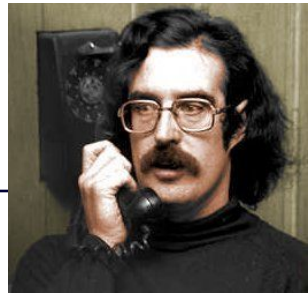


En Kötü Şöhrete Sahip Bilgisayar Korsanları



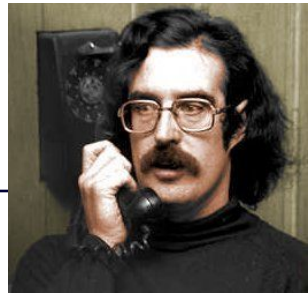
- John Draper:
  - 'Bilgisayar Korsanı' terimiyle anılabilecek olan ilk insanlardan birisidir.
  - 1970'li yıllarda John Draper, 'Cap'n Crunch' mısır gevreği kutusundan çıkan bir oyuncak düdüğü kullanarak, telefon hatlarını kırmayı başarmış ve sayısız telefon görüşmesi yapmıştır.
  - John Draper 1972 yılında, telefon şirketinin oldukça garip olan faturalarını incelemesi üzerine, yakalanmış ve 2 ay hapis cezasına çarptırılmıştır.

En Kötü Şöhrete Sahip Bilgisayar Korsanları



- John Draper:
  - 'Bilgisayar Korsanı' terimiyle anılabilecek olan ilk insanlardan birisidir.
  - 1970'li yıllarda John Draper, 'Cap'n Crunch' mısır gevreği kutusundan çıkan bir oyuncak düdüğü kullanarak, telefon hatlarını kırmayı başarmış ve sayısız telefon görüşmesi yapmıştır.
  - John Draper 1972 yılında, telefon şirketinin oldukça garip olan faturalarını incelemesi üzerine, yakalanmış ve 2 ay hapis cezasına çarptırılmıştır.

En Kötü Şöhrete Sahip Bilgisayar Korsanları



- John Draper:
  - 'Bilgisayar Korsanı' terimiyle anılabilecek olan ilk insanlardan birisidir.
  - 1970'li yıllarda John Draper, 'Cap'n Crunch' mısır gevreği kutusundan çıkan bir oyuncak düdüğü kullanarak, telefon hatlarını kırmayı başarmış ve sayısız telefon görüşmesi yapmıştır.
  - John Draper 1972 yılında, telefon şirketinin oldukça garip olan faturalarını incelemesi üzerine, yakalanmış ve 2 ay hapis cezasına çarptırılmıştır.

En Kötü Şöhrete Sahip Bilgisayar Korsanları


Kevin Mitnick

- Kevin Mitnick:
  - Her ne kadar Kevin Mitnick, bilgisayar korsancılığı radarına 1981 yılında (Daha 17 yaşındayken) girmiş olsa da, 1983 senesine kadar çok önemli bir suç işlemeyip, dikkatleri üzerine çekmemiştir.
  - Kevin Mitnick, USC (University of South Carolina / Güney Carolina Üniversitesi)'nde öğrenim görürken, ARPANet sistemine giriş yapabildi. ARPANet sistemine girebilmesi Kevin Mitnick'e, Pentagon'un ve Savunma Departmanı'nın tüm gizli dosyalarına erişebilme imkanı sağladı. Kevin Mitnick, burada bulunan verilerin hiç birisini çalmadı. Bu, onun için bir şöhret meselesiydi. Sistem yöneticileri olayların farkına varınca, Kevin Mitnick USC kampüsünde tutuklandı ve çocuk ıslahevinde, kısa süreli bir ceza süreci yaşadı.
  - Kevin Mitnick'in işlediğine karar verilen suçlardan ilki, yasal olmayan bir şekilde bir bilgisayar sistemine giriş yapmaktı. Bu olay ise, onun ikinci defa tutuklanmasına neden oldu.
  - Fakat iki defa tutuklanmasına rağmen Kevin Mitnick, sürekli olarak kendini FBI'ın radarında tutmaya devam etti ve o zamandan bu yana, bir çok soruşturma, dava ve tutuklama olayının baş aktörü olmaya devam etti.

