

YMH321 Bilgi Sistemleri ve Güvenliği

Bilgi Sistemleri ve Güvenliği

Bölüm: 1

Prof.Dr. Resul DAŞ
Fırat Üniversitesi, Teknoloji Fakültesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarısı

- Giriş
- Bilişim Suçları
- Bilgi ve Bilgi Güvenliği
- Sonuç
- Sorular
- Kaynaklar

Giriş

- Bilişim dünyasında bilgi ve bilgi varlıklarının öneminin gün geçtikçe artması, buna paralel olarak bilişim güvenliğinin öneminin de artmasını ortaya koymaktadır. Uluslar arası bir ağ sistemi olan internet ortamındaki verilerin veya bilgilerin korunması için donanımsal ve yazılımsal güvenlik tedbirleri alınmaktadır. Ancak, bu tedbirler sisteme veya bilişim cihazlarına yapılan saldırıları tamamen engelleyememektedir. Bu bağlamda bilişim suçlarının incelenmesi, saldırganların tespit edilmesi için birçok akademik ve ticari çalışmalar yapılmaktadır.

Giriş

- Bu bölümde, **bilişim suçları, bilgi ve bilgi güvenliği** konuları genel olarak incelenmiştir. Ayrıca bu konularda bilişim suçlarına örnek teşkil edecek saldırılar belirtilmektedir.

Bilgi ve Bilgi Güvenliği

(.Bilgi, Bilginin Değeri)

- En basit tanımlaması ile **bilgi** kişi ya da kurumlar için kıymet teşkil eden ve para gibi korunması gereken kıymetli bir metadır [25]. Meta ifadesi ile eşya kast edilirken bunun yerine varlık ifadesi de kullanılmaktadır.
- Günümüzde bilgi ön plana çıkışmış gibi gözükse de, aslında **bilgi**; dünün ve bugünün anahtarları iken, geleceğin şekillenmesinde de her zaman anahtar rollere sahiptir.

Bilgi ve Bilgi Güvenliği

(Bilginin Gelişim Evreleri)

- İnsan bilincinden bağımsız olarak var olanlar veya hikmete ulaşmak için veri haline gelmeye hazır doğada bulunan her şey *gerçeklikdir*.
- Bilişim teknolojisi açısından *veri*, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.
- *Bilgi*; verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. Bilgi; işlenmiş veri olarak ve bir konu hakkında var olan belirsizliği azaltan bir kaynak olarak da tanımlanabilmektedir. Kısaca, veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, v.s.) çıktısı, *bilgi* olarak ifade edilebilir.

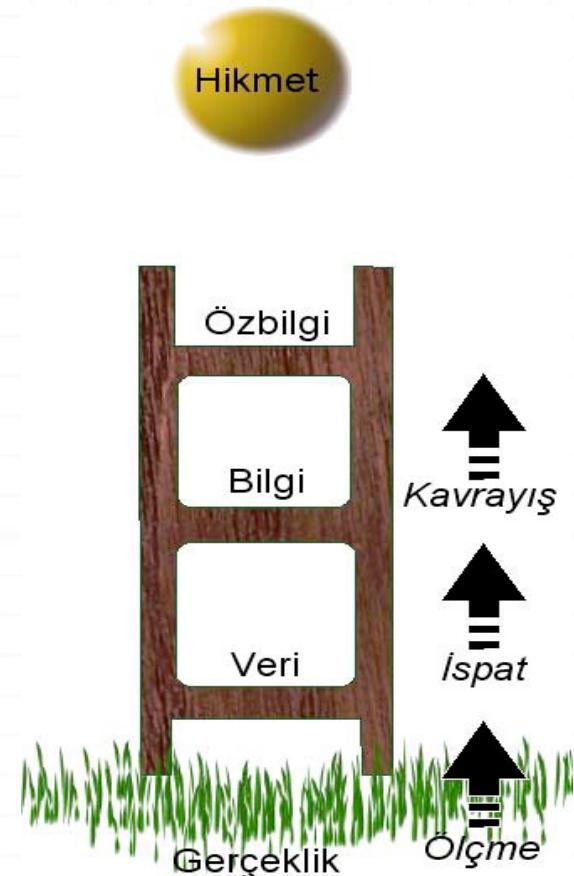
Bilgi ve Bilgi Güvenliği

(Bilginin Gelişim Evreleri)

- *Özbilgi*; tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Verilerin bir araya getirilip, işlenmesi bilgiyi oluştursa da özbilgi, kullanılan bilgilerin toplamından daha üstte bir kavramdır. Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir.

Bilgi ve Bilgi Güvenliği (Bilginin Gelişim Evreleri)

- Hikmet (wisdom), tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür. Hikmet, ayrıca, güvenilir yargıda bulunmak ve karar vermek için özbilginin nasıl kullanılacağını kavramak olarak da tanımlanmaktadır [23].



Bilgi ve Bilgi Güvenliği (Bilgi Güvenliği)

- *Bilgi güvenliği*; bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanır.
- *Bilgi güvenliği*, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür.

Bilgi ve Bilgi Güvenliği (Bilgi Güvenliği)

- Bilgi güvenliğinin sağlanması için kullanılabilecek birçok yöntem olmakla beraber yeni sayılabilenek **biometrik** alanda yapılan bilgi güvenliği çalışmaları da mevcuttur. Bu biometrik korunma yolları arasında parmak izi ile çalışan sistemler, el ve parmakların şekline göre çalışan sistemler, ses tanıma sistemleri, dijital imza, gözün retina ve iris tabakasından yararlanılarak çalışan sistemler mevcuttur. Buna örnek olarak Kuzey Carolina'daki uluslararası havaalanında kullanılan iris ile çalışan güvenlik sistemi örnek olarak gösterilebilir [18].

Bilgi ve Bilgi Güvenliği (Bilgi Güvenliği Sertifikasyonu)

- Büyüklüğü ne olursa olsun, ihtiyaç duyan tüm kurumların, kuruluşların bilgilerinin gizlilik, bütünlük ve erişebilirliklerini sağlamak amacıyla kurdukları bilgi güvenliği yönetim sistemini belgelendirmek ve bunu üçüncü taraflara kanıtlamak amacıyla aldıkları; bağımsız belgelendirme kuruluşlarının, yaptıkları denetim sonucu düzenledikleri ve kurumdaki bilgilerin güvenliklerinin sağlanması yönelik sistematik bir uygulamanın olduğunun kanıtını sağlamak üzere *kurum* adına düzenlenen sertifikaya veya belgeye **TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi** veya **TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Sertifikası** denir.

Bilgi ve Bilgi Güvenliği (Bilgi Güvenliği Sertifikasyonu)

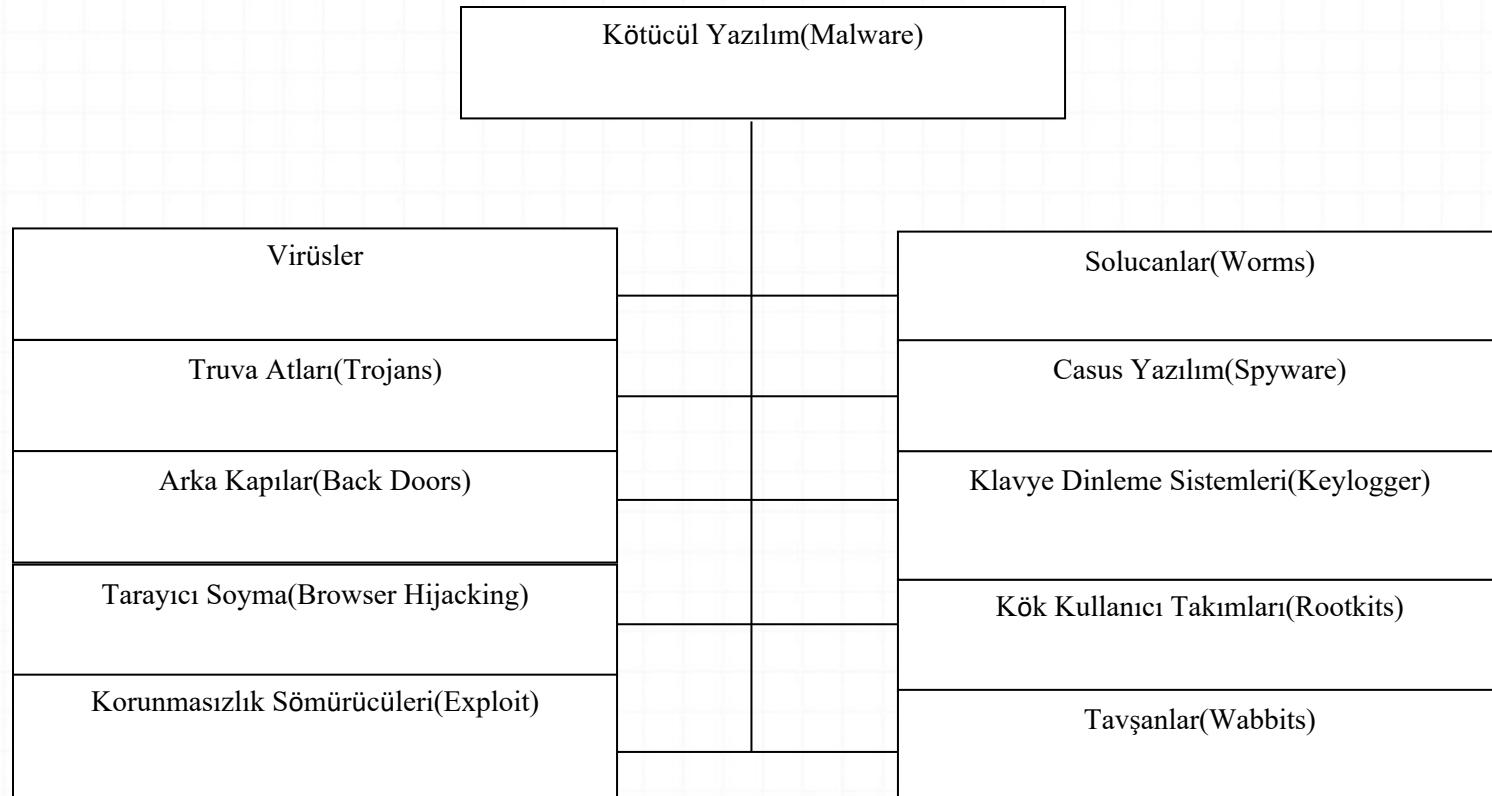
- TS ISO/IEC 27001 bilgi güvenliği yönetim sistemi kurmak ve belgelendirmek bir firmaya, şirkete veya kuruluşa bilgi güvenliği kavramının temel ilkelerini sağlamaktadır. Bilgi güvenliği kavramının temel ilkeleri kısaca G-B-U (C-I-A) kısaltması ile gösterilebilir. Bu kısaltmalar:
 - **Gizliliğin korunması** (bilgiye ulaşımın, sadece yetki sahibi kişilerce olabildiğinin garanti altına alınması)
 - **Bütünlük** (bilginin ve bilgi işleme yöntemlerinin, doğruluğunun ve eksiksizliğinin korunması)
 - **Ulaşılabilirlik** (gerekken durumlarda yetkili personelin, bilgiye ve ilgili varlıklara ulaşabilmesinin garanti edilmesi), şeklinde tanımlanır.

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımlar)

- Kötüçül yazılım (malware, İngilizce “malicious software”in kısaltılmış), bulasıtı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır. Özellikle Türkçe kaynaklı literatür tarandığında 11 adet ana kötüçül yazılımın varlığından bahsedilirken 38 adet yeni kötüçül casus yazılımdan bahsedilmektedir [26].

Bilgi ve Bilgi Güvenliği (Kötüçül Casus Yazılımlar)



Tablo 1. Kötüçül Yazılım Ana Türleri

Bilgi ve Bilgi Güvenliği (Kötüçül Casus Yazılımlar)

VİRÜS İSMİ	TİPİ	KARIŞTIĞI OLAYLAR	YÜZDE
Win32/Ska	File	140	13.28%
Laroux	Macro	124	11.76%
Marker	Macro	122	11.57%
Ethan	Macro	69	6.55%
Class	Macro	59	5.60%
Win32/Pretty	File	52	4.93%
Win32/NewApt	File	48	4.55%
Melissa	Macro	47	4.46%
Tristate	Macro	44	4.17%
Freelinks	Script	42	3.98%
Win32/Babylonia	File	32	3.04%
Cap	Macro	31	2.94%
Win32/Fix	File	31	2.94%
Thus	Macro	29	2.75%
Win32/Explore.Zip	File	21	1.99%
Win95/CIH	File	19	1.80%

Tablo 2. En Meşhur Virüsler

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımlar)

Yeni kötüçül yazılımlardan bir kısmı şunlardır:

- sazan avlama (phishing),
- koklayıcı (sniffer),
- kandırıcı (spoofing),
- şifre kıräciler (password cracker),
- reklâm yazılım(adware),
- ağ taşkını (flooder),

bununla beraber daha birçok yeni kötüçül yazılımın varlığından bahsedilmektedir.[26].

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımların Bulaşma Yöntemleri)

- Çoğunlukla ücretsiz dağıtılan uçtan uça dosya paylaşımı (P2P) programları, ekran koruyucular ve oyunlar içine casus yazılım bohçalanması ile bulaşma,
- Faydalı bir yazılım kurulumunun yanında; dosya, klasör ve sistem kütüğü isimlerini zararsız, bilindik veya sisteme ait isimler vererek saptanmasını ve sistemden kaldırılmasını zorlaştırarak sisteme yerleşme,
- Uç kullanıcı lisans sözleşmelerinde yaniltıcı veya eksik bildirim ile kullanıcıya zararlı bir yazılımı bilgisayarına kurdurtma,

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımların Bulaşma Yöntemleri)

- Herhangi bir programın kurulumu sırasında, aslında casus yazılım özelliği taşıyan başka yardımcı ve ek yazılımların kullanıcıya belirtilerek kurdurulması,
- E-posta dosya eklentisi ile e-posta'da verilen bir web adresine gidildiğinde veya doğrudan HTML içerikli e-postaların okunması ile casus yazılım bulaşması,
- İnternet tarayıcılarında bulunan korunmasızlık ve açıklardan yararlanarak kurulum,
- Özellikle internet üzerinden kullanıcıyı aldatıcı mesajlarla yanıltıp; her hangi bir casus yazılımın kurulumunun başlatılması,

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımların Bulaşma Yöntemleri)

- Çocukları ve bilinçsiz kullanıcıları aldatıcı taktikler kullanmak,
- Çok çeşitli sosyal mühendislik ve insan hatası kaynaklı yöntemler, olarak özetlenebilir.

Bilgi ve Bilgi Güvenliği

(Bilgisayarlarda Kötüçül Yazılımların Belirtileri)

- Bilgisayarın her zamanki başarımı düşüyorsa,
- İnternet üzerinde tarayıcı ile sörf ederken istenmedik siteler açılıyorsa,
- İnternet tarayıcısındaki arama çubuğu bölümünde aranmak istenen anahtar kelime girildiğinde ayarlanmış olan arama motoru yerine başka bir arama motoru arama sonuçlarını gösteriyorsa,
- İnternet tarayıcısındaki Sık Kullanılanlar (Favorites) veya Yer İmi (Bookmark) bölümünde yabancı sitelere bağlantılar eklenmişse,
- İnternet tarayıcısının başlangıçta gösterdiği site olan “Başlangıç Sayfası” (Home Page), ayarlanandan başka bir siteyi gösteriyorsa ve bu ayar tekrar düzeltildiğinde yine farklı siteler açılışta ortaya çıkıyorsa,

Bilgi ve Bilgi Güvenliği

(Bilgisayarlarda Kötüçül Yazılımların Belirtileri)

- Internet tarayıcısında daha önce olmayan araç çubukları varsa,
- Sistem tepsisinde (system tray) daha önce bilinmeyen bir simge varsa,
- Internet'e bağlantı olmadığı durumlarda bile kullanıcı adı ile hitap eden çıkiveren (pop-up) reklamlar görünüyorrsa,
- Internet sayfasında bazı tuşlar çalışmıyorsa (örneğin bir web formu doldururken bir sonraki yazım alanına geçmek için kullanılan sekme (tab) tuşu çalışmıyorsa),
- Bilgisayar ile faal olarak çalışmadığı bir sırada bilgisayar kasasındaki sabit disk hareketini gösteren lamba sürekli yanıp sönuyorsa,

Bilgi ve Bilgi Güvenliği

(Bilgisayarlarda Kötüçül Yazılımların Belirtileri)

- Internet'e erişim olmadığı sırada sistem tepsisindeki ağ bağlantısını gösteren (iki bilgisayar şeklinde gösterilen) simgede veri aktarımını gösteren hareketler görülmüyorsa,
- CD sürücüsü kendi kendine açılıp kapanıyorsa,
- Rastgele hata mesajları çıkıyorsa,
- Internet'e modem ile bağlanıp da büyük meblağlarda telefon faturası geliyorsa, sistemde çok büyük ihtimalle casus yazılım bulunmaktadır [19,26].

Bilgi ve Bilgi Güvenliği

(Bilgisayarların Kötüçül Casus Yazılımlardan Korunması)

Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler.

Alınabilecek bazı güvenlik önlemlerini gerçekleştirmek bilgisayar güvenliği açısından iyi sonuçlar verecektir. Bu güvenlik tedbirleri aşağıdaki başlıklar halinde özetlenebilir:

- *Kötüçül Yazılımlardan Korunma*
- *İşletim Sistemi Güncellemeleri:*
- *Anti-Spyware (Casus Karşı Yazılım):*
- *Host (Sunucu) Bloklama*

Bilgi ve Bilgi Güvenliği

(Bilgisayarların Kötüçül Casus Yazılımlardan Korunması)

- *E-posta kontrolü*
- *Browser (Internet Tarayıcısı) kullanımı*
- *Ofis Programları*
- *Güvenlik Duvarı (Firewall)*

Bilişim Suçları

- Büyük bir ivme ile önemi artmakta olan bilgi güvenliği ve gün geçtikçe artan bilişim suçlarının adli olarak incelenmesi konuları büyük önem kazanmaktadır.
- Bilişim suçları yakın zamanda ortaya çıkan bir ifade olduğundan bazı kavramların birleşimi ile kendisine tanım bulmaya çalışmıştır. Bu kavramlar tanımlanarak bilişim suçu tanımı daha iyi anlaşılabilecektir.

Bilişim Suçları

- Hukuki anlamda **suç**, bir toplumdaki hukuki kurumlar tarafından ceza veya güvenlik tedbiri yaptırımına bağlanmış fiildir [1]. Uygulamada ise **suç**; başka insanların veya tüzel kişiliklerin haklarına tecavüz etmek veya yanlış ya da zararlı olduğu için yasaklanan ve bazı durumlarda cezalandırılan davranış olarak tanımlanabilir [2]. Suçu gerçekleştiren kişiye **suçlu** denir. Hukuki anlamda bir kimsenin suçlu kabul edilebilmesi için suçun o kimse tarafından işlendiğinin hukuki süreçler sonucunda **somut deliller** ile ispatlanması gerekmektedir.

Bilişim Suçları

- **Bilişim**, elektronik cihazlar yardımıyla bilgilerin sistematik ve otomatik olarak işlenmesidir. Bilişim, insanoğlunun kullandığı tüm telekomünikasyon araçları başta olmak üzere ağ haberleşme sistemleri, bilgisayarlar, uydu sistemleri gibi iletişim içeren ve insan hayatını kolaylaştırmaya yönelik tasarlanan sistemleri kapsar. Bilişim sistemlerinin insan hayatında vazgeçilmezler arasına girmesi, beraberinde bazı sorunları da getirmektedir. Bu sorunların en öne çıkanı sanal ortamdaki bilgi hırsızlığıdır. Bu sanal ortamdaki sorunlar ise bilişim suçu kavramını ortaya çıkarmıştır.

Bilişim Suçları

- En genel anlamıyla bilişim alanında kullanılan araçlardan yararlanılarak işlenilen suçlar, **bilişim suçu** olarak tanımlanmaktadır. Bununla beraber bilişim suçları TCK'de bilişim sistemleri kullanılarak işlenen suçlar olarak tanımlanmaktadır. Bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi veya kopyalanması da, **bilişim suçları** olarak tanımlanmaktadır [4].

Bilişim Suçları

- Bir bilişim suçunu işlededeki nedenler arasında maddi kazanç elde etmek, kişilerin itibarını sarsmak, intikam almak, sosyal hayatı insanlara aktaramadığını sanal ortamda gerçekleştirmek, karalamak veya yakalanma ihtimalinin zor olduğunu düşünerek zevk amaçlı saldırı yapmak gibi sebepler ortaya çıkmaktadır.

Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- Ülkemizde meydana gelen bilişim suçlarına somut örnekler vermek de mümkündür. CHP eski genel başkanının şahsına yapılan ve sanal ortamda ülkemiz dışındaki bir sunucudan yayılan mahremiyete dair video görüntüleri bilişim suçlarının artık günümüzde her şekilde kullanılabileceğini göstermektedir.



Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- Internetin yaygınlaşması ile **bilişim suçu olarak tanımlayamayacağımız** ancak millet menfaatine gibi görünen olaylarda mevcuttur. Bu oylara somut bir örnek verilirse, mesai saatleri içerisinde bankada sıra bekleyerek işlemlerini tamamlamak isteyen müşterilerle ilgilenmeyen bir çalışanın, bilgisayarında oyun oynadığının görüntülenmesi ve görüntülerin internet ortamına aktarılması olayları da mevcuttur. Bu durum, suç kabul edilmeyip millet menfaatine gözüktüğünden görüntüyü internete aktaran kişi hakkında inceleme başlatılmamış olup, bilişim suçu kapsamına alınmamıştır.

Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- Ülkemizde artan bilişim suçlarının incelenmesi ve hukuki anlamda kontrolün sağlanması için çalışmalar yapıldığı görülmekte ancak uygulamada henüz istenen seviyeye ulaşılamaladığı anlaşılmaktadır.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Delil:** İşlenen bir suç olayında fail/faillerin ortaya çıkarılabilmesi için ipuçları niteliğinde toplanan kaynaklar *delil* olarak tanımlanır. Bu deliller, aydınlatılması istenen olayın en önemli parçalarıdır. Bu elde edilen deliller bir araya getirilerek tüm resim görülmeye çalışılır. Böylece aydınlatılmak istenen olay bir çözüme kavuşturulmuş olur.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Delillendirme:** Suçların tespiti ve yargılanmasındaki en önemli husus *delillendirme* olarak tanımlanmaktadır. *Delillendirme* kısaca, bir suç ile ilgili o suçun kim tarafından ve ne şekilde işlendiğini ispat edici nitelikte bilgiler elde edilmesi ve bunun adli mercilere sunulması şeklinde tanımlanabilir.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Dijital Delil:** Sanal ortamda işlenen suçlardaki, suçluların tespit edilmesi için elde edilen kanıtlar *dijital delil* olarak isimlendirilmektedir. Bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere dijital delil denilmektedir. Bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen veriler” olarak tanımlanmıştır.dijital deliller “bir suçun işlendiğini gösteren veya suç ile kurban ya da suç ile faili arasında bir ilişki sağlayan veriler” olarak karşımıza çıkmaktadır [7].

Bilişim Suçları

(Dijital Delillerin Özellikleri)

- Dijital deliller, parmak izi veya DNA gibi gizli veriler olabilirler.
- Dijital deliller, kolaylıkla ve hızla sınırları aşabilirler.
- Dijital deliller, kolaylıkla değiştirilebilir, zarar verilebilir veya silinebilirler.
- Dijital deliller, bazen zaman ile sınırlı olabilirler.
- Dijital deliller, genellikle uçucu verilerdir.
- Dijital deliller, güvenliği sağlanmaz ise çabuk deformasyona uğrayabilirler.
- Dijital deliler, yapı itibariyle, fiziksel delillere göre daha hassas ve kolay bozulur niteliktedirler.

Bilişim Suçları

(Dijital Delillerin Özellikleri)

Dijital deliller, normal somut delillere göre yapı itibariyle bazı sıkıntıları barındırmaktadır. Bu sıkıntılar şu şekilde özetlenebilir:

1. Dijital Delillerin Bütünlüğü
2. Dijital Delillerin Doğrulanması
3. Dijital Delillerin İnkar Edilememesi
4. Dijital Delillerin Doğruluğu:
5. Dijital Delillerin Daha Sonradan Ele Alınabilirliği [7,11].

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Bilişim suçlarındaki dijital delillerin elde edildiği birçok kaynak olabilir. Bunlar genel olarak şu şekilde sıralanabilir:

- Bilgisayar sistemleri (Masaüstü, dizüstü, sunucu vb.)
- Bilgisayar bileşenleri (HDD, memory vb)
- Erişim kontrol araçları(Smart kartlar, biometrik tarayıcılar)
- Çağrı cihazları, Dijital kameralar,PDA ve PALM cihazları
- Harici harddiskler , Hafıza kartları, Network araçları (Modem, yönlendirici, anahtar)
- Yazıcılar, tarayıcılar ve fotokopi makineleri
- Çıkarılabilir yedekleme üniteleri (Disket, CD, DVD...)
- Telefonlar,Kredi kartı okuyucuları, GPS

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Dijital deliller birçok tipte karşımıza çıkmaktadır. Bunlardan bazıları şunlardır:

- Veri dosyaları
- Kurtarılmış, silinmiş dosyalar
- Kayıp alanlardan kurtarılmış veriler
- Dijital fotoğraf ve videolar
- Sunucu kayıt dosyaları
- E-posta
- Chat kayıtları
- İnternet geçmişi
- Web sayfaları
- Kayıt (log)

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Dijital delillerin elde edildiği alanlardan en çok göze çarpanları şunlardır:

- Bilgisayarlar (Masaüstü, dizüstü bilgisayar, PDA, sunucu, istemci)
- Elektronik aygıtlar
- Veri havuzları
- Bir sistemde yapılan işlemleri gösteren kayıtlar, geçmiş bilgileri, erişim listeleri
- Yedekleme üniteleri
- Yazılımlar
- E-Postalar
- Çerezler gibi internet ile ilgili dosyalar[7,11].

Bilişim Suçları

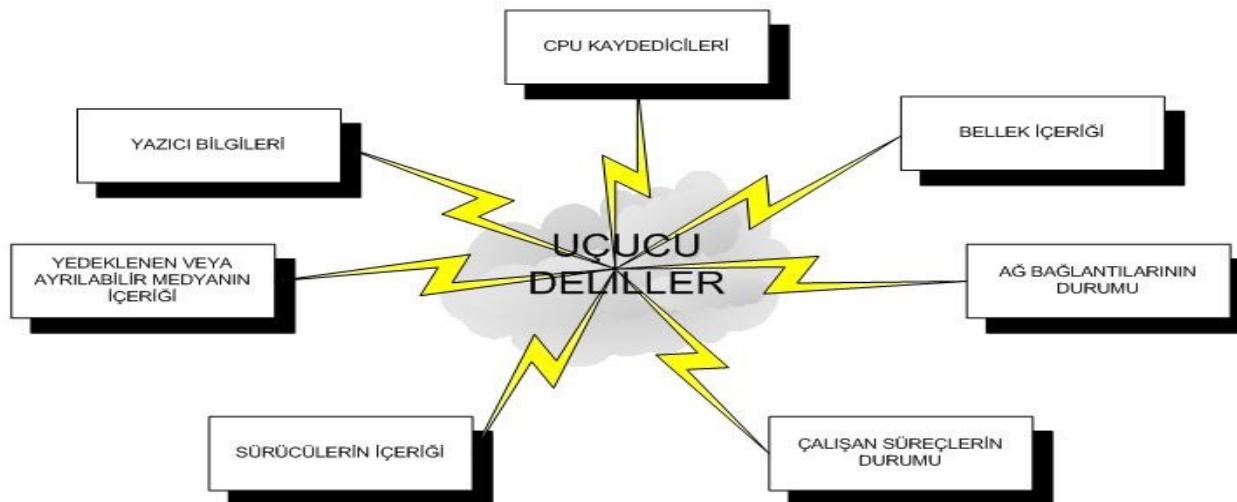
(Dijital Delillerin Toplanması)

- Sanal bir suçun varlığından şüpheleniliyor ise söz konusu suç veya vaka ile ilgili potansiyel delillerin toplanması gerekmektedir. Sürecin doğru bir şekilde işlemesi için öncelikle uygun prosedürleri ve gerekli hukuki şartları anlamak ve sağlamak büyük önem arz etmektedir. Geleneksel delil toplama, delillerin daha sonradan incelenmek üzere sahiplenilmesi anlamına gelmektedir. Fakat dijital delillerde durum biraz farklıdır. Delillerin doğrudan toplanması esnasında bazlarının kaybedilmesi, bozulması ile karşılaşılabilir.

Bilişim Suçları

(Dijital Delillerin Toplanması)

- Uçucu veriler (Ör: bellek, CPU kaydedicileri, çalışan süreçlerin durumu) dediğimiz elektrik kesildiğinde içeriği sıfırlanan ve tekrar kurtarılması mümkün olmayan delillerdir



Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Saldırı* ifadesi en bilindik anlamda kötülük yapmak, yıpratmak amacıyla, bir kimseye karşı doğrudan doğruya silahlı veya silahsız bir eylemde bulunma, hücum, taarruz veya bir sistemin kullanılamaz hale getirilmesi için yapılan her türlü meşru veya gayri meşru hareketler olarak tanımlanabilir. Bilişim sistemlerine yapılan saldırılar *da digital saldırı* olarak tanımlanmaktadır. Dijital saldırılardaki amaç, bilgiyi çalmak, bozmak, sızdırmak veya bilişim sistemindeki yazılım ve donanımlara zarar vermek olarak belirtilebilir. Dijital saldırıları aktif ve pasif saldırı olarak ikiye ayırmak mümkündür.

Bilişim Suçları

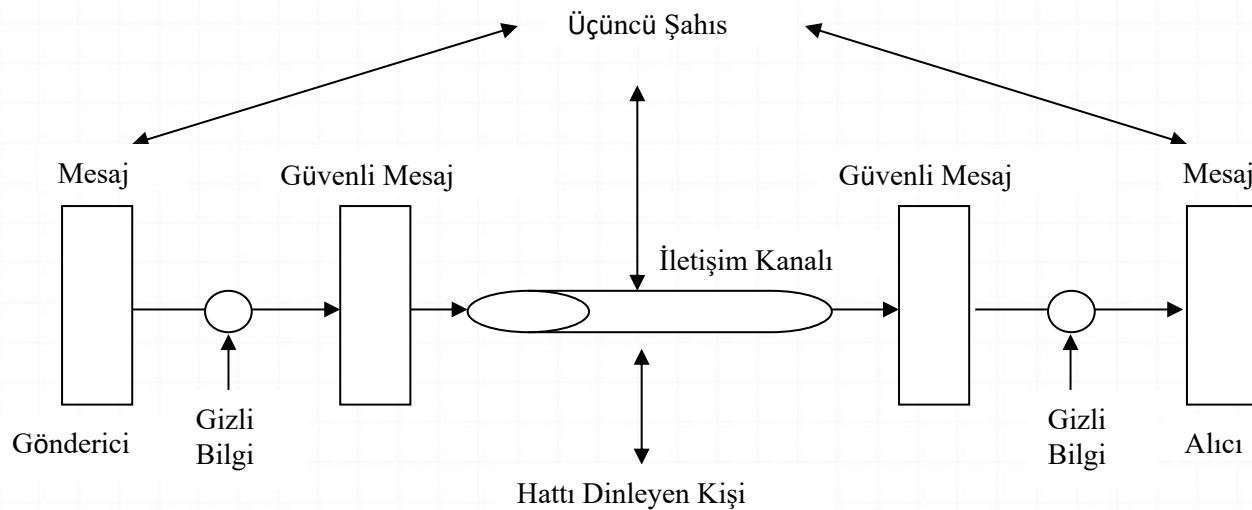
(Dijital Saldırılar ve Dijital Saldırganlar)

- *Pasif saldırıda*, saldırın taraf pasif davranmakta ve çoğu zaman sadece sistemi gözetlemekle yetinmektedir. Bu saldırı şeklindeki saldırın yakalanması çoğu zaman daha güç olmaktadır. Pasif saldırı yöntemlerine örnek olarak; Mesajın içeriğini edinme, trafigin akışını takip etme gibi yöntemler verilebilir.
- *Aktif saldırı* yönteminde ise saldırın aktif olarak rol oynar ve sistemin içerisine dahil olur. Sistemi savunan tarafın, saldırın yakalama veya tespit etme ihtimali yüksektir. Aktif saldırı yöntemlerine örnek olarak;
- Rol yapmak (Sniffer olayı, IP aldatmacası vb.)
- Eski mesajın tekrarlanması
- Aktarılan mesajı değiştirme
- Hizmet dışı bırakma/engelleme, gibi yöntemler sayılabilir.

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Şekil de görüleceği gibi aktif veya pasif saldırı mesajın çıkış noktasından başlayarak varış noktasına kadar üçüncü şahıs olarak adlandırılan saldırıcı tarafından herhangi bir bölgede gerçekleştirilebilir.



Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırırganlar)

- *Hackerlar(saldırırganlar)*, kültür ve bilgi düzeyi oldukça yüksek olan, en az bir işletim sisteminin yapısını tam olarak bilen, programcılık deneyimleri yüksek ve konusunda ileri eğitimler alarak uzun yıllarını bu işlere adamış kişilerdir [9]. Diğer bir tanımda ise işletim sistemlerini tam manası ile bilen, derinliklerine inen, bilgisayarla derinlemesine ilgilenen, programlamayı profesyonel düzeyde bilen bilgisayar uzmanlarıdır [8].

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Yapılan hacker tanımlamalarına bakılarak farklı niyette çalışan hackerler olduğu görülmektedir. Hackerlar; **beyaz şapkali hacker, siyah şapkali hacker** ve **gri şapkali hacker** olarak sınıflandırılmaktadırlar.
- *Hacking* olarak ifade edilen kavram ise bir sisteme sızma ya da zarar verme anlamında yapılan saldırıların genel adıdır.
- *Beyaz şapkali hackerlar* bilgi bakımından siyah şapkallardan aşağı kalmamakla beraber; iyi niyetli, zarar vermeyen, amaçları bilgisayar güvenliğini sağlamak olan kişilerdir [8].

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Siyah şapkalı hacker* kavramı ise tamamen kötü niyetli, sırf kazanç elde etmek ve karşıya zarar verme amacıyla sistemlere sızan, bilgi çalan, korsanlar için kullanılır. Bu grup hackerların amacı bilgi çalmak veya sisteme zarar vermektedir [8]. Siyah şapkalı hackerlar bazı çalışmalarda korsan, saldırıcı veya 3. şahıs olarak da adlandırılmaktadırlar.
- Beyaz şapkalı ve siyah şapkalı grubun arasında kalan *gri şapkalı hacker* olarak adlandırılan bir grup vardır ki bunlar yerine göre siyah yerine göre de beyaz şapkalı hacker gibi hareket ederler.

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Bilişim sistemlerine zarar vermek amaçlı çalışan kişiler genelde *cracker* tanımlamasına dahildirler.
- Siyah şapkalı hackerlara nazaran daha zararsız olarak tanımlayabileceğimiz *Lamer* ifadesi genelde küçük yaşta ve hacker özentisi olan, birkaç hacker işlemini bilen ancak programlama bilgisi olmayan, herkesin yapabileceği işleri yaparak ün kazanmak isteyen kullanıcılardır. *Script Kiddie* ise genelde lise çağında olan, programlama bilgisi olmayan genellikle e-postalara saldırıma işlemlerini öğrenen kişilerdir. Lamerlara göre fazla hacking bilgileri vardır [8].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- **Siber** kelimesi bilgisayar ağlarına ait olan, internete ait olan, sanal gerçeklik manalarına gelmektedir.
- Soyut olarak iletişim kurulan sistemler *siber alan* olarak tanımlanmaktadır. Dünya üzerindeki en büyük iletişim sistemi olan interneti anlatan sanal alem ve siber alem kavramlarının ikisi de doğru birer önermedir. Siber alanın yaygınlaşması bazı kavramlarında beraberinde ortaya çıkmasına sebep olmuştur.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Zorbalık denince sözlü veya fiziksel şiddet anımları akla gelir. *Siber zorbalık*, bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür. Elektronik zorbalık ve elektronik iletişim zorbalığı olmak üzere iki çeşit siber zorbalık mevcuttur.
- Siber zorbalık veya tehdidin en çok sosyal medya sitelerinde meydana geldiği görülmektedir. Genellikle fotoğraf ve video yayınılama tarzında gerçekleşen bu eylemler bazen sözlü alay ifadeleri ile mahremiyetlere zarar vermektedir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Elektronik zorbalık*, kişilerin şifrelerini ele geçirme, web sitelerini hackleme (bir sisteme izinsiz girmek), spam (zararlı virüs) içeren e-postalar gönderme gibi teknik olayları içeriyor. Bu tip saldırılar, bireylerin web siteleriyle sınırlı kalmayıp, kurumların ve devletlerin siteleri, yazılım ya da donanımlarını da olumsuz etkiliyor.
- *Elektronik iletişim zorbalığı* ise bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme (cyber-stalking), alay etme, isim takma, dedikodu yayma, hakaret ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi ilişkisel saldırı davranışlarını içeriyor. Bu da direkt olarak insanın duygusal ve psikolojisini etkiliyor [14].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Bilgi sistemleri doğrultusunda elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla, ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinlikler *siber saldırı* olarak isimlendirilmektedir. Siber saldırılar genellikle İnternet üzerinden yapılan tecrübeli hackerların yapabildiği saldırısı biçimidir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Siber Terörizm(Savaş)* belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırmaya, baskı altında tutma amacıyla kullanılmasıdır [13].
- Siber terörde, saldırganların elektronik bir saldırısı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğalgazı kapatabilecekleri, bilgisayar sistemlerini karmaşık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve finans sektörünü çökertebilecekleri, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dahilindedir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Siber ordular* ulusal güvenliği sanal ortamda sağlayan ordulardır. Siber orduların öneminin farkında olan Amerika Birleşik Devletleri gibi gelişmiş ülkeler sanal ortamda saldırı tespit yöntemleri oluşturmaya yönelik yarışmalar düzenleyerek konu hakkında yetenekli kişileri bu ordularına dahil etmektedirler. Pentagonun düzenlediği güvenlikle ilgili bir yarışmada birinci olan bir Türk öğrencinin Pentagon'dan davet mektubu alması buna bir örnektir [15].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Bilişim dünyasında yeni bir kavram olarak yer bulmaya başlayan **siber ahlak** olarak da tanımlayabileceğimiz siber etik en genel anlamıyla gerçek hayatı iyi bir birey olmak için yapılan fiillerin sanal ortamda da yapılması olarak tanımlanmaktadır.
- Sanal alemden davranış kuralları konusunda özellikle genç kuşağın eğitilmesi gerekmektedir. Günlük yaşamında hırsızlık yapmayı ahlaki değerleriyle veya toplumsal statüsü ile bağıdaştıramayan bir genç net ortamında rahatlıkla hırsızlık yapabilmekte veya başkalarına zarar verebilmektedir.

Bilişim Suçları

(Adli Bilişim)

- Adli kelimesi TDK'nin sözlüklerinde adliye teşkilâtı ve hizmeti ile ilgili, adaletle ilgili olarak tanımlanmaktadır. Bu bağlamda adalete intikal etmesi gereken hadiselerin tamamına ise *adli vaka* veya *adli olay* denmektedir.
- Adli bilişim teriminin kökeni, İngilizce orijinal ismi ile Computer Forensics'tir

Bilişim Suçları

(Adli Bilişim Çeşitleri)

- 1.Bilgisayar Adli Bilişimi (Computer Forensics) :** Daha çok bir bilgisayar üzerinde yapılacak araştırmalarla ilgilenir. Örneğin: Harddisk, RAM, işletim sistemi üzerinde yapılacak araştırmaları kapsar.
- 2.Bilgisayar Ağlarına Yönelik Adli Bilişim (Network Forensics) :** Ağ sistemleri ve iletişimine yönelik incelemeyi kapsar.
- 3.Bilgisayar Ağ Cihazlarına Yönelik Adli Bilişim (Network Device Forensics):** Yönlendirici, switch gibi cihazlar üzerinde yapılacak incelemeyi kapsar.
- 4.İnternet Adli Bilişimi (Internet Forensics):** Genel olarak internet kaynakları ve internet sistemleri üzerinde yapılan araştırmayı kapsar.
- 5.Bilgi Adli Bilişimi (Information Forensics):** Bütün olarak bilgiyi içeren her türlü materyali barındıran sistemler üzerinde yapılan incelemeyi kapsar.

Bilişim Suçları

(Adli Bilişim Çalışma Alanları)

- Adli bilişimin çalışma alanlarından bazıları ana başlıklar halinde şöyle sıralanabilir:
- Veri kurtarma
- Veri imha etme
- Veri saklama
- Veri dönüştürme
- Şifreleme(Kriptografi)
- Şifre çözme
- Gizlenmiş dosya bulma.

Bilişim Suçları

(Adli Bilişimin Faydaları)

- Adli bilişim, yalnızca bilişim suçlarına has bir delil toplama metodu değildir. Bilişim suçlarından başka, klasik suçlara ilişkin olarak da ihtiyaç duyulan deliller, yine elektronik aygıtlar içerisinde de yer alabilir. Örneğin, bir bilişim suçu olmayan bir hırsızlık vakasında, soygun planı ve buna ilişkin haritalar bilgisayar ile hazırlanmış ve halen bilgisayarda mevcut olabilir. Bu bilgilere ulaşmada da yine adli bilişim devreye girecektir. Bu duruma en bariz örnek olarak; hala devam etmekte olan *Ergenekon* soruşturması ile alakalı bazı verilere, bilgisayar kayıtlarından ulaşılması gösterilebilir.

Bilişim Suçları

(Adli Bilişim Uzmanlığı)

- *Adli bilişim uzmani*, bilişim sistemleri konusunda ileri derecede bilgi sahibi olan kimsedir.
- Adli bilişim uzmanı kabul edilmek için birtakım sertifika programları mevcuttur. Bu programlardan birine devam ederek sertifika almak ve adli bilişim uzmanı sıfatına sahip olmak mümkündür.
- Bu sertifika programlarından en çok kabul edilenleri şunlardır: EnCase Certified Examiner (ENCE), Certified Computer Examiner (CCE), Certified Computer Crime Investigator (CCCI), Computer Forensic Computer Examiner (CFCE), Certified Information Forensics Investigator (CIFI), Professional Certified Investigator (PCI) [16].

Bilişim Suçları

(Adli Bilişimde Dijital Delillerin Kanıt Olarak Kullanılabilmesi)

- Adli bilişimde elektronik bulgunun, bir hukuki delile dönüştürülme süreci belli prosedürleri takip eder. Uygulanan bu prosedürlerden sonra dijital delil, kendisini bir hukuki delil olarak ortaya koyar. İşte bu prosedüre, *adli bilişim safhaları* denilmektedir. Adli bilişimde dijital delillerin kanıt olarak kullanılabilmesi için incelenmesi gereken dört safha şu şekildedir [16]:
 - Toplama (Collection)
 - İnceleme (Examination)
 - Çözümleme (Analysis)
 - Raporlama (Reporting)

Sonuç

- Bilgi güvenliği konusunda güvenlik açıklarının önlenenebilmesi için, kişilerin ve kurumların basitten en karmaşık yöntemlere kadar bir dizi önlemler alması gereklidir. Ancak, tüm önlemler alınmış olsa da, sürekli gelişen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş kendini **%100** güvende hissetmemelidir. Saldırılar; kötü niyetli kişiler, arkadaşlarımız veya tanıdığımız kişilerden gelebilir.

Sonuç

- Alınması gereken en temel önlemler, risklere karşı sürekli uyanık olmak, bu çalışmada açıklanan saldırıcı tekniklerine karşı uyanık olmak, yeni gelişmeler ışığında gerekli güncellemeleri yaparak saldırılardan etkilenme olasılığını en aza indirmek olarak belirtilebilir. Güvenliğin statik değil dinamik bir süreç sahip olduğu, koruma ve sağlamlaştırma ile başladığını, bir hazırlık işlemine ihtiyaç duyulduğu, saldırıların tespit edilmesinden sonra hızlıca müdahale edilmesi gereği ve sistemde her zaman iyileştirme yapılması gereği unutulmamalıdır.

Sorularınız



YMH321 Bilgi Sistemleri ve Güvenliği

Bilgi Güvenliği

Bölüm - 1

Prof. Dr. Resul DAŞ

Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarları

- Genel Bakış ve Terminoloji
- Gündemdekiler
- Mevcut Durum Analizi
- Güncel Tehdit ve Tehlikeler
- Nasıl bir SBG? Öneriler
- Sonuç ve Değerlendirmeler

Tanım : Siber Güvenlik?

- “Kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojiler bütünü” olarak tanımlanıyor.

Bilgi Nedir ?