En Kötü Şöhrete Sahip Bilgisayar Korsanları


Robert Morris

- **Robert Morris** :
  - 23 yaşındaki Cornell mezunu Robert Morris, 1988 yılında daha sonraları 'Morris Worm' (Morris Solucanı) adıyla anılmaya başlanan ve 99 satırdan oluşan bir kodlama yazmıştı.
  - Bu kodlama, tüm ülkedeki bilgisayarlara bulaşıp yayılarak, bilgisayarların tamamen çökmesine neden olmuştu.
  - Robert Morris, kendisinin yazdığı bu kodun orijinal amacının, o anda internete bağlı olan bilgisayarları sayarak, internetin tahmini genişliğinin belirlenmesi olduğunu söylemişti.
  - Robert Morris 1989 yılında tutuklandıktan sonra, 1986 yılında yürürlüğe girmiş olan 'Bilgisayar Dolandırıcılığı ve Suiistimal Eylemi' suçuyla yargılanan ilk kişi oldu.
  - Robert Morris bu suçla yargılandıktan sonra, şartlı olarak tahliye edildi, kamu hizmeti cezasına ve 10.000 dolarlık bir para cezasına çarptırıldı.

En Kötü Şöhrete Sahip Bilgisayar Korsanları


Kevin Poulsen

- **Kevin Poulsen**:
  - 24 yaşındaki Kevin Poulsen, 1989 yılında bilgisayar ve telefon sunucularına izinsiz giriş yapmaktan tutuklandığı zaman, zaten belli bir süredir FBI'ın takip ettiği bir bilgisayar korsanıydı.
  - Los Angeles'taki bir radyo istasyonu olan 'KISS-FM', bir telefon bağlantısı yarışması düzenlemişti.
    - Bu yarışma sonucunda radyo istasyonu, telefonla programa bağlanan 102. kişiye bir 'Porsche 944-S2' marka araba hediye edecekti.
    - Kevin Poulsen ise, radyo istasyonunun telefon santrali hatlarının kontrolünü eline geçirerek, tüm gelen aramaları bloke etmeye başladı.
    - Bu sayede kendisinin, programa bağlanan 102. kişi olmasını garantileyerek araba ödülünü kazandı.
  - Kevin Poulsen, ismi açıklanmayan bir kişinin verdiği bilgiler sayesinde, 1991 yılında Los Angeles'ta bulunan bir süper markette yakalanarak tutuklanmıştır.

En Kötü Şöhrete Sahip Bilgisayar Korsanları


Vladimir Levin

- **Vladimir Levin**:
  - Vladimir Levin, CitiBank'ın analog kablo transfer ağına gizli bir şekilde giriş yaparak, birkaç tane büyük kurumsal banka hesabının, kullanıcı adını ve şifrelerini ele geçirmeyi başarabildi.
  - Vladimir Levin daha sonra, Amerika'da, Finlandiya'da, Hollanda'da, İsrail'de ve Almanya'da bulunan diğer banka hesaplarına, CitiBank'ın hesaplarından 10.7 milyon dolarlık bir para transferi yaptı.
  - Vladimir Levin daha sonra, 1997 yılında Amerika'ya iade edildi ve Amerika'da, üç yıllık bir hapis cezasına çarptırıldı. Ayrıca CitiBank'a, tazminat ödemesine karar verildi.

En Kötü Şöhrete Sahip Bilgisayar Korsanları


David Smith

- **David Smith**:
  - Dünya'ya bir virüsü yaymaya çalışan ilk bilgisayar korsanıdır.
  - 1999 yılında Davis Smith isimli bir bilgisayar korsanı, 'Melissa Solucanı' isimli bir virüsü Amerika'nın New Jersey eyaletinde bulunan bir bilgisayardan, çalınmış bir 'AOL' hesabını kullanarak serbest bıraktı. Bu solucan otomatik olarak kendini, kullanıcının 'Outlook' adres defterinde bulunan, ilk 50 kişiye yollamaya başladı.
  - Bu solucan, tüm Dünya çapında 300'ün üstünde büyük firmayı etkiledi. Etkilenen bu firmalar arasında 'Microsoft, Intel ve Lucent Technologies' gibi firmalar da bulunuyordu. Bu solucan, neden olduğu aşırı e-posta trafiği ve bu e-postaların kapladığı geniş yerlerden dolayı, bu büyük firmaların tüm e-posta veri yollarını kapamak zorunda kalmalarına neden oldu. Bu da yaklaşık olarak, 80 milyon dolara ulaşan bir finansal zarara neden oldu.
  - David Smith mahkemede suçlu bulunduktan sonra, hapis cezasına çarptırıldı.
  - Fakat David Smith, yeni yayınlanmaya başlayan virüsleri ve bu virüsleri yazan kişileri bulması için FBI'a gizli olarak yardım etmeye karar verdiği zaman, çarptırıldığı hapis cezası 20 aylık bir süreye düşürüldü.

En Kötü Şöhrete Sahip Bilgisayar Korsanları

- **Jonathan James**:
  - 1999 yılında 15 yaşında olan Jonathan James, Alabama'da bulunan Marshall Uzay Uçuş Merkezi'nden (Marshall Space Flight Center) çalınmış olan bir şifrenin yardımıyla, NASA'nın bilgisayarlarına gizli bir şekilde giriş yapmayı başarmıştır. Değeri 1.7 milyon dolar olan kaynak kodları ele geçirmiştir.
  - Bunun sonucunda ise NASA, 1999 yılının Temmuz ayında birkaç hafta boyunca, tüm bilgisayar ağını kapatmak zorunda kalmıştır.
  - Yargılandığı zaman 16 yaşına girmiş olan Jonathan James; 6 aylık bir hapis cezasına çarptırılmış ve 18 yaşına girene kadar, şartlı tahliye halinde gözetim altında tutulmuştur.

En Kötü Şöhrete Sahip Bilgisayar Korsanları

- **Mike Calce**:
  - 2000 yılının Şubat ayında Mike Calce, içlerinde Amazon, eBay, E*TRADE ve Dell gibi büyük firmaların bulunduğu, 11'den fazla önemli web şirketini derinden etkileyen, bir hizmet dışı bırakma saldırısı başlatmıştır.
  - Mike Calce bu saldırıyı, 52 farklı ağda bulunan 75 tane bilgisayarı kullanarak başlatmıştır.
  - Bu saldırının, 1.7 milyar Kanada doları (Yaklaşık olarak 1.6 milyar Amerikan doları) değerinde bir parasal zarara neden olduğu tahmin edilmektedir.
  - 2001 yılında mahkemede yargılanan Mike Calce, 8 ay boyunca tutuksuz gözaltında tutulma, sınırlı internet kullanımı, küçük miktarda bir para cezası ve bir yıl süreyle şartlı tahliye takibi cezasına çarptırılmıştır.

Saldırı Türleri ve Saldırıların Sınıflandırılması

- Saldırganlar sisteme ağ üzerinden ulaşabilecekleri için ağa bağlı cihazlar her zaman saldırıya açık durumdadır.
- Saldırganın yapacakları hedef makinaya ulaşmak, yazılım ve/veya donanıma zarar vermek şeklinde olabilir.
- Saldırgan istediği verileri alabilir yada kullanılamaz hale getirebilir.
- Bilgisayar ve ağ saldırıları için çeşitli sınıflandırmalar yapılmıştır.

Süreçsel Sınıflandırma

- Internet'te gerçekleştirilen veri transferi ile ilgili güvenlik sorunları dört kategoriye sokulabilir.
  - Engelleme
  - Dinleme
  - Değiştirme
  - Oluşturma (üretim)

Süreçsel Sınıflandırma

- Engelleme:
  - Sistemin bir kaynağı yok edilir veya kullanılamaz hale getirilir.
  - Donanımın bir kısmının bozulması, iletişim hattının kesilmesi veya dosya yönetim sisteminin kapatılması gibi….
- Dinleme:
  - İzin verilmemiş bir taraf bir kaynağa erişim elde eder.
  - Yetkisiz taraf, bir şahıs, bir program veya bir bilgisayar olabilir.
  - Ağdaki veriyi veya dosyaların kopyasını alabilir.