- İşlenmiş veridir.
- Bir konu hakkında belirsizliği azaltan kaynaktır (Shannon).
- Kişi/kurum/kuruluşlar için önemli ve değerli olan bir kaynaktır ve korunması gereklidir.
- Veri (data), bilgi (information), ve özbilgi (knowledge)

Bilgi Nedir ?

- Boşlukta ve zamanda yer kaplar.
- Gürültü çıkarmadan hareket edemez.
- Bilginin hareket etmesi için enerji gereklidir.
- Bilgi yaşam ve herhangi bir düzenli etkinlik için gereklidir.
- Bilgi hem maddesiz biçim; hem biçimlilik maddedir.
- Işık gibi, bilgi'nin de ağırlığı vardır. Bir GB, bir parmak izinden daha az ağırlıktadır.
- Bilgi zaman içinde hareketli veya donmuş olabilir.
- Bilgi, bir soruya tatmin edici, belki de rahatsızlık verici cevaptır.
- Bir taşın ağırlığı ile bunu tanımlamak için gerekli bilgi birbirine eşittir.
- Bilgi, katı hale sahiptir; donarak katılaşır (depolama).
- Bilgi, sıvı hale sahiptir; akar (iletişim).
- Bir yerlerde bilgi hareket eder; evren gümbürder ve gerceği gürler.
- Maddeden farklı olarak bilgi aynı anda birden fazla yerde olabilir.
- El sıkışma bir bilgidir. Bir baş sallama, bir bakış, bir iç çeküş.
- Bilgi, rastsallık denizinde parlar.

BİLGİ (Veri)?

- İngilizce karşılığı olarak “data”,
- Latince “datum” (çoğul şekli “data” ve “vermeye cesaret etmek” fiilinin geçmiş zamanı, dolayısıyla “verilen şey”)
- Latince “data” (dedomena) kavramının M.Ö. 300 yıllarında Öklid'in bir çalışmasında geçtiği bildirilmektedir.
- Dilimizde de verilen şey anlamında, “veri” olarak kullanılmaktadır.
- Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.

BİLGİ (Bilgi)?

- Bilgi, verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir.
- Veri ve ilişkili olduğu konu, bağlamı içinde 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.

BİLGİ (Özbilgi)?

- Tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır.
- Verileri bir araya getirip, işlemek bilgiyi oluştursa da; özbilgi, kullanılan bilgilerin toplamından daha yüksek bir değer sahip bir kavramdır.
- Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir.

Veri-Bilgi-Özbilgi ?

- Veri (data), bilgi (information), özbilgi (knowledge) basamaklarıdır.
- Gerçeklik (reality) ile hikmet (wisdom) arasında gösterilen bu merdivenin basamakları
- Çoğu durumda her basamak, atlanmadan teker teker geçilir.
- Yukarıya çıktıktan sonra elimizdeki şeyin miktarı azalırken; değeri artar.
- Yine yukarıya çıktıktan sonra bir sonraki basamağa adım atmak daha da zorlaşır ya da daha çok çaba ister.
- Genel olarak bilimin getirdiği yöntemlerden ölçme ile,
- eldeki gerçeklikten **veriye ulaşılır**;
- ispat ile, veriden **bilgiye ulaşılır ve**
- kavrayış ile, bilgiden **özbilgiye ulaşılır**.
- Bir özbilginin gerçeklik haline dönüştürülmesi de mümkündür. Bunun için yönetim biliminden yararlanılır.

Güvenlik?

- Karşılaşılabilecek tehditlere karşı önlem alma
- Kişi ve kurumların BT kullanırken karşılaşabilecekleri tehdit ve tehlikelerin daha önceden analizlerinin yapılarak gerekli önlemlerin alınmasını sağlama

Bilgi Güvenliği?

- Bilginin değerli veya degersiz olduğunu belirlemek veya bilginin taşıdığı değeri ölçmek, en az bilginin kendisi kadar önemlidir.
- Bilgiyi değerlendirdirirken bilginin kalitesini gösteren özelliklere bakılması gereklidir.
- Doğruluk, güncellik, konuya ilgili olma, bütünlük ve öz, gereksinimlere uyum gösterme, iyi sunulma ve fiziksel ve idrak yolu ile erişim gibi ölçütler bilginin kalitesini belirleyen etmenlerden bazlıdır.
- Bilginin çok önemli bir varlık olması, ona sahip olma ile ilgili bazı konuların düzenlenmesi ve yeni şartların getirdiği özelliklere göre ayarlanması gerekmektedir.
- Bilgi en basit benzetme ile para gibi bir metadır.

Bilgi Güvenliği?

- Dünya gündeminde bir konudur.
- Bilginin bir varlık olarak hasarlardan korunması
- Doğru teknolojinin doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler veya sistemler tarafından elde edilmesini önleme

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 **sürecidir**.



Siber Bilgi Güvenliği ?

- Bilgi Güvenliği nerede sağlanmalı ?
 - Üretim
 - Erişim
 - İşleme
 - Depolama
 - Aktarma
 - Yok etme



Siber Güvenliğin Temel Hedefi?

- Kurum ve kuruluşların veya en genel anlamda ulusların bilgi varlıklarını ve kaynaklarını hedeflenen amaçlar doğrultusunda organizasyon, insan, finans, teknik ve bilgi değerlerini dikkate alarak, varlıkların ve kaynakların başına **KÖTÜ BİR ŞEYLER GELMEDEN korumaktır.**

Tanım (ABD Başkanı Barack Obama)

- “Ülke olarak karşılaşılan çok ciddi ekonomik ve ulusal güvenlik sağlama hedeflerinden birisi olup hükümet veya ülke olarak henüz tam anlamıyla önlem alamadığımız bir husustur.” “Amerika’nın sayısal altyapısını kapsamlı olarak güven altına alma yaklaşımlarının geliştirilmesi ve bilgi ile haberleşme altyapısının savunulmasına yönelik olarak federal çözümlerin gözden geçirilmesi” emrini verir. **“21. yüzyılda Amerika’nın ekonomik zenginliği, siber güvenliğe bağlı olacaktır.” Mayıs 2009**

Ülkemizdeki Tanımlar..

Ulaştırma Bakanı Sn. Binali Yıldırım

- “bilgi sistemi güvenliğinde ortak akıl ve ortak hareketle hattı müdafaa yerine sathı müdafaanın başarılı bir şekilde gerçekleştirilme girişimi”,
- “devletin birinci dereceden ilgilenmesi gereken bir mesele olarak görüyoruz.”
- “siber savaş tehdidine karşı hazırlıklı olmanın, kurumların bilgi sistemi güvenliği olaylarına müdahale yeteneği ile kurumlar arası koordinasyon yeteneğini tespit ederek, alınacak önlemler ve bilincinin artırılmasını amaçlamak”

Faydalar

- 1.Zamandan bağımsızlık
- 2.Mekandan bağımsızlık
- 3.Hız
- 4.Verimlilik
- 5.Gelişim/Değişim
- 6.Hayatı kolaylaştırıyor
- 7.Yönetmeyi kolaylaştırıyor
- 8.Denetlemeyi kolaylaştırıyor



Zararlar

- 1.Bilmeyenler için kontrolü zor..
- 2.Açıklarını bilenleri öne çıkarıyor..
- 3.Kötülere çok yardımcı oluyor..
- 4.Bilmeyenlere hayatı dar ediyor..
- 5.Bağımlılık yapıyor..
- 6.Kişisel gelişimi kısmen olumsuz etkiliyor..
- 7.Gelişmemiştoplumları köleleştiriyor..

60 saniyede neler oluyor? -1

- 168 milyon e-posta gönderiliyor.
- 1500'den fazla blog iletisi yayılıyor.
- 70'den fazla domain adı alınıyor.
- Flickr üzerinden en az 6600 fotoğraf 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..

60 saniyede neler oluyor? -2

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.

60 saniyede neler oluyor? -3

Youtube

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

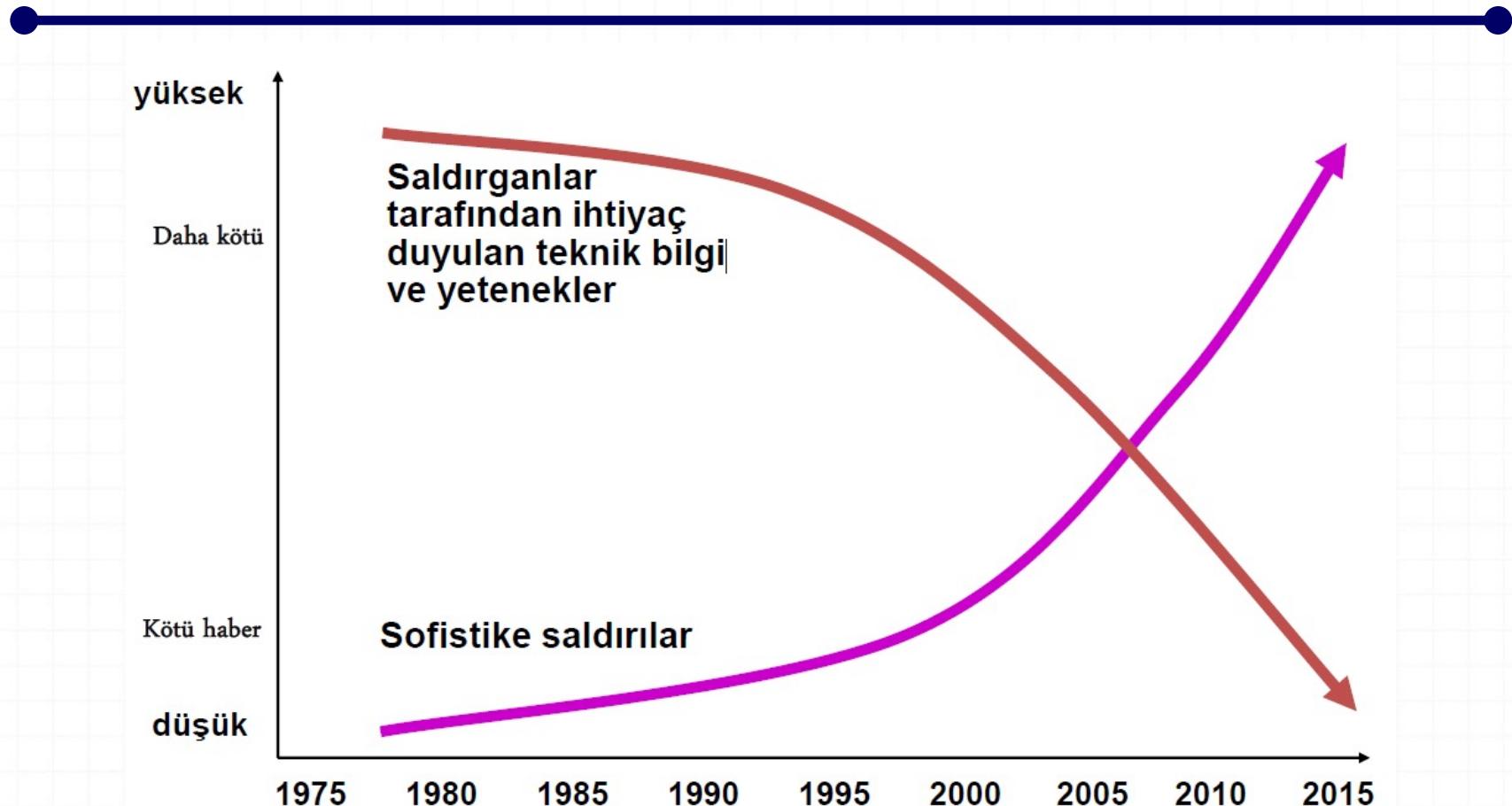
Yahoo

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

LinkedIn

- LinkedIn'e 100'den fazla profil ekleniyor.

Siber Ortamlar



Siber Ortamlar

Ulusal Askeri Stratejiler doğrultusunda;

- 15 Kasım 1940'da 500 savaş uçağı İngiliz Coventry şehrinini bombaladı.
- Kod adı "Ay Işığı Sonatı" (Ludwig van Beethoven)
- Bu saldırısı Enigma kullanılarak şifrelenmişti.
- Yüzlerce ölü ile beraber şehrin üçte ikisi yıkıldı.
- Kendi bilgi ve bilgi sistemlerimizi etkin bir şekilde kullanırken
- Amaç savaşı kazanmak

Siber Ortamlar

- 1952'de Amerikan Ulusal Güvenlik Ajansı (NSA)
- Amerikan karar vericilere ve askeri liderlere zamanında bilgi sağlamak için Başkan Truman tarafından kurulmuş 1960'da Rusya'ya iltica eden iki NSA görevlisi ABD'nin 40 ülkenin haberleşmesini dinlediğini açıklamışlardır.

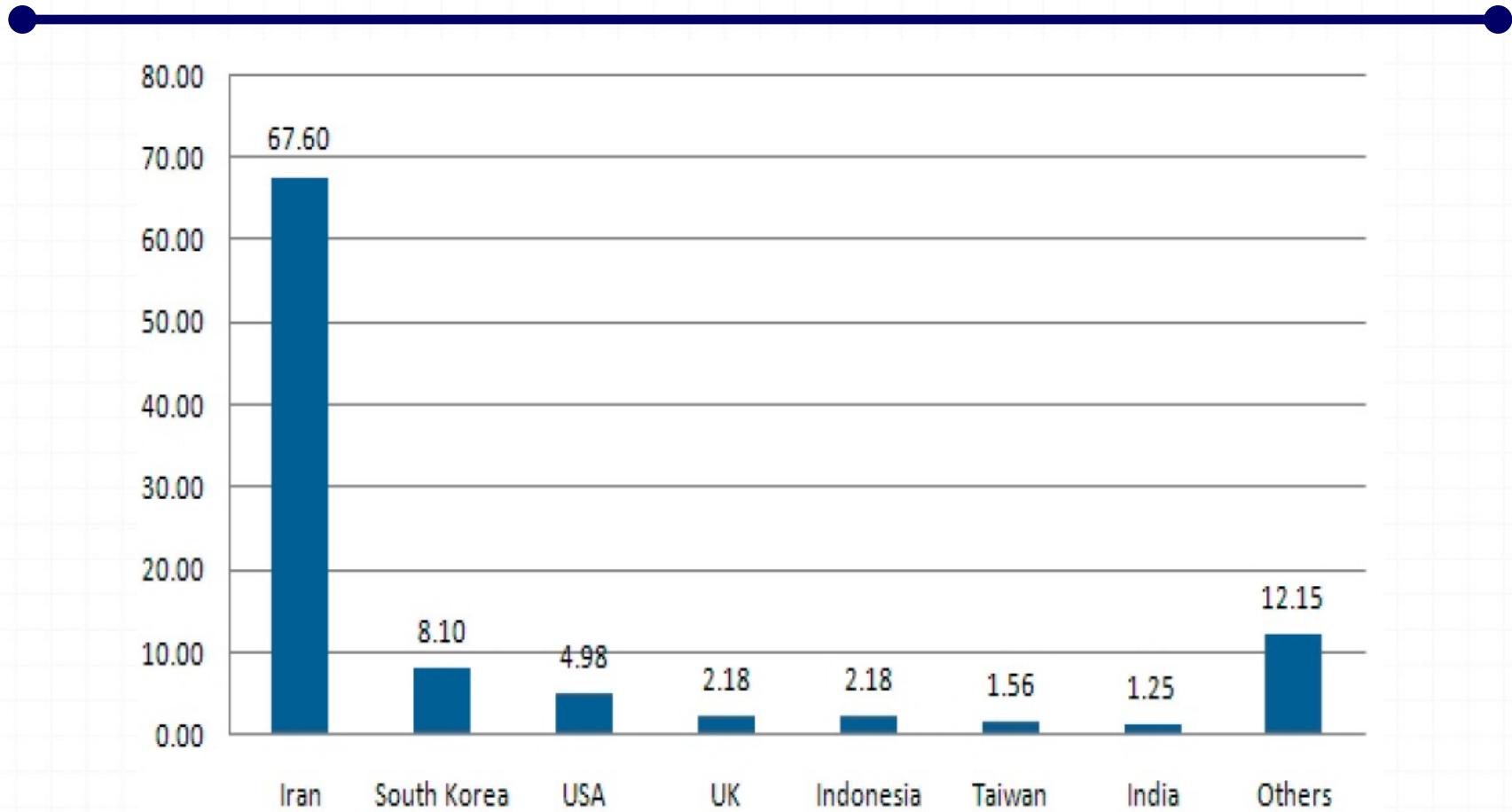
Siber Ortamlar

- Bilgiye her yerden erişilebiliyor..
- Arama motorları var..
- Sosyal ağlar..
- Sanal ortamda bir savaş var..
- İnsan beyni okunabiliyor..
- Akla hayale gelmedik yaklaşımalar geliştiriliyor..
- İzleme hat safhada..

STUXNET Neler Öğretti

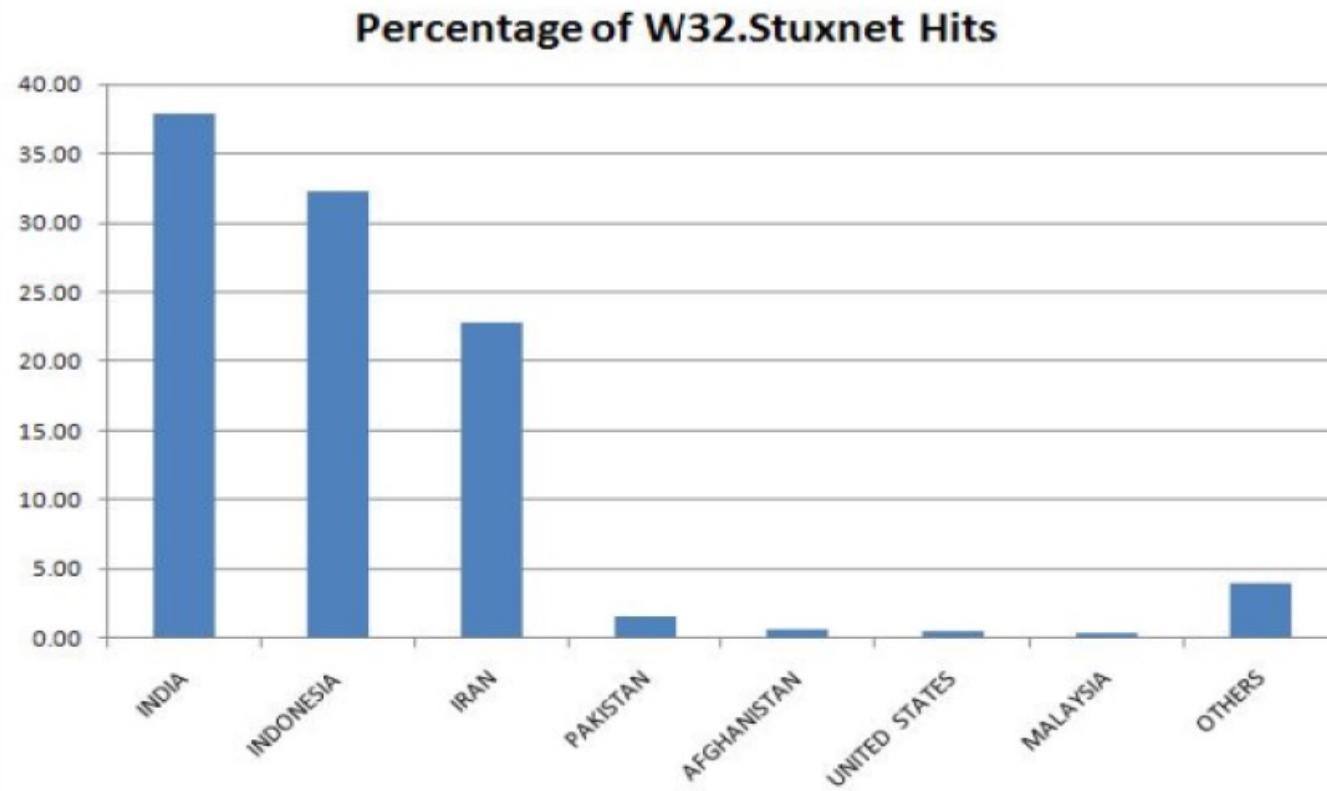
- Ezber bozan bir yaklaşım
- Altyapıya saldırı için planlanmış
- Önemli sistemlerin korunaklı olmadığı
- Kolaylıkla sistemlere zarar verilebileceği
- Bir ülkenin nükleer programını durdurabilecek kadar önemli
- Spekülasyon ile ülkelerin prestijlerine zarar verme

Etkilenen Sistemler



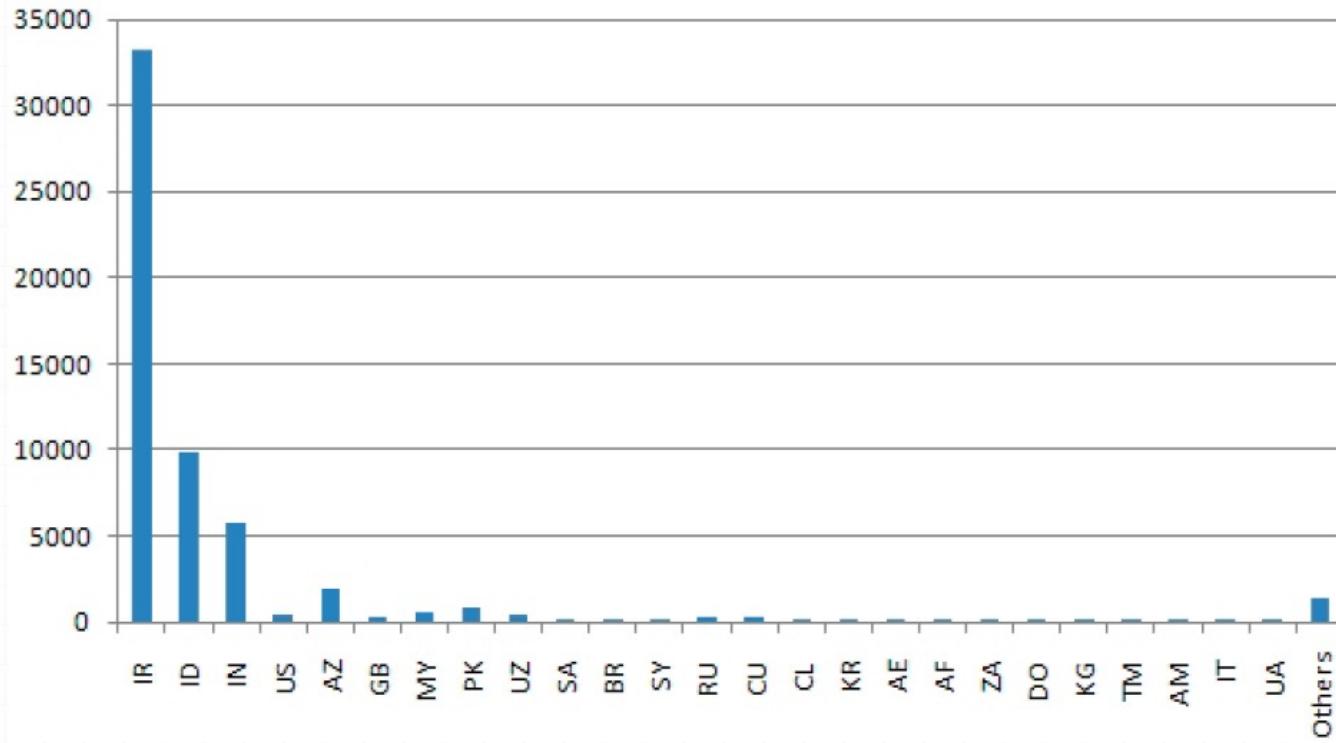
Etkilenen Sistemler

- USB Sürücülerde Yayılma

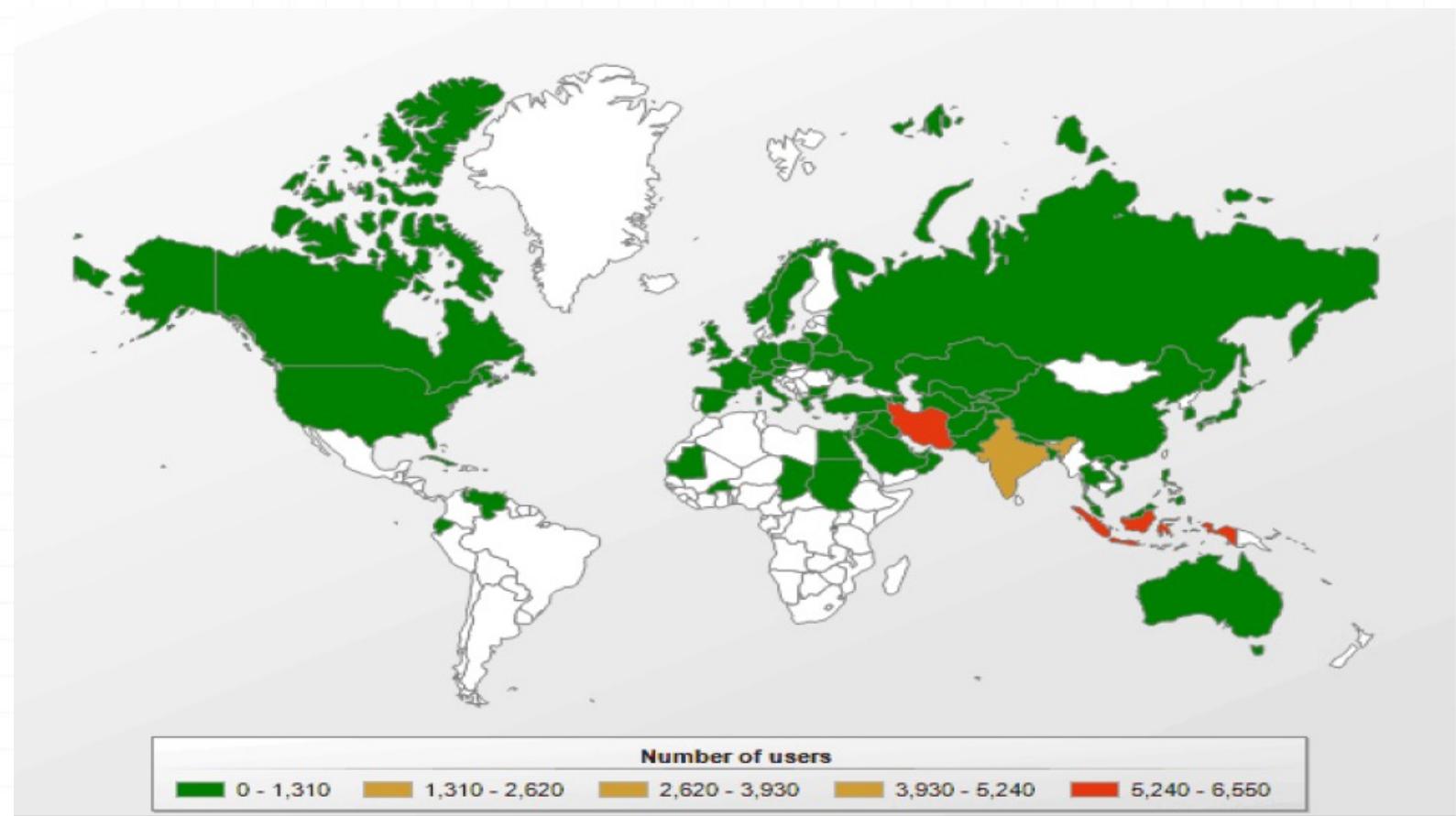


Etkilenen Organizasyonlar

■ WAN IP



Stuxnet'den Dünya Çapında Etkilenme



Siber Tehditlerin Amaçları

- Sisteme yetkisiz erişim
- Sistemin bozulması
- Hizmetlerin engellenmesi
- Bilgilerin
 - Değiştirilmesi
 - Yok edilmesi
 - İfşa edilmesi
 - Çalınması

Siber Ortamlar

İyilerin ve Kötülerin amansız savaşı

- Saldıran Taraf
- Savunan Taraf

Siber Ortamlar

■ Saldırı Taraf

- Saldırılar artmaka
- Saldırı bilgi seviyesi hızla azalmakta
- Kötüçül kodlar gelişerek ve değişerek hızla yayılmakta
- Organize sanal suç örgütlerini kurma
- İyilerden hep bir adım önde

Siber Ortamlar

Savunan Taraf

- Güvenliğin en zayıf halkası
- Bilgisizlik, ilgisizlik, hafife alma,
- %100 Güvenliğin sağlanamaması **%99,9 Korunma + %0,1 Korunmasızlık=%100 güvensizlik**
- Bilgi birikimi (Yatırım, Eğitim ve zaman)
- Kişilere güven duygusu
- E-dünyanın doğasında olan güvensizlik

Siber Ortamlar

Siber Bilgi Güvenliği ?

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

Siber Güvenlik Kültürüne Oluşturulması



Bireysel Stratejiler

- Tehlikelerin farkında olmak
- Çok katmanlı bir savunma mekanizması oluşturmak
 - Çoklu araçlar
 - Yama programları
 - Güncellemeler
- Sosyal medyada gizlilik seçeneklerini iyi değerlendirmek
- Verilerinizin nerede olduğundan emin olun
- Kötü çocuk gibi düşünün
- Çocukların erişilebilirliğinin sınırlayın

CIA

- Confidentiality – Gizlilik
 - Bilgi ne anlama geliyor
- Integrity – Bütünlük
 - Değişim olmadığı doğrulanabiliyor mu?
- Availability – Geçerlilik
 - İhtiyaç duyulduğunda bilgiye erişilebiliyor mu ?



Ek özellikler

- Non-repudiation – İnkar edememe
- Authentication -Yetkilendirme

Sonuç

- Bilgi Güvenliği **ürün veya hizmet değildir.**
- İnsan faktörü, teknoloji ve eğitim unsurları üçgeninde yönetilmesi zorunlu olan karmaşık süreçlerden oluşan, sürekli arz eden bir süreçtir.
- Üç unsur arasında tamamlayıcılık olmadığı sürece **yüksek seviyede bir güvenlikten bahsedebilmek mümkün değildir.**
- Yüksek seviyede E-Devlet güvenliğinden bahsedebilmek için **Kurumsal ve Bireysel anlamda Bilgi Güvenliğinin gerekleri yerine getirilmelidir.**

Sorular



Kaynaklar



YMH321 Bilgi Sistemleri ve Güvenliği

Bilgi Sistemleri ve Güvenliği

Bölüm: 1

Prof.Dr. Resul DAŞ
Fırat Üniversitesi, Teknoloji Fakültesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarısı

- Giriş
- Bilişim Suçları
- Bilgi ve Bilgi Güvenliği
- Sonuç
- Sorular
- Kaynaklar

Giriş

- Bilişim dünyasında bilgi ve bilgi varlıklarının öneminin gün geçtikçe artması, buna paralel olarak bilişim güvenliğinin öneminin de artmasını ortaya koymaktadır. Uluslar arası bir ağ sistemi olan internet ortamındaki verilerin veya bilgilerin korunması için donanımsal ve yazılımsal güvenlik tedbirleri alınmaktadır. Ancak, bu tedbirler sisteme veya bilişim cihazlarına yapılan saldırıları tamamen engelleyememektedir. Bu bağlamda bilişim suçlarının incelenmesi, saldırganların tespit edilmesi için birçok akademik ve ticari çalışmalar yapılmaktadır.

Giriş

- Bu bölümde, **bilişim suçları, bilgi ve bilgi güvenliği** konuları genel olarak incelenmiştir. Ayrıca bu konularda bilişim suçlarına örnek teşkil edecek saldırılar belirtilmektedir.

Bilgi ve Bilgi Güvenliği

(.Bilgi, Bilginin Değeri)

- En basit tanımlaması ile **bilgi** kişi ya da kurumlar için kıymet teşkil eden ve para gibi korunması gereken kıymetli bir metadır [25]. Meta ifadesi ile eşya kast edilirken bunun yerine varlık ifadesi de kullanılmaktadır.
- Günümüzde bilgi ön plana çıkmış gibi gözükse de, aslında **bilgi**; dünün ve bugünün anahtarları iken, geleceğin şekillenmesinde de her zaman anahtar rollere sahiptir.

Bilgi ve Bilgi Güvenliği

(Bilginin Gelişim Evreleri)

- İnsan bilincinden bağımsız olarak var olanlar veya hikmete ulaşmak için veri haline gelmeye hazır doğada bulunan her şey *gerçeklikdir*.
- Bilişim teknolojisi açısından *veri*, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.
- *Bilgi*; verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. Bilgi; işlenmiş veri olarak ve bir konu hakkında var olan belirsizliği azaltan bir kaynak olarak da tanımlanabilmektedir. Kısaca, veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, v.s.) çıktısı, *bilgi* olarak ifade edilebilir.

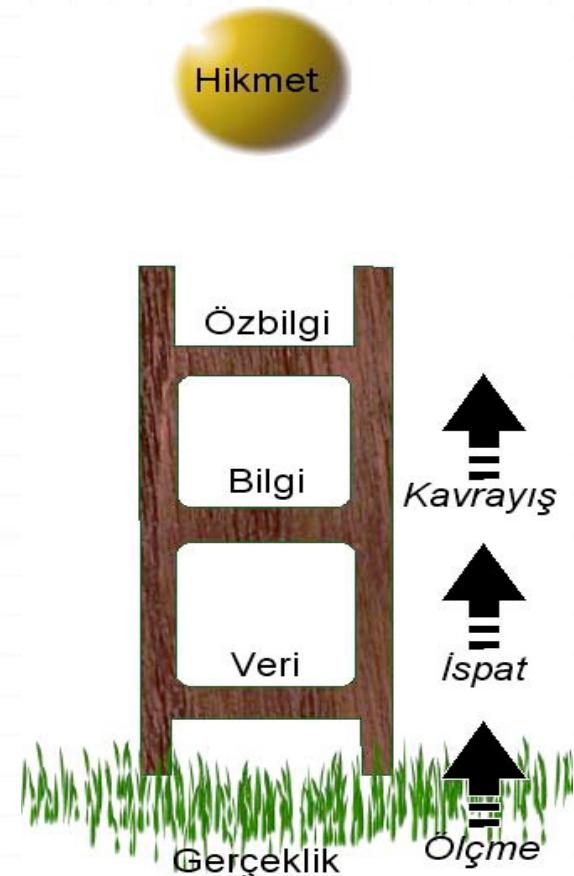
Bilgi ve Bilgi Güvenliği

(Bilginin Gelişim Evreleri)

- *Özbilgi*; tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Verilerin bir araya getirilip, işlenmesi bilgiyi oluştursa da özbilgi, kullanılan bilgilerin toplamından daha üstte bir kavramdır. Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir.

Bilgi ve Bilgi Güvenliği (Bilginin Gelişim Evreleri)

- Hikmet (wisdom), tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür. Hikmet, ayrıca, güvenilir yargıda bulunmak ve karar vermek için özbilginin nasıl kullanılacağını kavramak olarak da tanımlanmaktadır [23].



Bilgi ve Bilgi Güvenliği (Bilgi Güvenliği)

- *Bilgi güvenliği*; bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanır.
- *Bilgi güvenliği*, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür.

Bilgi ve Bilgi Güvenliği (Bilgi Güvenliği)

- Bilgi güvenliğinin sağlanması için kullanılabilecek birçok yöntem olmakla beraber yeni sayılabilenek **biometrik** alanda yapılan bilgi güvenliği çalışmaları da mevcuttur. Bu biometrik korunma yolları arasında parmak izi ile çalışan sistemler, el ve parmakların şekline göre çalışan sistemler, ses tanıma sistemleri, dijital imza, gözün retina ve iris tabakasından yararlanılarak çalışan sistemler mevcuttur. Buna örnek olarak Kuzey Carolina'daki uluslararası havaalanında kullanılan iris ile çalışan güvenlik sistemi örnek olarak gösterilebilir [18].

Bilgi ve Bilgi Güvenliği (Bilgi Güvenliği Sertifikasyonu)

- Büyüklüğü ne olursa olsun, ihtiyaç duyan tüm kurumların, kuruluşların bilgilerinin gizlilik, bütünlük ve erişebilirliklerini sağlamak amacıyla kurdukları bilgi güvenliği yönetim sistemini belgelendirmek ve bunu üçüncü taraflara kanıtlamak amacıyla aldıkları; bağımsız belgelendirme kuruluşlarının, yaptıkları denetim sonucu düzenledikleri ve kurumdaki bilgilerin güvenliklerinin sağlanması yönelik sistematik bir uygulamanın olduğunun kanıtını sağlamak üzere *kurum* adına düzenlenen sertifikaya veya belgeye **TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi** veya **TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Sertifikası** denir.

Bilgi ve Bilgi Güvenliği (Bilgi Güvenliği Sertifikasyonu)

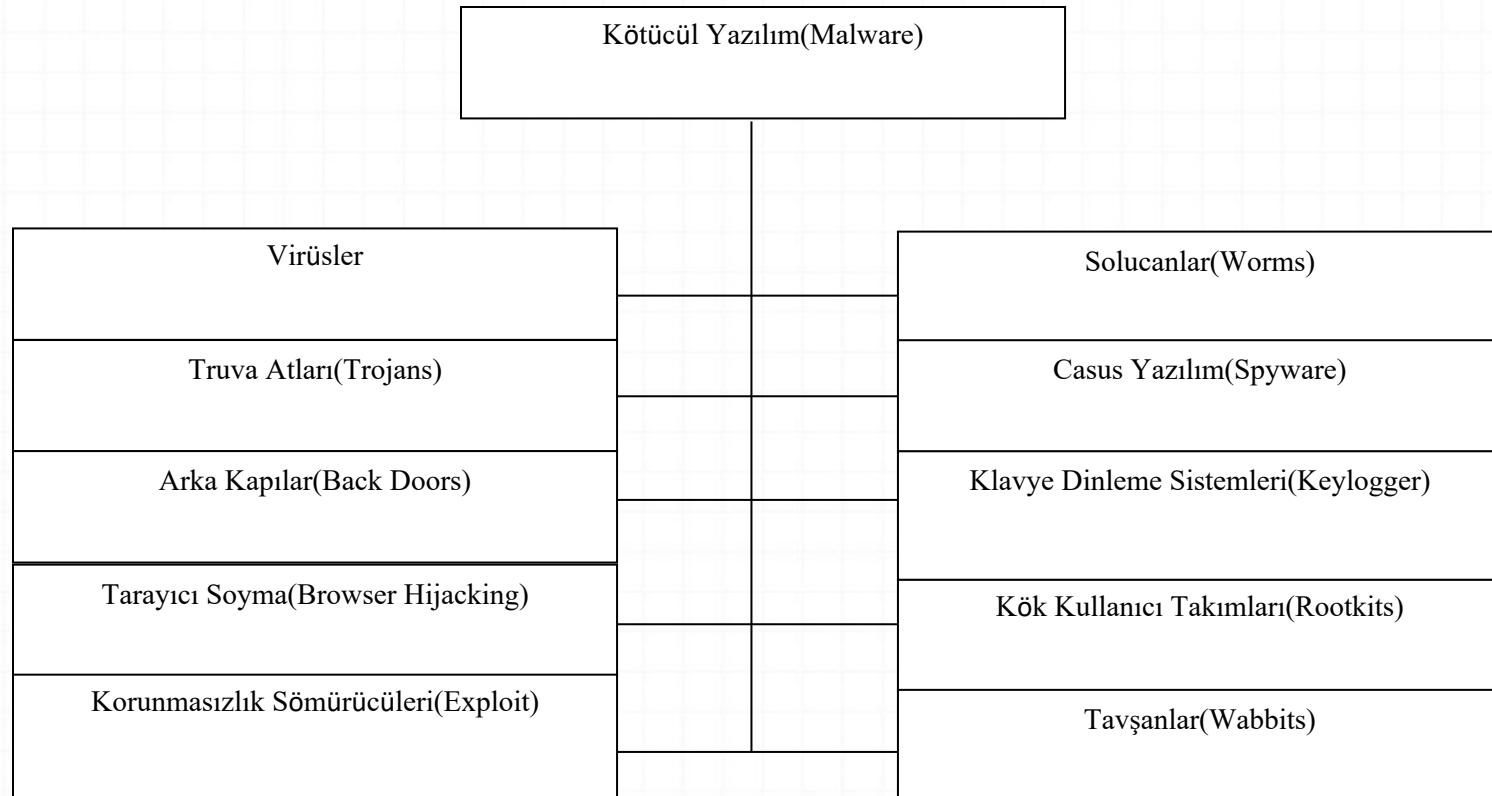
- TS ISO/IEC 27001 bilgi güvenliği yönetim sistemi kurmak ve belgelendirmek bir firmaya, şirkete veya kuruluşa bilgi güvenliği kavramının temel ilkelerini sağlamaktadır. Bilgi güvenliği kavramının temel ilkeleri kısaca G-B-U (C-I-A) kısaltması ile gösterilebilir. Bu kısaltmalar:
 - **Gizliliğin korunması** (bilgiye ulaşımın, sadece yetki sahibi kişilerce olabildiğinin garanti altına alınması)
 - **Bütünlük** (bilginin ve bilgi işleme yöntemlerinin, doğruluğunun ve eksiksizliğinin korunması)
 - **Ulaşılabilirlik** (gerekken durumlarda yetkili personelin, bilgiye ve ilgili varlıklara ulaşabilmesinin garanti edilmesi), şeklinde tanımlanır.

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımlar)

- Kötüçül yazılım (malware, İngilizce “malicious software”in kısaltılmış), bulasıtı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır. Özellikle Türkçe kaynaklı literatür tarandığında 11 adet ana kötüçül yazılımın varlığından bahsedilirken 38 adet yeni kötüçül casus yazılımdan bahsedilmektedir [26].

Bilgi ve Bilgi Güvenliği (Kötüçül Casus Yazılımlar)



Tablo 1. Kötüçül Yazılım Ana Türleri

Bilgi ve Bilgi Güvenliği (Kötüçül Casus Yazılımlar)

VİRÜS İSMİ	TİPİ	KARIŞTIĞI OLAYLAR	YÜZDE
Win32/Ska	File	140	13.28%
Laroux	Macro	124	11.76%
Marker	Macro	122	11.57%
Ethan	Macro	69	6.55%
Class	Macro	59	5.60%
Win32/Pretty	File	52	4.93%
Win32/NewApt	File	48	4.55%
Melissa	Macro	47	4.46%
Tristate	Macro	44	4.17%
Freelinks	Script	42	3.98%
Win32/Babylonia	File	32	3.04%
Cap	Macro	31	2.94%
Win32/Fix	File	31	2.94%
Thus	Macro	29	2.75%
Win32/Explore.Zip	File	21	1.99%
Win95/CIH	File	19	1.80%

Tablo 2. En Meşhur Virüsler

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımlar)

Yeni kötüçül yazılımlardan bir kısmı şunlardır:

- sazan avlama (phishing),
- koklayıcı (sniffer),
- kandırıcı (spoofing),
- şifre kıräciler (password cracker),
- reklâm yazılım(adware),
- ağ taşkını (flooder),

bununla beraber daha birçok yeni kötüçül yazılımın varlığından bahsedilmektedir.[26].

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımların Bulaşma Yöntemleri)

- Çoğunlukla ücretsiz dağıtılan uçtan uça dosya paylaşımı (P2P) programları, ekran koruyucular ve oyunlar içine casus yazılım bohçalanması ile bulaşma,
- Faydalı bir yazılım kurulumunun yanında; dosya, klasör ve sistem kütüğü isimlerini zararsız, bilindik veya sisteme ait isimler vererek saptanmasını ve sistemden kaldırılmasını zorlaştırarak sisteme yerleşme,
- Uç kullanıcı lisans sözleşmelerinde yaniltıcı veya eksik bildirim ile kullanıcıya zararlı bir yazılımı bilgisayarına kurdurtma,

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımların Bulaşma Yöntemleri)

- Herhangi bir programın kurulumu sırasında, aslında casus yazılım özelliği taşıyan başka yardımcı ve ek yazılımların kullanıcıya belirtilerek kurdurulması,
- E-posta dosya eklentisi ile e-posta'da verilen bir web adresine gidildiğinde veya doğrudan HTML içerikli e-postaların okunması ile casus yazılım bulaşması,
- İnternet tarayıcılarında bulunan korunmasızlık ve açıklardan yararlanarak kurulum,
- Özellikle internet üzerinden kullanıcıyı aldatıcı mesajlarla yanıltıp; her hangi bir casus yazılımın kurulumunun başlatılması,

Bilgi ve Bilgi Güvenliği

(Kötüçül Casus Yazılımların Bulaşma Yöntemleri)

- Çocukları ve bilinçsiz kullanıcıları aldatıcı taktikler kullanmak,
- Çok çeşitli sosyal mühendislik ve insan hatası kaynaklı yöntemler, olarak özetlenebilir.