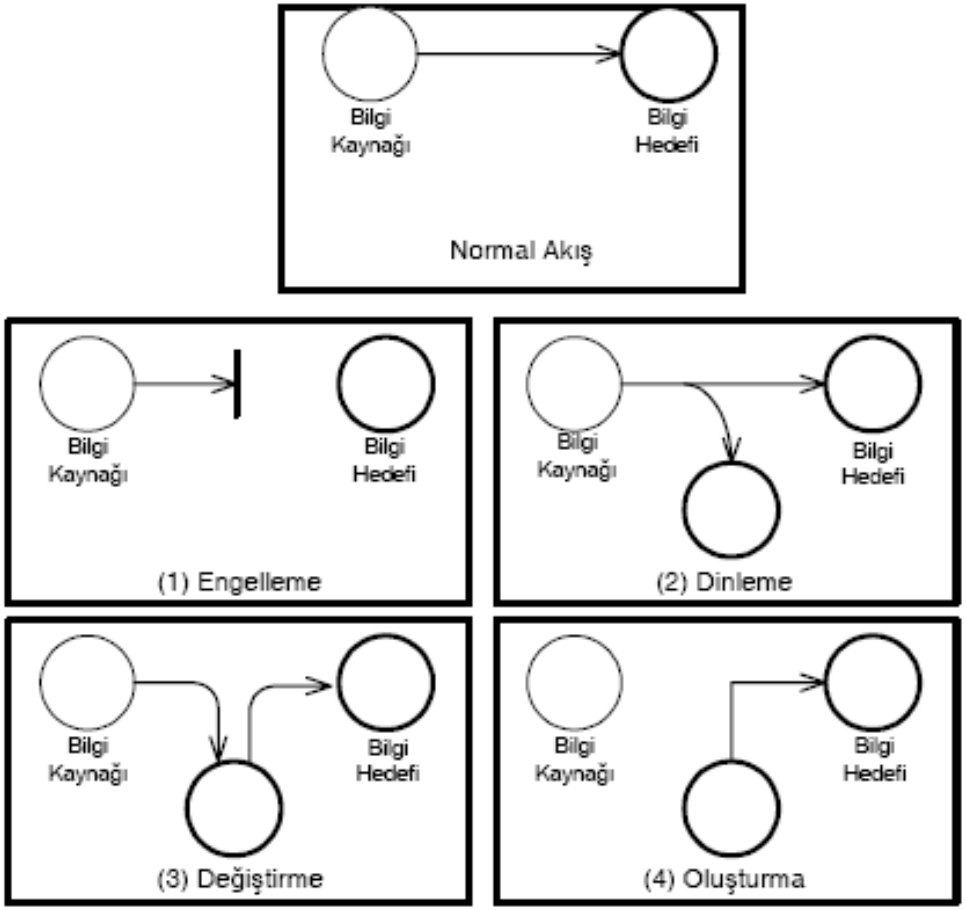
Süreçsel Sınıflandırma

- Değiştirme:
  - İzin verilmemiş bir taraf bir kaynağa erişmenin yanı sıra üzerinde değişiklikte yapar.
  - Bir veri dosyasının değiştirilmesi, ağdaki bir mesajın değiştirilmesi gibi…..
- Oluşturma (üretim):
  - İzin verilmemiş bir taraf , sisteme yeni nesneler ekler.
  - Ağ üzerinde sahte mesaj yollanması veya bir dosyaya ilave kayıt eklenmesi gibi….

Süreçsel Sınıflandırma

- Dinleme pasif bir saldırı türü olarak kabul edilmektedir.
- Engelleme, değiştirme ve oluşturma ise etkin(aktif) bir saldırı türü olarak görülmektedir.

Süreçsel Sınıflandırma

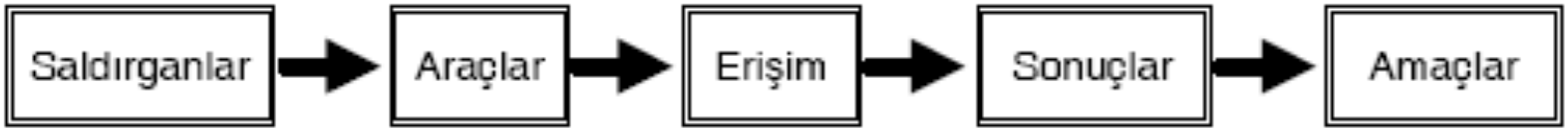


Süreçsel Sınıflandırma

Saldırı	Hedef Güvenlik Unsuru	Yaklaşımlar	Çözüm
Yarıda kesme (interruption)	kullanılabilirlik (availability)	• Donanım yıkımı • İletişim hatlarına fiziksel hasar verme • Gürültü yayma • Rota (routing) şaşırtma • Program ve dosya silimi • DoS (hizmet aksattırma) saldırıları	Etkin bir çözüm yok.
Gizli dinleme (intercept)	gizlilik (confidentiality) ve kişisel gizlilik (privacy)	• Gizli dinleme (Eavesdropping) • Hat izleme • Paket yakalama • Sistemle uzlaşma	Şifreleme/şifre çözme
Değiştirme (modification)	bütünlük (integrity)	• Veritabanı kayıtlarını değiştirme • İletişimde gecikmelerden yararlanma • Donanımda değişiklik yapma	Her bir mesaj paketi için sayısal imza kullanımı
İmalat veya üretim (fabrication)	asıllık (authenticity)	• Veritabanına yeni kayıt ekleme • IP kandırma ile yeni ağ paketi ekleme • Sahte e-posta veya bölge adları kullanma	Kimlik kanıtlama (authentication)

İşlemsel Sınıflandırma

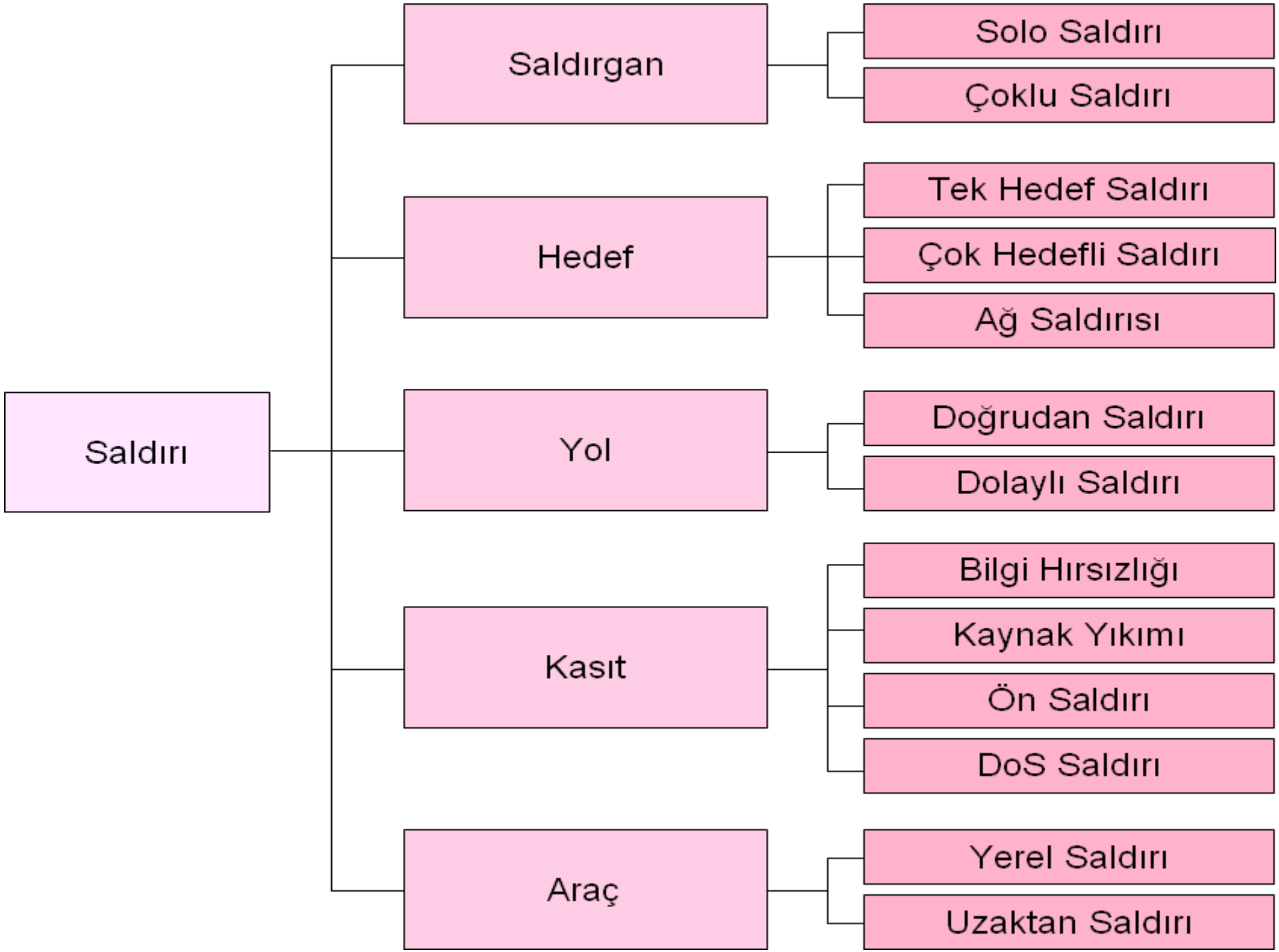
- Genel anlamda bir saldırı; yöntemler, kullanılan yollar ve sonuçları açısından düşünülebilir.
- Bilgisayar ya da bilgisayar ağına saldıran kişi, istediği sonuçlara çeşitli adımlardan geçerek ulaşmak zorundadır.