Bilgi ve Bilgi Güvenliği

(Bilgisayarlarda Kötüçül Yazılımların Belirtileri)

- Bilgisayarın her zamanki başarımı düşüyorsa,
- İnternet üzerinde tarayıcı ile sörf ederken istenmedik siteler açılıyorsa,
- İnternet tarayıcısındaki arama çubuğu bölümünde aranmak istenen anahtar kelime girildiğinde ayarlanmış olan arama motoru yerine başka bir arama motoru arama sonuçlarını gösteriyorsa,
- İnternet tarayıcısındaki Sık Kullanılanlar (Favorites) veya Yer İmi (Bookmark) bölümünde yabancı sitelere bağlantılar eklenmişse,
- İnternet tarayıcısının başlangıçta gösterdiği site olan “Başlangıç Sayfası” (Home Page), ayarlanandan başka bir siteyi gösteriyorsa ve bu ayar tekrar düzeltildiğinde yine farklı siteler açılışta ortaya çıkıyorsa,

Bilgi ve Bilgi Güvenliği

(Bilgisayarlarda Kötüçül Yazılımların Belirtileri)

- Internet tarayıcısında daha önce olmayan araç çubukları varsa,
- Sistem tepsisinde (system tray) daha önce bilinmeyen bir simge varsa,
- Internet'e bağlantı olmadığı durumlarda bile kullanıcı adı ile hitap eden çıkiveren (pop-up) reklamlar görünüyorrsa,
- Internet sayfasında bazı tuşlar çalışmıyorsa (örneğin bir web formu doldururken bir sonraki yazım alanına geçmek için kullanılan sekme (tab) tuşu çalışmıyorsa),
- Bilgisayar ile faal olarak çalışmadığı bir sırada bilgisayar kasasındaki sabit disk hareketini gösteren lamba sürekli yanıp sönuyorsa,

Bilgi ve Bilgi Güvenliği

(Bilgisayarlarda Kötüçül Yazılımların Belirtileri)

- Internet'e erişim olmadığı sırada sistem tepsisindeki ağ bağlantısını gösteren (iki bilgisayar şeklinde gösterilen) simgede veri aktarımını gösteren hareketler görülmüyorsa,
- CD sürücüsü kendi kendine açılıp kapanıyorsa,
- Rastgele hata mesajları çıkıyorsa,
- Internet'e modem ile bağlanıp da büyük meblağlarda telefon faturası geliyorsa, sistemde çok büyük ihtimalle casus yazılım bulunmaktadır [19,26].

Bilgi ve Bilgi Güvenliği

(Bilgisayarların Kötüçül Casus Yazılımlardan Korunması)

Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Alınabilecek bazı güvenlik önlemlerini gerçekleştirmek bilgisayar güvenliği açısından iyi sonuçlar verecektir. Bu güvenlik tedbirleri aşağıdaki başlıklar halinde özetlenebilir:

- *Kötüçül Yazılımlardan Korunma*
- *İşletim Sistemi Güncellemeleri:*
- *Anti-Spyware (Casus Karşı Yazılım):*
- *Host (Sunucu) Bloklama*

Bilgi ve Bilgi Güvenliği

(Bilgisayarların Kötüçül Casus Yazılımlardan Korunması)

- *E-posta kontrolü*
- *Browser (Internet Tarayıcısı) kullanımı*
- *Ofis Programları*
- *Güvenlik Duvarı (Firewall)*

Bilişim Suçları

- Büyük bir ivme ile önemi artmakta olan bilgi güvenliği ve gün geçtikçe artan bilişim suçlarının adli olarak incelenmesi konuları büyük önem kazanmaktadır.
- Bilişim suçları yakın zamanda ortaya çıkan bir ifade olduğundan bazı kavramların birleşimi ile kendisine tanım bulmaya çalışmıştır. Bu kavramlar tanımlanarak bilişim suçu tanımı daha iyi anlaşılabilecektir.

Bilişim Suçları

- Hukuki anlamda **suç**, bir toplumdaki hukuki kurumlar tarafından ceza veya güvenlik tedbiri yaptırımına bağlanmış fiildir [1]. Uygulamada ise **suç**; başka insanların veya tüzel kişiliklerin haklarına tecavüz etmek veya yanlış ya da zararlı olduğu için yasaklanan ve bazı durumlarda cezalandırılan davranış olarak tanımlanabilir [2]. Suçu gerçekleştiren kişiye **suçlu** denir. Hukuki anlamda bir kimsenin suçlu kabul edilebilmesi için suçun o kimse tarafından işlendiğinin hukuki süreçler sonucunda **somut deliller** ile ispatlanması gerekmektedir.

Bilişim Suçları

- **Bilişim**, elektronik cihazlar yardımıyla bilgilerin sistematik ve otomatik olarak işlenmesidir. Bilişim, insanoğlunun kullandığı tüm telekomünikasyon araçları başta olmak üzere ağ haberleşme sistemleri, bilgisayarlar, uydu sistemleri gibi iletişim içeren ve insan hayatını kolaylaştırmaya yönelik tasarlanan sistemleri kapsar. Bilişim sistemlerinin insan hayatında vazgeçilmezler arasına girmesi, beraberinde bazı sorunları da getirmektedir. Bu sorunların en öne çıkanı sanal ortamdaki bilgi hırsızlığıdır. Bu sanal ortamdaki sorunlar ise bilişim suçu kavramını ortaya çıkarmıştır.

Bilişim Suçları

- En genel anlamıyla bilişim alanında kullanılan araçlardan yararlanılarak işlenilen suçlar, **bilişim suçu** olarak tanımlanmaktadır. Bununla beraber bilişim suçları TCK'de bilişim sistemleri kullanılarak işlenen suçlar olarak tanımlanmaktadır. Bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi veya kopyalanması da, **bilişim suçları** olarak tanımlanmaktadır [4].

Bilişim Suçları

- Bir bilişim suçunu işlededeki nedenler arasında maddi kazanç elde etmek, kişilerin itibarını sarsmak, intikam almak, sosyal hayatı insanlara aktaramadığını sanal ortamda gerçekleştirmek, karalamak veya yakalanma ihtimalinin zor olduğunu düşünerek zevk amaçlı saldırı yapmak gibi sebepler ortaya çıkmaktadır.

Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- Ülkemizde meydana gelen bilişim suçlarına somut örnekler vermek de mümkündür. CHP eski genel başkanının şahsına yapılan ve sanal ortamda ülkemiz dışındaki bir sunucudan yayılan mahremiyete dair video görüntüleri bilişim suçlarının artık günümüzde her şekilde kullanılabileceğini göstermektedir.



Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- Internetin yaygınlaşması ile **bilişim suçu olarak tanımlayamayacağımız** ancak millet menfaatine gibi görünen olaylarda mevcuttur. Bu oylara somut bir örnek verilirse, mesai saatleri içerisinde bankada sıra bekleyerek işlemlerini tamamlamak isteyen müşterilerle ilgilenmeyen bir çalışanın, bilgisayarında oyun oynadığının görüntülenmesi ve görüntülerin internet ortamına aktarılması olayları da mevcuttur. Bu durum, suç kabul edilmeyip millet menfaatine gözüktüğünden görüntüyü internete aktaran kişi hakkında inceleme başlatılmamış olup, bilişim suçu kapsamına alınmamıştır.

Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- Ülkemizde artan bilişim suçlarının incelenmesi ve hukuki anlamda kontrolün sağlanması için çalışmalar yapıldığı görülmekte ancak uygulamada henüz istenen seviyeye ulaşılamaladığı anlaşılmaktadır.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Delil:** İşlenen bir suç olayında fail/faillerin ortaya çıkarılabilmesi için ipuçları niteliğinde toplanan kaynaklar *delil* olarak tanımlanır. Bu deliller, aydınlatılması istenen olayın en önemli parçalarıdır. Bu elde edilen deliller bir araya getirilerek tüm resim görülmeye çalışılır. Böylece aydınlatılmak istenen olay bir çözüme kavuşturulmuş olur.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Delillendirme:** Suçların tespiti ve yargılanmasındaki en önemli husus *delillendirme* olarak tanımlanmaktadır. *Delillendirme* kısaca, bir suç ile ilgili o suçun kim tarafından ve ne şekilde işlendiğini ispat edici nitelikte bilgiler elde edilmesi ve bunun adli mercilere sunulması şeklinde tanımlanabilir.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Dijital Delil:** Sanal ortamda işlenen suçlardaki, suçluların tespit edilmesi için elde edilen kanıtlar *dijital delil* olarak isimlendirilmektedir. Bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere dijital delil denilmektedir. Bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen veriler” olarak tanımlanmıştır.dijital deliller “bir suçun işlendiğini gösteren veya suç ile kurban ya da suç ile faili arasında bir ilişki sağlayan veriler” olarak karşımıza çıkmaktadır [7].

Bilişim Suçları

(Dijital Delillerin Özellikleri)

- Dijital deliller, parmak izi veya DNA gibi gizli veriler olabilirler.
- Dijital deliller, kolaylıkla ve hızla sınırları aşabilirler.
- Dijital deliller, kolaylıkla değiştirilebilir, zarar verilebilir veya silinebilirler.
- Dijital deliller, bazen zaman ile sınırlı olabilirler.
- Dijital deliller, genellikle uçucu verilerdir.
- Dijital deliller, güvenliği sağlanmaz ise çabuk deformasyona uğrayabilirler.
- Dijital deliler, yapı itibariyle, fiziksel delillere göre daha hassas ve kolay bozulur niteliktedirler.

Bilişim Suçları

(Dijital Delillerin Özellikleri)

Dijital deliller, normal somut delillere göre yapı itibariyle bazı sıkıntıları barındırmaktadır. Bu sıkıntılar şu şekilde özetlenebilir:

1. Dijital Delillerin Bütünlüğü
2. Dijital Delillerin Doğrulanması
3. Dijital Delillerin İnkar Edilememesi
4. Dijital Delillerin Doğruluğu:
5. Dijital Delillerin Daha Sonradan Ele Alınabilirliği [7,11].

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Bilişim suçlarındaki dijital delillerin elde edildiği birçok kaynak olabilir. Bunlar genel olarak şu şekilde sıralanabilir:

- Bilgisayar sistemleri (Masaüstü, dizüstü, sunucu vb.)
- Bilgisayar bileşenleri (HDD, memory vb)
- Erişim kontrol araçları(Smart kartlar, biometrik tarayıcılar)
- Çağrı cihazları, Dijital kameralar,PDA ve PALM cihazları
- Harici harddiskler , Hafıza kartları, Network araçları (Modem, yönlendirici, anahtar)
- Yazıcılar, tarayıcılar ve fotokopi makineleri
- Çıkarılabilir yedekleme üniteleri (Disket, CD, DVD...)
- Telefonlar,Kredi kartı okuyucuları, GPS

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Dijital deliller birçok tipte karşımıza çıkmaktadır. Bunlardan bazıları şunlardır:

- Veri dosyaları
- Kurtarılmış, silinmiş dosyalar
- Kayıp alanlardan kurtarılmış veriler
- Dijital fotoğraf ve videolar
- Sunucu kayıt dosyaları
- E-posta
- Chat kayıtları
- İnternet geçmişi
- Web sayfaları
- Kayıt (log)

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Dijital delillerin elde edildiği alanlardan en çok göze çarpanları şunlardır:

- Bilgisayarlar (Masaüstü, dizüstü bilgisayar, PDA, sunucu, istemci)
- Elektronik aygıtlar
- Veri havuzları
- Bir sistemde yapılan işlemleri gösteren kayıtlar, geçmiş bilgileri, erişim listeleri
- Yedekleme üniteleri
- Yazılımlar
- E-Postalar
- Çerezler gibi internet ile ilgili dosyalar[7,11].

Bilişim Suçları

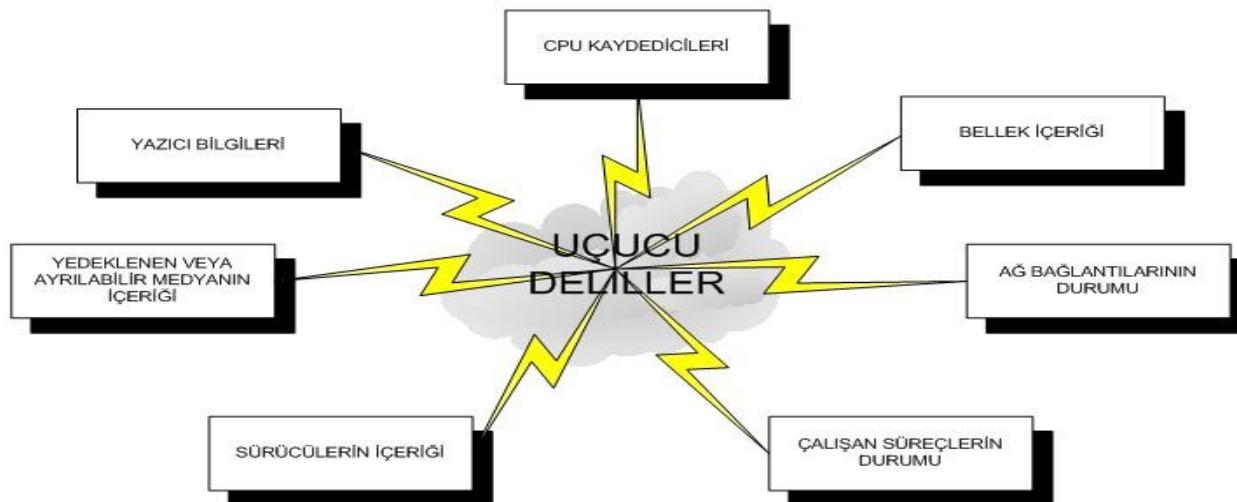
(Dijital Delillerin Toplanması)

- Sanal bir suçun varlığından şüpheleniliyor ise söz konusu suç veya vaka ile ilgili potansiyel delillerin toplanması gerekmektedir. Sürecin doğru bir şekilde işlemesi için öncelikle uygun prosedürleri ve gerekli hukuki şartları anlamak ve sağlamak büyük önem arz etmektedir. Geleneksel delil toplama, delillerin daha sonradan incelenmek üzere sahiplenilmesi anlamına gelmektedir. Fakat dijital delillerde durum biraz farklıdır. Delillerin doğrudan toplanması esnasında bazlarının kaybedilmesi, bozulması ile karşılaşılabilir.

Bilişim Suçları

(Dijital Delillerin Toplanması)

- Uçucu veriler (Ör: bellek, CPU kaydedicileri, çalışan süreçlerin durumu) dediğimiz elektrik kesildiğinde içeriği sıfırlanan ve tekrar kurtarılması mümkün olmayan delillerdir



Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Saldırı* ifadesi en bilindik anlamda kötülük yapmak, yıpratmak amacıyla, bir kimseye karşı doğrudan doğruya silahlı veya silahsız bir eylemde bulunma, hücum, taarruz veya bir sistemin kullanılamaz hale getirilmesi için yapılan her türlü meşru veya gayri meşru hareketler olarak tanımlanabilir. Bilişim sistemlerine yapılan saldırılar *da digital saldırı* olarak tanımlanmaktadır. Dijital saldırılardaki amaç, bilgiyi çalmak, bozmak, sızdırmak veya bilişim sistemindeki yazılım ve donanımlara zarar vermek olarak belirtilebilir. Dijital saldırıları aktif ve pasif saldırı olarak ikiye ayırmak mümkündür.

Bilişim Suçları

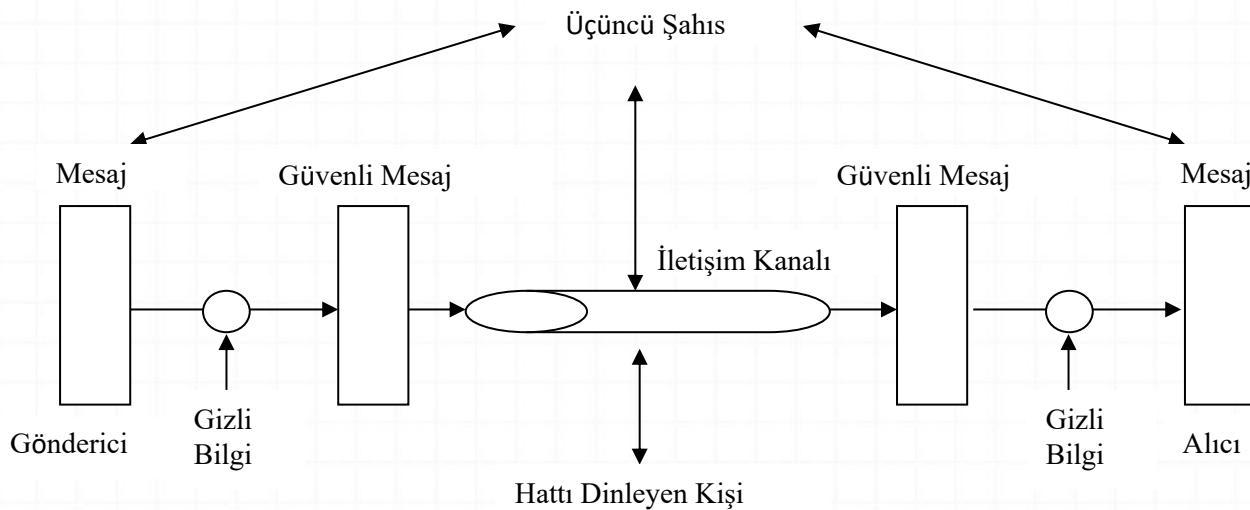
(Dijital Saldırılar ve Dijital Saldırganlar)

- *Pasif saldırıda*, saldırın taraf pasif davranmakta ve çoğu zaman sadece sistemi gözetlemekle yetinmektedir. Bu saldırı şeklindeki saldırın yakalanması çoğu zaman daha güç olmaktadır. Pasif saldırı yöntemlerine örnek olarak; Mesajın içeriğini edinme, trafigin akışını takip etme gibi yöntemler verilebilir.
- *Aktif saldırı* yönteminde ise saldırın aktif olarak rol oynar ve sistemin içerisine dahil olur. Sistemi savunan tarafın, saldırın yakalama veya tespit etme ihtimali yüksektir. Aktif saldırı yöntemlerine örnek olarak;
- Rol yapmak (Sniffer olayı, IP aldatmacası vb.)
- Eski mesajın tekrarlanması
- Aktarılan mesajı değiştirme
- Hizmet dışı bırakma/engelleme, gibi yöntemler sayılabilir.

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Şekil de görüleceği gibi aktif veya pasif saldırı mesajın çıkış noktasından başlayarak varış noktasına kadar üçüncü şahıs olarak adlandırılan saldırıcı tarafından herhangi bir bölgede gerçekleştirilebilir.



Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Hackerlar(saldırganlar)*, kültür ve bilgi düzeyi oldukça yüksek olan, en az bir işletim sisteminin yapısını tam olarak bilen, programcılık deneyimleri yüksek ve konusunda ileri eğitimler alarak uzun yıllarını bu işlere adamış kişilerdir [9]. Diğer bir tanımda ise işletim sistemlerini tam manası ile bilen, derinliklerine inen, bilgisayarla derinlemesine ilgilenen, programlamayı profesyonel düzeyde bilen bilgisayar uzmanlarıdır [8].

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Yapılan hacker tanımlamalarına bakılarak farklı niyette çalışan hackerler olduğu görülmektedir. Hackerlar; **beyaz şapkali hacker, siyah şapkali hacker** ve **gri şapkali hacker** olarak sınıflandırılmaktadırlar.
- *Hacking* olarak ifade edilen kavram ise bir sisteme sizma ya da zarar verme anlamında yapılan saldırıların genel adıdır.
- *Beyaz şapkali hackerlar* bilgi bakımından siyah şapkallardan aşağı kalmamakla beraber; iyi niyetli, zarar vermeyen, amaçları bilgisayar güvenliğini sağlamak olan kişilerdir [8].

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Siyah şapkalı hacker* kavramı ise tamamen kötü niyetli, sırf kazanç elde etmek ve karşıya zarar verme amacıyla sistemlere sızan, bilgi çalan, korsanlar için kullanılır. Bu grup hackerların amacı bilgi çalmak veya sisteme zarar vermektedir [8]. Siyah şapkalı hackerlar bazı çalışmalarda korsan, saldırıcı veya 3. şahıs olarak da adlandırılmaktadırlar.
- Beyaz şapkalı ve siyah şapkalı grubun arasında kalan *gri şapkalı hacker* olarak adlandırılan bir grup vardır ki bunlar yerine göre siyah yerine göre de beyaz şapkalı hacker gibi hareket ederler.

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Bilişim sistemlerine zarar vermek amaçlı çalışan kişiler genelde *cracker* tanımlamasına dahildirler.
- Siyah şapkalı hackerlara nazaran daha zararsız olarak tanımlayabileceğimiz *Lamer* ifadesi genelde küçük yaşta ve hacker özentisi olan, birkaç hacker işlemini bilen ancak programlama bilgisi olmayan, herkesin yapabileceği işleri yaparak ün kazanmak isteyen kullanıcılardır. *Script Kiddie* ise genelde lise çağında olan, programlama bilgisi olmayan genellikle e-postalara saldırıma işlemlerini öğrenen kişilerdir. Lamerlara göre fazla hacking bilgileri vardır [8].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- **Siber** kelimesi bilgisayar ağlarına ait olan, internete ait olan, sanal gerçeklik manalarına gelmektedir.
- Soyut olarak iletişim kurulan sistemler *siber alan* olarak tanımlanmaktadır. Dünya üzerindeki en büyük iletişim sistemi olan interneti anlatan sanal alem ve siber alem kavramlarının ikisi de doğru birer önermedir. Siber alanın yaygınlaşması bazı kavramlarında beraberinde ortaya çıkmasına sebep olmuştur.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Zorbalık denince sözlü veya fiziksel şiddet anımları akla gelir. *Siber zorbalık*, bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür. Elektronik zorbalık ve elektronik iletişim zorbalığı olmak üzere iki çeşit siber zorbalık mevcuttur.
- Siber zorbalık veya tehdidin en çok sosyal medya sitelerinde meydana geldiği görülmektedir. Genellikle fotoğraf ve video yayınılama tarzında gerçekleşen bu eylemler bazen sözlü alay ifadeleri ile mahremiyetlere zarar vermektedir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Elektronik zorbalık*, kişilerin şifrelerini ele geçirme, web sitelerini hackleme (bir sisteme izinsiz girmek), spam (zararlı virüs) içeren e-postalar gönderme gibi teknik olayları içeriyor. Bu tip saldırılar, bireylerin web siteleriyle sınırlı kalmayıp, kurumların ve devletlerin siteleri, yazılım ya da donanımlarını da olumsuz etkiliyor.
- *Elektronik iletişim zorbalığı* ise bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme (cyber-stalking), alay etme, isim takma, dedikodu yayma, hakaret ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi ilişkisel saldırı davranışlarını içeriyor. Bu da direkt olarak insanın duygusal ve psikolojisini etkiliyor [14].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Bilgi sistemleri doğrultusunda elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla, ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinlikler *siber saldırı* olarak isimlendirilmektedir. Siber saldırılar genellikle İnternet üzerinden yapılan tecrübeli hackerların yapabildiği saldırısı biçimidir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Siber Terörizm(Savaş)* belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırmaya, baskı altında tutma amacıyla kullanılmasıdır [13].
- Siber terörde, saldırganların elektronik bir saldırısı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğalgazı kapatabilecekleri, bilgisayar sistemlerini karmaşık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve finans sektörünü çökertebilecekleri, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dahilindedir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Siber ordular* ulusal güvenliği sanal ortamda sağlayan ordulardır. Siber orduların öneminin farkında olan Amerika Birleşik Devletleri gibi gelişmiş ülkeler sanal ortamda saldırı tespit yöntemleri oluşturmaya yönelik yarışmalar düzenleyerek konu hakkında yetenekli kişileri bu ordularına dahil etmektedirler. Pentagonun düzenlediği güvenlikle ilgili bir yarışmada birinci olan bir Türk öğrencinin Pentagon'dan davet mektubu alması buna bir örnektir [15].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Bilişim dünyasında yeni bir kavram olarak yer bulmaya başlayan **siber ahlak** olarak da tanımlayabileceğimiz siber etik en genel anlamıyla gerçek hayatı iyi bir birey olmak için yapılan fiillerin sanal ortamda da yapılması olarak tanımlanmaktadır.
- Sanal alemden davranış kuralları konusunda özellikle genç kuşağın eğitilmesi gerekmektedir. Günlük yaşamında hırsızlık yapmayı ahlaki değerleriyle veya toplumsal statüsü ile bağıdaştıramayan bir genç net ortamında rahatlıkla hırsızlık yapabilmekte veya başkalarına zarar verebilmektedir.

Bilişim Suçları

(Adli Bilişim)

- Adli kelimesi TDK'nin sözlüklerinde adliye teşkilâti ve hizmeti ile ilgili, adaletle ilgili olarak tanımlanmaktadır. Bu bağlamda adalete intikal etmesi gereken hadiselerin tamamına ise *adli vaka* veya *adli olay* denmektedir.
- Adli bilişim teriminin kökeni, İngilizce orijinal ismi ile Computer Forensics'tir

Bilişim Suçları

(Adli Bilişim Çeşitleri)

- 1.Bilgisayar Adli Bilişimi (Computer Forensics) :** Daha çok bir bilgisayar üzerinde yapılacak araştırmalarla ilgilenir. Örneğin: Harddisk, RAM, işletim sistemi üzerinde yapılacak araştırmaları kapsar.
- 2.Bilgisayar Ağlarına Yönelik Adli Bilişim (Network Forensics) :** Ağ sistemleri ve iletişimine yönelik incelemeyi kapsar.
- 3.Bilgisayar Ağ Cihazlarına Yönelik Adli Bilişim (Network Device Forensics):** Yönlendirici, switch gibi cihazlar üzerinde yapılacak incelemeyi kapsar.
- 4.İnternet Adli Bilişimi (Internet Forensics):** Genel olarak internet kaynakları ve internet sistemleri üzerinde yapılan araştırmayı kapsar.
- 5.Bilgi Adli Bilişimi (Information Forensics):** Bütün olarak bilgiyi içeren her türlü materyali barındıran sistemler üzerinde yapılan incelemeyi kapsar.

Bilişim Suçları

(Adli Bilişim Çalışma Alanları)

- Adli bilişimin çalışma alanlarından bazıları ana başlıklar halinde şöyle sıralanabilir:
- Veri kurtarma
- Veri imha etme
- Veri saklama
- Veri dönüştürme
- Şifreleme(Kriptografi)
- Şifre çözme
- Gizlenmiş dosya bulma.

Bilişim Suçları

(Adli Bilişimin Faydaları)

- Adli bilişim, yalnızca bilişim suçlarına has bir delil toplama metodu değildir. Bilişim suçlarından başka, klasik suçlara ilişkin olarak da ihtiyaç duyulan deliller, yine elektronik aygıtlar içerisinde de yer alabilir. Örneğin, bir bilişim suçu olmayan bir hırsızlık vakasında, soygun planı ve buna ilişkin haritalar bilgisayar ile hazırlanmış ve halen bilgisayarda mevcut olabilir. Bu bilgilere ulaşmada da yine adli bilişim devreye girecektir. Bu duruma en bariz örnek olarak; hala devam etmekte olan *Ergenekon* soruşturması ile alakalı bazı verilere, bilgisayar kayıtlarından ulaşılması gösterilebilir.

Bilişim Suçları

(Adli Bilişim Uzmanlığı)

- *Adli bilişim uzmani*, bilişim sistemleri konusunda ileri derecede bilgi sahibi olan kimsedir.
- Adli bilişim uzmanı kabul edilmek için birtakım sertifika programları mevcuttur. Bu programlardan birine devam ederek sertifika almak ve adli bilişim uzmanı sıfatına sahip olmak mümkündür.
- Bu sertifika programlarından en çok kabul edilenleri şunlardır: EnCase Certified Examiner (ENCE), Certified Computer Examiner (CCE), Certified Computer Crime Investigator (CCCI), Computer Forensic Computer Examiner (CFCE), Certified Information Forensics Investigator (CIFI), Professional Certified Investigator (PCI) [16].

Bilişim Suçları

(Adli Bilişimde Dijital Delillerin Kanıt Olarak Kullanılabilmesi)

- Adli bilişimde elektronik bulgunun, bir hukuki delile dönüştürülme süreci belli prosedürleri takip eder. Uygulanan bu prosedürlerden sonra dijital delil, kendisini bir hukuki delil olarak ortaya koyar. İşte bu prosedüre, *adli bilişim safhaları* denilmektedir. Adli bilişimde dijital delillerin kanıt olarak kullanılabilmesi için incelenmesi gereken dört safha şu şekildedir [16]:
 - Toplama (Collection)
 - İnceleme (Examination)
 - Çözümleme (Analysis)
 - Raporlama (Reporting)

Sonuç

- Bilgi güvenliği konusunda güvenlik açıklarının önlenenebilmesi için, kişilerin ve kurumların basitten en karmaşık yöntemlere kadar bir dizi önlemler alması gereklidir. Ancak, tüm önlemler alınmış olsa da, sürekli gelişen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş kendini **%100** güvende hissetmemelidir. Saldırılar; kötü niyetli kişiler, arkadaşlarımız veya tanıdığımız kişilerden gelebilir.

Sonuç

- Alınması gereken en temel önlemler, risklere karşı sürekli uyanık olmak, bu çalışmada açıklanan saldırıcı tekniklerine karşı uyanık olmak, yeni gelişmeler ışığında gerekli güncellemeleri yaparak saldırılardan etkilenme olasılığını en aza indirmek olarak belirtilebilir. Güvenliğin statik değil dinamik bir süreç sahip olduğu, koruma ve sağlamlaştırma ile başladığını, bir hazırlık işlemine ihtiyaç duyulduğu, saldırıların tespit edilmesinden sonra hızlıca müdahale edilmesi gereği ve sistemde her zaman iyileştirme yapılması gereği unutulmamalıdır.

Sorularınız



YMH321 Bilgi Sistemleri ve Güvenliği

Güvenlik ve Hacking Kavramları

Bölüm - 3

Prof.Dr. Resul DAŞ

Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarları

- Bilişim güvenliği
- Bilişim güvenliği niçin önemlidir ?
- Hacker,
- Hacker çeşitleri,
- Hacker'lardan korunma yolları,
- Sosyal Mühendislik kavramı,
- Sosyal Mühendislik çeşitleri,
- Sosyal Mühendislerin kullandığı yöntemler,
- Sosyal Mühendislerinden korunma yolları

BİLİŞİM GÜVENLİĞİ NEDİR VE NİÇİN ÖNEMLİDİR?

- Bilişim suçları ve Güvenlik araştırmasıının her yıl hazırladığı rapora göre bilişim suçları neredeyse her yıl 2 katına arttığı gözlenmiştir.
- Bilişim teknolojilerinin hayatımızın her alanında girmiş olmasıyla birlikte faydaları kadar bize dokunan zararları da ortaya çıkmıştır. Bilişim teknolojileri gelişikçe sistemlere yapılan saldırılar artmakta ve saldırı teknolojileri gelişmektedir.

BİLGİ GÜVENLİĞİMİZ İÇİN NELER YAPABİLİRİZ ?

- Şifre güvenliği
- Güvenilmeyen adreslerden gelen e-posta'ları okumak için dahi olsa açmamak (Resimli E-posta eklentileri)
- Geliştiricisi bilinmeyen Facebook Application 'lara katılmamak
- Tanımadığımız kişilerden gelen isteklere, aktivitelere katılmamak (Facebook, MSN vs.)
- Gerçek bilgilerimizi her yerde paylaşmamak (e-posta, TC kimlik No vs.)
- İnternette verdigimiz tüm bilgilere birilerinin ulaştığını düşünerek her düşündüğümüzü, yaptığımızı vs. ulu orta paylaşmamak ☺
- Bilgi güvenliğimiz için birden fazla adres (e-posta vs.) kullanmaya özen göstermeliyiz.

Bunları biliyor muydunuz ?

- MSN'de hotmail ve windowslive.com gibi uzantılarda tek bir şifre ile korunurken, gmail vs. gibi Microsoft haricindeki diğer uzantılarda MSN ve mailin aynı şifre olması zorunlu değil.
- Facebook 'da hangi bilgisayardan (hatta browser'dan) giriş yaptıysan o bilgisayarın bilgilerini kayıt edip, eğer bilmediğin bir ortamdan adresine giriş yapmış ise oturumu sonlandırabiliriz.
- WLM 2011 ile birlikte bir bilgisayarı güvenilen bir bilgisayar olarak gösterip, şifreni unuttuğunda direk güvenilen bilgisayar üzerinden hiçbir soru sorulmaksızın yeni şifre oluşturabiliriz.

HACK – HACKER KAVRAMLARI ?

- Hacker: Bilişim teknolojilerindeki bilgisini İYİ veya KÖTÜ olmak üzere bir sistemi ele geçirmek üzere kullanan kişi
- Hack: Kısaca bir hacker'ın yaptığı saldırıyla verilen genel ad

DÜNYADAKİ BİLİŞİM SUÇLARI EN ÇOK HANGİ ÜLKELERDE İŞLENİYOR ?

- Türkiye, Rusya ve Brezilya
- Sebep: Bilişim suçlarına olan cezaların yetersiz kalması ve yeterince uygulanamaması

HACKER ÇEŞİTLERİ

- Yaptığı saldırısı düzeyine göre Beyaz ve siyah şapkaklı olmak üzere ikiye ayrılır.
- Ayrıca, siyah şapkaklı hackerlar kendi içinde ayrılabilir.
- -Script Kiddies (Lamer): Kendini bir şey zanneden hacker ☺
- -Phreakers: Santral ve telefon hatlarının açıklarını kullanan hacker
- -Crackers: PC yazılımlarını kıran ve yayinallyan hacker
- -Grey Hat Hackers: Hem savunma hemde saldırı amaçlı çalışan hacker. Amacı sadece kazanmaktır

DÜNYANIN EN ÜNLÜ HACKER'I KİMDİR ? YAPTIĞI SALDIRILAR

- Kevin David Mitnick (**Condor** olarak da bilinir) (d. 6 Ağustos, 1963), ilk bilgisayar korsanlarından olup en meşhurudur. 15 Şubat 1995'te FBI tarafından yakalanmıştır. Fujitsu, Motorola, Nokia ve Sun Microsystems gibi şirketlerin bilgisayar ağlarına izinsiz girmekten suçlu bulunarak 5 yıl hapis cezası almıştır. Cezası 21 Ocak 2000'de, bilgisayarlara yaklaşma yasağı 21 Ocak 2003'te bitmiştir. Günümüzde, beyaz şapkalı bir bilgisayar korsanı olarak güvenlik danışmanlığı yapmakta ve dünya çapında kongrelere katılmaktadır.
- Mitnick, fotoğrafı FBI'in "En Çok Arananlar" listesinde yer alan ilk hacker olarak kayıtlara geçti ve neredeyse listeden hiç eksik olmadı. "İflah olmaz bir suçlu" olan çocuk ruhlu Mitnick "Sanal Dünya'nın Kayıp Çocuğu" olarak da tanındı.

DENNIS RITCHIE VEYA KEN THOMPSON'I TANIYOR MUSUNUZ ?

- İlk başlar siyah şapkalı hacker olup sonradan beyaz şapkalılara katılan ünlü hacker'lardan.
- Esas ünleri C ve C++ Dillerini yazıp, Unix işletim sisteminin baş mimarı olmalarıdır.
- C programlama dili bugün hâlâ yazılım dünyasında aktif olarak kullanılmaktadır ve C++, Java, C# gibi modern programlama dillerini de etkilemiş konumdadır.

DENNIS RITCHIE VEYA KEN THOMPSON'I TANIYOR MUSUNUZ ?

- Ünlü Linux işletim sistemi ve onun araçları Dennis Ritchie'nin yaptıklarına dayanmaktadır. Windows işletim sistemi de Unix uyumlu araçlar ve geliştiriciler için C derleyicileri içermektedir.



Ken Thompson (solda) ile Dennis Ritchie (sağda)

SOSYAL MÜHENDİSLİK

KAVRAMI =?

- Akıllı insan kendi aklını kullanır. Daha akıllı insan ise hem kendi aklını hem de başkalarının aklını kullanır.
- BT alanında yeterli teknik bilgiye sahip olup açık aramaktansa insanların zayıf ve bilgisiz noktalarını kötü niyetli kullanan yaratiktır

SOS. MÜH. ÇEŞİTLERİ ?

- İnsan tabanlı ve PC Tabanlı olmak üzere ikiye ayıralabiliriz.
- PC tabanlı Sos. Müh. hem aklını hem de PC bilgilerini kullanan kişidir desek herhalde yanlış olmaz.

SOS. MÜH. ÖRNEKLERİ?

- Sahte mail (Bir kişi ya da kurum adına mail göndererek kandırma)
- Bir web sitesinin tasarım olarak benzerini yapıp, domain olarakta çok benzer bir domain alıp, bilgilerimize erişmek
- Reklam'lara tıkla para kazan vs. sahte siteler.
- Kendisini bir firmanın yetkili kişisi gibi tanıtip bilgilerine erişmek.

Sonuç



Sorular



YMH321 Bilgi Sistemleri ve Güvenliği

Ağ Güvenliği

Bölüm - 4

Prof. Dr. Resul DAŞ

Fırat Üniversitesi – Teknoloji Fakültesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarları

- Wireshark
- Wimax
- Güvenli İşletim Sistemleri

Wireshark

- Wireshark, 1998 yılında Ethereal adıyla faaliyete başlayan bir projedir.
- Wireshark ismiyle çıkan bu yazılım bilgisayara ulaşan paketleri yakalamaya ve bu paketlerin içeriğini görüntülemeye imkan tanır. Bir başka deyişle bilgisayara bağlı olan her türlü ağ kartlarındaki (Ethernet kartı veya modem kartı) tüm TCP/IP mesajlarını analiz eden bir programdır.
- Wireshark günümüzde çok amaçlı kullanılmaktadır.
 - *Şebeke problemlerinde sorun çözme
 - *Güvenlik problemlerini sınamak
 - *Uygulamaya konan protokollerde oluşan hataları onarmak veya arındırmak
 - *Ağ problemlerinin içindeki bilgileri öğrenebilmek amacıyla kullanılmaktadır.

WiRESHARK ÖZELLİKLERİ

- Windows, Unix, OS X, Solaris, FreeBSD, NetBSD ve birçok işletim sistemleri için uygundur.
- Yerel ağ arayüzünden paketleri tutar, ayrıntılı bir şekilde protokol bilgileriyle görüntüler.
- Tutulan bilgileri kaydetme özelliği vardır.
- Çeşitli kriterlerde paket arar ve filtreler.
- Çeşitli istatistikleri yapılan ayarlar doğrultusunda kullanıcıya sunar.
- Birçok protokol için şifre çözme desteği sunar.
(IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, ve WPA/WPA2'yi içerir).

Wireshark kullanımı ile ilgili örnekler

- Ağ trafik tespiti
- Veri madenciliği
- Saldırı tespiti
- Port tarama tespiti
- Virüslerin bulaştığını veya Denial of Service(Dos) ataklarını bulma tespiti
- Bağlantı sorunu tespiti
- Casus yazılım tespiti

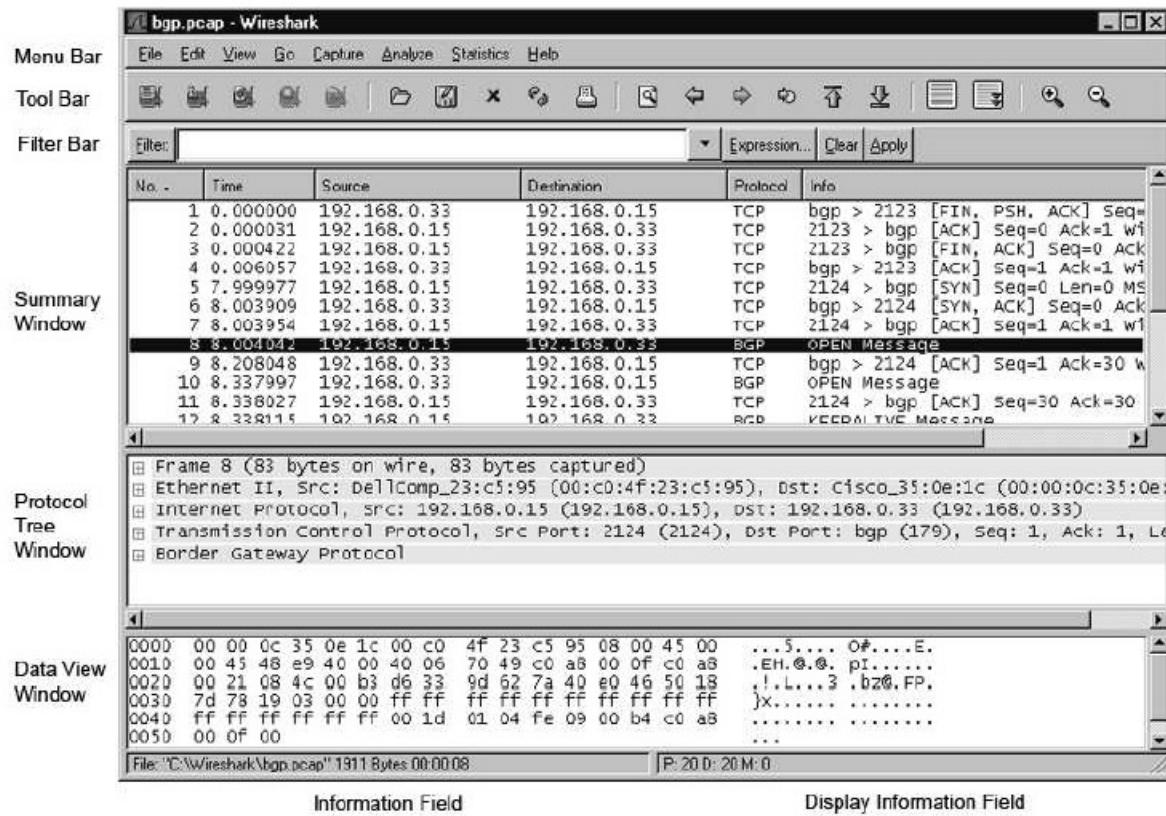
Wireshark bileşenleri

- Wireshark iletişim ağının iç yüzünde neler olduğunu kavramamızı sağlar.
- Bu özelliğiyle; uygulama protokollerinde, ağ uygulamalarındaki sorunları
- çözmede, ağı test etmede ve canlı ağ bağlantılarındaki sorunları
- çözmemizde bize yardımcı olur. Yani, iletişim ağı ile teknik düzey
- arasında etkileşim sağlayarak pek çok problemi çözmemizi sağlar. Bu
- bölümde wireshark'ın grafiksel kullanıcı ara yüzündeki ana bileşenleri
- tanımlayacağız :

Wireshark bileşenleri

- Main window
- Menu bar
- Tool bar
- Summary window
- Protocol Tree window
- Data View window
- Filter bar
- Information field
- Display information

Wireshark Görüntüsü



ANA PENCERE (MAIN WINDOW)

Menu Bar	Menudeki maddelerin, grafiksel ara yüzünü içeren klasik bir uygulamadır.
Tool Bar	Wireshark'ın sık kullanılan fonksiyonlarının kısa yollarını içerir. Kullanıcıya göre ayarlanabilir.
Filter Bar	Yakalanan paketleri, istenilen şekilde ayrılarak gösterilmesini sağlar.
Summary Window	Yakalanan paketlerin her biri için, bir satırlık özet bilgi sunar.
Protocol Tree Window	Summary window 'da seçili olan paketin detaylı bilgilerini, kullanıcıların anlayacağı şekilde düzenleyerek sunar.
Data View Window	Summary Window 'da seçili olan paketin, detaylı bilgilerini, herhangi bir düzenleme yapmadan sunar.
Display Information Field	Yakallanmış paketlerin numaralarını, güncel olarak gösterir.

SUMMARY WINDOW

- Yakallanmış paketlerin tamamına buradan bakılabilir. Her bir dosyanın içeriği bir satır olarak sunulur, satırlar belli özelliklerine göre sütunlara ayrılır.

Sütun adı	Tanımı
No	Yakalanan dosyanın içindeki paketlerin numarasını temsil eder. Görüntüleme filtresi (display fitler) kullanılmadığı sürece bu numara değiştirilemez.
Time	Paketin zaman damgasıdır.
Source	Paketin nereden geldiğini gösterir.
Destination	Paketin nereye gittiğini gösterir.
Protocol	Protokol isminin kısa versiyonudur.
Info	Paket içeriği hakkında ekstra bilgi gösterir.