Saldırıların Gruplandırılması

- Saldırılar;
  - Saldırıda kullanılan yöntem
  - Saldırganın kullandığı yöntem
  - Saldırının amaçladığı uygulamalar
  - Saldırı sonucunda oluşan zararlar

  Açısından değişik şekillerde gruplanabilir.


Saldırı
Saldırgan
Solo Saldırı
Çoklu Saldırı
Hedef
Tek Hedef Saldırı
Çok Hedefli Saldırı
Ağ Saldırısı
Yol
Doğrudan Saldırı
Dolaylı Saldırı
Kasıt
Bilgi Hırsızlığı
Kaynak Yıkımı
Ön Saldırı
DoS Saldırı
Araç
Yerel Saldırı
Uzaktan Saldırı

1. CERT Gruplandırması

- Computer Emergency Responce Team (CERT) tarafından yapılmış olan saldırı türleri ve gruplandırması ve açıklamaları şu şekildedir.

Probe,Scan,Scam	Bir sistemdeki açık ve kullanılan portların taranması ve bu portlardan hizmetlere yönelik saldırıları türüdür.
Prank	Kullanıcı hesaplarının yanlış oluşturulması sonucu oluşan açıklardan yapılan saldırı türleridir.
Email spoofing	Başka bir kullanıcı adına e-posta gönderilmesi...
Email bombardment	Bir e-posta adresine genelde farklı adresten çok sayıda e-posta gönderilmesi
Sendmail attack	Smtp portuna yönelik saldırılardır...
Break-in	Verilen hizmetlerin devre dışı bırakılmasına yönelik saldırı türüdür.
Intruder gained root access	Saldırganın normal kullanıcı olarak girdiği sistemde süper kullanıcı yetkisini kazanması.

CERT Gruplandırması

Intruder installed trojan horse program	Saldırganın girdiği sisteme genelde daha sonra tekrar rahat girebilmesi ya da uzaktan yönetim için ajan program yerleştirimesi.
Intruder installed packed sniffer	Saldırgan tarafından hedef makinaya yönelik paket dinleyici yerleştirilerek yapılan saldırı türüdür. Bu şekilde bir yerel ağ korumasız bir konak üzerinden saldırılara açık hale gelebilir.
NIS attack	Ağ kullanıcı yönetim sistemine yönelik saldırı türüdür.
NFS attack	Ağ dosya yapısına yönelik saldırı türüdür. Genellikle ağ erişimini devre dışı bırakmada kullanılır.
Telnet attack	Uzaktan erişim protokolünün açıklarından faydalanılarak yapılan saldırı türüdür.
Rlogin or rsh attack	Uzaktan erişimde kullanılan servislerin açıklarına yönelik yapılan saldırı türüdür.
Cracked password	Kolay tahmin edilebilir parolaların tahmini ya da şifreli hallerine göre sözlük saldırısı yapma türüdür.

CERT Gruplandırması

Anoymous FTP abuse	Anonim erişim izni verilen dosya aktarım sunucularına yönelik saldırılardır.
IP spoofing	IP adres yanıltmasıyla yapılan saldırı türüdür.
Configuration error	Çok kullanılan programdaki kullanıcılardan kaynaklanan konfigürasyon hatalarından doğan açıklıklardır.
Misuse of hosts resources	Konak kaynaklarının yanlış kullanımı sonucu ortaya çıkan açıklıklar.
Worm,Virus	Konaklarda kullanıcılardan habersiz çalışan zararlı programlar.