SUMMARY WINDOW

- Bu dosyalar daha ayrıntılıda incelenebilir. Herhangi bir dosya seçilirse "Packet Details" ve "Packet Bytes" pencereleri açılır. Bir paketin içeriğine bakılacak olursa, Ethernet paketinin içinde IP, onun içinde TCP bulunur. Ethernet tarayıcısı kendi bilgisini(örneğin Ethernet Adresleri) yazar, IP tarayıcısı onun üstüne kendi bilgisini(örneğin IP adresleri) yazar ve TCP tarayıcısı da onun üstüne IP bilgisini yazacaktır.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [FIN, PSH, ACK] Seq=1 Ack=1
2	0.000031	192.168.0.15	192.168.0.33	TCP	2123 > bgp [ACK] Seq=0 Ack=1
3	0.000422	192.168.0.15	192.168.0.33	TCP	2123 > bgp [FIN, ACK] Seq=0 Ack=1
4	0.006057	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [ACK] Seq=1 Ack=1
5	7.999977	192.168.0.15	192.168.0.33	TCP	2124 > bgp [SYN] Seq=0 Len=0
6	8.003909	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [SYN, ACK] Seq=0 Ack=1
7	8.003954	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=1 Ack=1
8	8.004042	192.168.0.15	192.168.0.33	BGP	OPEN Message
9	8.208048	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [ACK] Seq=1 Ack=30
10	8.337997	192.168.0.33	192.168.0.15	BGP	OPEN Message
11	8.338027	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=30 Ack=30
12	9.229115	192.168.0.15	192.168.0.22	PCP	KEEPALIVE Message

Tablo 1.3 : Summary Window Sütunu

SUMMARY WINDOW

- Gözüktüğü gibi bu paket; Border Gateway Protocol (BGP) oturumunda, *192.168.0.15* ve *192.168.0.33* adresleri arasında yakalanmıştır. Bu paket seçilerek, açılan "Protocol Tree Window" ve "Data View Window" bölümlerinden daha da ayrıntılı incelenebilir.

PROTOCOL TREE WINDOW

- Paketi bütün protokollerin bir üst ağacı (tree) olarak canlandırıralım. Her bir protokol için ağaç düğümü(tree node) oluşturulur. Bu ağaç düğümleri sayesinde, protokol alanı Daha geniş bir şekilde tanımlanabilir. Herhangi bir ağaç düğümünün alt ağaca sahip olması, Onun daha geniş bilgiler gösterecek şekilde genişletilebileceğini veya sadece özet bilgiler gösterecek şekilde daraltılabileceğini gösterir. Protocol tree window, wireshark'ın paketi çözümleyerek oluşturduğu ağacı denetleme imkanı sunmaktadır.

PROTOCOL TREE WINDOW

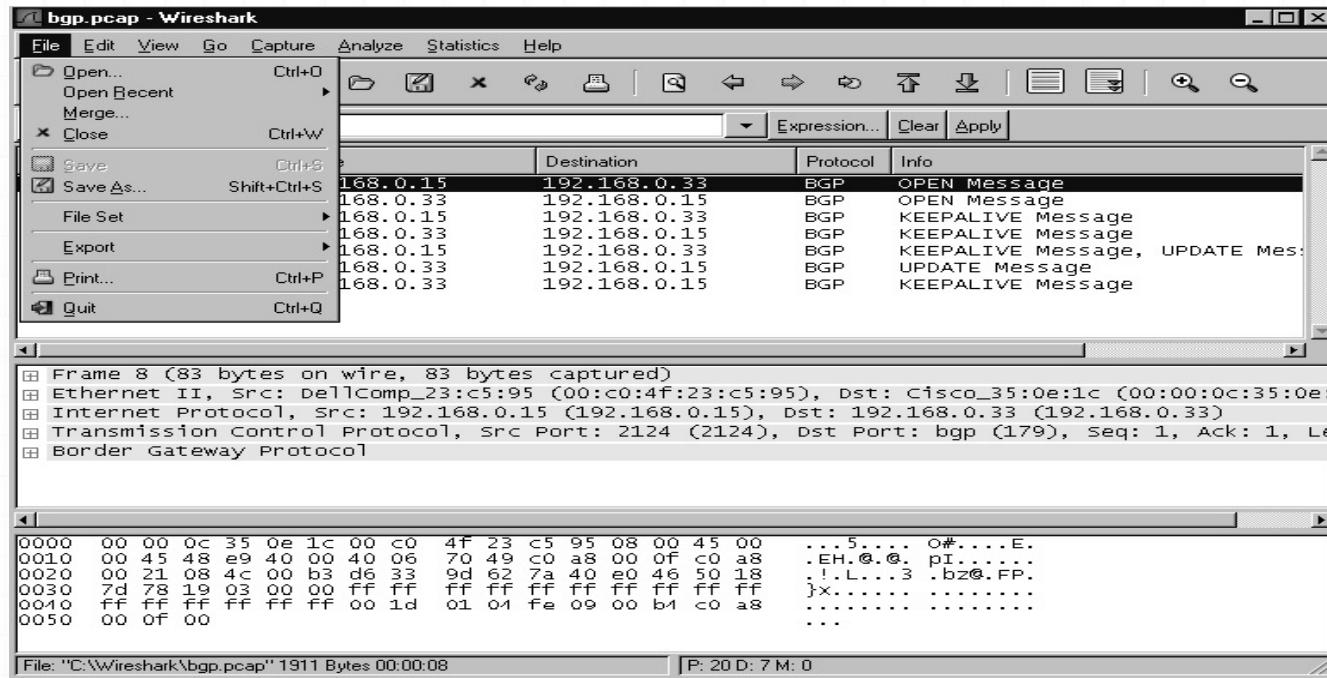
Wireshark arayüzü ;menü çubuğu, araç çubuğu, görüntüleme filtresi çubuğu, özet Alanı, protokol ağacı alanı ve veri alanı olmak üzere 6 bölümden oluşur. Menü Çubuğu;

- File (Dosya Menüsü)
- Edit (Ekleme Menüsü)
- View (Görüntü Menüsü)
- Go (Git Menüsü)
- Capture (Yakalama Menüsü)
- Analyze (Analiz Menüsü)
- Statistics (Statik Menüsü)
- Help (Yardım Menüsü)

olmak üzere 8 bölümden oluşmaktadır.

File(dosya menüsü)

- Bu menü dosya açma, kaydetme,yazdırma gibi temel işlevleri yapabileceğimiz bölümdür.



Tablo 1.4

File(dosya menüsü)

- Open (*ctrl+O*): Hazırda var olan önceden kaydedilmiş wireshark ya da başka desteklediği paket analiz yazılımlarının ürettiği dosyaları görüntülemek için kullanılır.
- Open Recent(Son dosyayı aç): Son kullanılan dosyaları açmada kolaylık sağlar.
- Merge(Birleştir): Kaydedilmiş dosyaları birleştirmede kullanılır.
- Close (*ctrl+W*): Açık olan dosyadan çıkar.
- Save (*ctrl+S*): Görüntülenmekte olan paketleri kaydeder.
- Save As (*ctrl+shift+S*): Farklı kaydeder.
- File Set(Dosya Ayarları):
 - List Files(Dosya Listesi): Dosya listesini oluşum tarihi, son değişim tarihi, boyutu şeklinde dosya dizisi içerisinde gösterir.
 - Next File(Sonraki dosya): Dosya dizisi içinde varolanı kapatıp sonrakine atlar
 - Previous File(Önceki dosya): Dosya dizisi içinde varolanı kapatıp bir öncekine atlar.

Export

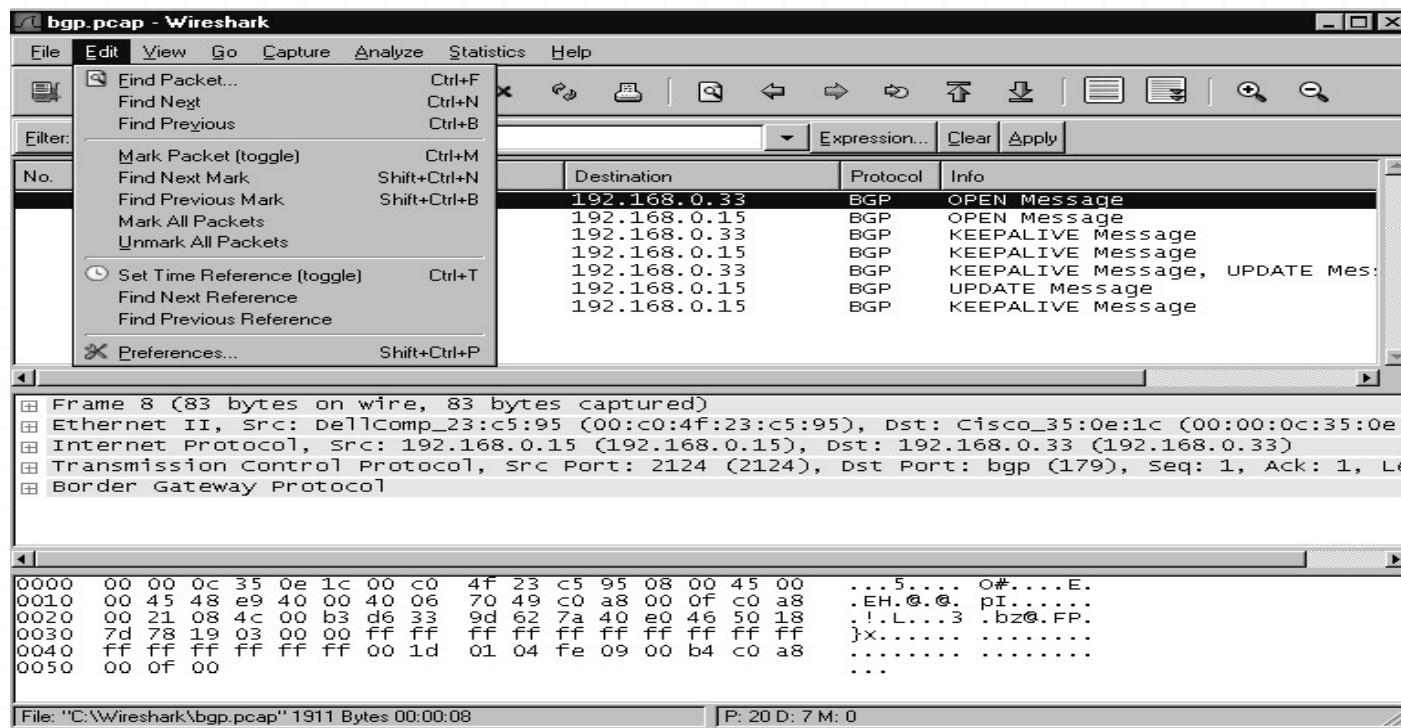
- As "Plain Text" File: Toplanan paketleri metin dosyası olarak dışa aktarmaya yarar. Özeti ve ayrıntı bölümlerini aktarır.
- As "PostScript" File: İstenen paketleri postscript dosyası olarak dışa aktarmaya yarar. Wireshark seçilen ayrıntı bölümünü bilgilerini aktarır.
- As "CSV" (Comma Separated Values packet summary) File: Wireshark özeti bölümündeki bilgileri virgülle ayrılmış şekilde düz metin dosyası olarak dışa aktarır.
- As "C Arrays" Paket Bytes File: Paket veri değerlerini hex byteları olarak aktarır.
- As XML "
- PSML" (Packet Summary) File: Paketleri PSML (packet summary markup language) XML dosya formatında dışa aktarmaya yarar.
- As "PDML" File: Paketleri PDML (packet details markup language) XML dosyası olarak aktarmaya yarar.

Selected Packet Bytes

- Objects > http : Paketler içerisindeki http protokollü paketleri ve Objelerini dışarı aktarmaya yarar.
- Print (*ctrl+P*): Seçilen paketleri yazdırma yarar.
- Quit(*ctrl+Q*): Programdan çıkar.

Edit

- Edit menüsü kullanıcı tanımlı işlemleri ve paket arama gibi işlemleri yapmamızı sağlar. Edit menüsünün içeriği gösterilmiştir.



Edit

- **Copy (*Shift+ctrl+C*):** Veri bölmesinden tıklanan değeri filtre ifadesi olarak kopyalar. İstenilen bölüm seçilerek sağ fare menüsünden de yapılabilir .
- **Find Packet (*ctrl+F*):** Birçok kriterde göre arama yapmanıza imkan sağlar. Display filter seçeneği seçiliyse wireshark filtreleme kriterlerine göre arama yapar. Basit protokol taramalarından kuvvetli filtreleme ifadelerine kadar birçok türde etkin arama yapabilirsiniz.
- **Hex Value:** Paket veri kümesi içerisinde belirtilen hex değerlerinde arama yapar.
- **String:** Girilen string i liste, ayrıntı ya da veri alanlarında belirlenen kriterlere göre arar .String options alanında arama büyük küçük harf duyarlı ve karakter seti belirtilerek yapılabilir. Direction alanında ise taramanın aşağı yada yukarı yapılacakı belirtilir.
- **Find Next (*ctrl+N*):** Belirlenen kriterde bir sonraki paketi bulur.
- **Find Previous (*ctrl+B*) :** Belirlenen kriterde bir önceki paketi bulur.

Edit

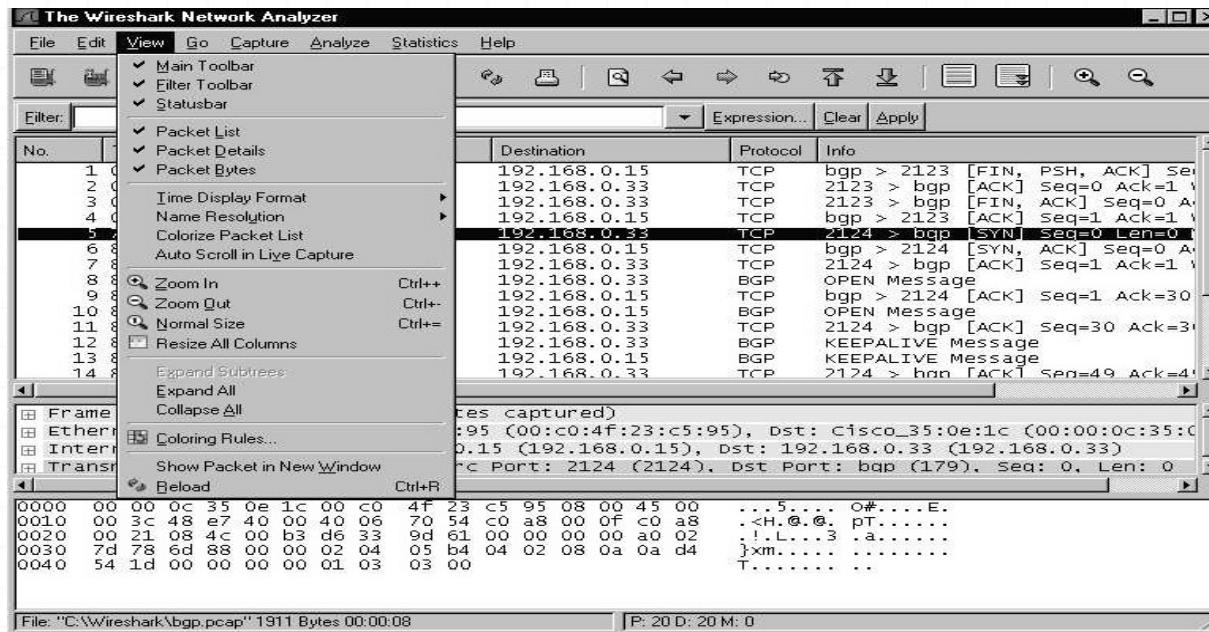
- Mark Packet (*ctrl+M*) : Seçilen paketi işaretler.
- Find Next Mark (*shift+ctrl+N*) : Bir sonraki işaretli paketi bulur.
- Find Previous Mark (*shift+ctrl+B*) : Bir önceki işaretli paketi bulur.
- Mark All Packet: Bütün paketleri işaretler.
- Unmark All Paket: Bütün işaretleri kaldırır.
- Set Time Reference (*ctrl+T*): Seçilen paketi zaman referansı olarak alır ve sonraki paketlerde o pakete göre zaman değerleri alır.
- Find Next Reference: Bir sonraki referans alınan paketi bulur.
- Find Previous Reference: Bir önceki referans alınan paketi bulur.
- Configuration Profiles (*shift+ctrl+A*): Profil ekle sil işlemlerini yapar.
- Preference (*shift+ctrl+P*): Programla ilgili ayarlamaları yaptığımız bölümdür.
- User Interface bölümünde program için pencere düzeni, renk, font ayarlamaları ve bunlar gibi görünümü kişiselleştirmeye yarayan seçenekler bulunur.

Edit

- Capture : Paketleri yakalamak için kullanılacak default ağ arabirimi, eş zamanlı paket görüntüleme ve promiscuous mod seçimi (promiscuous mod : Yönlendirme olmadan bütün paketlerin bütün istemcilere dağıtıldığı durumda paketin hedefine bakılmadan bütün paketlerin takibi olayıdır. Root yetkisi gerektirir.), otomatik kaydırma çubuğu hareketi, ve yakalanan paketlerin türlerine göre sayıları ve % oranlarını veren info penceresinin saklanması seçenekleri bulunur.
- Printing: Yazdırma için gereken ayarlar bulunmaktadır. Dosya çıktısı konumu, yazdırma komutu ve çıktı türü “düz metin ya da post script seçenekleri” Bulunmaktadır .Varsayılan yazdırma komutu lpr dir.
- Name Resolutions: Adres dönüşüm işlemlerini etkinleştireceğiniz alandır.
- Protocols: ihtiyaca göre wireshark üzerinde paketlerin protokollere göre kullanım ayarlamalarını yapabileceğiniz bölümdür.

View

- Wireshark ana ekranımızın görüntüsünü düzenlememizi sağlayan menüdür.
- Toolbar lar eklenebilir, çıkarılabilir, paketlere özel renk ayarları yapılabilir.



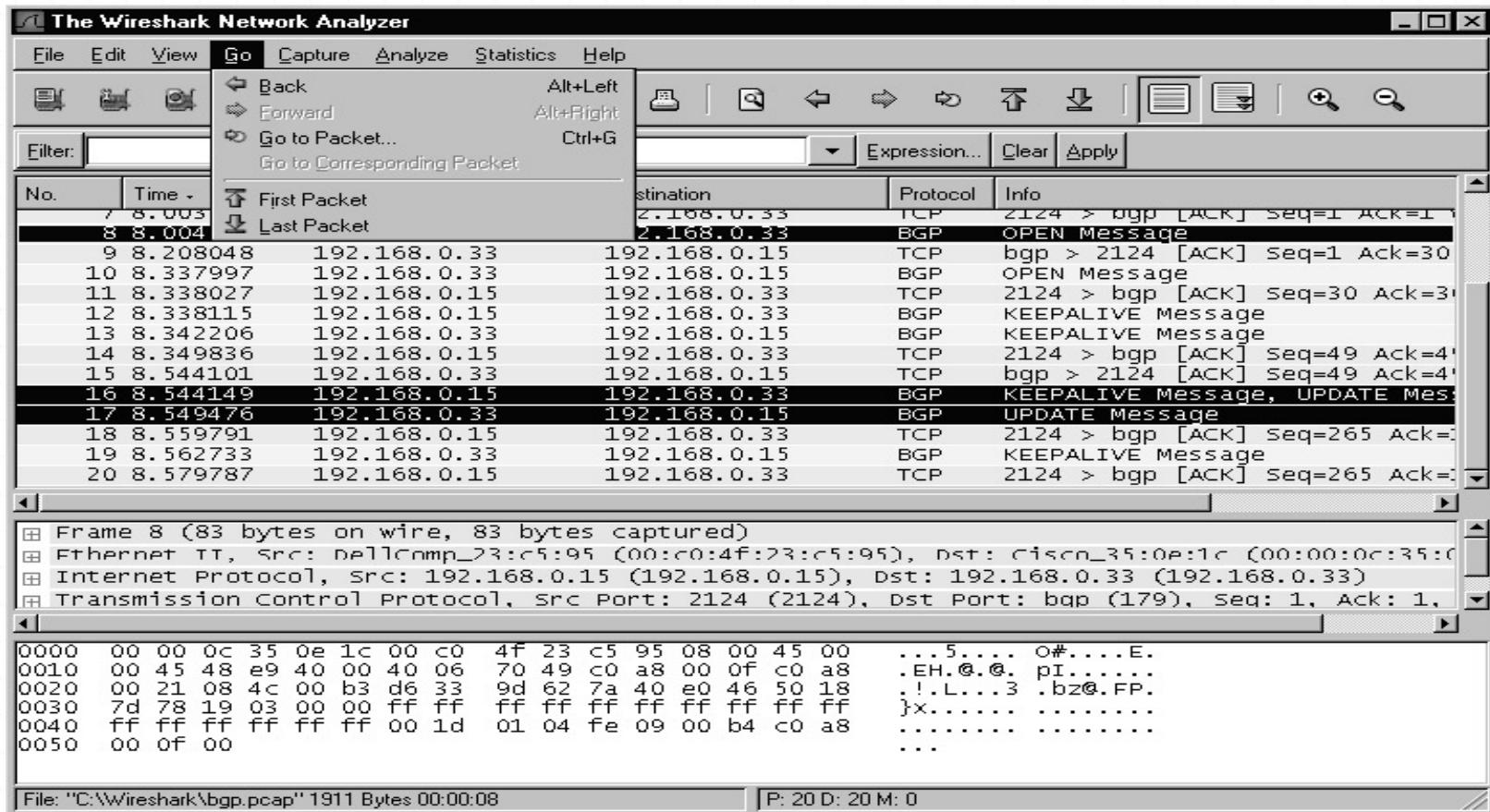
View

- Packet Details(Paket Detayları): Paketlerin detaylarını ASCII kodunda gösteren
- Bölgeyi ekler ya da kaldırır.
- Packet Bytes: Data Window penceresini ekler ya da kaldırır.
- Time Display Format Summary: Window da zaman görünümün nasıl gözükeceğini ayarlamamızı sağlar.
- Colorize Packet List: Paketlerin renk özelliğini açar ya da kapar.
- Auto Screen in Live Capture: Summary Windowun güncellenmesini açıp kapamaya yarar.
- Zoom In: Font ve column size ları büyütmeye yarar.
- Zoom Out: Font ve column size ları küçültmeye yarar.
- Normal Size: Zoom In ve out la büyütüp küçültüğümüz fontları default değere döndürmemizi sağlar.
- Expand Subtrees: Protocol tree deki seçili alt diziyi açar.

View

- Expand All: Protocol tree deki bütün alt dizileri açar.
- Collapse All: Protocol tree deki bütün alt dizileri kapatır.
- Coloring Rules: Paketler için Renk ayarlarını yapmamızı sağlar.
- Show Packet in New: Window Paket detaylarını yeni bir pencerede görmemizi sağlar.

Go



Tabel 1.7

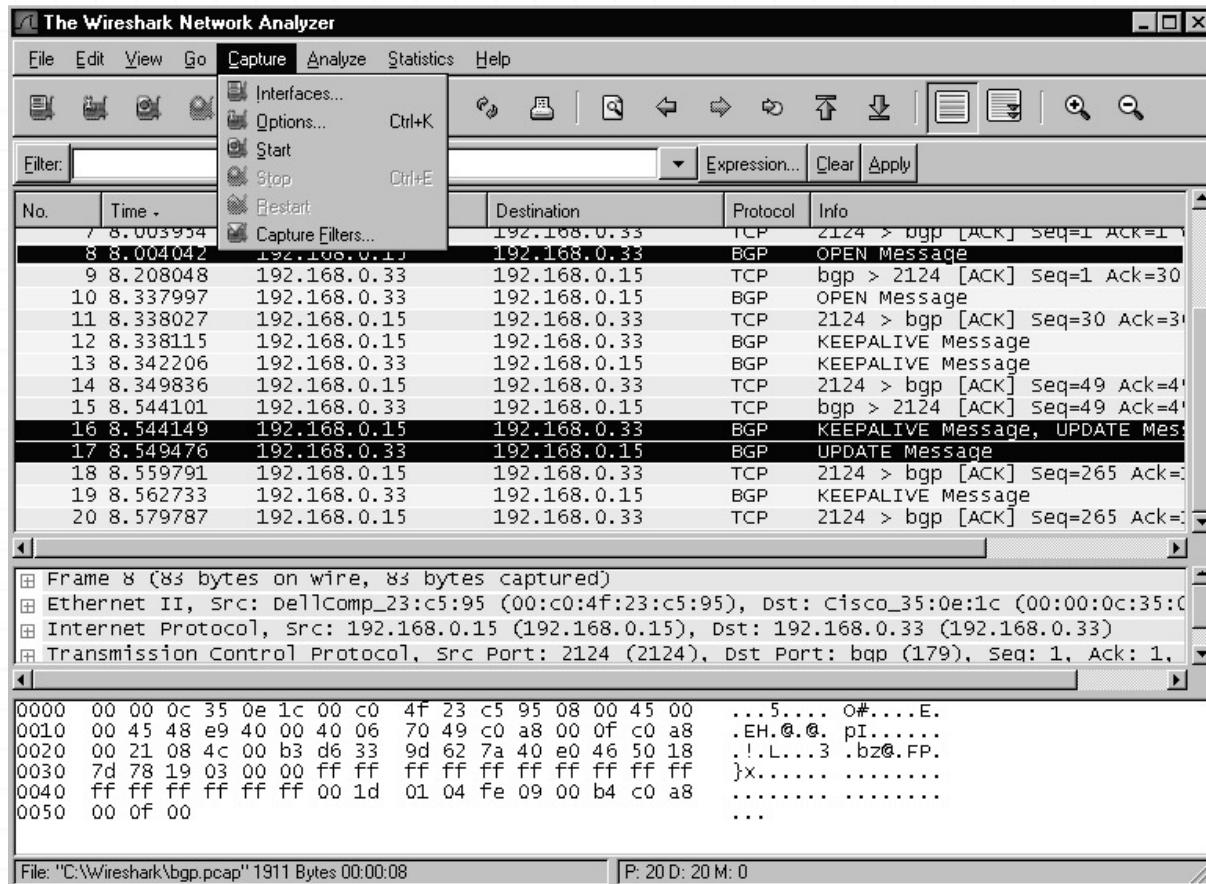
Prof. Dr. Resul DAS

26/97

Go

- Back (*ctrl+sol*): Bir önceki baktığınız pakete atlar.
- Forward (*ctrl+sağ*): Ziyaret edilen bir sonraki pakete zıplar.
- Go To Packet (*ctrl+G*): Paket numarasına göre istenilen pakete zıplar.
- Go To Corresponding Packet: Seçilen pakete karşılık gelen pakete zıplar .
- Previous Packet (*ctrl+yukarı*): Seçili paketten önceki pakete zıplar.
- Next Packet (*ctrl+aşağı*): Seçili paketten sonraki pakete zıplar.
- First Packet: Yakalanan ilk pakete zıplar.
- Last Packet: Yakalanan son pakete zıplar.

Capture



Capture

- Interfaces: Wiresharkın kullanacağı ağ arabirimini ve özelliklerini ayarlar.
- Options: Uygulama sırasında kullanılacak ağ arabirimini seçimi adres çözümleme özellikleri, görünüm özellikleri uygulama durdurmak için ayarlanacak özellikler gibi bir çok ayarlanabilir bölüm içermektedir.
- IP address: Seçilen ağ arabiriminin sahip olduğu ip adresidir.
- Limit each packet to n bytes : Paket yakalama işlemi sırasında uyulacak tampon sınırlıdır. Seçili olmadığı durumda default değeri 65535 bytes tır. Default değerde bırakmanız önerilir.
- Capture packets in promiscuous mode : Hub kullanılan ağlarda yalnızca kullanılan makine ile ilgili paketleri değil gelen bütün paketleri hedeflerine bakmadan toplama özelliğidir.
- Capture Filter: Paket yakalama sırasında filtreleme özelliği sunar. İstenmeyen paketlerin yakalanmasını engelleyerek hem analiz işlemini kolaylaştırır hemde programın çalışması sırasında daha az paket ile sistem kaynaklarını idareli kullanır.

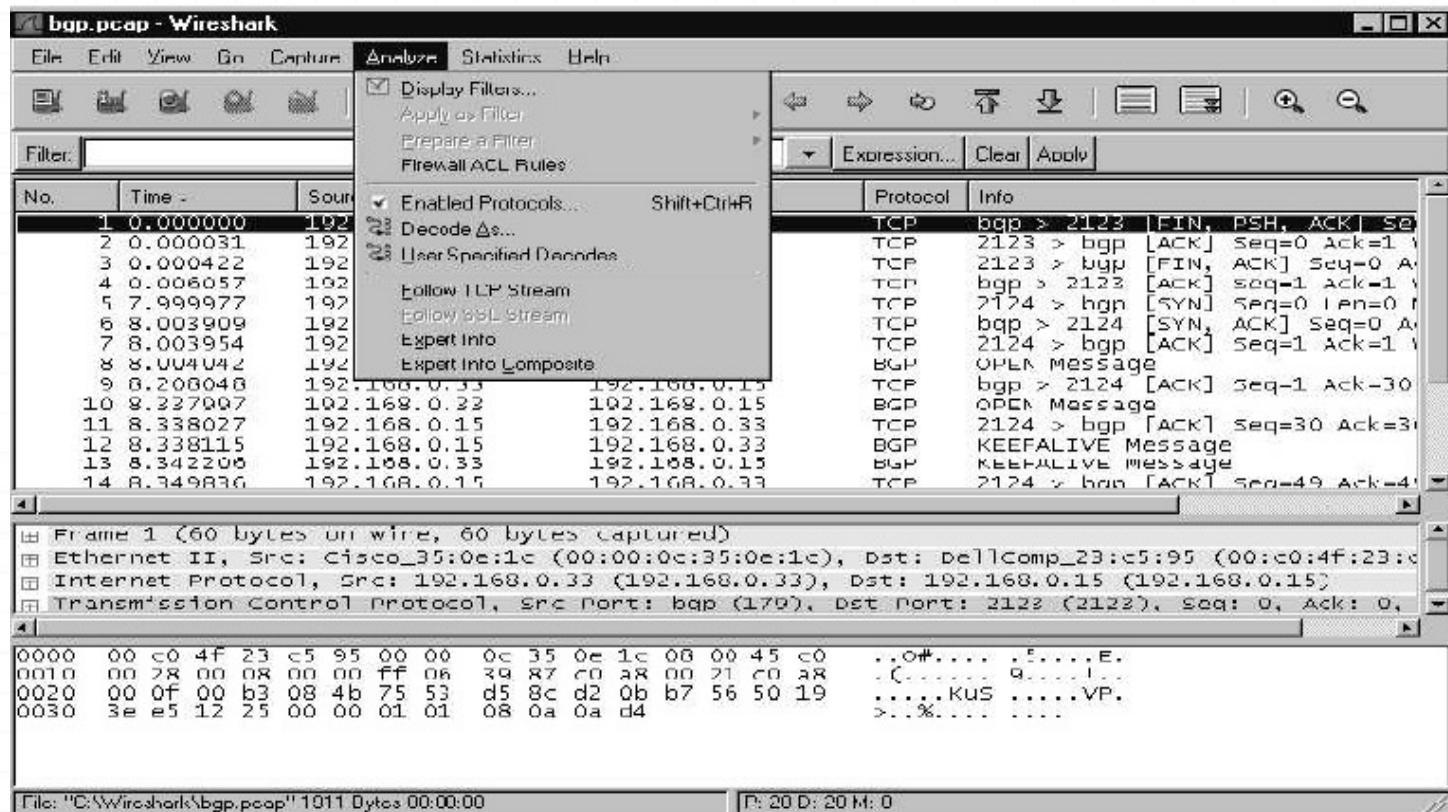
Capture File(s) Alanı

- File: Yakalama dosyası olarak kullanılacak dosya ismi belirtmene yarar. Default olarak boştur.
- Use multiple files: Tek dosya kullanımı yerine wireshark otomatik olarak yeni bir dosyayla yer değiştirir.
- Next file every n megabyte(s): Belirtilen boyutta (kilobyte,megabyte,gigabyte) paket yakalandıktan sonra bir diğer dosyaya geçer.
- Next file every n minute(s): Belirtilen süre geçtikten sonra diğer dosyaya geçer.
- Ring buffer with n files: Belirtilen sayıda dosya aşıldığında en eski dosyayı siler.
- Stop capture after n file(s): Belirtilen sayıda dosya değişikten sonra yakalama işlemini durdurur.

Stop Capture. Alanı

- ... after n packet(s) : Belirtilen sayıda paket yakalandıktan sonra yakalama işlemini durdurur.
- ... after n megabytes(s): Belirtilen kb,mb,gb miktarından sonra yakalama işlemini durdurur.
- ... after n minute(s): Belirtilen süre sonunda (saniye, dakika, saat, gün) yakalama işlemini durdurur.
- Display Options Alanı:
- Update List Of Packets İn Real Time: Yakalanan paketleri eşzamanlı olarak anında ekranда görmenize yarar.
- Automatic Scrolling in Live Capture: Kaydırma çubuğu otomatik olarak son yakalanan pakete göre iner.
- Hide Capture info Dialog: Yakalanan paketlerin protokollere göre sayı ve Oranını veren bilgi penceresini saklar.

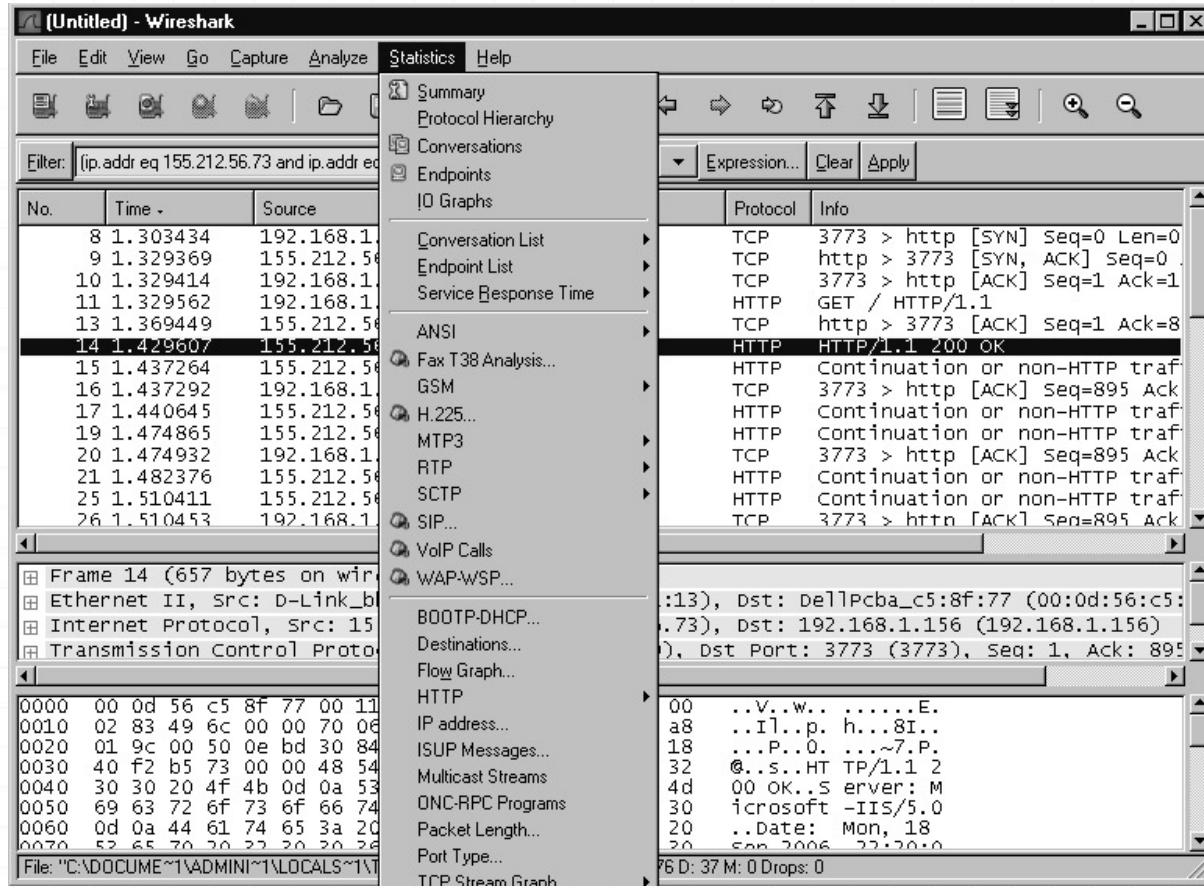
Analyze



Analyze

- Display Filter: Yakalanan paketleri belirtilen ifadelere göre sıralar.
- Apply As Filter: Seçilen paketin kaynak ve hedef adresine göre filtreleme yapar. And (&&), or(||), and not (&& !) ve or not (|| !) eklemeleriyle ifade güçlendirilir ve daha özelleşmiş arama yapılabilir.
- Prepare a Filter: Filtre ifadesini değiştirir ama hemen uygulamaz. Üstteki filtre uygulaması koşulları bunun içinde geçerlidir.
- Firewall ACL Rules :Cisco IOS, Linux Netfilter (iptables), OpenBSD pf ve Windows Firewall (via netsh) için firewall kural ifadesi oluşturur. Yeni kullanıcılar için mükemmel ötesi bir özelliktir.
- Decode As: Paketleri belirli protokollere göre decode eder.
- Enabled Protocols (*shift+ctrl+R*): Yakalama işlemi sırasında istenmeyen protkollerin kaldırılmasına imkan verir. Capture filter gibi düşünülebilir.
- Decode As: Geçici olarak protokol çevrim işi yapar.
- User Specified Decodes: Hali hazırda var olan çevrimleri görüntüler.
- Follow TCP Stream: Seçilen paketle ilgili tcp bağlantılarının tüm tcp segmentlerini ayrı bir pencerede gösterir.
- Follow SSL Stream: Follow TCP stream ile aynı özelliktedir fakat SSL stream için çalışır.

Statistics



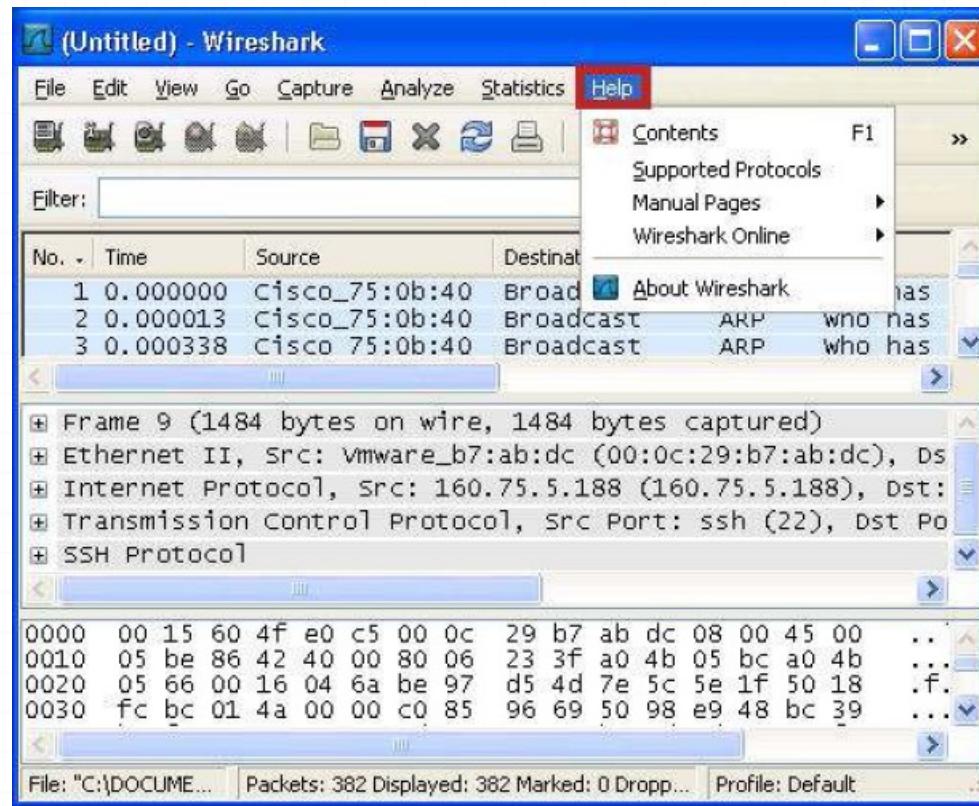
Statistics

- Summary: Açık olan yakalama dosyasında dosya formatı, paket sayısı, boyut, ilk ve son paket yakalama zamanları , filtre ve yakalama arabirimine ilişkin verileri içerir.
- Protocol Hierarchy : Yakalanan paketlerin ağaç şeklinde katman ve protokol hiyerarşisini gösterir. Her sıra bir protokole ait istatistiksel değerleri tutar. Seçilen sıra filtre ifadesi olarak kullanabilir.
- Conversations: Kaynak ve hedef noktaları arasındaki trafigin istatistik bilgisini verir. Noktalar arasındaki toplam gelen giden paket ve byte miktarı portlara göre listelenir. Conversations penceresi endpoint penceresiyle benzerdir. Listedeki her bir sıra bir diyalogun istatistiksel değerlerini verir. Adres çözümleme özelliği Conversations penceresi içinde, programın başlangıcında “capture options” bölümünden, preferences altında name resolutions bölümünden ya da view menusu altında name resolutions bölümünden seçildikten sonra kullanılabilmektedir. Limit to display filter özelliği ise herhangi bir filtreleme yönergesi tanımlandığı durumda kullanılabilmektedir.
- Endpoints: Hedef ve kaynak adresi ayrimı yapmadan her son nokta için istatistik bilgisini verir. Desteklenen her protokol için ayrı bir sekme mevcuttur .Her sekmede yakalanan son nokta sayıları belirtilmektedir.

Statistics

- IO Graphs: Belirtilen özelliklerde paketlerin zamana göre akış grafiğini verir. Ağda durum kontrolü için oldukça faydalı bir özelliklektir. Bu özellikle normal paket akış diyagramında ağda meydana gelecek herhangi bir anormallik hemen farkedilebilir.
- Graphs: Grafik ayarlamalarının yapıldığı kısımdır.
- Service Response Time: İstek ve cevap arasındaki zamanı gösterir. Service response time istatistikleri DCERPC,Fibre, Channel, H.225 RAS, LDAP,MGCP, ONC-RPC, SMB, ANSI,GSM,H.225 gibi protokoller için kullanılır.
- Wlan Traffic Statics: Yakalanan kablosuz ağ trafiginin istatistik bilgisinin sunar.

Help



Help

- Help kısmı Wireshark'ın yardım menüsünün bulunduğu kısımdır.
- Contents: Wireshark online yardımı gösterir.
- Supported Protocols: Desteklenen protokollerı gösterir.
- Manual Pages :UNIX-Style kullanıcı sayfalarına ulasan bir alt menüdür.
- Wireshark Online: Online wireshark kaynaklarına ulaşmak için bir alt menüdür.
- About Wireshark :Wireshark ile ilgili bilgileri gösterir.

Filtreleme

- Filtre özelliği,
- Wiresharkta dinleme sırasında veya dinlemenin ardından paketler arasında istenilen özellikteki paketleri görüntülemekte kullanılabilir. Capture options penceresinden belirtilen capture filter, paket yakalama sırasında wiresharkın uyacağı koşulları belirtir. Capture filter penceresinde Wiresharkın paket yakalama sırasında uyacağı kurallar için bir liste sunulmuştur.
- Ethernet address 00:08:15:00:08:15 : Ethernet II altında kaynak veya hedef adreslerinde belirtilen mac adresine ait paketleri yakalar.
- not broadcast and not multicast: Broadcasting ve multicasting paketlerini yakalamaz.
- not arp: Arp paketlerini yakalamaz.

Filtreleme

- IP address 192.168.0.1 : Belirtilen ip adresini hedef yada kaynak adres kısımlarında barındıran paketler yakalanır.
- IPX only : İlgili protokole ilişkin paketleri yakalar.
- TCP only : İlgili protokole ilişkin paketleri yakalar.
- UDP only : İlgili protokole ilişkin paketleri yakalar.
- TCP or UDP port 80 (http) : Port 80 için tcp ve udp paketlerini yakalar.
- HTTP TCP port (80) : Port 80 için http ve tcp paketlerini yakalar.
- No ARP and no DNS : DNS ve ARP paketleri harici paketleri yakalar NonHTTP and nonSMTP to/from www.wireshark.org : Belirtilen adres için http ve smtp harici paketleri yakalar.