2.İletişim Protokollerini Kullanan Saldırılar

- IP sahteciliği (IP Spoofing)
- TCP dizi numarası saldırısı (TCP sequence number attack)
- ICMP atakları
- Ölümcül ping
- TCP SYN seli atağı (TCP SYN Flood Atatck)
- IP parçalama saldırısı (IP Fragmentation Attack)
- Internet yönlendirme saldırısı (Internet Routing Attack)
- UDP sahteciliği ve dinleme (UDP Spoofing and Sniffing)
- UDP potunu servis dışı bırakma saldırısı (UDP port Denial of Sevice attack)
- Rastgele port taraması (Random port scanning)
- ARP saldırıları (ARP attacks)
- Ortadaki adam saldırıları

3. IP Saldırıları

- IP V4'te bulunan güvenlik eksikliklerinden faydalanılarak yapılan atak türleridir. Bazıları şunlardır.
  - Out of Band Nuke
  - Land
  - Teardrop
  - Boink
  - Smurf
  - Suffer3 ……

4. İşletim Sistemine Özel Saldırılar

- Exploit olarak isimlendirilen bu saldırılar sistem tabanlı olarak çalışırlar.
- Yani Unix için yapılan bir exploit Windows için çalışmaz.

5. Uygulama Katmanı Saldırıları

- DNS, SMTP, NFS saldırıları
- Uzaktan giriş ile saldırılar
- URL sahteciliği
- Kötü niyetli java ve ActiveX uygulama parçacıklar
- Sistem log seli (güvenlik dosyasına çok sayıda giriş yapılarak log dosyasının dolmasına ve sistemin kapatılmasına neden olur)

İşletim Sistemlerinin Güvenliği

- İşletim sistemleri seçilirken göz önünde bulundurulan özellikler şunlardır:
  - Kurulum kolaylığı
  - Donanım gereksinimleri, sürücü edinebilme
  - Kullanım ve yönetim
  - Güvenilirlik
  - Güvenlik
  - Uyumluluk
  - Fiyat
  - Destek

İşletim Sistemlerinin Güvenliği

- Bu özelliklerden güvenlik, eğer sistemimiz ağa açılacaksa çok büyük önem taşımaktadır.
- İşletim sistemlerinin güvenlikleri için sürekli yeni çalışmalar yapılmakta ve her sürümle güvenlik açıkları kapatılmaya çalışılmaktadır.

Sistem Güvenlik Seviyeleri

- Sistemlerin içerdikleri donanım ve yazılımlara göre güvenlik seviyeleri belirlenmiş ve standartları oluşturulmuştur.
- Güvenlik seviyelerinde çeşitli fiziksel korumalar, işletim sistemini güvenli hale getirme gibi işlemler bulunur.
- 1985 yılında DoD (Department of Defence) tarafından yayınlanan TCSEC Trusted Computer System Evaluation Criteria) yayınında dört güvenlik seviyesi ve alt sınıfları belirtilmiştir.

Sistem Güvenlik Seviyeleri

- **D seviyesi**
  - D1 Seviyesi
    - Mevcut en düşük güvenlik olanaklarını sunar.
    - Bu seviyede bir güvenliğe sahip sistem bütün olarak güvensizdir.
    - Donanım elemanları için herhangi bir koruma mekanizması yoktur.
    - İşletim sistemi kolaylıkla ele geçirilebilir ve istenen amaca uygun bir şekilde kullanılabilir.
    - Sistem kaynaklarına yetkili kişilerin ulaşmasını denetleyecek bir erişim kontrol sistemi yoktur.
    - MS-DOS, MS-Windows 3.1/95/98 ve Apple Macintosh bu sınıftadır.

Sistem Güvenlik Seviyeleri

- **C seviyesi**
  - C1 ve C2 olmak üzere iki alt güvenlik seviyesine ayrılmıştır.
  - Bu seviye güvenlikte kullanıcı için hesap tutma (account) ve izleme (audit) yapılmaktadır.

Sistem Güvenlik Seviyeleri

- C1 seviyesi:
  - Sınırlı bir güvenlik koruması vardır.
  - Daha çok kullanıcı hatalarından sistemi korumak için gerekli tanımlamaları vardır.
  - Dışarıdan gelecek saldırılara karşı koruma mekanizmaları yoktur.
  - Ayrıca donanım için bazı güvenlik mekanizmaları bulunmaktadır. Donanım elemanlarına istenmeyen kişilerin ulaşması zorlaştırılmıştır.
  - Erişim kontrolü kullanıcı adı ve parolasına göre yapılmakta ve hakkı varsa sisteme alınmaktadır.
  - UNIX ve IBM MVS (Multiple Virtual Storage) bu sınıfa örnektir.