EN ÇOK KULLANILAN FİLTRELER

■ 1. IP FILTERS

Filter	Tip	Tanım
ip.addr	IPv4 adresi	Source(kaynak) veya Destination(hedef)kaynak
ip.src	IPv4 adresi	Source adres
ip.dst	IPv4 adresi	Destination adres
ip.host	Karakter dizisi	Source veya Destination host adres
ip.src.host	Karakter dizisi	Source host adres
ip.proto	8 bit integer	Protokol
ip.version	8 bit integer	IP versiyonu

EN ÇOK KULLANILAN FİLTRELER

■ 2.ETHERNET FILTERS

Filter	Tip	Tanım
eth.addr	6 bit mac adres	Source(kaynak) veya Destination(hedef) adres
eth.src	6 bit mac adres	Source adres
eth.dst	16 bit integer	Destination adres
eth.len	16 bit integer	Uzunluk
eth.type	16 bit integer	Tip

EN ÇOK KULLANILAN FİLTRELER

■ 3.TCP FILTERS

Filter	Tip	Tanım
tcp.ack	32 bit integer	Acknowledgement numarası
tcp.analysis.ack_lost_segment	-	Ack yapılmış kayıp paket tcp.analysis.duplicate_ack - Tekrar edilmiş ack
tcp.analysis.duplicate_ack	-	Tekrar edilmiş ack
tcp.analysis.duplicate_ack_num	32 Bit integer	Tekrar edilen ack numarası
tcp.analysis.flags	-	TCP analiz bayrakları(uyarı)
tcp.port	16 bit integer	Source veya Destination port numarasına göre

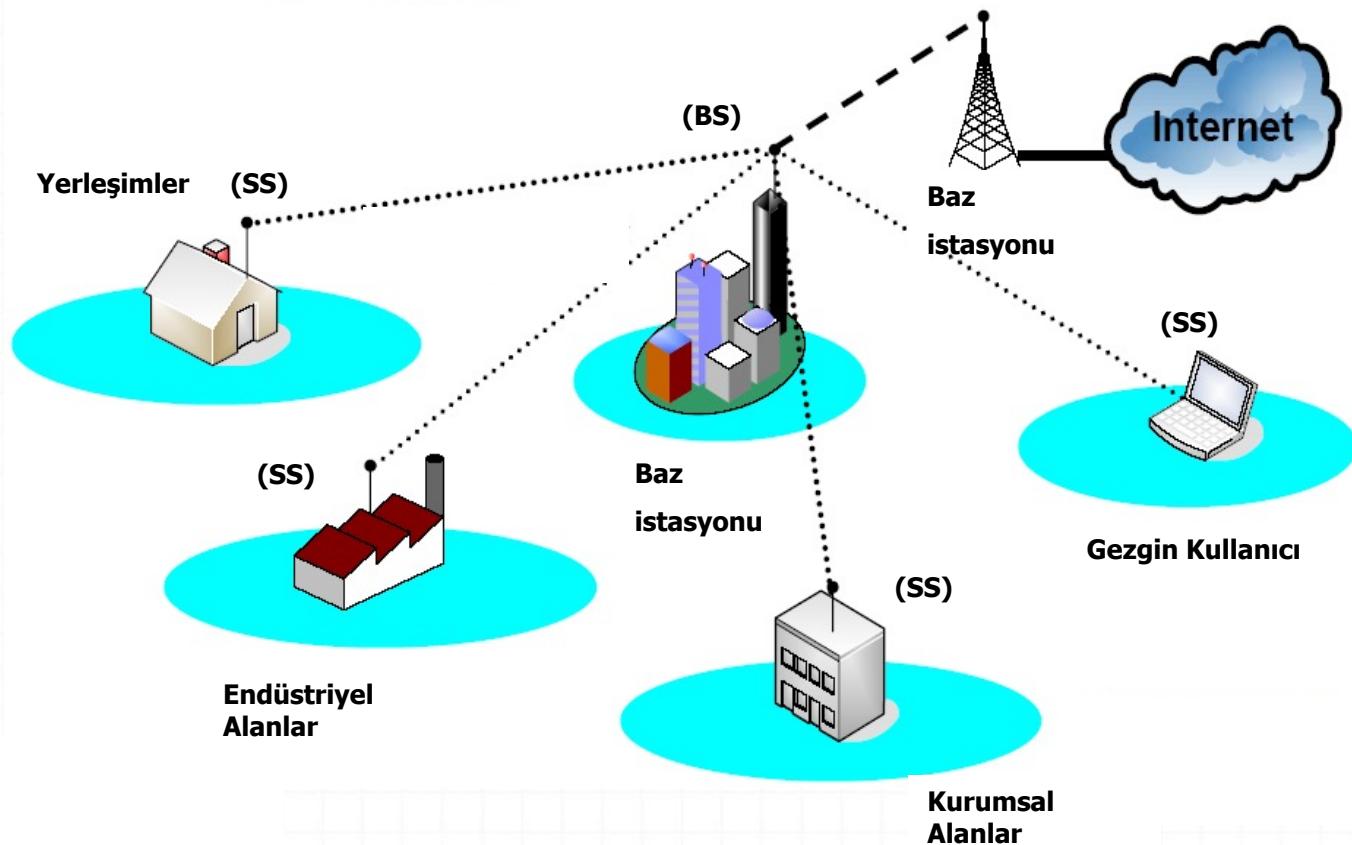
IEEE 802.16 ve WiMAX

- IEEE 802.16: Telsiz Kentsel alan ağı standardı (Wireless MAN),(1999).
- WiMAX (Worldwide Interoperability for Microwave Access):
802.16 standardını destekleyen üç birimlere telsiz alanda yüksek bandgenişliği (BWA) sağlamayı amaçlayan bir forumun standardı (2001).
- Yüksek hızda kesintisiz telsiz iletişim
 - 70 Mbps
 - Kapsama alanı: 50-70 km'ye kadar
 - Veri
 - Ses (isteğe-bağılı)
 - Görüntü (isteğe-bağılı)
 - VoIP
 - Videokonferans

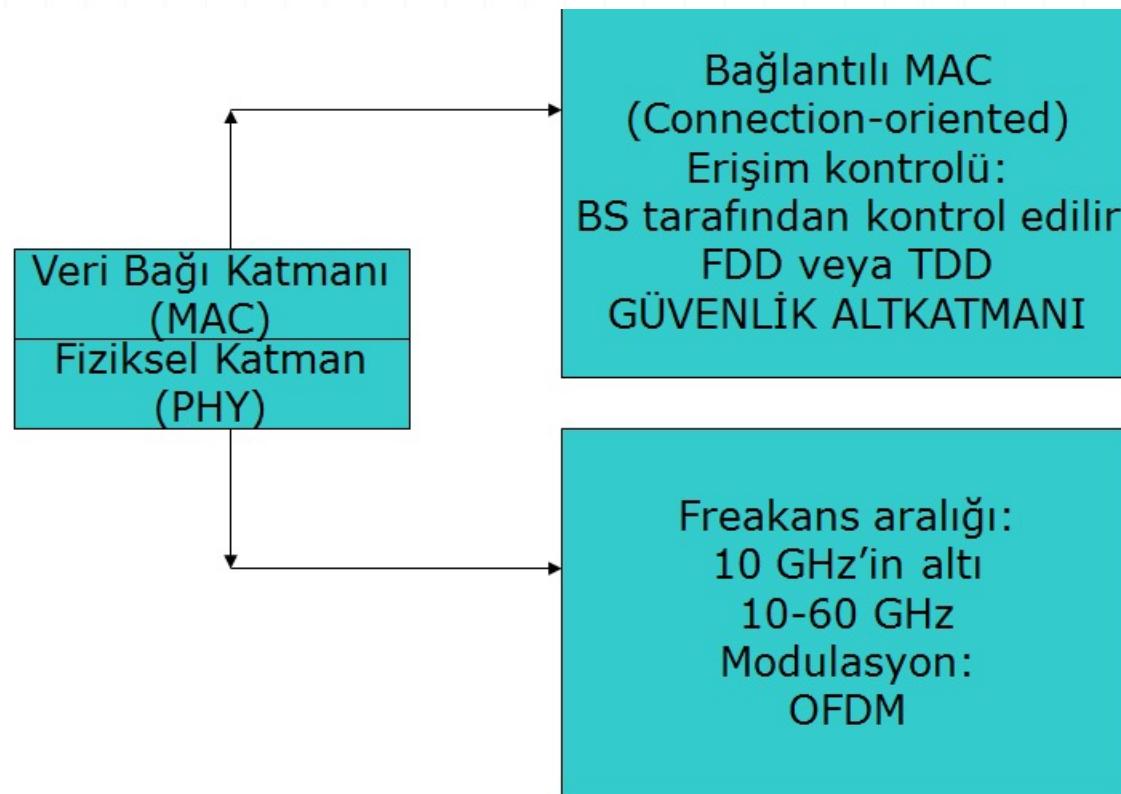
IEEE 802.16 ve WiMAX

- İletişim Türleri:
 - Baz istasyonu(BS) → Kullanıcı İstasyonu(SS): Downlink
 - Kullanıcı İstasyonu(SS) → Baz İstasyonu(BS): Uplink
 - Baz İstasyonu(BS)-kullanıcı İstasyonları (SS) arası
 - Tek noktadan Çok noktaya (PMP)
 - Kullanıcı İstasyonları arası
 - Ağ (mesh) yapısı

WiMAX Genel Yapısı



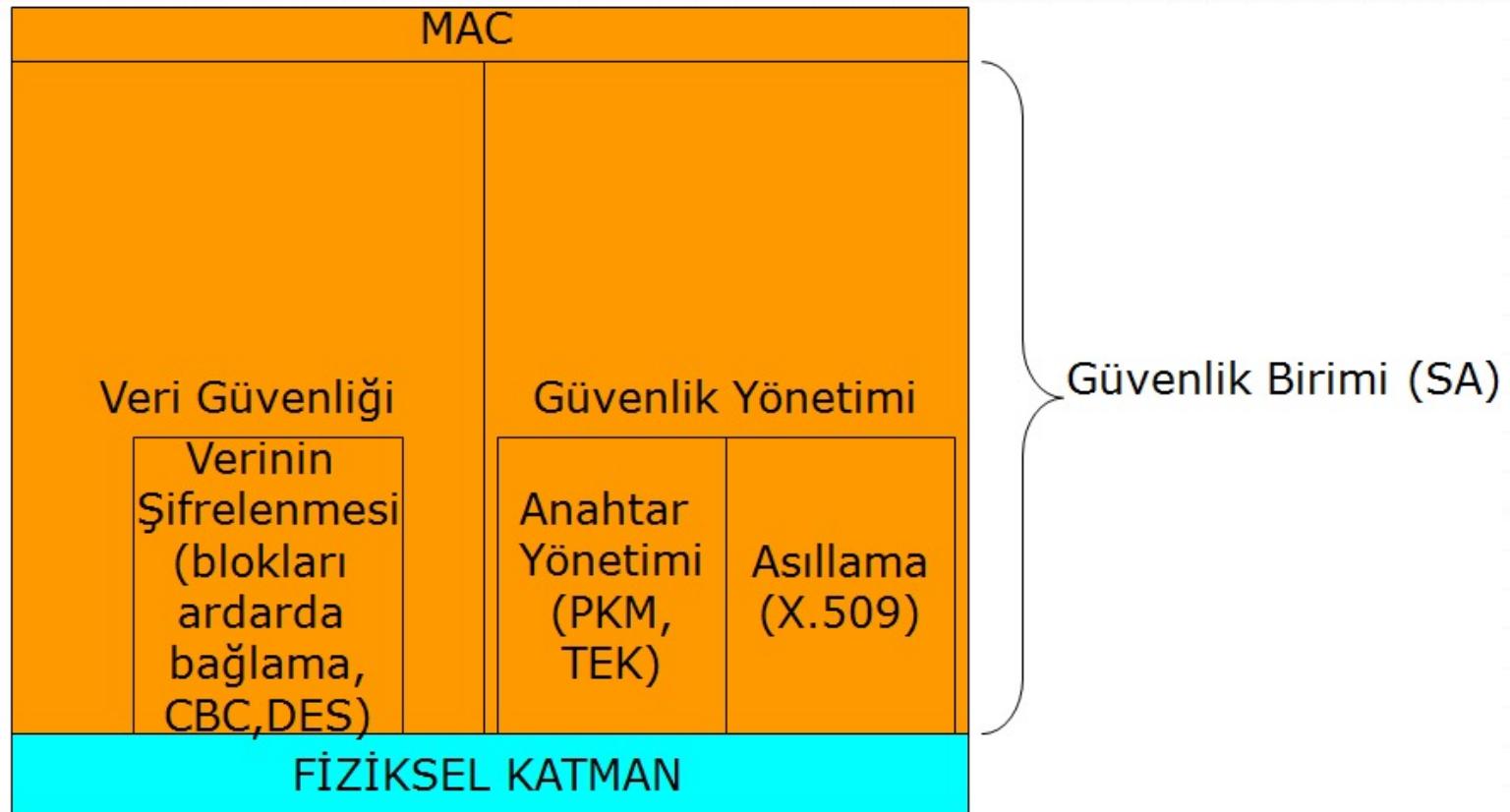
WiMAX katmansal Analiz



802.16 Güvenlik Standardı

- 5 kavrama dayalı bir yapı
 - Veri Şifreleme
 - MAC başlığı dışındaki kısma uygulanıyor
 - Anahtar Yönetimi
 - PKM
 - “Güvenlik Birimi” nin oluşturulması
 - Birimler arasında saydam bir iletişim kontrolü
 - Bağlantıların güvenlik birimine iletilmesi
 - Kriptografik süreç
 - Güvenlik biriminin veri şifrelemesi, asıllama ve anahtar alışverişi sırasında uyguladığı metodlar ve girdiği durumlar

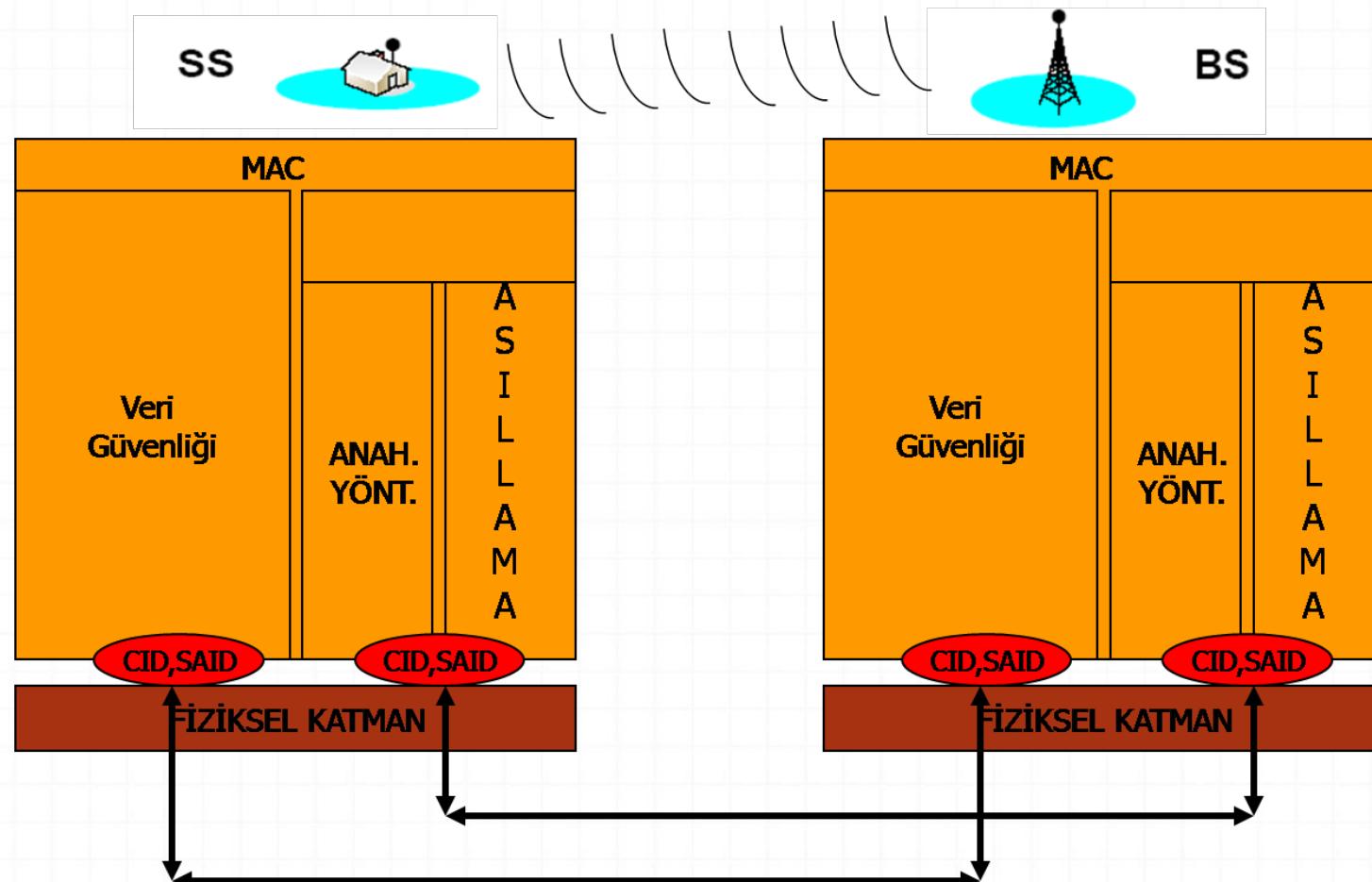
WiMAX Güvenlik Altkatmanı(1/2)



WiMAX Güvenlik Altkatmanı(2/2)

- Güvenlik Birimi (SA):
 - BS-SS arasındaki her türlü güvenlik bağlantısını sağlar.
 - 16-bitlik bir belirteci vardır (SAIP).
 - Tutulan parametler:
 - Her düzey için bir bağlantı ID'si(CID).
 - Kriptografik bilgiler(CBC, DES vs)
 - Güvenlik Bilgileri(Anahtar, IV)

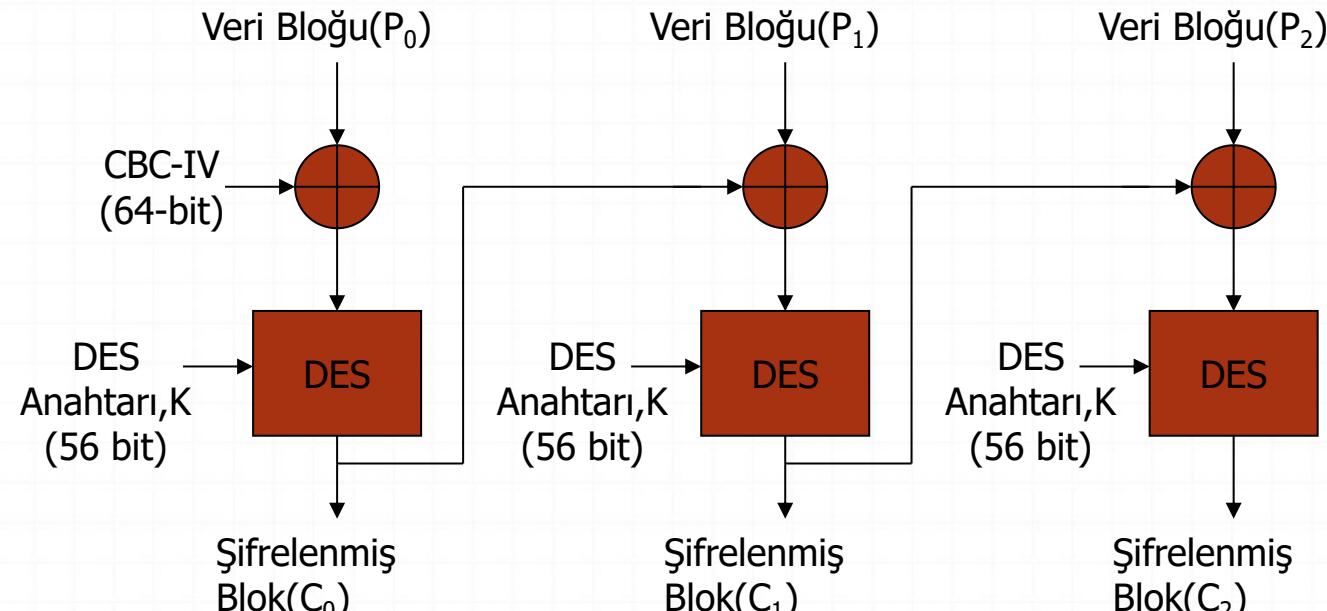
WiMAX Güvenlik Altyapısı



Veri Güvenliği (1/2)

- Şifreleme
 - Kullanılan Algoritma
 - DES
 - 56 bit anahtar
 - 64 bitlik bloklar
 - Kullanılan Şifreleme Kipi
 - “Şifreleme Bloklarını ardarda Bağlama Kipi” (Cipher Block Chaining,CBC)
 - CBC-IV: başlama vektörü TEK anahtar değiştokusu sırasında öğrenilir
 - XOR: Çerçeveerdeki senkronizasyon alanında belirtilir.

Veri Güvenliği (2/2)



Şifreleme:

$$C_i = K[P_i \oplus C_{i-1}]$$

Şifre Çözme:

$$P_i = C_{i-1} \oplus K^{-1}[C_i]$$

Güvenlik Yönetimi(1/7)

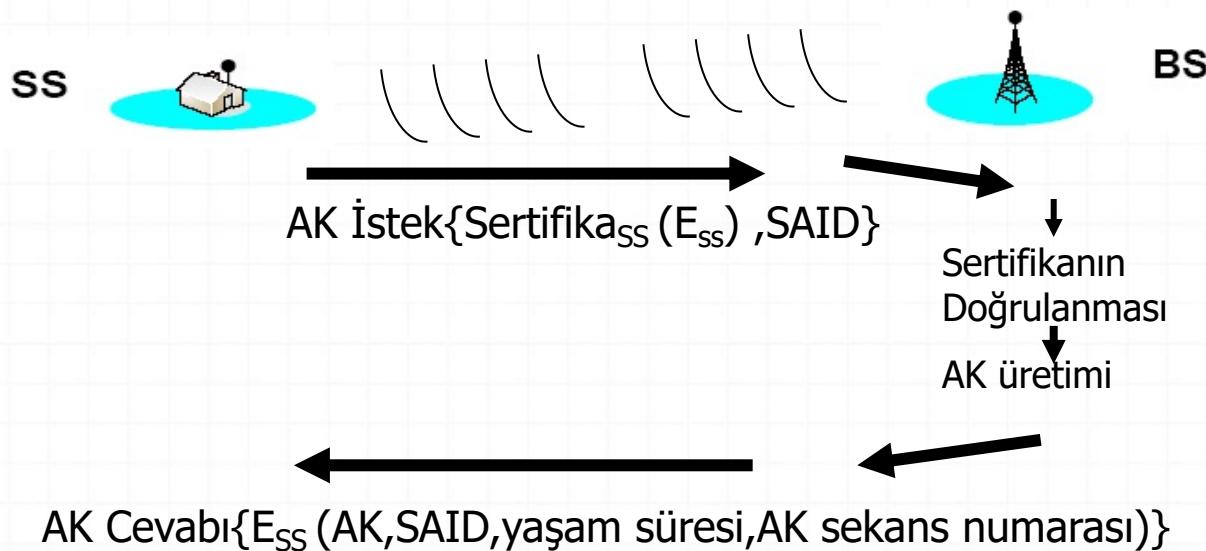
- Asıllama
 - Açık anahtarlı kriptografi kullanılır.
 - SS ile BS arasında SAID alışverişi
 - SS için kullanılan yöntem: X.509 sertifikalama
 - Üretici Sertifikası
 - Kendi kendine veya üçüncü kişi tarafından
 - Üretici bilgileri(WiMAX forumuna uygunluk)
 - SS sertifikası
 - Üretici tarafından
 - SS'in Seri numarası
 - SS'in MAC adresi
 - SS'ler açık-gizli anahtar çiftleri ile donatılmıştır
 - RSA tabanlı bir algoritma ile
 - Herhangi bir lokal algoritmayla dinamik olarak

Güvenlik Yönetimi(2/7)

- BS için ayrıca asıllama yok
- BS, üretici sertifikasının açık anahtarını kullanarak SS'i asıllar.
- Böylece standarda uygunluk anlaşılmış olur.
- SS'in gizli anahtarının iyi saklandığı varsayıılır.

Güvenlik Yönetimi(3/7)

- Asıllama anahtarı(AK,128-bit) alışverişi yapılır
 - Açık anahtar ile şifreli olarak gönderilir.
 - BS ve SS AK'yi elde ettikten sonra asıllama tamamlanmış olur.
 - SS periyodik olarak AK tazelemesi yapar.



Güvenlik Yönetimi(4/7)

- Anahtar oluşumu
 - Privacy Key Management (PKM)
 - Güvenlik birimi(SA) tarafından yönetilir.
 - SS'ler, PKM protokolünü BS'den asıllama ve trafik güvenliği parametrelerini almak için kullanır.
 - Asıllama anahtarı ve oturum tazeleme de PKM tarafından yönetilir.

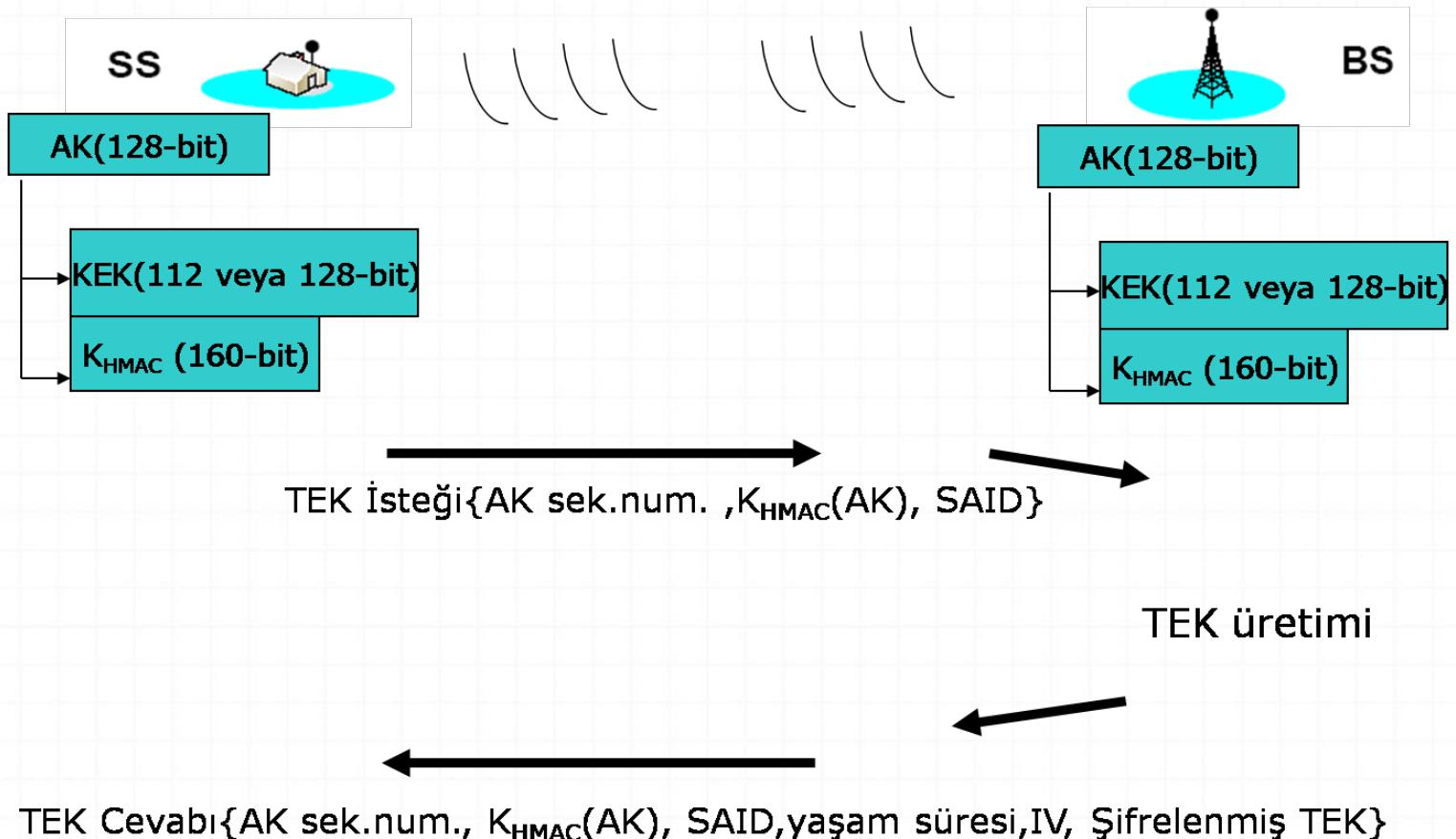
Güvenlik Yönetimi(5/7)

- Anahtar alışverişi
 - AK oluşumundan sonra, Traffic Encryption Keys (TEK) alışverişi yapılmalıdır.
 - TEK'ler 56-bitlik DES anahtarlarıdır.
 - Bu aşamda da AK'dan yardım alınır.
 - AK, BS'te anahtar oluşturulmasında kullanılacak olan Key-Encryption Key(KEK) oluşturulmasında(112 yada 128 bit olabilir) ve HMAC'teki K anahtarı olarak kullanılır.
 - TEK, yukarıdaki anahtarlardan bağımsız olarak BS tarafından üretilir

Güvenlik Yönetimi(6/7)

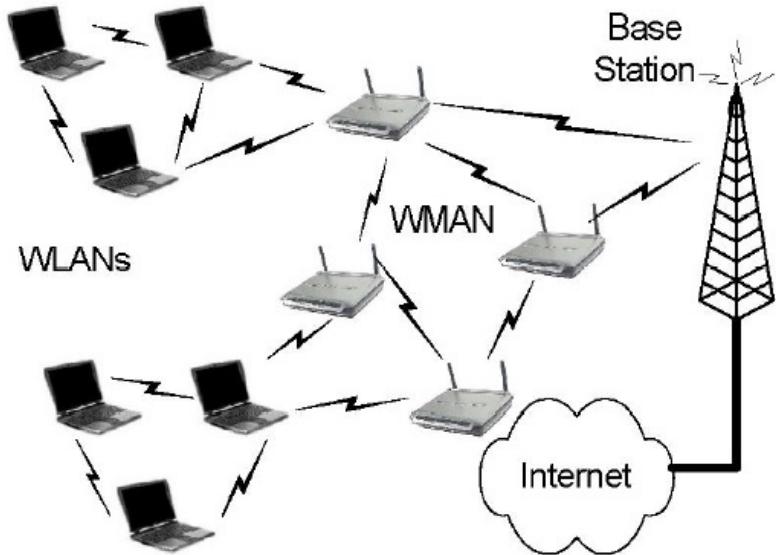
- TEK'in gönderilmesi:
 - 3DES ile
 - (112-bitlik KEK ile)
 - RSA ile
 - (SS'in Açık anahtarı ile)
 - AES ile
 - (128-bitlik KEK ile)
- Anahtar alışverişindeki asıllama,AK doğrulaması ve bütünlük HMAC-SHA1 ile sağlanır.

Güvenlik Yönetimi(7/7)



WiMAX Ağ(Mesh) yapısında Güvenlik(1/2)

- SS'ler BS olmadan birbirleriyle haberleşebilir → Mesh yapının en önemli özelliği BS'nin kapsama alanında artış olur
- Ağda bir düğüm çöktüğünde yada BS çöktüğünde tüm iletişim kesilmez.



WiMAX Ağ(Mesh) yapısında Güvenlik(2/2)

- Ağa katılmak isteyen bir düğüm kendisine en yakın düğümü “sponsor düğüm” ilan eder.
- İstemci düğüm,kendisini asıllaması için elçi düğüme mesaj gönderir.
- PMP’teki güvenlik işlemlerinin benzeri sponsor düğüm tarafından yapılır.
- Asıllama işini yapan gerçek düğümle bir tünel kuran elçi düğüm, istemci düğüme mesajları iletilir.
 - Asıllama mesajları
 - Anahtar alışverişi
- Mesh’e dahil olan düğüm, diğer düğümlerle iletişime geçebilir.

Güvenlik Altyapısının Analizi(1/5)

- Veri şifrelemesindeki sorunlar
 - DES algoritması günümüzde kırılabilir bir algoritma haline gelmiştir.
 - Deneme-yanılma ve Brute-Force saldırularına dayanıksızdır.
 - 128-bitlik AES kullanılabilir
 - Daha yavaş ama güvenliği arttıracı bir yöntem

Güvenlik Altyapısının Analizi(2/5)

- Tekrar saldıralarına dayanıksızdır.
 - Aktif saldırılar gerçekleştirilebilir.
 - Telsiz ortamın doğasından kaynaklanan araya girebilme özelliğini ortadan kaldıracak bir yapı yok
 - Tekrar saldıruları için
 - Rastgele bir sayı
 - Paket numarası
 - Sekans numarası

Güvenlik Altyapısının Analizi(3/5)

- CBC Başlangıç vektörü tahmin edilebilir.
 - Seçilen Açık metin saldırısı yapılarak gerçek metin elde edilebilir.
 - Bazı çözümler
 - Başlangıç vektörü için
 - Her bir metin için değil, her bir çerçeve için IV üretimi
 - Bu IV'nin veriye gömülmesi
 - Şifreleme yükü artar!

Güvenlik Altyapısının Analizi(4/5)

- Anahtar Yönetimindeki sorunlar:
 - TEK'te kullanılan sekans numarasının 2-bit olması
 - Her bir tekrar saldırısında %25 bir olasılıkla TEK bulabilinir!
 - Rastgele üretilen TEK'lerin nasıl bir rassal fonksiyonla üretildiği konusunda bilgilendirme yapılmıyor.
 - Değişik üreticilerin oluşturduğu bir ağda güvensizlik ve dengesizlik yaratabilir.
 - BS tarafından oluşturulan AK'nin tazeligine güvenilmeli!
 - SS bunu kontrol etmiyor.

Güvenlik Altyapısının Analizi(5/5)

- Asıllamadaki problemler
 - Çift taraflı bir asıllama yok.
 - BS asıllanmıyor.
 - Ortadaki adam saldırısı yapılabilir.
 - Asıllama protokolunde gönderilen mesajlar doğrulama için yetersiz
 - EAP(Extensible Authentication Protocol) tabanlı bir asıllama yapılabilir.
 - EAP-TLS(Transport Layer Security)
 - EAP-MD5

GÜVENLİ İŞLETİM SİSTEMLERİ

- ✓ Tarihçe
- ✓ Linux İşletim sistemi nedir , nelerden oluşur
- ✓ Linux Mimarisi
- ✓ Neden Linux ?
- ✓ Linux İşletim Sistemlerinin Özellikleri

LINUX

➤ Tarihçe

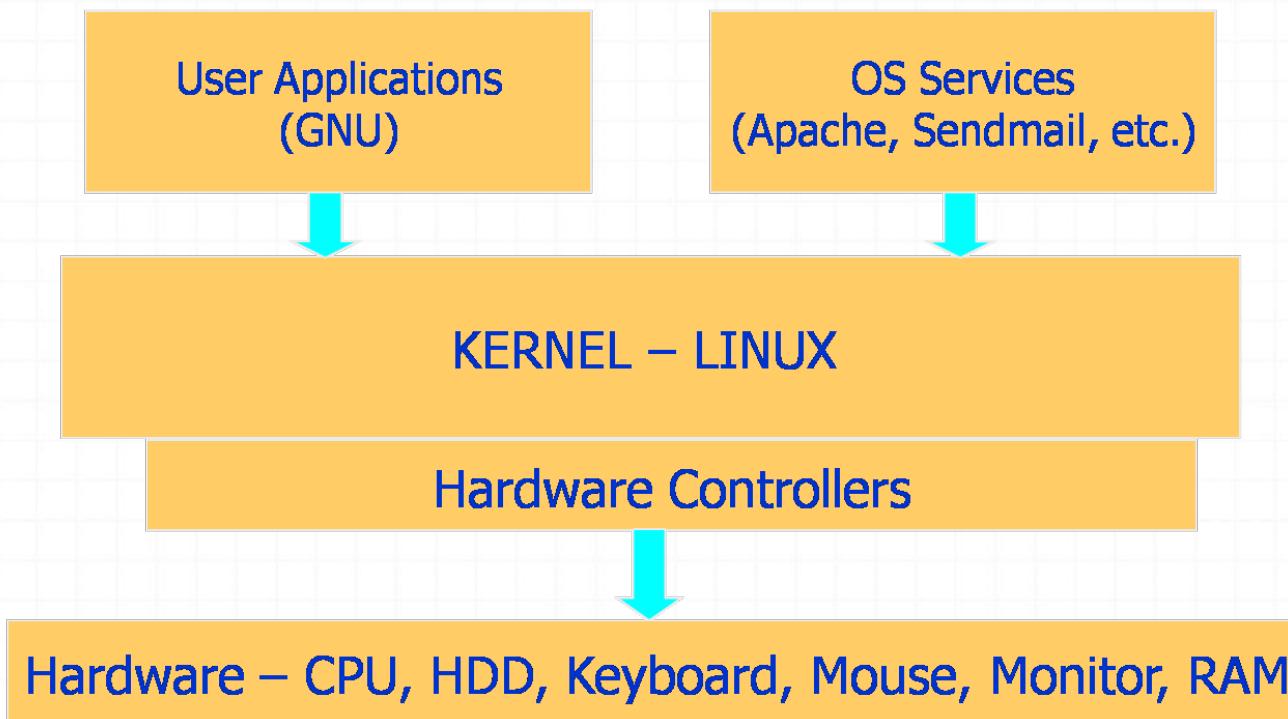
- 1991'de Linus Torvalds adında Finlandiyalı bir öğrenci bilgisayar mühendisliği eğitimi alırken Intel'in 80386 geliştirmek için çıkartmıştır.
- Minix de olmasının istediği özellikleri yeni işletim sistemine ekledi.
- 5 Ekim 1991 de Linux'un ilk sürümü 0.02 yi MIT'nin haber listelerinde Dünya ya duyurdu.

Linux işletim sistemi nedir?

- Unix bir işletim sistemi ailesine verilen ortak bir isimdir.
- Linux (resmi olarak olmasa da), OpenBSD, FreeBSD, Irix, Solaris, Aix... çeşitli Unix türevleridir.
- Linux, Unix sistemlerinin tüm avantajlarını taşır.Çok kullanıcılı ve bilgisayar ağlarında kullanılmak üzere tasarlanmıştır.
- Linux dağıtımları ;
 - Suse, Red Hat, Fedora, Knoppix vs

Linux işletim sistemi

LINUX MİMARİSİ



Neden LINUX ?

- Hız
- Maliyet
- Yaygınlık
- Güvenlik
- Sağlamlık

LINUX İşletim Sistemi Özellikleri

- Birden çok kullanıcı desteği
- Çok görevli olması
- Çok işlemci desteği
- TCP/IP desteği
- Dosya yapısı
- Kabuklar (shell)

1.Fiziksel Güvenlik

■ 1.1 BIOS Güvenliği

- Parola ayarı yapmak gereklidir.
- Konulan parola caydırıcı etki yapabilir.
- Tam anlamıyla güvenli sayılmaz.

2. Çekirdek (Kernel) Güvenliği

- Güncel tutmak
- Yamalı Çekirdek olmasından emin olmak
- Çekirdeğin derlenmesi gereklidir.

3. Kullanıcı Güvenliği

- Kullanıcılara yeni hesap açarken onlara gerekli olan kadar , minimum imtiyaz hakkı verilmelidir.
- Ne zaman login ,log-off olduklarını belirleyen kayıtlar mutlaka tutulmalıdır.
- Aktif olmayan hesaplar silinmelidir.Aktif olmayan hesaplar log dosyaları kontrol ederek görülebilir.

3. Kullanıcı Güvenliği

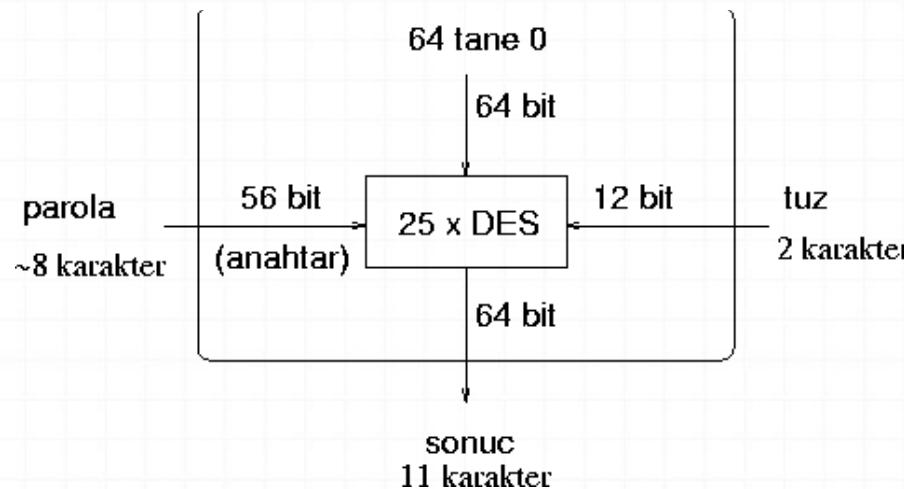
- Root hesabı adına dikkat edilmesi gerekenler ;
- Root olarak giriş izni çok kullanıcıya verilmemelidir.
- Root olarak rlogin/sh/rexec(r-utilities) kullanılmamalıdır. Kesinlikle .rhosts dosyası yanı özel erişim dosyası yaratılmamalıdır.

4. Parolalar

- Çok-kullanıcılı işletim sistemlerinde kullanıcının kimliğinin belirlenmesi büyük önem taşımaktadır. Hem sistemi kullanmaya yetkisi olmayan kişilerin sisteme girmelerinin engellenmesi, hem de sistemdeki kullanıcıların birbirlerinden ayrı edilebilmeleri için, her kullanıcıya bir parola verilir ve sisteme giriş başta olmak üzere tüm kritik işlemlerde kullanıcıya parolası sorulur.
- Parolalar, diğer kullanıcı bilgileriyle birlikte, parola dosyasında (**/etc/passwd**) tutulur. Bu dosyadaki her satır, bir kullanıcı ile ilgili bilgileri saklar. Bir satırdaki alanlar, sırasıyla, kullanıcı adı, parola, kullanıcı numarası, grup numarası, ad, kişisel dizin ve komut yorumcusudur.

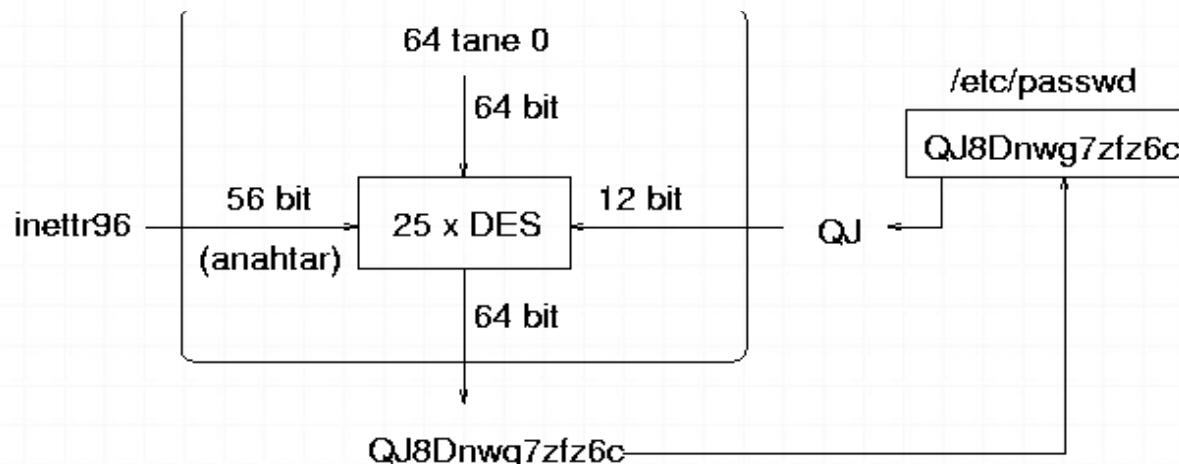
4.1 Parolaların Şifrelenmesi

- Crypt fonksiyonu ile şifreleme



4.1 Parolaların Şifrelenmesi

■ Parola Denetimi



4.2 Parola Seçimi

Şu tip parolalar kolay tahmin edilebilen parolalar sayılmaktadır:

- Kullanıcı ile yakınlığı olan kişilerinkiler (kendisi, ailesi, arkadaşları, yakınları) basta olmak üzere bütün erkek ve kadın isimleri
- Doğum tarihleri
- Kullanıcı ile ilgili herhangi bir bilgi (kullanıcı adı, oda numarası, telefon numarası, arabasının plaka numarası, sosyal güvenlik numarası)
- Yer isimleri
- Bilgisayar terimleri
- Klavyede belli bir düzene göre ardarda gelen harflerden oluşan parolalar (qwerty)
- Anlamlı bir sözcük
- Yalnızca küçük (ya da yalnızca büyük) harflerden oluşan parolalar
- Yukarıdakilerden birinin başına ya da sonuna bir rakam eklenerek oluşturulan parolalar
- Yukarıdakilerin ters yazılışları

4.2 Parola Seçimi

İyi bir parola üretmek için önerilen iki yöntem vardır:

- İki sözcüğün arasına bir rakam ya da noktalama işaretini konarak birleştirilmesi
- Seçilen bir cümlenin sözcüklerinin bas harfleri

4.3 Tehlikeler

Bir saldırganın parola dosyasını eline geçirmesi birkaç şekilde mümkün olabilir:

- Bir kullanıcının parolasını elde ederek sisteme girer ve dosyayı alır.
- Bazı programlardaki hatalardan yararlanarak sisteme girmeden dosyayı alır.
- Sistemdeki bir kullanıcı parola dosyasını saldırgana gönderir.
- Saldırgan, sistemdeki kullanıcılarından biridir.