Sistem Güvenlik Seviyeleri

- C2 seviyesi:
  - C1 seviyesine göre daha güvenli hale getirilmiştir.
  - Bu seviyede kaynaklara kontrollü erişim sağlanabilmektedir.
  - Yani erişimler için sadece geçerli haklar göz önünde bulundurulmayarak sonradan yapılan yetkilendirilmelerde kontrol edilir.
  - Bunun için de sistemde yapılan her iş için kayıt tutulur.
  - Yapılan işlemlerin kontrol edilmesi ve kayıt edilmesi C1'de ortaya çıkabilen güvenlik problemlerini ortadan kaldırmaktadır.
  - Fakat fazladan yapılan kontrol ve kayıt işlemleri işlemci zamanını harcayacak ve diskten alan alacaktır. Güvenlik arttıkça kaynaklara erişimdeki hız düşecektir.
  - Bu seviyeye örnek sistemler Windows NT 4.0 ve Digital Equipment VAX/VMS 4.x 'tir.

Sistem Güvenlik Seviyeleri

- **B seviyesi**
  - Üç alt güvenlik seviyesine ayrılır.
  - Zorunlu erişim denetimi kullanılır.
  - Sistemdeki her nesnenin güvenlik seviyeleri tanımlanır.

Sistem Güvenlik Seviyeleri

- B1 seviyesi:
  - Çok katmanlı güvenlik yapısı kurulmasını sağlar (gizli, en gizli vb.)
  - Sistemde güvenliği sağlanacak nesnelerin diğerlerinden kesinlikle ayrılması gerekmektedir bu nesneler manyetik ortamlarda saklanır.
  - Bu seviyeye örnek olarak OSF/1, AT&T V/MLS, IBM MVS/ESA sistemleri verilebilir.

Sistem Güvenlik Seviyeleri

- B2 seviyesi:
  - Bu seviyedeki güvenlik için sistemdeki tüm nesnelerin (birimlerin) etkilenmesi gerekir.
  - Disk ile saklama birimleri veya terminaller bir ve ya daha fazla olabilecek güvenlik seviyesi ile ilişkilendirilebilir.
  - Güvenlik düzeyi yüksek bir cihaz ile düşük bir cihazın haberleşmesinde problem çıkacaktır, bunlara dikkat edilmesi ve çözülmesi gereklidir.
  - Bu seviyeye örnek olarak Honeywell Information System'in Multics sistemi ve Trusted XENIX verilebilir.

Sistem Güvenlik Seviyeleri

- B3 seviyesi:
  - Güvenliği donanımların uygun kurulumlarıyla sağlamaya çalışan yöntemi içerir. B2 seviyesine göre daha sağlam ve ciddi bir sistem tasarımı vardır. Güvenlik yönetimi, güvenli kurtarma ve saldırı ya da oluşan zararların sistem yöneticisine bildirilmesi gibi özellikleri içerir.
  - Bu seviyeye örnek olarak Honeywell XTS-200 verilebilir.

Sistem Güvenlik Seviyeleri

- **A seviyesi**
  - A1 tek seviyesini içerir.
  - En üst güvenliği sunan seviyedir.
  - Donanım ve yazılım açısından dizayn, kontrol ve doğrulama işlemlerini içerir.
  - Daha önce bahsedilen güvenlik seviyelerindeki tüm bileşenleri içerir.
  - Bir sistemin dizayn, geliştirme ve gerçekleştirme aşamalarında güvenlik isteklerinin sağlanması beklenir.
  - Her aşamayla ilgili olarak dökümantasyonun da yapılması gerekmektedir.

Sistem Güvenlik Seviyeleri

Güvenlik Seviyesi	Alt Seviye	Özet Bilgi
D	D1	En düşük düzeyde güvenlik
C	C1	İsteğe (kullanıcıya) bağlı güvenlik
	C2	Kontrollü erişim
B	B1	Etiketli güvenlik
	B2	Yapısal güvenlik
	B3	Güvenlik alanlı Koruma
A	A1	En yüksek düzeyde güvenlik