4.4. Önlemler

- Parola Seçiminin Kullanıcıya Bırakılmaması
 - Sistem sorumlusu ya da rasgele parola üreten program tarafından parola verilmesi gerekir.
 - mkpasswd programı
- Parola Seçiminin Kısıtlanması
 - anlpasswd
- Parola Dosyasının Sistem Sorumlusu Tarafından Kırılması
 - crack
- Parolaların Geçerlilik Surelerinin Kısıtlanması
- Gölge Parolalar
 - Parolalar gölge dosyasına (/etc/shadow) şifrelenmiş parolalar konur.
 - Shadow Password Suite

5. Dosya Güvenliği

- Her dosyanın bir sahibi, bir de grubu vardır. Dosya üzerinde kimin hangi işlemleri yapabileceğine dosyanın sahibi olan kullanıcı karar verir. Erişim hakları, dosyanın sahibi, grubu ve diğerleri için ayrı ayrı belirtilir.
- Her biri için dosyanın okunmasına (read), yazılmasına (write) ve çalıştırılmasına (execute) izin verilebilir. Böylece her dosya için üç tane üçlüden oluşan bir erişim hakları listesi elde edilir.

-rwxr-x--- 1 karin users 4030 Dec 4 15:30 deneme

- Örnekteki ``deneme'' dosyasının sahibi "karin" kullanıcısı, grubu "users" grubudur. "karin" kullanıcısı dosyayı okuyabilir, yazabilir ve çalıştırabilir; "users" grubundaki kullanıcılar okuyabilir ve çalıştırabilir; diğer kullanıcıların ise hiçbir hakkı yoktur.

5.1. Tehlikeler

➤ Dosyanın izinsiz Olarak Okunması

- Kullanıcıların kişisel dosyalarının ve e-postalarının okunması

➤ Dosyanın Yetkisiz Kişilerce Değiştirilmesi

- Sistem dosyalarının değiştirilmesi
- Yetkili kullanıcı yaratılabilir
- Kayıt dosyalarının silinebilmesi

5.2. Önlemler

➤ Dosya Değişikliklerinin Denetimi

- Dosya imzaları oluşturma
- Tripwire paketi kullanılmalı

➤ Şifreleme

- PGP (Pretty Good Privacy) kullanılması
- CFS (Cryptographic File System)

Sonuç

- 802.16 standardındaki 2 düzeyli yapı, 802.11'e göre geliştirilmeye daha elverişli bir altyapı oluşturmakta.
- Sertifika otoriteleri hakkında daha açık bilgiler verilmeli.
- Veri şifreleme yöntemi: DES yetersiz
- Tek taraflı bir asıllama söz konusu
 - Geliştirilmesi gereken bir nokta
 - EAP kullanılabilir
- Anahtar üretiminde problemler var
 - Tekrar saldırılarının engellenebilmesi için rastgele sayıların üretilmesi gerekiyor.

Sorular



Kaynaklar

- [1] IEEE Std 802.16-2004--IEEE standard for local and metropolitan areanetworks, part 16: "**Air Interface for Fixed Broadband Wireless Access Systems**".
- [2] David Johnston ve Jesse Walker--INTEL: "**Overview of IEEE 802.16 Security**"
- [3] Kitti Wongthavarawat--Thai Computer Emergency Response Team (ThaiCERT) National Electronics and Computer Technology Center,Thailand: "**IEEE 802.16 WiMax Security**"
- [4] Loutfi Nuaymi, Patrick Maillé, Francis Dupont, Raphaël Didier--École Nationale Supérieure des Télécommunications de Bretagne:"**Security issues in WiMAX/IEEE 802.16 BWA System**"
- [5] Yun Zhou ve Yuguang Fang--Department of Electrical and Computer Engineering,University of Florida, Gainesville:"**Security of 802.16 in Mesh Mode**"

Kaynaklar

- <http://www.linuxplanet.com/linuxplanet/interviews/4495/1>
- www.linuxsecurity.com
- www.linux.org.tr
- IMPROVING THE SECURITY OF YOUR UNIX SYSTEM ,David A. Curry, Systems Programmer ,Information and Telecommunications Sciences and Technology Division
- Linux Sistem Güvenliği Raporu ,2003

Ağ ve Bilgi Güvenliği Yönetimi
Güvenlik Duvarı (Firewall)
Saldırı Tespit Sistemleri (Intrusion Detection System-IDS)
E-Posta Güvenliği
WWW Güvenliği

Prof. Dr. Resul Daş

Ağ ve Bilgi Güvenliği Yönetimi

Ağ ve Bilgi Güvenliği Yönetimi

- Bilgi güvenliği çerçevesinde kurulacak güvenlik sistemi altyapısının ve politikasının doğru bir şekilde belirlenebilmesi için, korunmak istenen bilginin değerlendirilmesi ve güvenlik yönetiminin doğru ve eksiksiz bir şekilde yapılması gereklidir.
- Güvenlik yönetimi, bilgi ve bilgisayar güvenliğini olumsuz yönde etkileyebilecek faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir.

Güvenlik Risklerini Değerlendirmek

- Risk, bir olayın ve bu olayın sonucunun olasılıklarının birleşimi olarak tanımlanmaktadır.
- Risk yönetiminin bir adımı olan risk değerlendirmesi, risklerin tanımlandığı ve tanımlanan bu risklerin etkilerinin ve önceliklerinin belirlendiği bir süreçtir.
- Risk yönetimi, kabul edilebilir düzeyde bir riskin belirlenmesi, hali hazırdaki riskin değerlendirilmesi, bu riskin kabul edilebilir düzeye indirilebilmesi için gerekli görülen adımların atılması ve bu risk düzeyinin sürdürülmesidir.

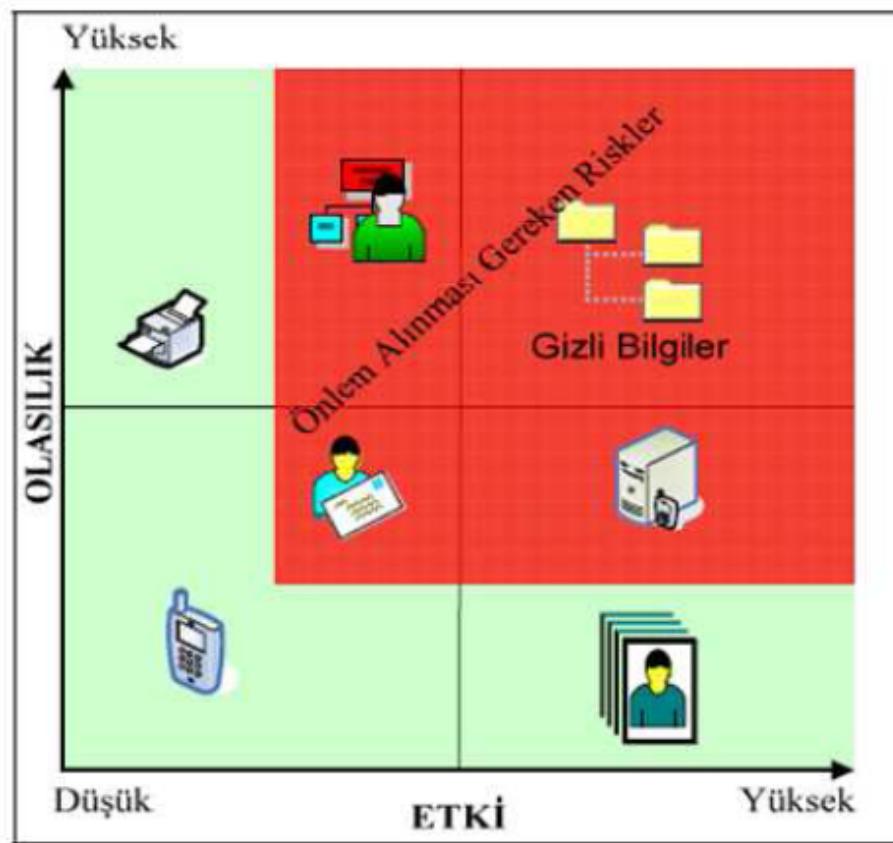
Güvenlik Risklerini Değerlendirmek

- Korunması gereken bilgi ya da varlıkların belirlenmesi;
 - Bu varlıkların kuruluşlar açısından ne kadar değerli olduğunu saptanması;
 - Bu varlıkların başına gelebilecek bilinen ve muhtemel tehditlerden hangilerinin önlenmeye çalışılacağının ortaya konulması;
 - Muhtemel kayıpların nasıl cereyan edebileceğinin araştırılması;
 - Her bir varlığın maruz kalabileceği muhtemel tehditlerin boyutlarının tanımlanması;
 - Bu varlıklarda gerçekleşebilecek zararların boyutlarını ve ihtimallerini düşürmek için ilk planda yapılabileceklerin incelenmesi ve ileriye yönelik tehditleri asgari seviyede tutmak için atılması gereken adımların planlanması
- risk değerlendirmesinin belli başlı saflarındanandır.

Güvenlik Risklerini Değerlendirmek

- Bilgi ve diğer varlıklar, bu varlıklara yönelik tehditler, var olan sistemde bulunan korunmasızlıklar ve güvenlik sistem denetimleri, mevcut riski tayin eden bileşenlerdir.
- Hangi bilgi varlıklarının korunacağı belirlendikten sonra kuruluşa uygun risk değerlendirme yönteminin seçilerek risklerin tanımlanması yapılır.
- Seçilen risk değerlendirme yöntemine göre bilgi varlıkları şekilde örneği gösterilen risk haritasında konumlandırılır.
- Değerlendirilme yapıldıktan sonra risk değerlendirme haritasında, etkisi ve olasılığı yüksek olan tehditler için risklerin iyileştirilerek kontrol altına alınması işlemlerini kapsar.
- Risk haritasında bilgi varlıklarının yeri değişiminden risk değerlendirme haritası düzenli olarak güncellenmeli ve gerekli önlemler alınmalıdır.

Güvenlik Risklerini Değerlendirmek



Güvenlik Risklerini Değerlendirmek

- Risk yönetimi sonucunda kurulacak ve yürütülecek güvenlik sisteminin maliyeti, dikkate alınması gereken bir başka önemli husustur.
- Güvenlik sisteminin maliyeti, korunan bilginin değeri ve olası tehditlerin incelenmesiyle belirlenen risk ile sınırlı olmalıdır.
- %100 güvenliğin olmayacağı ilkesi ile beraber, bilgi güvenliğinin ideal yapılandırılması üç süreç ile gerçekleştirilir.
- Bu süreçler,
 - önleme (prevention),
 - saptama (detection) ve
 - karşılık vermedir (response ya da reaction).

Güvenlik Süreçleri - Önleme

- Güvenlik sistemlerinin en çok üzerinde durduğu ve çalıştığı süreçtir.
- Bir evin bahçesine çit çekmek, çelik kapı kullanmak gibi güncel hayatı kullanılan emniyet önlemleri gibi, bilgisayar sistemlerine yönelik tehdit ve saldırılara karşı, sistemin yalıtılmış olması için çeşitli önlemler geliştirilmektedir.

Güvenlik Süreçleri - Önleme

- Kişisel bilgisayar güvenliği ile ilgili önlemler;
 - virüs tarama programlarının kurulu olması, ve bu programların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması,
 - bilgisayarda şifre korumalı ekran koruyucu kullanılması,
 - bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkışması,
 - kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi, bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi,

Güvenlik Süreçleri - Önleme

- Kişisel bilgisayar güvenliği ile ilgili önlemler;
 - disk paylaşımlarında dikkatli olunması,
 - Internet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi,
 - önemli belgelerin parola ile korunması veya şifreli olarak saklanması,
 - gizli veya önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi,
 - kullanılmadığı zaman İnternet erişiminin kapatılması,
 - önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması

Güvenlik Süreçleri - Önleme

- Kurumsal ortamlarda bilgisayar güvenliğinde uygulanması gereken önleme adımları daha geniş ve karmaşıktır.
- Güvenlik ile ilgili uzmanlaşmış kişilerin çalıştığı bu tür sistemlerde, önleme ile ilgili yapılanlardan bazıları:
 - İşletim sistemi ve yazılımların servis paketlerinin ve güncellemelerin düzenli aralıklarla incelenmesi,
 - Kullanıcı haklarının asgari seviyede tutulması, kullanılmayan protokol, servis, bileşen ve proseslerin çalıştırılmaması,
 - Veri iletişiminde şifreleme tekniklerinin, korunmasızlık tarayıcıları, Sanal Özel Ağ (Virtual Private Network) kullanılması,
 - Açık Anahtar Altyapısı (Public Key Infrastructure) ve e-imza kullanımı
 - Biometrik tabanlı sistemlerin kullanımı olarak sıralanabilirler.

Güvenlik Süreçleri - Saptama

- Güvenlik, sadece önleme ile sağlanabilecek bir mesele değildir.
- Örneğin bir müzede iyi bir korunmanın sağlanmış olması, müzenin çevresinin çitlerle çevrili olması, kapıların kapalı ve kilitli olması, o müzede geceleri bekçi kullanılmamasını gerektirmez.
- Aynı şekilde bilgisayar sistemlerinde de saldırı girişimlerini saptayacak yöntemlerin de kullanılması şarttır.

Güvenlik Süreçleri - Saptama

- Önleme, saldıruları güçlestiren (ama imkânsız kılmayan) veya saldıriganların cesaretini kıran (ama yok etmeyen) bir engel inşa etmeyi sağlar.
- Saptama ve karşılık verme olmadan önlemenin ancak sınırlı bir faydası olabilir.
- Sadece önleme ile yetinilseydi, yapılan çoğu saldıridan haberdar bile olunamazdı.
- Saptama ile daha önce bilinen veya yeni ortaya çıkan saldırular, rapor edilip, uygun cevaplar verebilir.
- Saptamada ilk ve en temel basamak, sistemin bütün durumunun ve hareketinin izlenmesi ve bu bilgilerin kayıtlarının tutulmasıdır.
- Bu şekilde ayrıca, saldırı sonrası analiz için veri ve delil toplanmış olur.

Güvenlik Süreçleri - Saptama

- Saptama sürecinde kullanılan yöntemlerden bazıları şunlardır:
 - Güvenlik duvarları
 - Saldırı tespit sistemleri (intrusion detection system)
 - Ağ trafigi izleyiciler
 - Kapı (port) tarayıcılar
 - Gerçek zamanlı koruma sağlayan karşı virüs ve casus yazılım araçları
 - Dosya sağlama toplamı (checksum) kontrol programları
 - Ağ yoklayıcı (sniffer) algılayıcıları

Güvenlik Süreçleri- Karşılık Verme

- Bekçiler, köpekler, güvenlik kameraları, algılayıcılarla donatılmış bir yerin, hırsızların dikkatini çekmesi gibi, gerçek zamanlı saptama sistemlerine sahip bilgisayar sistemleri de bilişim korsanları ve saldırınrlara cazip gelir.
- Hızlı karşılık verme, bu saldırıları püskürtmek için güvenlik sistemini tamamlayan esaslı bir öğe olarak ortaya çıkmaktadır.

Güvenlik Süreçleri- Karşılık Verme

- Karşılık verme, önleme süreci ile baş edilemeyen ve saptama süreçleri ile belirlenmiş saldırısı girişimlerini, mümkünse anında veya en kısa zamanda cevap verecek eylemlerin ifa edilmesi olarak tanımlanabilir.
- Saldırı tespit sistemleri, bu tespite cevap verecek birilerinin veya bir sistemin olması ile anlam kazanabilir.
- Aksi takdirde bu durum, hiç kimsenin duyup da önemsemediği bir araba alarmının getireceği faydadan öteye gitmez.
- Bu açıdan karşılık verme güvenlik sürecini tamamlayan önemli bir halkadır.

Güvenlik Süreçleri- Karşılık Verme

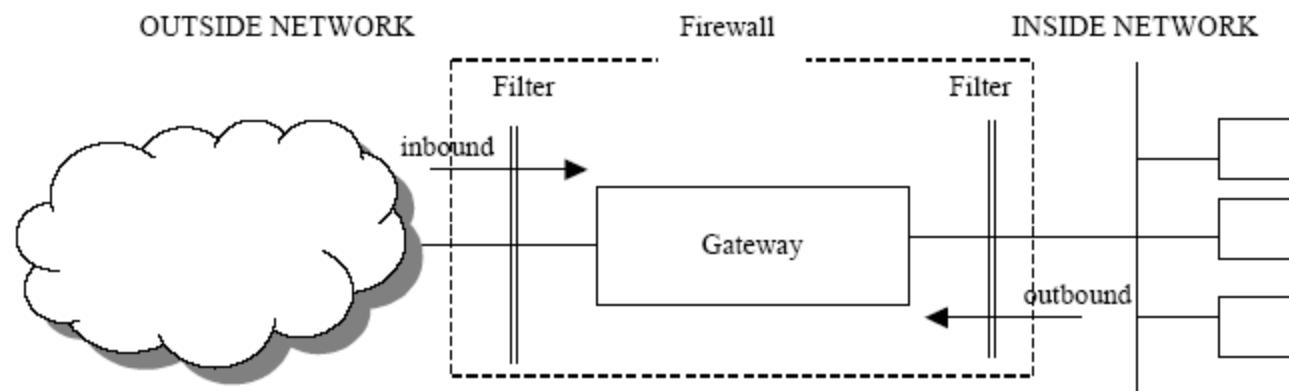
- Saldırı tam olarak önlenneme bile; sistemin normal durumuna dönmesine, saldırıyla sebep olan nedenlerin belirlenmesine, gerektiği durumlarda saldırının yakalanmasına, güvenlik sistemi açıklarının belirlenmesine ve önleme, saptama ve karşılık verme süreçlerinin yeniden düzenlenmesine olanak verir.
- Saldırı tespit edilince yapılması gereken işlerin, daha önceden iyi bir şekilde planlanması, bu sürecin etkin bir şekilde işlemesini ve zaman ve para kaybetmemeyi sağlayacaktır.
- Yıkım onarımı (disaster recovery), bu aşama için gerçekleştirilen ve en kötü durumu ele alan esaslı planların başında gelir.

Güvenlik Duvarları (Firewall)

Güvenlik Duvarı

- Bir güvenlik duvarı, bilgisayara ve ağa veri geçişini denetleyen, belirli kriterlere uymayan paketleri geçirmeyen bir yazılım programı veya donanım parçasıdır.
- Kullanılan güvenlik duvarının tipine göre bu işlem, verinin kaynağıyla istemci bilgisayar arasında olabilir veya bilgisayarda bir uygulama olabilir.

Güvenlik Duvarları



Güvenlik Duvarları

- 3'e ayrılırlar:
 - Paket Filtreleyici Güvenlik Duvarları (Packet Filtering Firewalls)
 - Devre Düzeyinde Güvenlik Duvarları (Circuit-Level Firewalls)
 - Uygulama Düzeyinde Güvenlik Duvarları veya Vekil Sunucular (Application-Level Firewalls or Proxy Servers)

Paket Filtreleyici Güvenlik Duvarları

- Gelen IP paketlerinin iletilip iletilmeyeğine daha önceden belirlenmiş bir takım kurallara göre karar veren çok portlu bir araçtır.
- Bu güvenlik duvarları, üzerlerinden geçen paketleri incelerler ve bunları verinin kaynağına, hedefine, kaynak ve hedef portuna bağlı olarak çeşitli kurallarla karşılaştırırlar.
- Bu güvenlik duvarları ile bilgilerin belirli türlerini engellemek, iyi bilinen portları kapatmakla kolayca yapılabilir.

Paket Filtreleyici Güvenlik Duvarları

- Bu güvenlik duvarları verinin içeriğine bakmazlar.
- Sadece şu bilgilere göre filtreleme yaparlar:
 - Kaynak ve hedef IP adresleri
 - Kaynak ve hedef port numaraları
 - TCP bağlantı bayrakları

Paket Filtreleyici Güvenlik Duvarları

- Paket filtreleme yapan yönlendiricilere perdeleyici yönlendiriciler (screening routers) denir
 - Örneğin,
Standart izin listesi

```
Interface Ethernet0
Ip address 172.16.1.1 255.255.255.0
Ip access-group 1
Access-list 1 deny host 172.16.3.10
Access-list 1 permit any
```
- Paket filtreleyiciler yönlendirme yapmak zorunda değildirler

Paket Filtreleyici Güvenlik Duvarları

- İkiye ayrırlırlar:
 - Durumsuz (Stateless)
 - Durumlu (Stateful)
- Durumsuz olanlarda pratikte problemler yaşanmaktadır.
- Bu problemleri engellemek için “stateful inspection” yöntemi kullanılır.

Paket Filtreleyici Güvenlik Duvarları

- Stateful inspection
 - Checkpoint Software Technologies tarafından bulunmuştur.
 - Eski IP paketlerine ait bilgiler saklanır.
 - Arkadan gelen paketler daha hızlı geçerler

Paket Filtreleyici Güvenlik Duvarları

- Dezavantajları
 - Sistem yöneticisinin saldırıları anlamasına yardımcı olabilecek kayıt tutma (logging) kabiliyeti çok azdır.
 - Paket filtreleme kuralları doğrudan test edilmek için zordurlar. Dolayısıyla, test edilemeyen açık noktalar kalabilmektedir.
 - Eğer karışık filtreleme kuralları gerekirse bunlar yönetilemez bir hale gelebilirler.
- Çoğu kablo/DSL cihazları bu güvenlik duvarlarını korumalarının bir parçası olarak kullanırlar.

Devre Düzeyinde Güvenlik Duvarları

- Bu tip güvenlik duvarları, dışarıdan bilgi akışına sadece içerisindeki bilgisayarlardan istek geldiğinde izin verir.
- Dışarıya giden isteklerin kaydı tutulur ve sadece isteğe karşılık gelen cevaba izin verilir.
- Bu tip bir güvenlik duvarının en önemli avantajlarından biri, dışarıdakilerin bütün bir ağı sadece güvenlik duvarının adresi olarak görmesidir. Böylelikle, ağın gerisi korunmuş olur.

Devre Düzeyinde Güvenlik Duvarları

- Bunun en büyük avantajı, içерiden istek gelmediği takdirde dışarıdan içeriye girilmesine izin verilmemesidir.
- Güvenlik duvari açana kadar bütün portlar kapalıdır.
- Ana dezavantajı ise, diğer filtreleme yöntemleriyle birleştirilmemiği takdirde içерiden gelen herhangi bir veri isteğine izin vermesidir.

Devre Düzeyinde Güvenlik Duvarları

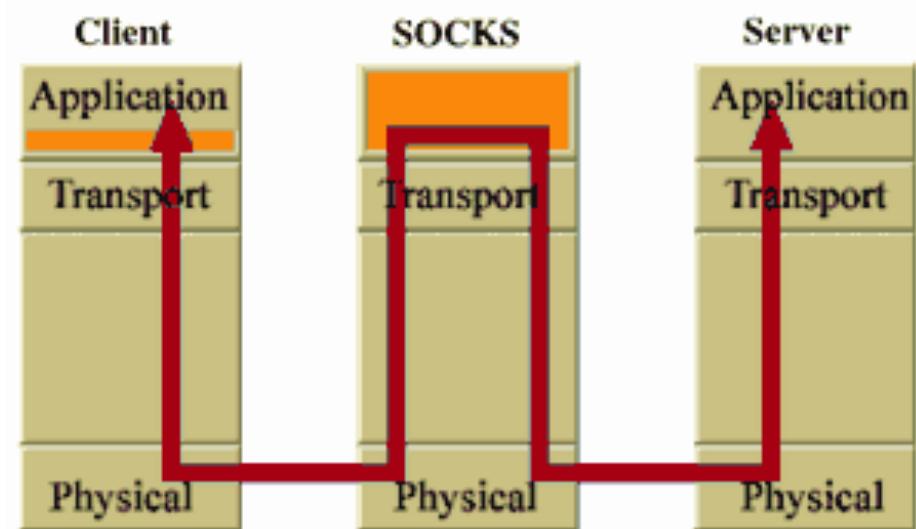
- Kablo/DSL yönlendiricileri bu yöntemi birincil olarak kullanırlar.
- Daha belirgin olarak, bunlar internet paylaşımı devre düzeyinde ağ geçitlerinin bir kombinasyonu olan NAT (Network Address Translation) kullanırlar.
- Devre düzeyinde ağ geçitleri arasında SOCKS yaygın olarak kullanılmaktadır.

SOCKS

- İstemci yazılımına ve/veya TCP/IP yığınına modifikasyon gerektirir
- İki parçadan oluşur
 - SOCKS sunucusu (daemon)
 - SOCKS istemcisi (kütüphanesi)

SOCKS

- SOCKS sunucusu uygulama katmanında çalışır
- SOCKS istemcisi uygulama ve ulaşım katmanları arasında çalışır



Uygulama Düzeyinde Güvenlik Duvarları

- “Proxy” olarak da anılan bu güvenlik duvarları, devre düzeyindekilere benzer şekilde, ağa giriş ve çıkış için tek geçiş olarak davranışırlar.
- En önemli fark ise bilgiyi ele alış şekillerindedir.
- Devre düzeyindeki güvenlik duvarları adres ve port bilgisine bakarken, bu güvenlik duvarları daha detaylı olarak inceler ve içeriğe bakar.
- Bu yöntemi kullanan güvenlik duvarları, yaygın veri türlerinin güvenlik duvarından geçmesine izin vermeden önce proxy uygulamaları çalıştırırlar.

Uygulama Düzeyinde Güvenlik Duvarları

- Bunun iki önemli avantajı vardır.
 - İlkisi, dış kaynaklar güvenlik duvarı arkasındaki bilgisayarlar arasında doğrudan bağlantıya izin vermemesi,
 - diğeri ise verinin içeriğine bakılarak filtreleme yapılabilmesidir.

Uygulama Düzeyinde Güvenlik Duvarları

- Uygulama düzeyindeki güvenlik duvarları sundukları kontrol düzeyleri nedeniyle çok güvenlidirler fakat önemli konfigürasyon gereksinimleri vardır.
- Ayrıca, paketleri geçirmekte de, çalışan proxy uygulamaları nedeniyle, diğer güvenlik duvarlarına göre yavaşırlar.
- İstemci bilgisayarlara da dışarıdaki kaynaklara erişim için ayrıca proxy konfigürasyonları yapılması gereklidir.

Uygulama Düzeyinde Güvenlik Duvarları

- Kullanıcı asıllama ve yetkilendirmesi yapılır
- Kullanıcı asıllama için gerekli bilgiler başka bir güvenlik sunucusunda tutulabilir
- Bunun için en çok kullanılan protokoller
 - Livingston Enterprises firmasına ait olan RADIUS
 - Cisco firmasına ait olan TACACS
- Bir sunucuya bağlanmadan önce uygulama düzeyinde bir ağ geçidine bağlanmak işlemi saydamlaştırılabilir. Buna “saydam vekillik (transparent proxy)” denir

Uygulama Düzeyinde Güvenlik Duvarları

- Bu güvenlik duvarları da devre düzeyindeki güvenlik duvarları gibi internet paylaşımı ile bütünleşmiştir.
- Bu tip güvenlik duvarları genellikle büyük bilgisayar ağlarını korumak için iş amaçlı kullanılmaktadır.

Güvenlik Duvarı Konfigürasyonları

- Değişik çeşitleri vardır.
- En yaygın kullanılan ikisi:
 - Çift-Evli Güvenlik Duvarları (Dual-Homed Firewalls)
 - Perdelenmiş Alt Ağ Güvenlik Duvarı (Screened Subnet Firewall)

Güvenlik Duvarı - Özeti

- Paket filtreleyici güvenlik duvarları basit bir güvenlik çözümü sağlarlar ve paketlerdeki verinin içeriğine bakmazlar
- Devre düzeyindeki güvenlik duvarları dışarıdan gelen paketler için tek giriş noktasıdır. Dışarıdaki bilgisayarlar sadece bunun adresini bilirler. Böylelikle, arkasındaki ağ güvenli bir şekilde korur. Ayrıca, asıllama ve yetkilendirme de yapılır. Burada da verinin içeriğine bakılmaz
- Uygulama düzeyindeki güvenlik duvarları ise bilginin içeriğine bakarak paketi geçip geçirmeyeceğine karar verir. Asıllama ve yetkilendirme mekanizmaları kullanır.

Güvenlik Duvarı - Özeti

- ☐ Çift-evli güvenlik duvarları daha güvenli bir yapı sunarken performans ve esneklik bakımından perdelenmiş alt ağ güvenlik duvarlarından daha düşük seviyedirler.

Saldırı Tespit Sistemleri

Saldırı Tespiti Nedir?

- Saldırı tespit sistemleri bir bilgisayar sisteminde veya ağında meydana gelen olayları **görüntüleme** ve bu olayların bilgisayar veya ağın mahremiyetine, bütünlüğüne, kullanılılığına uyuşma teşebbüsleri veya güvenlik sistemini atlatma olarak tanımlanan **izinsiz olarak erişim işaretini** işaret etmesini analiz eden süreçtir.

Saldırı Tespiti Nedir?

- İzinsiz olarak erişim;
 - Sisteme internetten erişen saldırganlar,
 - Yetkisi kapsamında olmayıp ilave ayrıcalık kazanma teşebbüsünde bulunan sistem yetkili kullanıcıları,
 - Kendilerine verilen ayrıcalıkları yanlış kullanan sistem yetkili kullanıcılar tarafından kaynaklanmaktadır.
- Saldırı tespit sistemleri bu görüntüleme ve analiz sürecini **otomasyona çeviren yazılım ve donanım** ürünleridir.

Saldırı Tespit Sistemleri Neden Kullanılmalıdır?

- Saldırı tespit sistemleri her şirketin güvenlik altyapısına ilave gerekli tedbir olarak geçerliliğini kazanmıştır.
- Saldırganların cezalandırılması ve keşfedilme riskinin artmasıyla problemli davranışları engellemek,
- Saldırıları ve diğer güvenlik ölçütleri tarafından önlenemeyen diğer güvenlik ihlallerini bulmak,
- Saldırı başlangıçlarını bulmak ve çözmek,

Saldırı Tespit Sistemleri Neden Kullanılmalıdır?

- Özellikle geniş ve karmaşık şirketlerin güvenlik dizaynı ve yönetimi için kalite kontrolcüsü olarak rol almak,
- İzinsiz olarak erişimler hakkında faydalı bilgi sağlamak.
- Var olan tehdidi belgelendirmek,

Başlıca Saldırı Tespit Sistemleri

- Farklı görüntüleme ve analiz yaklaşımlarıyla karakterize olan birkaç çeşit saldırı tespit sistemi mevcuttur.
- Her yaklaşımın avantaj ve dezavantajları vardır.
- Bütün yaklaşımalar saldırı tespit sistemleri için **soysal süreç modeli** terimi ile tanımlanabilir.
 - Süreç,
 - Zamanlama,
 - Bilgi kaynakları.

Ağ Tabanlı Saldırı Tespit Sistemleri

- Temel amacı ağ üzerinden yapılan saldırıları ağ trafigini gözetleyerek tespit etmektir.
- Ağ paketlerini yakalayıp bunları analiz ederek saldırı tespiti yaparlar.
- Bir bilgisayar ağının tamamını ya da belli bir kısmını izlerler.

Ağ Tabanlı Sistemlerin Avantajları

- İyi yerleştirilmiş birkaç ağ tabanlı nüfuz tespit sistemi geniş bir ağı görüntüleyebilir.
- Genellikle ağı dinleyen pasif cihazlar oldukları için mevcut ağa etkileri yok denecek kadar azdır.
- Saldırılara karşı büyük güvenlik sağlayabilirler ve çoğu saldırgan tarafından fark edilmeleri zordur.

Ağ Tabanlı Sistemlerin Dezavantajları

- Geniş veya yoğun ağlarda tüm paketleri işlemede zorluklar yaşanmakta ve dolayısıyla yoğun trafik zamanlarında saldırıları sezmede hataya düşebilmektedir.
- Şifrelenmiş bilgi incelememektedir. Bu daha çok sanal özel ağ (Virtual Private Network-VPN) kullanılarak yapılan saldırırlarda baş gösteren bir sorundur.
- Bir çok ağ tabanlı saldırısı tespit sistemi sadece ağa saldırısının olduğunu tespit etmekte saldırısının başarılı olup olmadığını sezememektedir.
- Anahtarlama cihazları bulunan ağlarda çalışmamaktadır.

Host Tabanlı Saldırı Tespit Sistemleri

- Belli bir bilgisayarı izlerler.
- İki tür bilgi kaynağı kullanırlar:
 - işletim sistemi izleme seçenekleri ve
 - sistem günlük dosyaları.

Host Tabanlı Sistemlerin Avantajları

- Host tabanlı saldırı tespit sistemleri yerelden hosta kadara olan olayları görüntüleme yetenekleriyle ağ tabanlı saldırı tespit sistemleriyle tespit edilemeyen saldırıları sezebilmektedirler.
- Host tabanlı saldırı tespit sistemleri genellikle host tabanlı bilginin veri şifrelenmeden önce ve/veya varış hostunda veri şifresi çözüldükten sonra analiz yaptığından trafigi şifrelenmiş koşularda çalışabilmektedirler.

Host Tabanlı Sistemlerin Avantajları

- Anahtarlama cihazlı ağlardan etkilenmemektedirler.
- Host tabanlı saldırı tespit sistemleri işletim sistemleri denetleme denemeleri üzerine çalıştığı zaman trojenleri ve yazılımla bütünleşik açıkları içeren saldırıları sezmeye yardımcı olabilmektedir.

Host Tabanlı Sistemlerin Dezavantajları

- Host tabanlı saldırı tespit sistemleri görüntülenen her host için yapılandırılması ve yönetilmesi gerektiğinden yönetimi daha zordur.
- Saldırıya uğrayabilir ve saldırının bir parçası olarak hizmet dışı bırakılabilirler.
- Host tabanlı saldırı tespit sistemleri ağ taramalarını sezmem veya tüm ağı hedef alan gözetleme için uyumlu değildir; çünkü ait olduğu hostun aldığı ağ paketlerini görebilmektedirler.

Uygulama Tabanlı Saldırı Tespit Sistemleri

- Avantajları:
 - Bireysel kullanıcıların yetkisiz işlemlerini takip edilmesine yarayan, kullanıcılar ve uygulamalar arasındaki etkileşimleri görüntüleyebilirler.
 - Genellikle uygulama hareketlerinin son noktasını ara yüzledikleri için şifreli koşullarda çalışabilmektedirler.
- Dezavantajları:
 - Saldırıya daha açiktır.
 - Genellikle kullanıcı seviyesindeki olayları görüntülemekte olup, trojen veya diğer yazılım saldırısını sezmemektedir.
 - Bundan dolayı uygulama tabanlı saldırı tespit sistemlerinin host tabanlı ve/veya ağ tabanlı sistemlerle birlikte kullanılması uygundur.

E-Posta Güvenliği

E-Posta Güvenliği

- E-posta sistemleri geleneksel posta sistemi ile büyük benzerlik göstermektedir:
 - İletilmesi istenen mesaj hazırlanarak sonra alıcı tarafın e-posta adresi de eklenerek uygun bir program veya ücretsiz internet siteleri aracılığıyla mesaj gönderilir.
 - E-posta öncelikle bir sunucuya iletılır.
 - Sunucu ise alıcı alanındaki e-posta adresine mesajın gönderilmesini sağlar.

E-Posta Güvenliğine Yönerek Tehditler

- Gizlilik Adımındaki Eksiklik
- Brute Force
- Fake Mail
- Phishing
- Keylogger-Trojan
- Uygulama Zaafları
- Sosyal Mühendislik
- XSRF-CSRF-XSS
- Clickjacking

Tehditler- Gizlilik Adımındaki Eksiklik

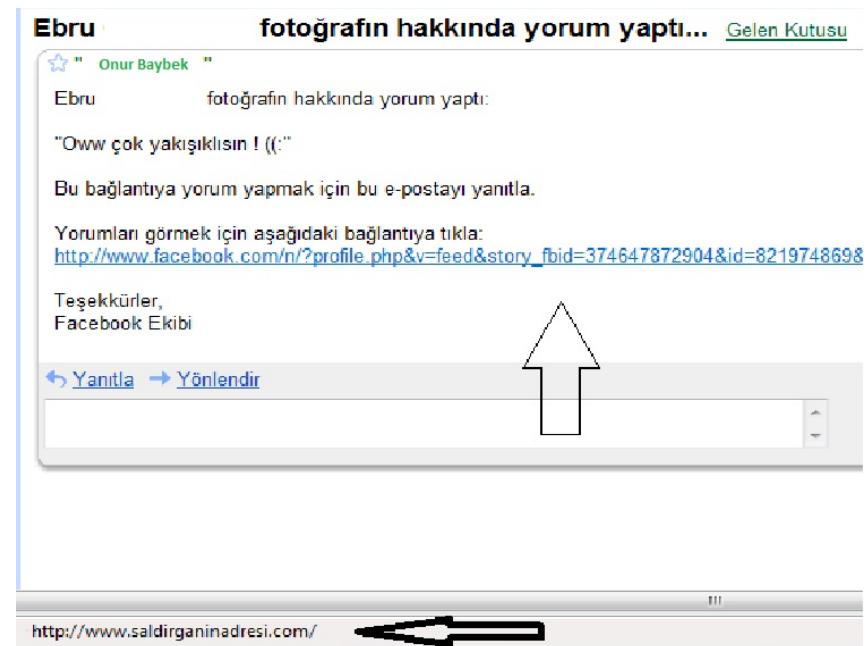
- Herhangi bir web sayfasına üye olduğunuz anda o sayfanın arama motorlarının robotları tarafından indexlenmesi sonucunda mail adresiniz “bulunabilir” olacaktır.
- Diğer bir ihtimal ise üyelik profilineinden e-posta adresinizin okunabilmesidir.
- Arama motoru kayıtlarına mail adresiniz girdiği anda spam listelerine de girmiş olursunuz, bu durumda da brute force (kaba kuvvet) ile saldırı yapanlarında “tesadüfen” saldırısı listesine dahil olabilirsiniz.
- Üye olduğunuz web uygulamasının veritabanı kırıldığı (hacklendiği) zaman eğer şifreniz kriptolanmamış ya da bir hash fonksiyonu içinden geçirilip kaydedilmemiş ise üyelik için kullandığınız şifre de ele geçirilecektir. Genel olarak kullanıcıların birçok yerde aynı şifreyi kullandığını düşünürsek bu ciddi bir durumdur.
- **Bu nedenlerden dolayı başkaları tarafından ele geçirildiğinde sizin için sorun olacak mail adreslerinizi sitelere üye olmak için kullanmamalısınız.**

Tehditler- Brute Force (Kaba Kuvvet) Atak

- Deneme yanılma yada bazı kelime listeleri kullanarak şifreyi tahmin etmeye çalışan saldırısıdır.
- Günümüzde teknoloji saldırıcılar lehinde çalışarak tanıldığınız kişilerin bazı bilgilerini girip onlardan şifre üreten ve deneyen programlar geliştirilmiştir.
- **Bu saldırılardan korunmak için e-posta şifrelerimizi küçük-büyük harfleri, rakamları ve özel karakterleri birlikte kullanarak oluşturmamız gereklidir.**

Tehditler- Fake Mail (Sahte Mail) Atak

- Posta kutunuza giriş yaptığınız sayfanın veya herhangi bir web sayfasının fake'inin (sahte) basit html kodları ve formmail ile hazırlanmış halidir.
- Kullanıcıyı bu adresle bir mail yardımı ile çekmeye çalışmak ve bu sahte giriş panelinden giriş yapmasını sağlamaya çalışma işlemidir.
- **Saldırıdan korunmak için dikkatli davranışlarak tıklanacak bağlantının nereye götüreceğini gösteren adres çubuğu incelenmelidir.**



Tehditler- Phishing

- “Sosyal Mühendislik” teknikleri kullanılarak, kurbanın kredi, Debit/ATM kart numaraları/CVV2, şifreler ve parolalar, hesap numaraları, internet bankacılığına girişte kullanılan kullanıcı kodu ve şifreleri gibi büyük önem arz eden ve çok iyi korunması gereken bilgilerini, kurbanı aldatarak elde etme yöntemi olarak tanımlanabilir.
- Başka bir ifadeyle Phishing; kişileri, yasal bir şirket, ajans veya organizasyon olduğuna inandırarak, kişisel ve finansal bilgilerini ele geçirme yöntemidir.
- Mail'i gönderen kişinin adresine aşina olmanız, bu mailin gerçekten o kişi tarafından yollandığı anlamına gelmez ! Gönderen kısmında yazan adres saldırgan tarafından istediği gibi değiştirilebilir.
- **Tek korunma yöntemi dikkatli ve bilinçli olmaktır.**

Tehditler- Keylogger / Trojan

- Bir malware (Zararlı Yazılım) genellikle temel olarak 2 kısımdan oluşur.
 - Bunlar “server-sunucu” ve “client-istemci”tir.
 - Zararlı dosya hedef kişiye çeşitli yöntemlerle kabul ettirilmeye çalışılır.
 - Server dosyasını hedef kişi çalıştırdığı andan itibaren hedef üzerinden veri gönderilir/alınır, ekran görüntüsü yada klavye vuruşları alınabilir.
 - Bir keylogger veya trojan sayesinde hedef seçilen bilgisayarda yapılan işlemlerin kayıtları da elde edilebilir..
- **Sürekli olarak değişikliğe uğrayan ve yenileri yayılan bilgisayar virüslerine (keylogger – trojan) karşı alınabilecek en belirgin önlem düzenli olarak veritabanları güncellenen bir antivirus programıdır.**
- **Antivirüs programları doğrudan kullanıcının masaüstü bilgisayarında çalışabileceği gibi e-posta sunucu sistemleri, içerik tarama uygulamaları, firewall gibi merkezi yapılar üzerinde de çalıştırılabilir.**

Tehditler- Uygulama Zaafları

- **E-posta hesabınıza girişlerinizde tarayıcılarınızın “beni hatırla” seçeneğini aktif edilmemelidir.**
 - Hatırla demeniz durumunda browser'in (tarayıcı) şifreleri barındırdığı dosyanın çeşitli yollarla saldırganın eline gelmesi ile mail adresiniz hacklenebilir .
 - Firefox'un hatırladığı şifreleri görüntüleyebilirsiniz.
 - Outlook şifreleriniz “Protected Storage PassView” gibi yazılımlarla çalınabilir.
- **Outlook gibi yazılımlarda zaman zaman bulunan zaaflar ile mail güvenliğiniz tehlikeye düşebilir.**
- **Bu yüzden otomatik güncelleştirmeleri açık tutmak tavsiye edilir.**

Tehditler- Sosyal Mühendislik

- Sosyal mühendislik kişileri kandırarak değerli bilgi ve parolalarını ellerinden almayı amaçlamaktadır.
- Günümüzde google, bloglar, sosyal ağlar ve daha bir çok yöntem ile hedef kişi hakkında bilgi toplanabilir.
- Günümüzde google, bloglar, sosyal ağlar ve daha bir çok yöntem ile hedef kişi hakkında bilgi toplanabilir.
- Sosyal Mühendislik sanatı kişisel iletişim ve ikna kabiliyeti gerektiren bir iştir.
 - Karşı tarafın şüphesini çekmeden elde edilmek istenilen bilgiyi almak her zaman sanıldığı kadar kolay olmayabilir.
 - Bu yüzden “sabır” çok önemli bir faktördür.

Tehditler- XSRF-CSRF-XSS

- Saldırganın çoğunlukla JavaScript kodunu siteye enjekte etmesiyle ortaya çıkar.
- Saldırganın özel oluşturduğu bir linki kurbana gönderdiğini düşünelim.
 - Kurbanın linke tıklamasıyla JavaScript kodu çalışmaya başlar ve kurbanın cookieleri saldırana gider, cookieler sayesinde hedef kişinin oturumu yetkisizce çalınabilir.
 - Hedef kişinin oturum bilgileri, saldırının kurduğu sniffer'da toplanır.
- **Bu tür saldırılarından korunmanın herhangi bir yolu yoktur.**
- **Tek çözüm bilmediğiniz linklere tıklamamanız ve Hex'li url'lere karşı şüpheli yaklaşmanızdır.**

Hex'li url örneği :

<http://3513587746@3563250882/d%65f.%61%73p%3F%69d=522>

Tehditler- Clickjaking

- Bir browser güvenlik açığıdır.
- Iframe ; Bir web sayfasına zararlı bir web sayfasının (opacity(şeffaflık) değeri=0) olarak gizlenmesidir. Sayfa içinde sayfa mantığıdır.
- Click and Redirect; Normal bir link yerine tıklanış esnasında farklı bir action(yönlendirme) sağlanmış, tuzaklanmış linklerdir.
- Clickjacking ile basit bir web sayfası hazırlayıp, ufak bir sosyal mühendislik senaryosu ile bir formu submit ettirebilir, dolayısı ile XSRF saldırısı gerçekleştirebilir, HTML Downloader, Keylogger gibi yazılımları ile saldırı yapılabilir.
- **Çözümü dikkatli davranıştır.**

WWW Güvenliği

WWW Güvenliği

- WWW, Web, ya da W3 (World Wide Web), yazı, resim, ses, film, animasyon gibi pek çok farklı yapıdaki verilere kompakt ve etkileşimli bir şekilde ulaşmamızı sağlayan bir çoklu hiper ortam sistemidir.
- Hiper ortam, bir dökümandan başka bir dökümanın çağırılmasına (navigate) olanak sağlar (iç içe dökümanlar). Bu ortamdaki her veri (object), başka bir veriyi çağrıbilir .

WWW Güvenliği

- WWW (World Wide Web) kısacası dünyadaki bilgisayarların birbiriyle iletişim kurabildiği, görüntü, ses, veri paylaşımının yapılabildiği global bir ağdır.
- Bu ağa üye olan milyonlarca bilgisayar web sayfalarını düzenleyip belli bir web sunucusu üzerinde yayınlanmaktadır.
- Her bir sitenin kendine ait **www** ile başlayan bir web adresi vardır.
 - Bu web adreslerini görüntülememize yarayan çeşitli yazılımlar vardır.
 - Bunlara web tarayıcı (Browser) denir. (Internet Explorer, Google Chrome, Mozilla Firefox gibi)

WWW Güvenliği

- Bir Web dokümanına ulaştığımızda her şey 4 ana fazda gerçekleşir:
 - 1) Bağlantı
 - 2) Ne istediğimizin web servisine iletilmesi
 - 3) Cevap
 - 4) İlgili sayfaya yapılan bağlantının kesilmesi
- Bu ana safhalar, web üzerinde iletişim kurallarını tanımlayan bir protokolü oluştururlar.
- Bu protokole de, Hyper Text Transfer Protocol (HTTP) denir.

WWW Güvenliği

- Bağlantı safhasında, web erişiminde kullanılan bir web listeleyici (browser, web client), ilgili bilginin olduğu web servisine bağlanır.
 - Bu servislere **HTTP servisleri** de denir.
- Bağlantı sağlandıktan sonra web istemci programımız http servisine "ne istediğini" bildirir.
 - Bu istek "http", "ftp", "e-mail" gibi bazı protokol kurallarını içerir ve bu işlemlere genel olarak "**navigate**" de denir.
- Bu isteği alan http servisi de, istediğimiz işlemi yapar ve cevabı bize gönderir.
 - Biz de gelen cevabı web istemci programımızda görürüz.
 - Eğer istek gerçekleştirilemiyorsa bir hata mesajı ile karşılaşırız.
- Son safhada ise, http servisine yaptığımız bağlantı kesilir.

WWW Güvenliği

- Günümüzde World Wide Web (WWW), güncel ve doğru bilgiyi insanlara ulaştırmak için en kolay ve en etkin yöntem olarak karşımıza çıkmaktadır.
- Kurulan bir web sunucusu ve içine hazırlanan site içeriği üzerinden, kurumunuz hakkında bilgiyi sunabilir ve ticaret yapabilirsiniz.
- Web sitesi saldırıları (web defacement) her geçen gün artmaktadır.
 - Bunun nedeninin web sitesi güvenliğinin yeterince ciddiye alınmaması olduğu düşünülmektedir.
- Yine WWW üzerinde girdiğimiz kişisel bilgiler de saldırganlar tarafından kolaylıkla elde edilebilir durumdadır.

WWW'de Korunma Yöntemleri

- %100 güvenmediğiniz sitelerden program indirmeyin, bu programları kullanmayın.
- Tanımadığınız kişi veya kurumlardan gelen e-postalardaki ekli dosyaları açmayın, chat gibi güvensiz yollarla gelen dosyalar almayın.
- Bilmediğiniz veya güvenliğinden emin olmadığınız sitelere kişisel bilgilerinizi kesinlikle vermeyiniz.
- İnternet üzerindeki güvenlik ile ilgili konu ve bilgileri yakından takip ediniz. İşletim sisteminizi ve programlarınızı korumak için yeni teknolojileri kullanınız.
- Bankaların Internet şubelerinde ya da kimlik doğrulaması yaparak giriş yaptığınız tüm sitelerde işlemlerinizi sona erdirdikten sonra mutlaka "Güvenli Çıkış" butonunu kullanın.

WWW'de Korunma Yöntemleri

- Kredi kartınızı kullandığınız ya da kişisel bilgilerinizi yazdığınız bilgisayarın güvenli olmasına dikkat edin.
 - Internet cafe gibi yerlerde bu tarz bilgilerinizi kesinlikle girmeyin.
- Kullanmakta olduğunuz işletim sisteminiz ve tarayıcı programınız için üretici firma tarafından yayınlanan güvenlik güncellemeleri ve yamalarını mutlaka kullanın.
 - Microsoft Internet Explorer kullanıyorsanız, Microsoft Security ana sayfasından www.microsoft.com/security/ 'den konu ile ilgili özel güvenlik ayarlarını yükleyin.
- Trojanların, virüsler gibi, tamamen masum programlara ilistirileceğini unutmayın. İstedığınız program bilinen ve saygı duyulan bir şeye bile, kişisel sayfalardan ziyade, yapımcının sayfasından edinin.

WWW'de Korunma Yöntemleri

- Bilgisayarınızı risklerden korumanın en önemli yollarından birisi de bir Kişisel Firewall yazılımı edinmektir.
 - Firewall (ateş duvarı) ile bilgisayarınız ile art niyetli kullanıcılar arasına bir set çekilmiş olur.
 - Temelde hem şüpheli haberleşmeyi kısmen engellemek, hem de şüphesiz haberleşmelere izin vermek gibi bir fonksiyonu yerine getirir.
 - Bir başka deyişle Firewall, e-posta da dahil olmak üzere pek çok kanaldan size ulaşan bilgi ve belgeleri kontrol eder ve uygun olmayan ya da şüpheli bilgi girişini engeller.

WWW'de Korunma Yöntemleri

- Internet'te paylaşmanız gerekenden fazlasını paylaşmayın. Gerçekten ihtiyacınız olmadıkça 'File and Printer sharing' gibi şeyleri yüklemeyin.
- Bir network üzerindeyseniz ve dosyalarınızdan bir kısmını paylaşımı açmak zorundaysanız, onları şifre korumalı olarak paylaşın.
 - 'ky8xdj33bgyt67' gibi uzun ve rasgele bir şifre kullanmalı ve düzenli olarak değiştirmelisiniz.
- Erişmek istediğiniz web sayfasının adresini tarayıcınızıın adres satırına kendiniz yazın.

WWW'de Korunma Yöntemleri

- Internetten indirdiğiniz her dosyayı çalıştırılmamalı ve her soruya "Yes" ya da "Evet" butonuna tıklayarak cevap verme alışkanlığına son vermelisiniz.
 - Hatta son zamanlarda "No" ya da "Hayır" tuşuna basmakla da bu programların kendiliğinden yüklenemilmektedir.
 - Pencerenin sağ üst köşesinde yer alan "X" yani pencereyi kapa düğmesine tıklamak en garantili yol gözükmemektedir.
- Müzik, resim, film indirmek istediğinizde uzantılara dikkat etmelisiniz.
 - ".exe" uzantısı gördüğünüzde indirmeyip o siteyi kapatmalısınız.
 - Çünkü dialer programları sadece tıklama yapıldığında değil, siz o sayfayı açtığınızda hiçbir yere tıklamasanız da bilgisayarınıza kendiliğinden yüklenebilmektedir.

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 paylaşımı 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 Sistemi dir.

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 anımları 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 gereklidir.

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

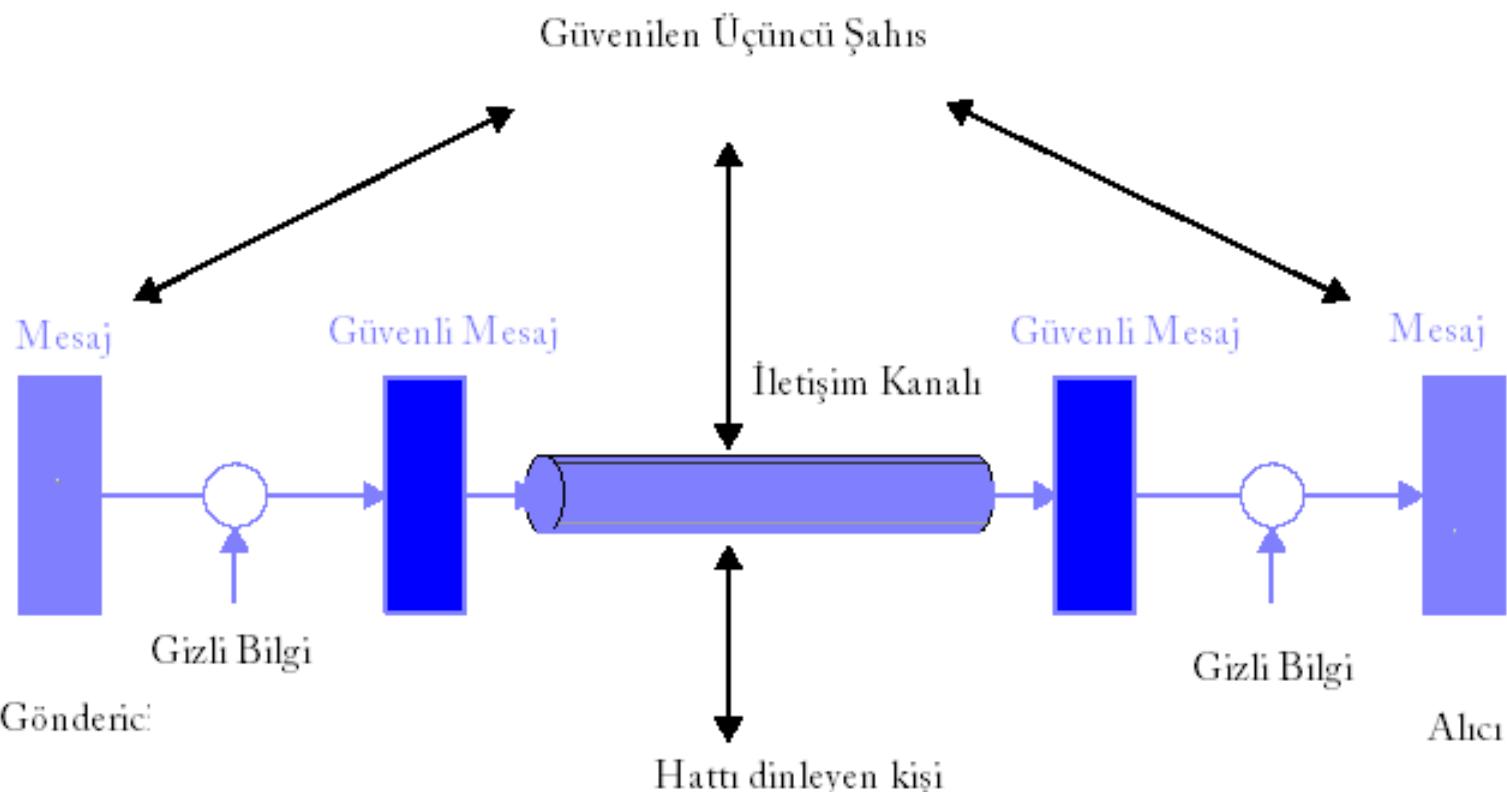
Ağ Güvenliği

- 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 sizma denetim sistemleri verilebilir.

Ağ Güvenliği İçin Bir Model



Gönderici ve alıcı mesajları gizli olarak ileterken, güvenli bir üçüncü şahıs gizli bilgilerin dağıtımıcısı olarak hizmet vermektedir, her iki taraf arasında noter görevi görmektedir.

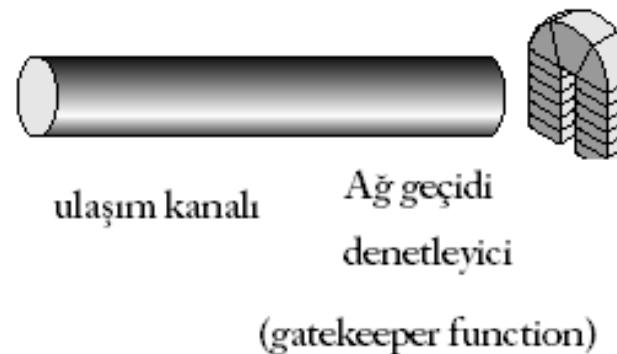
Ağ Güvenliği İçin Bir Model

- 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 dağıtımını ve paylaşımı için yöntem geliştirme
 - Güvenlik algoritmasını ve güvenlik servisini sağlayacak gizli bilginin kullanımını sağlayacak protokol belirleme

Bilgisayar Güvenliği İçin Bir Model

Hattı Dinleyen

-kişi
-yazılım (virus,
bilgisayar kurdu)



Bu modeli kullanmak için:

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

Güvenlik Sisteminin Katmanları

Tüm Sistemin Güvenliği

Güvenlik Protokolleri

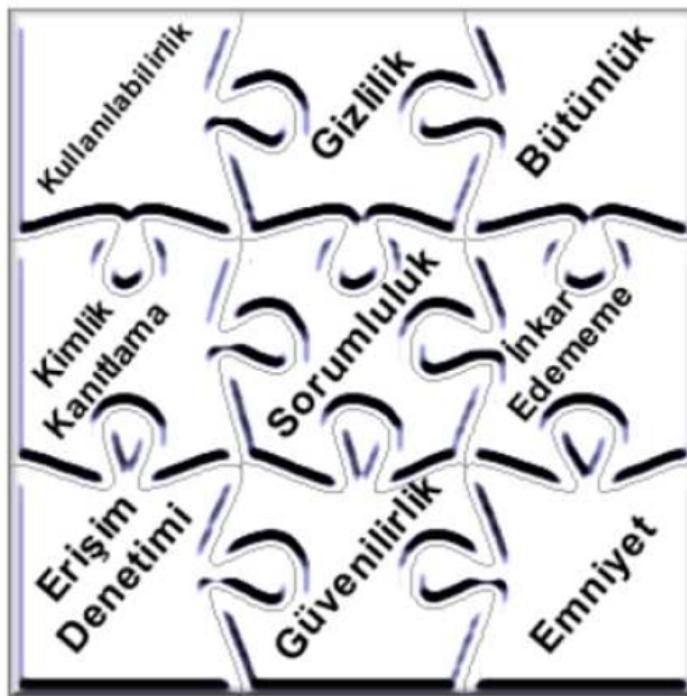
Kriptografi (Şifreleme)

- Ağ güvenliğinde şifreleme yapıtaşısı 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 doğrulama (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 görüleceği 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 dağıtım (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 değiştirilmemiğiyle 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 Protokollerı

- Ağ üzerinde iki bilgisayarın karşılıklı veri aktarabilmesi ve ortak süreçler yürütebilmesi için bilgisayarların karşılıklı çalışabilme yeteneğinin olması gereklidir.
- 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 Protokollerı

- Katmanlarına göre güvenlik protokollerı şu şekildedir.
 - Uygulama katmanındaki güvenlik protokollerı
 - Kerberos, S/MIME, PGP
 - Ulaşım katmanındaki güvenlik protokollerı
 - 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

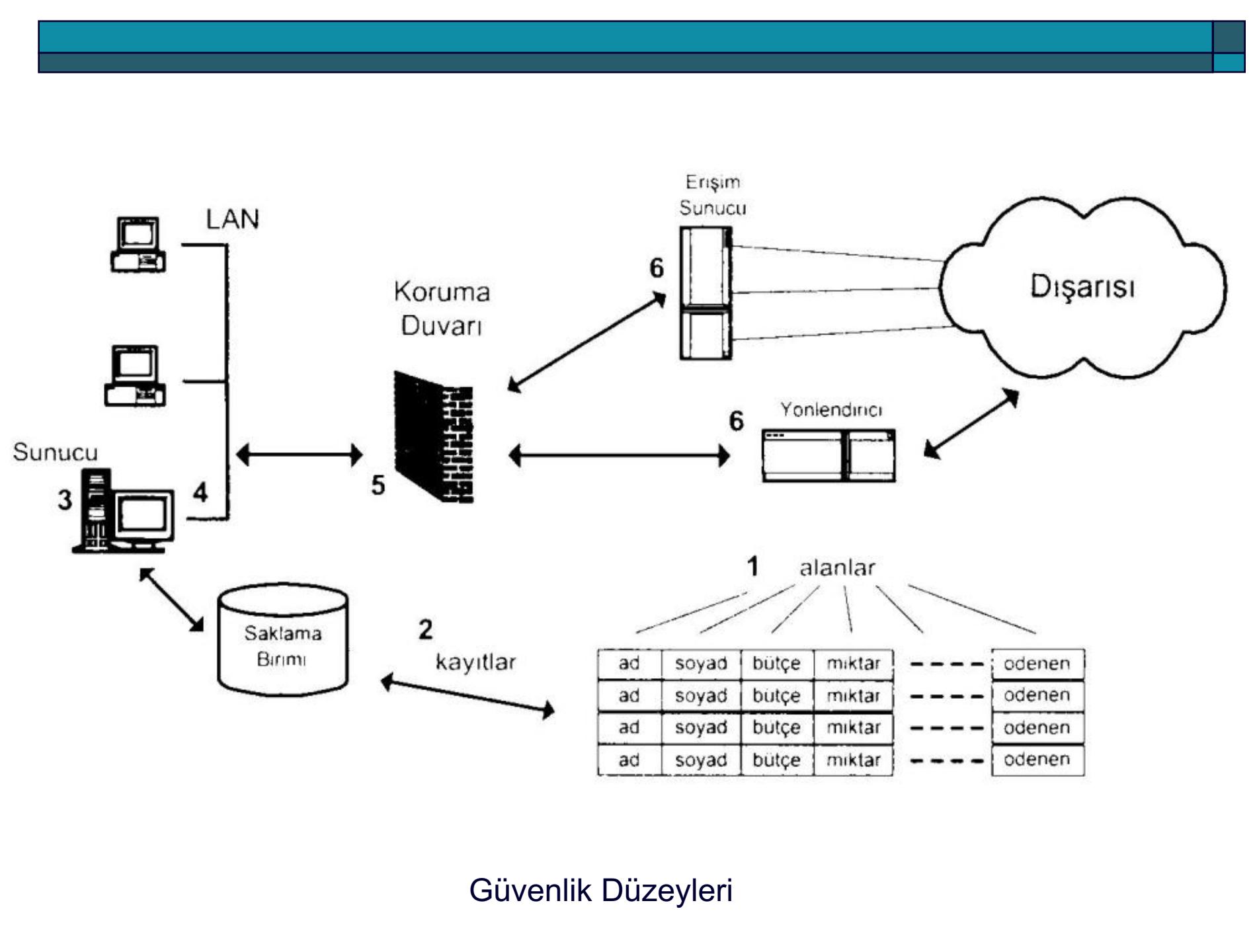
- Güvenlik düzeyleri 6'ya ayrılabilir. Bunlar:
 1. **Kayıt alanı düzeyinde koruma**
 2. **Veri kayıdı düzeyinde koruma**
 3. **Uygulama programı düzeyinde sorgulama/koruma**
 4. **Bilgisayara bağlanmayı sorgulama**
 5. **Ağ kaynaklarını hizmet türleri açısından koruma**
 6. **Ağa girişi sorgulama/koruma**

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, diğer ise bilgisayar sisteme 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 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 faydalananmak, 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 gerektigidir.
- 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 istediği 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 saygınılığını 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 kaybedecekтир.

Korunacak Varlıklar - Saygınlık

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

Bilgisayar Ağına Saldırı

- Internetin 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 faydalananarak bilgi hırsızlığı yapmaktadır.

Saldırganlar

- İstatistiki raporlara göre saldırıların çoğunun firma içerisinde 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 saldırular ve kötü niyetli olmayan saldırular olmak üzere ikiye ayrırlılar.

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	Yapılardırma zayıflıkları	Hizmet çalma	Sosyal statüye meydan okuma
Meraklılar	Dağıtık araçlar	İzinsiz erişim	Hizmet önleme	Zevk için
Profesyonel suçlular	Veri dinleyici sistemler			

Saldırganlar ve amaçları

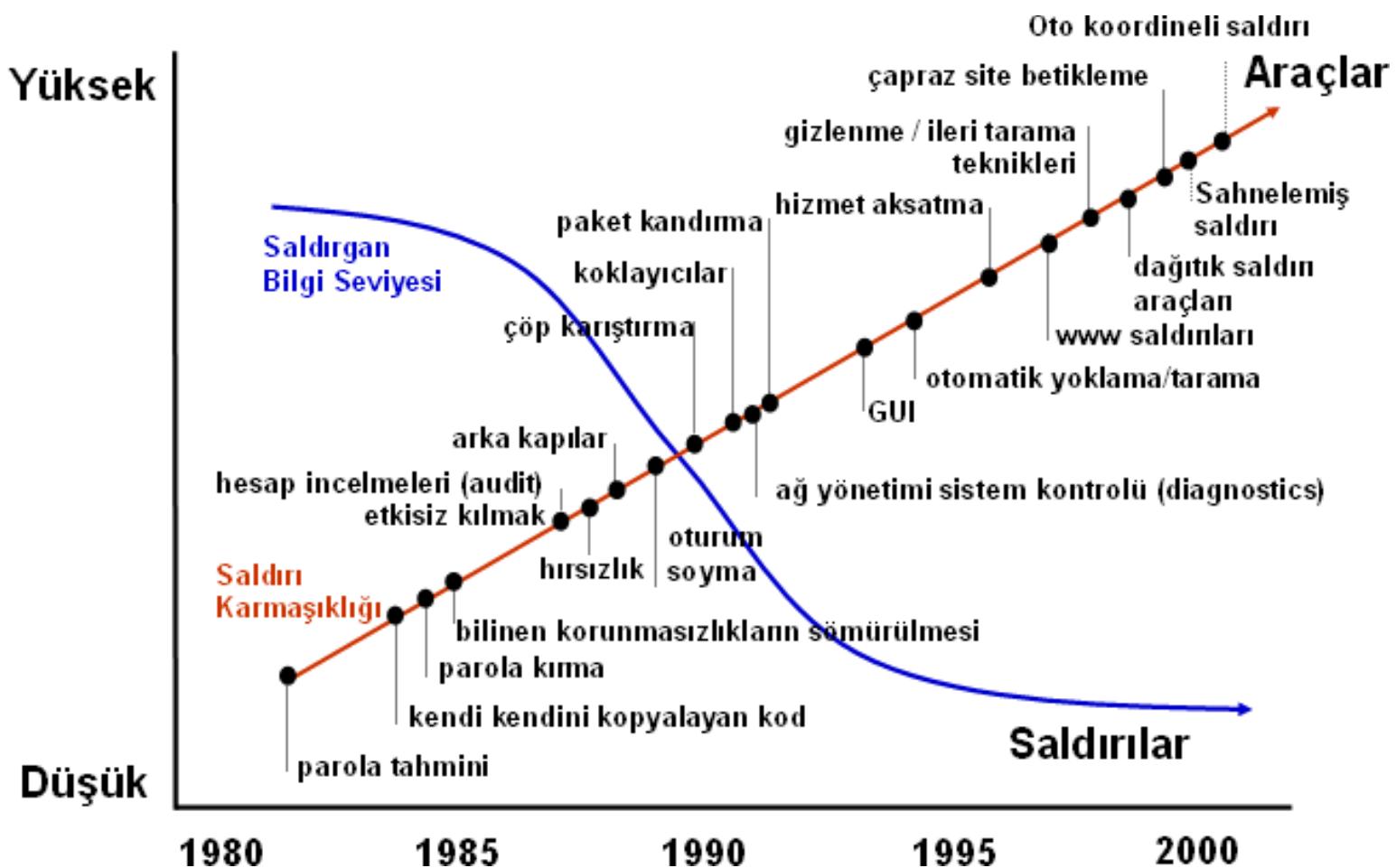
Saldırganlar

- 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 notlarının 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) saldırırlara bırakmıştır.
- Saldırılar veya saldırılarda kullanılan araçlar teknik açıdan gittikçe karmaşıklaşıırken, 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 meselesiyydi. 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'nın 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 :

- 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 çaptırıldı.



Robert Morris

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 düzenlemiştir.
 - 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, 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.



Vladimir Levin

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.
- Yargıldığını 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 (ürtim)

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 kaynağı erişim elde eder.
 - Yetkisiz taraf, bir şahıs, bir program veya bir bilgisayar olabilir.
 - Ağdaki veriyi veya dosyaların kopyasını alabilir.

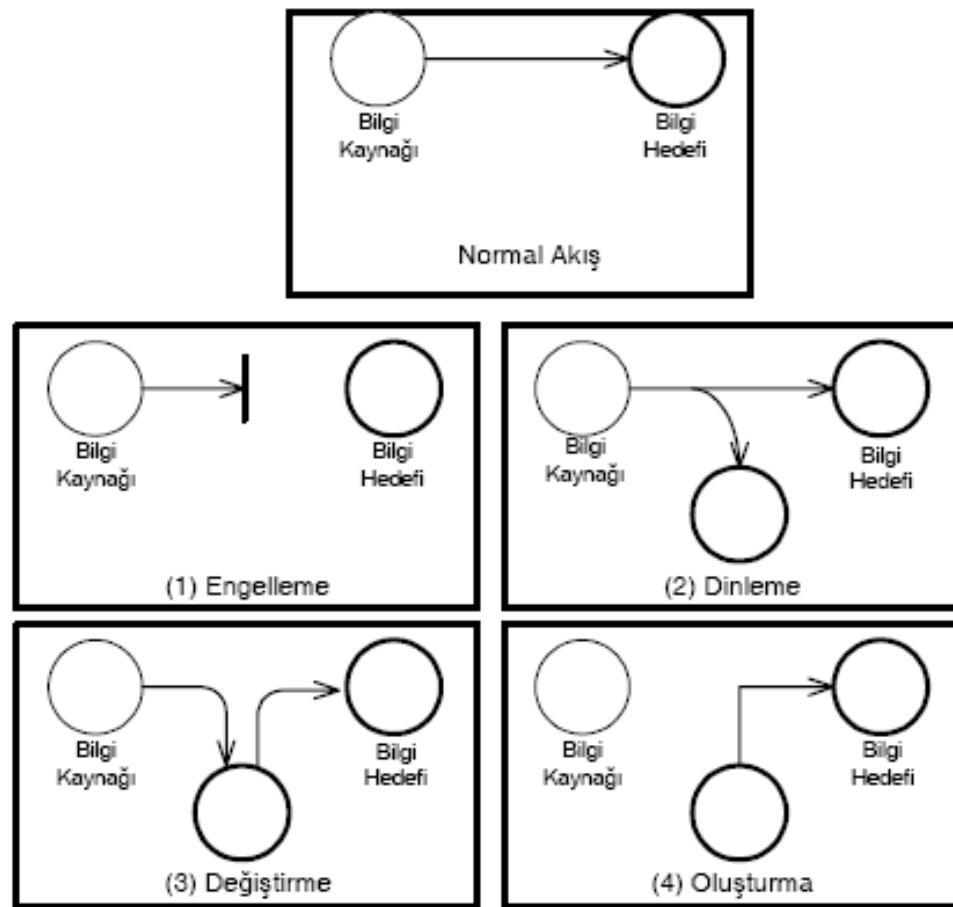
Süreçsel Sınıflandırma

- **Değiştirme:**
 - İzin verilmemiş bir taraf bir kaynağa erişmenin yanı sıra üzerinde değişiklikte yapar.
 - Bir veri dosyasının değiştirilmesi, ağdaki bir mesajın değiştirilmesi gibi.....
- **Oluşturma (ürtim):**
 - 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.
- Engellemeye, değiştirme ve oluşturma ise etkin(aktif) bir saldırı türü olarak görülmektedir.

Süreçsel Sınıflandırma

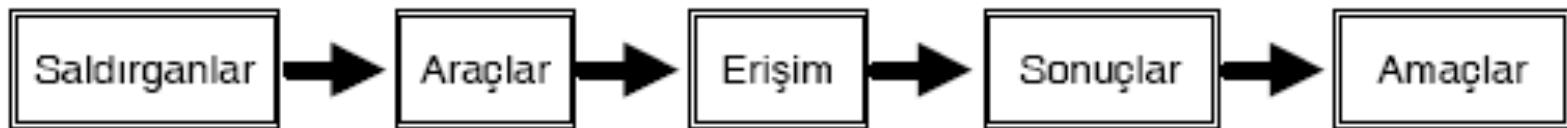


Süreçsel Sınıflandırma

Saldırı	Hedef Güvenlik Unsuru	Yaklaşımlar	Çözüm
Yarıda kesme (interruption)	kullanılabilirlik (availability)	<ul style="list-style-type: none">Donanım yıkımıIletişim hatlarına fiziksel hasar vermeGürültü yaymaRota (routing) şaşırıtmaProgram ve dosya silimi<u>DoS (hizmet aksattırma) saldırıcıları</u>	Etkin bir çözüm yok.
Gizli dinleme (intercept)	gizlilik (confidentiality) ve kişisel gizlilik (privacy)	<ul style="list-style-type: none">Gizli dinleme (Eavesdropping)Hat izlemePaket yakalamaSistemle uzlaşma	Şifreleme/şifre çözme
Değiştirme (modification)	bütünlük (integrity)	<ul style="list-style-type: none">Veritabanı kayıtlarını değiştirmeIletişimde gecikmelerden yararlanmaDonanımda değişiklik yapma	Her bir mesaj paketi için sayısal imza kullanımı
İmalat veya üretim (fabrication)	asılık (authenticity)	<ul style="list-style-type: none">Veritabanına yeni kayıt eklemeIP kandırma ile yeni ağ paketi eklemeSahte e-posta veya bölge adları kullanma	Kimlik kanıtlama (authentication)

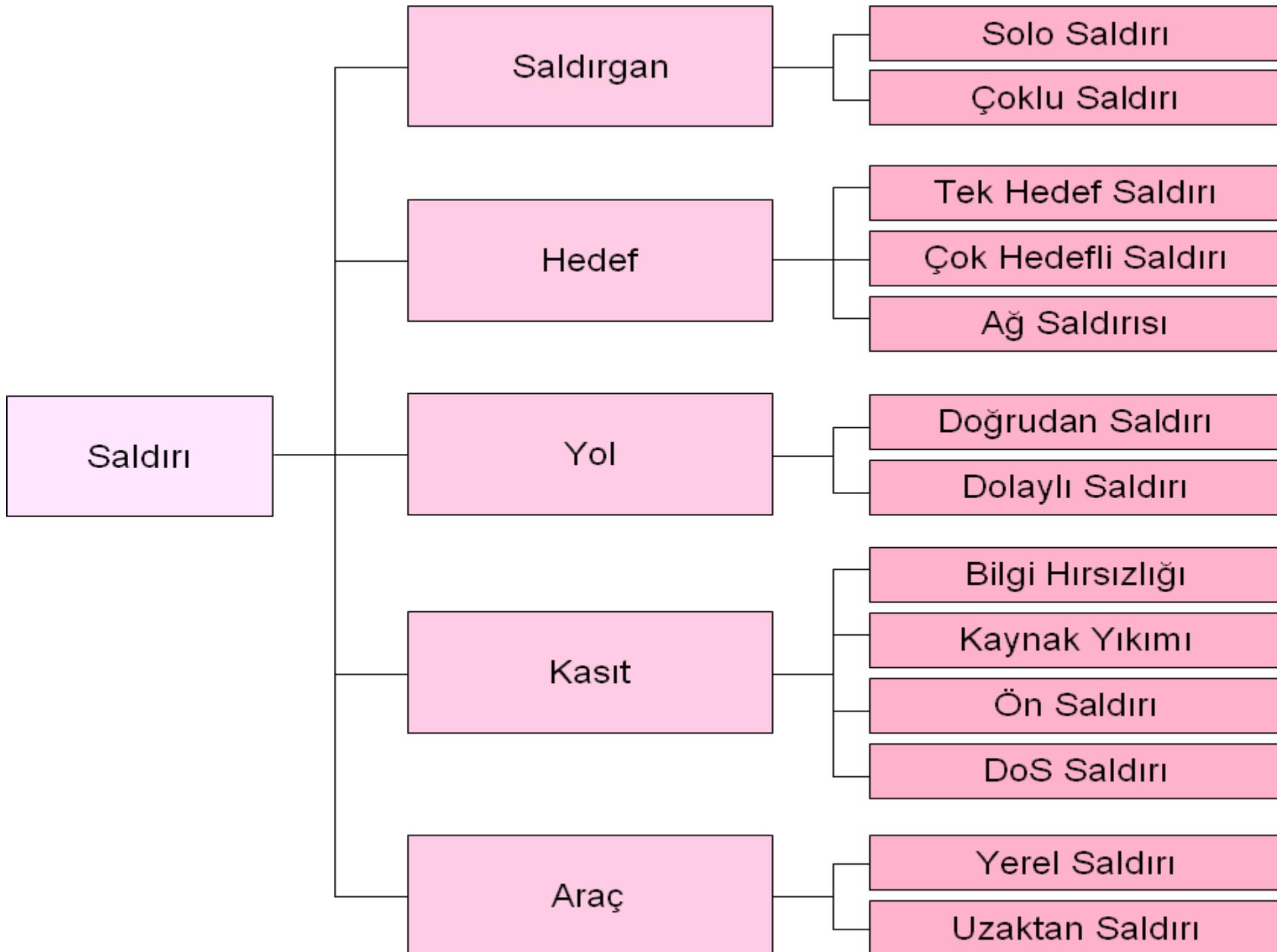
İşlemsel Sınıflandırma

- Genel anlamda bir saldırısı; 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.



1. CERT Gruplandırması

- Computer Emergency Response 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 saldıruları 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	Smtplib 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 saldırırlara 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 bırakmadada kullanılır.
Telnet attack	Uzaktan erişim protokolünün açıklarından faydalananlarak 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 abuse	FTP	Anonim erişim izni verilen dosya aktarım sunucularına yönelik saldırılardır.
IP spoofing		IP adres yanıltmasıyla yapılan saldırısı türüdür.
Configuration error		Çok kullanılan programdaki kullanıcılarından kaynaklanan konfigürasyon hatalarından doğan açıklıklardır.
Misuse of hosts resources		Konak kaynaklarının yanlış kullanımı sonucu ortaya çıkan açıklıklar.
Worm,Virus		Konaklarda kullanıcılarından habersiz çalışan zararlı programlar.

2.İletişim Protokollerini Kullanan Saldırılar

- IP sahteciliği (IP Spoofing)
- TCP dizi numarası saldırısı (TCP sequence number attack)
- ICMP atakları
- Ölümcul ping
- TCP SYN seli atağı (TCP SYN Flood Attack)
- 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 Service attack)
- Rastgele port taraması (Random port scanning)
- ARP saldırıları (ARP attacks)
- Ortadaki adam saldırıları

3. IP Saldırıları

- IP V4'te bulunan güvenlik eksikliklerinden faydalalarak 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 sınıfı 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 ayrılmasının 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 gereklidir.
 - 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 çözülmeli 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 saldırısı 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 gerçekleştirmeye 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

YMT311 Bilgi Sistemleri ve Güvenliği

Şifreleme Bilimi ve Teknikleri

Prof. Dr. Resul DAŞ

Bölüm - 5

1

Prof. Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarısı

- Kriptoloji
- Sezar
- Pigpen
- Ebcded
- Enigma
- Echelon
- Steganografi
- MD5
- RSA
- SHA1
- SHA2

Şifreleme Bilimi ve Şifreleme Teknikleri

■ Kriptoloji

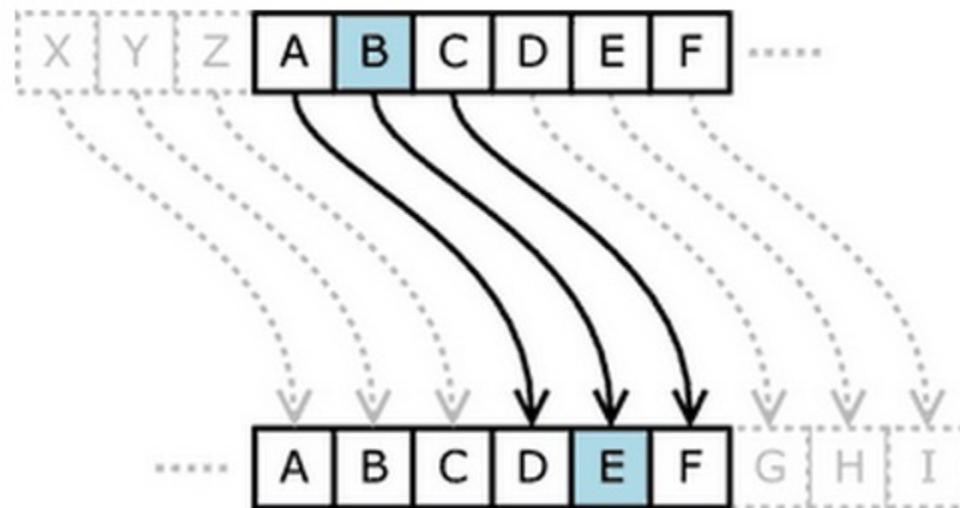
- **Kriptografi** :Bilgiyi şifreli hale dönüştürme işlemidir.
- **Kriptoanaliz** :Bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek, şifreli mesajın açık halini elde etmeye çalışan kriptoloji disiplinidir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Şifreleme (Encryption):** Düz metni şifreli metne çevirme sürecidir.
- **Şifre Çözme (Description):** Şifrelenmiş metni düz metne çevirme işlemidir.
- **Anahtar (Key):** Şifreli metnin nasıl elde edildiğine dair kod parçasıdır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Sezar Şifreleme**
- Şifrelenecek metin alfabe'de kendinden sonra gelecek 3. harfle yer değiştirerek oluşturulmaktadır.



Şifreleme Bilimi ve Şifreleme Teknikleri

$$C \equiv P + 3 \pmod{29}$$

Şifrelemek istediğimiz metnimiz “BU MESAJ ÇOK ÖNEMLİDİR” olsun.

Mesaja karşılık gelen sayısal denklileri yazmadan önce belli kelimelerin tanınmasına dayana başarılı şifre çözme tekniklerini engellemek için mesajı beşli bloklara böleriz..

BUMES AJÇOK ÖNEMLİDİR.

Harflerin sayısal denkliliklere dönüştürülmesiyle;

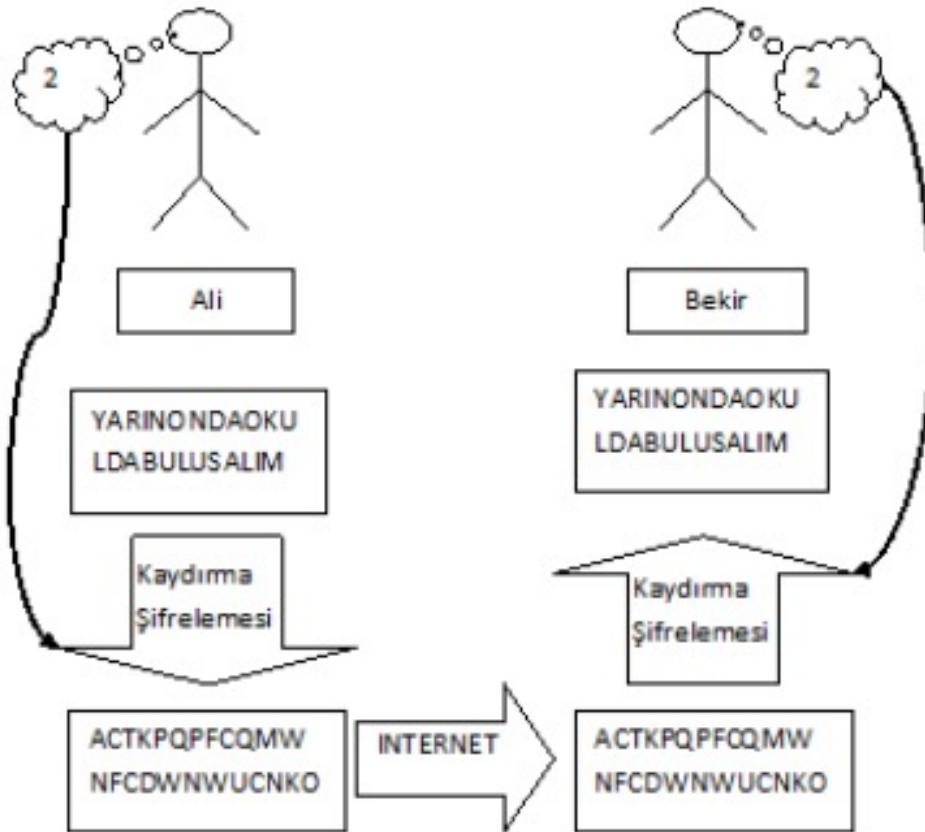
1 24 15 5 21 0 12 3 17 13 18 16 5 15 14 11 4 11 20

elde ederiz.

$C \equiv P + 3 \pmod{29}$ Caesar dönüşümünün uygulanmasıyla

4 27 18 8 24 3 15 6 20 16 21 19 8 18 17 14 7 14 23

Şifreleme Bilimi ve Şifreleme Teknikleri



Şifreleme Bilimi ve Şifreleme Teknikleri

■ EBCED HESABI

- Ebcded hesabı, Ebced rakamlarını yani alfabetik bir sayı sistemini kullanarak, kelimelerin sayısal değerini hesaplamaktır. Arap alfabetesinin eski sıralanışından (elif, ba, cim, dal) ilk dört harfinin okunuşlarıyla (E-B-Ce-D) türetilmişdir.

elif إ	1	Ha ح	8	sin س	60	te ت	400
be ب	2	Tı ط	9	'ayn ع	70	peltek se ش	500
cim ج	3	yâ ي	10	fe ف	80	Hı خ	600
dal د	4	kef ك	20	Sad ص	90	zel ذ	700
he ه	5	lâm ل	30	kaf ق	100	Dad ض	800
vav و	6	mim م	40	ra ر	200	Zı ظ	900
ze ز	7	nun ن	50	şin ش	300	ğayn خ	1000

Şifreleme Bilimi ve Şifreleme Teknikleri

- Özellikle Mimar Sinan'ın eserlerinde, boyutların modüler düzende çok sık kullanılmıştır.
- Süleymaniye'de zeminden kubbe üzengi seviyesi 45
- kubbe alemi 66 arşın yüksekliktedir .
- Ebced'e göre "Âdem' 45, "ALLAH" lafzi da 66 etmektedir.
- Yine Selimiye'de de kubbeyi taşıyan 8 ayağın merkezlerinden geçen dairenin çapı 45 arşındır.
- Kubbe kenarı zeminden 45,
- minare alemi buradan itibaren 66 arşındır.
- Süleymaniye ve Selimiye'nin görünen siluetleri 92 arşındır
- bu da "Muhammed" kelimesinin ebced karşılığıdır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Tarih düşürme sanatı**
- Ebced hesabının en fazla kullanıldığı yer hiç şüphesiz tarih düşürmedir.
- Bunun için o olayın tarihini verecek ustalıkla bir kelime veya mısra söylenir ki, hesaplandığında o olayın tarihi ortaya çıkar.
- “*Tarih düşürme sanatı*” adı verilen bu sanat divan edebiyatı boyunca kullanılmış ve kitabelerde yer almıştır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Pigpen (Mason) Şifrelemesi

A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R

S
T U
V

W
X Y
Z

V J C F

Q A F D Q

V Q S D F

Şifreleme Bilimi ve Şifreleme Teknikleri

■ Echelon Sistem

- Dünyanın en büyük casusluk ağı olarak bilinir.
- Dünyadaki sayısal trafiğin %90 bu sistem ile dinlendiği iddia edilmektedir.
 - Belirli kelimeler sisteme girilerek bu kelimelerin geçtiği konuşmalar incelenmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Diğer bir sistem ise **PROMİS** (Dava Yönetim Sistemi)
- Bu sistem ile;
 - Birçok ülkenin banka sisteminin kilitlenebileceği
 - Kontrollü mali krizler çıkarılabilceğii
 - Uluslar arası ihalelere girecek şirketlerin dinlendiği

İddia edilmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

■ ENİGMA

- Elektromekanik bir şifre çözme makinesidir.
- 1919 yılında geliştirilen makine Almanlar tarafından kullanılmıştır.
- II. Dünya savaşında önemli bir rol oynamıştır.
- İngilizler tarafından ele geçirilen bir gemide enigmanın kullanma kitabı ele geçirilmiştir.
- II. Dünya savaşının bu sayede 1 yıl daha erken bittiği düşünülmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

■ Steganografi

- Eski Yunanca'da "gizlenmiş yazı" anlamına gelen bilgiyi gizleme bilimidir.
- Resim
- Ses
- Video

ortamlarına bilgiler gizlenebilir.

Şifreleme Bilimi ve Şifreleme Teknikleri



Bilginin Saklandığı Resim



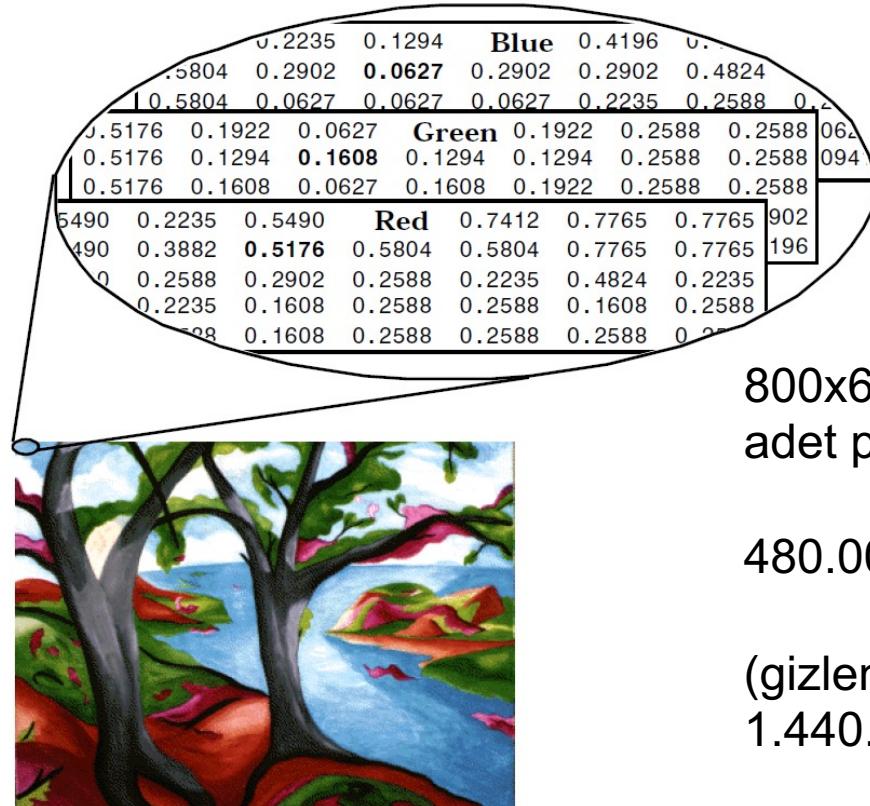
Saklanan Resim

Şifreleme Bilimi ve Şifreleme Teknikleri

■ Steganografi

- Resim dosyalarının özellikleri;
- - 1- Bütün resimler dosya başlığı (header) ve piksellerden oluşur.
 - - 2- Her piksel sadece bir renk içeren küçük bir bloktur.
 - - 3- Her pikseldeki renk temel 3 rengin karışımından elde edilir.
 - - 4- Her pikselde bu 3 rengin verileri tutulur. Her temel renk 1 pikselde 1 byte (0..255) yer kaplar, yani 1 piksel 3 byte veri taşır.

Şifreleme Bilimi ve Şifreleme Teknikleri



800x600 ebatında bir resimde 480.000 adet piksel bulunur.

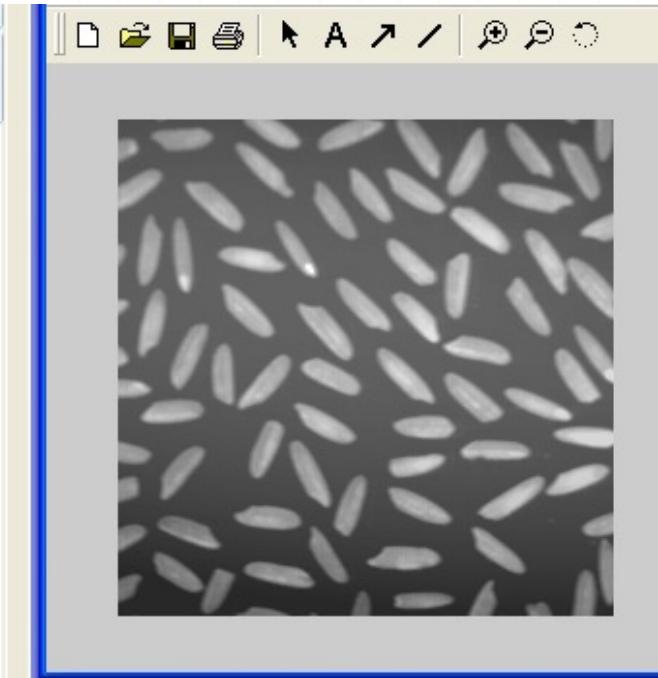
$$480.000 \times 3 \text{ bit} = 1.440.000 \text{ bit}$$

(gizlenecek olan veri için kalan yer)

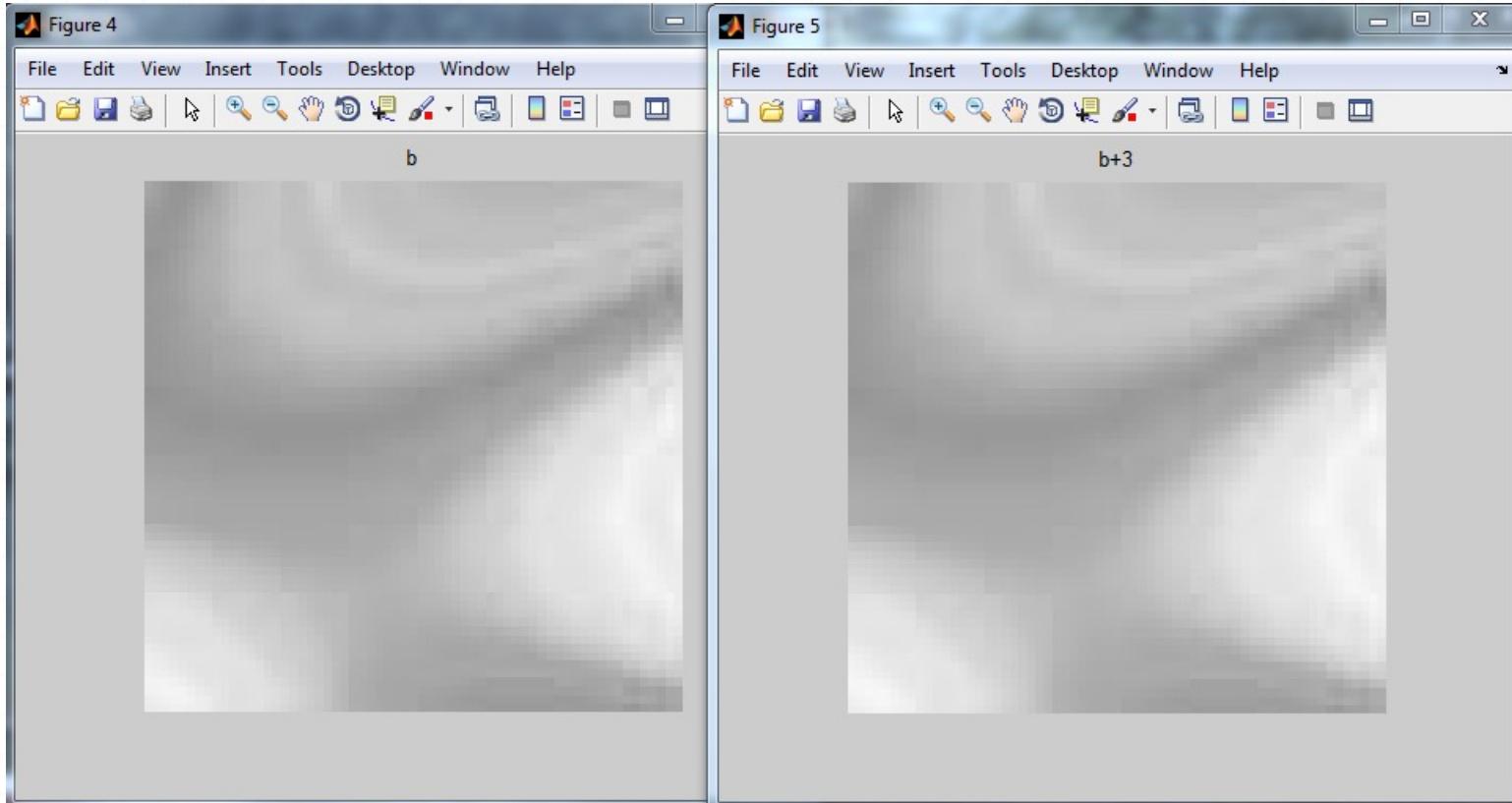
$$1.440.000 \text{ bit} = 175,7 \text{ KiloByte}$$

Şifreleme Bilimi ve Şifreleme Teknikleri

1	2	3	4	5	6	7	8
81	80	81	81	81	81	81	81
81	81	81	82	81	81	81	81
82	81	81	81	81	82	81	81
81	82	82	82	82	82	82	82
82	82	82	82	82	82	82	82
82	82	82	82	82	82	82	82
82	83	83	83	83	83	83	83
83	83	83	83	83	83	83	83
83	83	83	84	84	84	84	84
91	90	96	97	98	100	100	97
112	113	118	120	120	126	126	123
131	132	135	135	136	142	146	143
145	145	146	145	147	153	159	162
148	149	149	149	148	155	166	169
152	148	149	149	150	160	174	179
152	149	149	152	152	166	177	184
157	153	155	155	157	168	177	175
161	155	155	157	152	163	158	155
160	158	152	152	144	141	133	124
156	151	146	136	127	118	110	99
143	135	128	115	109	98	94	88



Şifreleme Bilimi ve Şifreleme Teknikleri



Şifreleme Bilimi ve Şifreleme Teknikleri

■ HASH

- Büyük tanım bölgelerini küçük değer bölgelerine dönüştürür.
- Hash fonksiyonu girdi olarak bir mesajı alır ve **hash kodu**, **hash sonucu**, **hash değeri** veya kısaca **hash** ile belirtilen bir çıktı üretir.
- Daha kesin bir ifadeyle bir hash fonksiyonu keyfi sonlu boyutlu bit şeritlerini n-bit diyebileceğimiz sabit uzunluklu şeritlere dönüştürür.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **HASH**

- Başka bir ifadeyle hash fonksiyonu gönderilecek mesajdan matematiksel yollarla sabit uzunlukta sayısal bilgi üretme işlemidir.
- Üretilen sayısal bilgi "mesaj özeti" olarak bilinir. Mesaj özeti anlamsız bir bilgidir.
- Hash fonksiyonu geri dönüşümü olmayan bir fonksiyondur.
- Yani mesajın özetine bakarak mesajın kendisini elde etmek mümkün değildir. En iyi bilinen hash fonksiyonları MD-4, MD-5 ve SHA'dır.
- Örneğin; Sayısal İmzalama

Şifreleme Bilimi ve Şifreleme Teknikleri

- Bu süreci kimyasal bir reaksiyon gibi düşünebilirsiniz.
- Yumurta pişirildikten sonra yumurtanın eski haline dönüştürülmesi imkansızdır. Bu durumda hash sonucu karşısındaki bilgisayara gönderildiği esnada, orijinal mesajın da hash sonucuyla birlikte gönderilmesi gerekiyor.
- Alıcı bilgisayar, orijinal mesaja hash fonksiyonunu uygulayıp, çıkardığı sonucu kendisine orijinal mesajla gönderilen hash sonucuya karşılaştırıyor.
- Eğer alıcı bilgisayarın oluşturduğu hash sonucu, mesajla birlikte gönderilen hash sonucuya aynıysa, alıcı bilgisayar kendisine gelen orijinal mesajın üzerinde oynamaya yapılmadığından emin olmuş oluyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- ▶ **MD5(Message-Digest algorithm5)**
- ▶ Tek yönlü (açık anahtarlı) şifreleme tekniğidir. Bir yere gönderilecek veri 128 bitlik özetler hâlinde şifrelenir.
- “**oktay**” kelimesi için MD5 şifreleme:
- f55694370a2e688a08edd2a3ee184e0d

Şifreleme Bilimi ve Şifreleme Teknikleri

- **SHA-1(Secure Hash Algorithm)**
- Tek yönlü (açık anahtarlı) şifreleme tekniğidir. Verileri 160 bit uzunlığında özetler.
- Web alanında geniş kullanımı vardır.
- SHA-2 adı altında hazırlanmış 224, 256, 384, 512 bit uzunlığunda özetler üreten çeşitleri vardır.

Şifreleme Bilimi ve Şifreleme Teknikleri

Şifreleme Algoritması	Şifrelenecek Veri	Şifrelenmiş Veri
MD5	fatma	38ab93488e52710515c3095a83a92bcf
MD5	burak	39109a5bb10ccb7aff1313d369804b74
MD5	fırat	fbc06de89851f43007f2996a31e9f1b1
MD5	fırat	e652dc5596070e8dc3fedfb32be655a6
SHA-1	fatma	5e927503d30f50bd44c9a31c6625984c442b78ae
SHA-1	burak	da7169592c4847350b7262ccf9f7b41b72c9d0be
SHA-1	fırat.edu.tr	cdfc0a27180d66d4a4f69494c3f417786b15ba20
SHA-1	www.fırat.edu.tr	26e8799f7d049f8fd908b597b7f4bd28c3f8edfd

Şifreleme Bilimi ve Şifreleme Teknikleri

Örneğin “oktay” kelimesinin SHA-1 ve SHA-2 özetleri aşağıdaki gibidir.

SHA-1 (160bit)	22771aca22f13b0e26b3011542bde186a5c47690
SHA-256	f6ff3f7aa48c6357fb3f9d09f8fdde97060e3121afc0db0e35ec807c62922456
SHA-384	d64f697923b1c8c425643c0f03f86c3c12b0af576521e41096cef9e95474661f94745 3a5ab2430928dfd02a381af93e2
SHA-512	278179b20946ee2cb093545ca8727f53607ba058acb2ed888aac8f32ecaf74d85724 79ff6380fbf34be9c274080eeb1e7f055b32e3204ce2bda6afd1714ac75c

Şifreleme Bilimi ve Şifreleme Teknikleri

- **DES (Veri Şifreleme Standardı, Data Encryption Standard)**
- DES, veri şifrelemek ve şifrelenmiş verileri açmak için geliştirilmiş bir standarttır.
- Esas olarak kullanılan algoritmaya DEA yani Data Encryption Algorithm (Veri Şifreleme Algoritması) adı verilir.
- Bu algoritmanın standartlaştırılmış haline DES denilmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

■ RSA Açık Anahtar Algoritması

RSA, güvenliği tam sayıları çarpanlarına ayrımanın algoritmik zorluğuna dayanan bir tür Açık anahtarlı şifreleme yöntemidir. 1978'de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından bulunmuştur.

Bir RSA kullanıcısı iki büyük asal sayının çarpımını üretir ve seçtiği diğer bir değerle birlikte ortak anahtar olarak ilan eder. Seçilen asal çarpanları ise saklar. Ortak anahtarını kullanan biri herhangi bir mesajı şifreleyebilir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Yeterince büyük iki adet asal sayı seçilir: Bu sayılar örneğimizde p ve q olsunlar.
- $\square n = pq$
- $\square \varphi(n) = (p-1)(q-1)$ (*Totient değeri*)
- $\square 1 < e < \varphi(n)$
- $\square d \equiv 1 \pmod{\varphi(n)}$. (*e'nin mod($\varphi(n)$) çarpmaya göre tersi*)

- \square Şifreleme işlemi:
- $\square c = me \pmod{n}$

- \square Şifrenin Açılması:
- $\square m = c^d \pmod{n}$

Şifreleme Bilimi ve Şifreleme Teknikleri

- İki farklı asal sayı seçelim. $p=61$ ve $q=53$ olsun.
- $n=pq$ değerini hesaplayalım. $61 \times 53 = 3233$
- Totient değerini hesaplayalım. $(61-1)(53-1)=3120$

- 1 ile 3120 arasında 3120 ile aralarında asal olan bir değeri seçelim. $e=17$ olsun.

- d değeri, e 'nin mod (3120)'e göre çarpmaya göre tersi olarak hesaplayalım. $d=2753$.

- **Ortak Anahtar: ($n=3233$, $e=17$)**
- Her bir m mesajını şifreleyecek fonksiyon $m^{17}(\text{mod } 3233)$.
- **Özel Anahtar($n=3233$, $d=2753$)**
- Herhangi bir c şifreli mesajını çözme fonksiyonu $c^{2753}(\text{mod } 3233)$.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Örneğin;
- $m=65$ i şu şekilde şifreleriz. *(bitler)*
 - $c=65^{17} \pmod{3233}=2790.$
- $c=2790$ 'nın şifresini şu şekilde çözeriz.
 $m=2790^{2753} \pmod{3233}=65$

Örneğin $m=123$ olsun:

$17 \text{ mod } 3233 = 855$ olarak şifreli metin bulunur.
açacak taraf için tersi işlem uygulanır:

$2753 \text{ mod } 3233 = 123$ şeklinde orijinal mesaj geri elde edilir.

Şifreleme Bilimi ve Şifreleme Teknikleri

■ BitLocker Şifreleme

- Windows 7 işletim sistemi ile gelen özelliklerden biri de Bitlocker sürücü şifreleme özelliğidir.
- Windows'un eski versiyonlarında dosyalar ayrı ayrı şifrelenebiliyordu. Bu özellik sayesinde sürücünün kendisi şifrelenebilmektedir.
- Şifrelenmiş bir sürücüye yeni bir dosya attığımızda bu dosya bitlocker tarafından otomatik olarak şifrelenir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Ayrıca bitlocker ile yapılan şifreleme işlemlerinde şifreleme için gerekli dosyalarda sürücü içersinde depolanır.
- Dolayısıyla şifrelerimizi ele geçirmek isteyenler için gerekli olan bilgiler de sürücü içersinde muhafaza edilerek güvenlik düzeyi artırılmış oluyor.
- Bitlocker ile şifrelenmiş bir sürücüye erişmek için parola koruması yada akıllı kartlarda kullanabiliyoruz.
- Windows 7 de,Vista'dan farklı olarak harici depolama aygıtlarımızı da şifreleyebiliyoruz.Yani flash disklerimizi de şifreleyebiliyoruz.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **WEP Şifreleme**
- WEP (Wired Equivalent Privacy), kablosuz ağ Veri bağ tabakasında çalışan şifreleme yöntemidir.
- Standart olan WEP şifrelemesi WEP-64 olarak bilinir ve 40 bitlik anahtar kullanır.
- Günümüzde WEP kullanan ağlarda daha çok 104 bitlik anahtar kullanan WEP-128'e rastlanır. Daha güvenli ağlar 232 bitlik anahtarı mümkün kılan WEP-256 kullanıyor olabilir.
- Günümüzde bu şifreleme yetersiz kaldığından daha güvenli olan WPA şifreleme yöntemi yaratılmıştır

Şifreleme Bilimi ve Şifreleme Teknikleri

■ WPA Şifreleme

- WEP şifreleme sisteminden daha güvenli olduğu söylenen ve WEP şifrelemeden daha yeni bir teknolojidir.
- WPA (Wi-Fi Protected Access) Wi-Fi korumalı Erişim olarak adlandırılır. WPA , WEP'in açıklarını geçici olarak da olsa kapatmaya yönelik bir standarttır.
- İki modda çalışır.
- Birincisi WPA-PSK denilen paylaşımı anahtar koruması ,
- İkincisi ise yeni protokol olan TKIP(Temporal Key Integrity Protocol)'in şifrelemesi ve 802.1X asıllama ile güvenlidir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **WPA Şifrelemesi**
- İstemci ile AP (Erişim Noktası) bağlantı kurmadan önce, aygıtların birbirini bulması gerekiyor.
- Mevcut WLAN ağlarının bir listesini görüntülemek için, istemci “araştırma sorusu” gönderir.
- Yani “*Merhaba, biri var mı?*” mesajıdır bu.
- “*Evet, burdayız*” diye karşılık gelince daha sonra AP’ler SSID bilgisini (Hizmet Kümesi Tanımlayıcı) yani WLAN’ın
 - ismini
 - zaman bilgisini
 - ve diğer bilgileri aktarır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Daha sonra istemci “Açık Sistem İsteği” (Open System Request) göndererek ağlara şifreli olup olmadıklarını soruyor.
- Yönlendirici de buna uygun yanıtını veriyor.
- İstemcinin sıradaki adımı ise, yönlendiriciden kendisini ağa dahil etmesini istemek.
- Bu “Bağlanma İsteği”ne AP’den bir “Bağlanma Yanıtı” geliyor.
- Eğer sistem şifresiz ise, istemci “Açık Sistem Doğrulama” (OSA) ile kimliğini doğruluyor.
- AP bunun üzerine kimlik saptamanın başarılı olduğunu belirten bir ileti yayinallyip bağlantıyı kuruyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Şifreli bir bağlantı kurmak içinse;**
 - WPA'nın da kendi içinde iki çeşidi var:
 - Biri işyerlerine, diğeri ise küçük özel ağlara yöneliktir.
- Aralarındaki fark;
- Bağlantı kurma sırasında, istemcinin sizin belirlediğiniz bir parolayı, yani PSK (önceden paylaşılmış anahtar) kullanıyor olması
- Şirket WLAN'larında ise anahtar dağıtımından sorumlu "*Radius server*" adlı özel bir sunucunun PSK'nın yerine geçiyor olması

Şifreleme Bilimi ve Şifreleme Teknikleri

- WPA'nın ilk adımında;
- İstemci ile erişim noktası, WLAN ağ adı SSID'yi, ana parola olarak kullanarak bir PMK (eşleştirme ana anahtarı) oluşturuyorlar.
- Aygıtlar şu anda PMKSA (Eşleştirme Ana Anahtarı Güvenlik Bağlantısı) denilen bir konumda bulunuyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Daha sonra taraflar, adına PTK (Geçici Eşleştirme Anahtarı) denilen 512 bitlik bir anahtar oluşturuyorlar.
- Bunun için de aygıtlar 4 taraflı bir el sıkışma protokolü uyguluyor.
- Yönlendirici, öncelikle istemciye içinde rasgele rakam bulunan bir çerçeve yolluyor.
- Bu ileti şifresiz olduğundan,kablosuz ağ üzerinden salt metin olarak iletiliyor.Ancak bu,güvenliği tehlikeye atmıyor çünkü en kötü durumda 4 taraflı el sıkışma başarısız oluyor ve yönlendirici bu işlemi yeni baştan başlatıyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- İstemci ise aşağıdaki parametreleri kullanarak PTK (Geçici Eşleştirme Anahtarı)'yi oluşturuyor:
- SNonce (gelişgüzel bir sayı)
- ANonce (AP için bir gelişgüzel sayı)
- PMK (Eşleştirme Ana Anahtarı) ve aygıtların MAC adresleri.

Şifreleme Bilimi ve Şifreleme Teknikleri

- PTK (Geçici Eşleştirme Anahtarı)'dan yönlendirici ve istemci tarafından dört geçici anahtar daha elde ediliyor:
- EAPOL anahtarı-şifreleme anahtarı
- EAPOL anahtarı-doğrulama anahtarı (bu sayede aygıtlar daha sonra asıl veri anahtarının aktarımını şifreleyebiliyor),
- veri şifreleme anahtarı
- ve veri doğrulama anahtarı.
- Bunların hepsi de 128 bit uzunluğundadır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Sıradaki ileti, istemciden yönlendiriciye gidiyor ve SNonce(gelişigüzel bir sayı)'ı içeriyor. Böylece yönlendirici aynı PTK'yi hesaplayabiliyor.
- Bağlantı henüz şifrelenmemiş olsa da, değişiklikleri saptayan MIC algoritması (Mesaj Doğruluk Denetimi) üzerine kuruludur.
- Gönderici, veri paketlerini seri olarak numaralıyor. Seri numarası da mesaja ekleniyor.
- Alıcı, seri numarası verilen paketleri kontrol ediyor ve paketler eşleşmezse, alıcı bu paketleri çöpe atıyor. Bu da çoğu korsan saldırısını daha en baştan eliyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- 4 taraflı el sıkışmanın üçüncü aşamasında yönlendirici istemciye bir “başarılı” paketi göndererek iki aygıtın da aynı geçici anahtara sahip olduğunu doğruluyor.
- El sıkışmasını sona erdirmek için, istemci, yönlendiriciye anahtar oluşturmanın sonlandığını belirten bir MIC mesajı gönderiyor.
- Bunun üzerine, yönlendirici, MIC’i kullanarak mesajı kontrol ediyor ve üzerindeki anahtarları etkinleştiriyor.

Sonuç



Sorular



Kaynaklar

- [1] IEEE Std 802.16-2004--IEEE standard for local and metropolitan areanetworks, part 16: "**Air Interface for Fixed Broadband Wireless Access Systems**".
- [2] David Johnston ve Jesse Walker--INTEL: "**Overview of IEEE 802.16 Security**"
- [3] Kitti Wongthavarawat--Thai Computer Emergency Response Team (ThaiCERT) National Electronics and Computer Technology Center,Thailand: "**IEEE 802.16 WiMax Security**"
- [4] Loutfi Nuaymi, Patrick Maillé, Francis Dupont, Raphaël Didier--École Nationale Supérieure des Télécommunications de Bretagne:"**Security issues in WiMAX/IEEE 802.16 BWA System**"
- [5] Yun Zhou ve Yuguang Fang--Department of Electrical and Computer Engineering,University of Florida, Gainesville:"**Security of 802.16 in Mesh Mode**"

Şifreleme Algoritmaları ve Bazı Saldırı Yöntemleri

Prof. Dr. Resul Daş

Kriptosistemler ve Şifreleme Yöntemleri

Kriptosistemler

- Kimlik doğrulama ve şifreleme verinin güvenliğini sağlamaya yarayan birbiriyle bağlantılı iki teknolojidir.
- Kimlik doğrulama, haberleşmede her iki tarafta bulunanların ne söylüyorkar ise onun doğru olmasını sağlama sürecidir.
- Şifreleme ise iletişim sırasında verinin hem güvenliğini sağlamak hem de değiştirilmesini önlemeye yönelik işlemlerdir.

Güvenliğin Geliştirilmesi İhtiyacı

- 1970'li yıllarda IPv4 Internette kullanılmaya başlandığında ağ güvenliği önemli bir konu değildi.
- Bu nedenle IP tüm veriyi açık metin şeklinde göndermektedir.
- Bunun anlamı gönderilen paketler dinlenirse içeriğinin öğrenilebileceği ve istenilirse değiştirilebileceğidir.
- Ağ analizi yapan bir saldırgan, hem oturumları öğrenebilir hem de veri paketlerinin içeriklerini değiştirebilir.

Güvenliğin Geliştirilmesi İhtiyacı

- Aşağıdaki protokoller açık metin kullanan protokollerdir.
 - **FTP (File Transfer Protocol), Telnet, IMAP (Internet Message Access Protocol), SNMP (Simple Network Management Protocol)**: Doğrulama işlemi açık metin ile yapılır.
 - **SMTP (Simple Mail Transfer Protocol)**: Posta mesajlarının içeriği açık mesaj olarak dağıtıılır.
 - **http (Hyper Text Transfer Protocol)**: Sayfa içeriği ve formlardaki bilgilerin içeriği açık metin olarak gönderilir.

Ağ Üzerinden Yapılan Saldırı Türleri

- 1) **İfşaatt-Açığa Çıkarma (Disclosure):** mesaj içeriğinin herhangi birisine verilmesi veya uygun kriptografik anahtara sahip olmama
- 2) **Trafik Analizi:** ağdaki trafik akışının analiz edilmesi. Bağlantı esaslı uygulamalarda bağlantının sıklığı ve süresi belirlenebilir. Bağlantısız ortamda ise mesajların sayısı ve uzunluğu belirlenebilir.
- 3) **Gerçeği Gizleme (Masquerade):** hileli bir kaynaktan ağa mesaj ekleme. Bu işlem saldırgan tarafından yetkili bir kullanıcından geliyormuş gibi mesaj oluşturulmasını içerir.

Ağ Üzerinden Yapılan Saldırı Türleri

- 4) **İçerik Değiştirme (Content Modification):** Ekleme, silme, sırasını değiştirme veya içeriğini değiştirme yöntemleri ile mesajın değiştirilmesi
- 5) **Sıra Değiştirme (Sequence Modification):** Ekleme, silme ve yeniden sıralama ile mesajın sırasında değişiklik yapmak.
- 6) **Zamanlamayı Değiştirme (Timing Modification):** Mesajları geciktirme veya yeniden yollama. Bir bağlantı temelli uygulamada bütün oturum ve mesajların bir kısmı istendiğinde geciktirilebilir yada yeniden yollanabilir.
- 7) **İnkarcılık (Repudiation):** Alınan mesajın varış tarafından inkarı veya gönderilen mesajın kaynak tarafından inkar edilmesi.

Şifreleme Nedir?

- Bir açık metinin bir şifreleme algoritması yardımıyla anlaşılır olamaz hale getirilmesi işlemine şifreleme denir.



Şifreleme Nedir?

- Şifrelenecek mesaj plaintext (düz-metin) olarak adlandırılır.
- Şifreleme(encryption); veriyi alıcının haricinde kimse okuyamayacak şekilde kodlamaktır.
- Şifrelenmiş mesaja ciphertext (şifreli-mesaj) denir
- Şifre Çözme(Decryption) ise şifrelenmiş veriyi çözüp eski haline getirme işlemidir.
- Veriyi şifrelerken ve çözerken kullanılan matematiksel metoda ise şifreleme algoritması denilmektedir.
- Şifreleme ve çözme genelde bir anahtar(Key) kullanılarak yapılır

Şifreleme Algoritmalarının Performans Kriterleri

- Kırılabilme süresinin uzunluğu.
- Şifreleme ve çözme işlemlerine harcanan zaman (Zaman Karmaşıklığı).
- Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı (Bellek Karmaşıklığı).
- Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği.
- Bu uygulamaların dağıtımındaki kolaylık yada algoritmaların standart hale getirilebilmesi.
- Algoritmanın kurulacak sisteme uygunluğu.

Şifreleme Algoritmaları

- Kriptografide şifreleme için kullanılan anahtarın özellikleri ve çeşidine göre temel olarak iki çeşit şifreleme algoritması bulunmaktadır.
 - Simetrik şifreleme algoritmaları
 - Asimetrik şifreleme algoritmaları

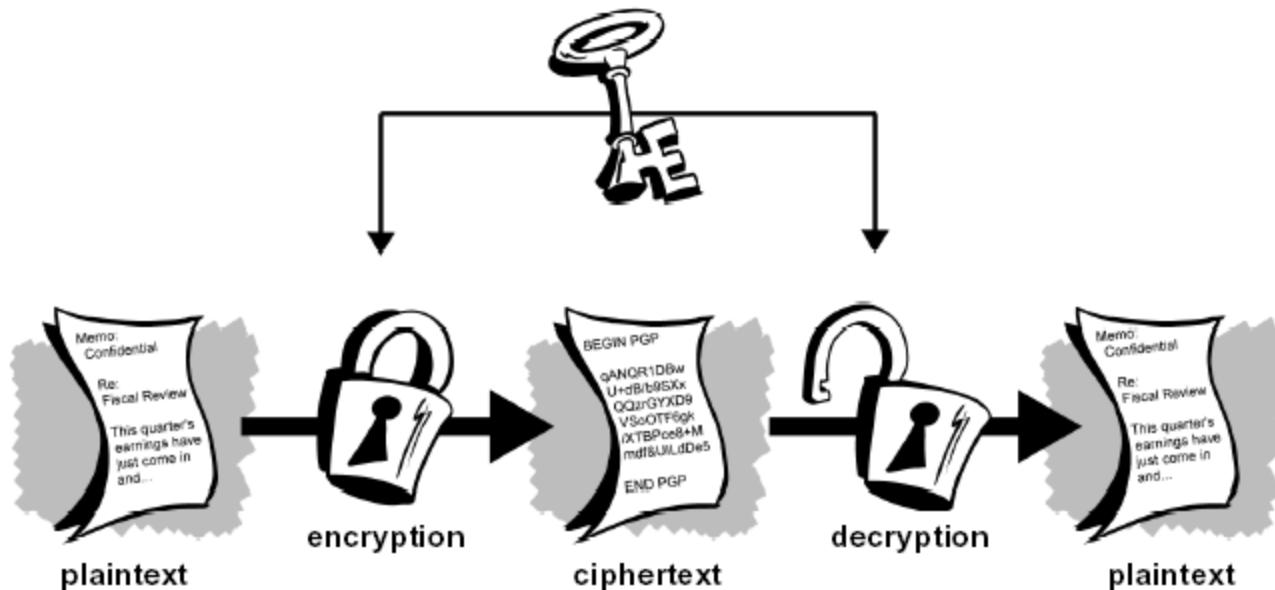
Simetrik Şifreleme Algoritmaları

- Bu algoritmada şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır.
- Kullanılan anahtar başkalarından gizlidir ve şifreleme yapan ile şifrelemeyi çözecek kişilerde arasında anlaşılmış ortak bir anahtardır.
- Gonderilecek gizli metinle beraber üstünde anlaşılmış olan gizli anahtar da alıcıya gönderilir ve şifre çözme işlemi gerçekleştirilir.

Simetrik Şifreleme Algoritmaları

- Simetrik şifrelemenin en önemli avantajlarından birisi oldukça hızlı olmasıdır.
- Asimetrik şifrelemeyle karşılaştırıldığında hız konusunda simetrik algoritmalar çok daha başarılıdır.
- Bununla birlikte simetrik algoritmayı içerdiği basit işlemlerden dolayı elektronik cihazlarda uygulamak çok daha kolaydır.
- Ayrıca simetrik algoritmalarla kullanılan anahtarın boyu ve dolayısıyla bit sayısı çok daha küçüktür.

Simetrik Şifreleme Algoritmaları



Simetrik Şifreleme Algoritmaları

- Kuvvetli Yönleri;
 - Algoritmalar olabildiğince hızlıdır.
 - Donanımla birlikte kullanılabilir.
 - Güvenlidir.
- Zayıf Yönleri;
 - Güvenli anahtar dağıtımını zordur.
 - Kapasite sorunu vardır.
 - Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

Simetrik Şifreleme Algoritmaları

- Simetrik algoritmalar blok şifreleme ve dizi şifreleme algoritmaları olarak ikiye ayrılmaktadır.
- Blok Şifreleme Algoritmaları veriyi bloklar halinde işlemektedir.
- Bazen bağımsız bazen birbirine bağlı olarak şifrelemektedir.
- Bu algoritmalarla iç hafıza yoktur, bu yüzden hafızasız şifreleme adını da almıştır.
- Bütünlük kontrolü gerektiren uygulamalarda genellikle blok şifreleme algoritmaları tercih edilir.

Simetrik Şifreleme Algoritmaları

- Dizi şifreleme algoritmaları ise veriyi bir bit dizisi olarak almaktadır.
- Bir üreteç aracılığı ve anahtar yardımıyla istenilen uzunlukta kayan anahtar adı verilen bir dizi üretilir.
- Kayan anahtar üretimi zamana bağlıdır ve bu yüzden bu algoritmalarla aynı zamanda hafızalı şifreleme denir.
- Telsiz haberleşmesi gibi gürültülü ortamlarda ses iletimini sağlamak için genellikle dizi şifreleme algoritmaları kullanılır.

Simetrik Şifreleme Algoritmaları - DES

- DES (Data Encryption Standard) : DES yapısı itibarı ile blok şifreleme örneğidir.
- Yani basitçe şifrelenecek olan açık metni parçalara bölerek (blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrelenmiş metni açmak içinde aynı işlemi bloklar üzerinde yapar.
- Bu blokların uzunluğu 64 bittir.

Simetrik Şifreleme Algoritmaları - DES

- Dünyada en yaygın kullanılan şifreleme algoritmalarından birisidir.
- DES, IBM tarafından geliştirilmiştir. 1975 yılında “Federal Register” tarafından yayınlanmıştır.
- DES 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler.
- Ayrıca klasik Feistel Ağrı kullanılarak temelde şifreleme işleminin deşifreleme işlemiyle aynı olması sağlanmıştır.
- Kullanılan teknikler yayılma ve karıştırılmıştır.

Simetrik Şifreleme Algoritmaları - DES

- DES'in en büyük dezavantajı anahtar uzunluğunun 56 bit olmasıdır.
- 1975 yılında yayınlanan bu algoritma günümüzde geliştirilen modern bilgisayarlar tarafından yapılan saldırılar (BruteForce) karşısında yetersiz kalmaktadır.
- Daha güvenli şifreleme ihtiyacından dolayı DES, Triple-DES olarak geliştirilmiştir.
 - Triple -DES algoritması geriye uyumluluğu da desteklemek amacıyla 2 adet 56 bitlik anahtar kullanır.

Simetrik Şifreleme Algoritmaları – Triple DES

- Triple-DES, IBM tarafından geliştirilip 1977'de standart olarak kabul edilmiştir.
- Fakat 1997 yılında İsrail'liler tarafından kırılmış bulunmaktadır.
- Şifreleme metodunun çözülmüş olmasına rağmen günümüz bankacılık sistemlerinde kullanılmakta olan şifreleme sistemidir.
- Triple-DES algoritması, DES algoritmasının şifreleme, deşifreleme, şifreleme şeklinde uygulanmasıdır.

Simetrik Şifreleme Algoritmaları – Triple DES

- Standart DES'in 112 veya 168 bitlik iki veya üç anahtar ile artarda çalıştırılması ile oluşturulan bir şifreleme tekniğidir.
- Anahtar alanı 2¹¹² veya 2¹⁶⁸ sayısına ulaşınca bugün için veya tahmin edilebilir bir gelecekte çözülmesi mümkün olmayan bir kod olmaktadır

Simetrik Şifreleme Algoritmaları – IDEA

- IDEA (International Data Encryption Algorithm) 1991 yılında geliştirilmiştir.
- 128 bit anahtar uzunluğu kullanır.
- XOR, 16 bit tam sayı toplama ve 16 bit tam sayı çarpma matematik işlemlerini kullanır.
- Alt anahtar üretim algoritması dairesel kaydırma üzerindedir.

Simetrik Şifreleme Algoritmaları – Twofish

- 1993 yılında yayınlanan bu algoritma Bruce Schneier - John Kelsey - Doug Whiting – David Wagner - Chris Hall - Niels Ferguson tarafından oluşturulan simetrik blok şifreleme algoritmasıdır.
- AES kadar hızlıdır.
- Aynı DES gibi Feistel yapısını kullanır.
- DES'den farklarından biri anahtar kullanılarak oluşturulan değişken S-box (Substitution box – Değiştirme kutuları)' lara sahip olmasıdır.

Simetrik Şifreleme Algoritmaları – Twofish

- Ayrıca 128 bitlik düz metni 32 bitlik parçalara ayırarak işlemlerin çoğunu 32 bitlik değerler üzerinde gerçekleştirir.
- AES'den farklı olarak eklenen 2 adet 1 bitlik rotasyon, şifreleme ve deşifreleme algoritmalarını birbirinden farklı yapmış, bu ise uygulama maliyetini arttırmış, aynı zamanda yazılım uygulamalarını %5 yavaşlatmıştır

Simetrik Şifreleme Algoritmaları – IRON

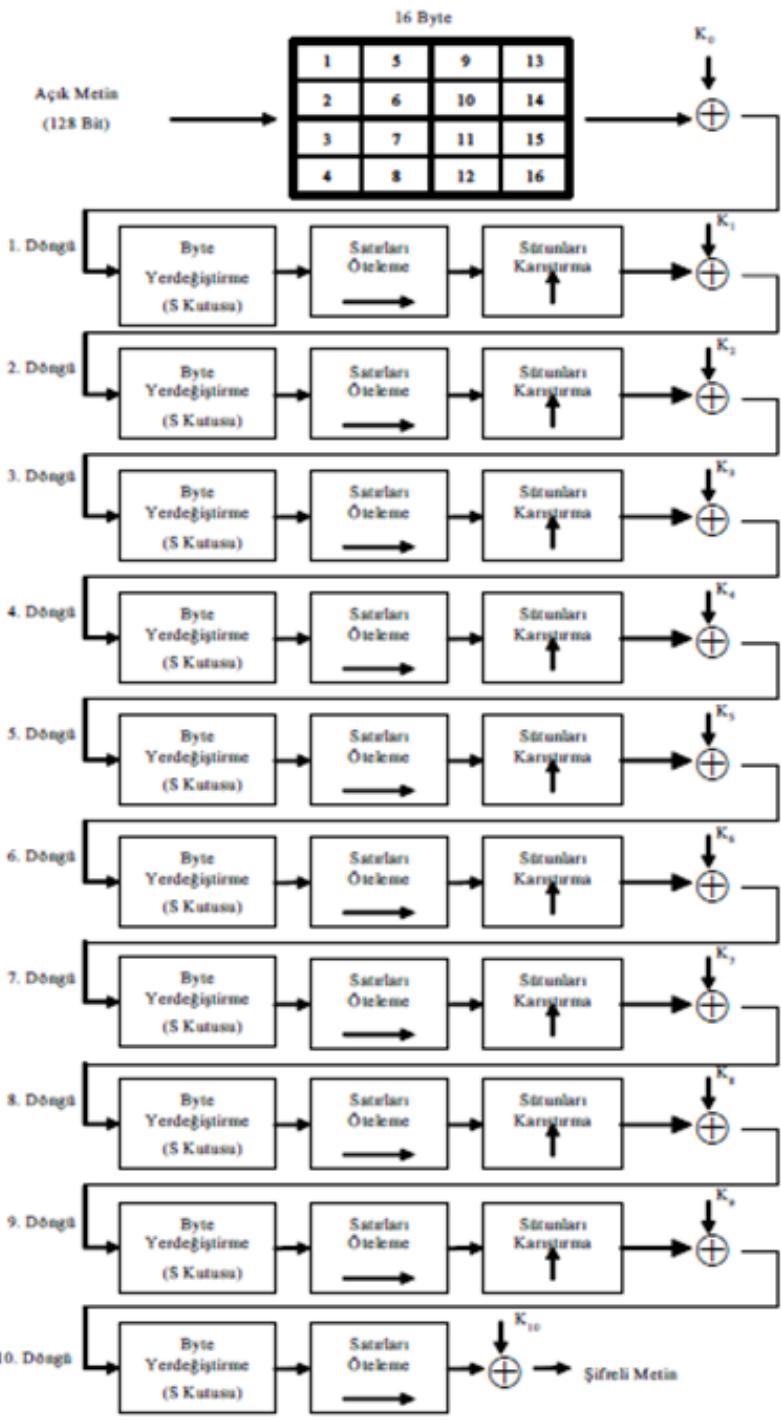
- Diğer iki algoritma gibi Feistel yapısını kullanır.
- IRON, **64 bitlik veri bloklarını 128 bitlik anahtarla şifrelemede kullanılır.**
- Döngü (round) sayısı 16 ile 32 arasındadır.
- Alt anahtarların sayısı döngü sayısına eşittir.
 - Bu nedenden dolayı **algoritma anahtar bağımlıdır**. Var olan algoritmalarдан **farkı da** budur.
- Bu algoritmanın avantajı **bitler yerine 16-tabanındaki (hex) sayılar kullanmasıdır**, dezavantajı ise yazılım için tasarlanmış olmasıdır.

Simetrik Şifreleme Algoritmaları – AES

- AES, John Daemen ve Vincent Rijmen tarafından **Rijndael adıyla geliştirilmiş ve 2002 yılında standart** haline gelmiştir.
- AES uzunluğu **128 bitte sabit olan blok** ile uzunluğu **128, 192 ya da 256 bit olan anahtar** kullanır.
- Kullanılan tekniklerden bazıları baytların yer değiştirmesi, **4x4' lük matrisler üzerine yayılmış metin** parçalarının satırlarına uygulanan kaydırma işlemleridir.
- **2010 yılı itibarıyle en popüler simetrik algoritmaların biridir.**

AES Döngü Yapısı

	Kelime Uzunluğu	Tur Sayısı
AES-128	4	10
AES-192	6	12
AES-256	8	14



AES Döngü Yapısı

- Her döngü tersi alınabilir dönüşümler kullanır.
- Her döngü, son döngü hariç, 4 dönüşüm kullanır: SubBytes, ShiftRows, MixColumns ve AddRoundKey.
- Son döngüde MixColumns dönüşümü göz ardı edilir.
- Her döngüde farklı anahtar materyali kullanılır.
- Farklı anahtar materyalleri anahtar planlama evresinde gelen anahtarlardır. Master anahtardan farklı anahtarlar elde edilerek şifrede kullanılır.
- Deşifreleme kısmında ters dönüşümler kullanılır: InvSubByte, InvShiftRows, InvMixColumns ve AddRounKey (tersi kendisidir- XOR işlemi).

Simetrik Şifreleme Algoritmaları – RC4

- **RC4 algoritması şifrelenecek veriyi akan bir bit dizisi olarak algılar.**
- RC4 belirlenen anahtar ile veriyi şifreleyen bir algoritmadır.
- Genellikle hız gerektiren uygulamalarda kullanılır.
- **Şifreleme hızı yüksektir ve MB/sn seviyesindedir.**
- Güvenliği rastgele bir anahtar kullanımına bağlıdır.
- Anahtar uzunluğu değişkendir.
- **128 bitlik bir RC4 şifrelemesi sağlam bir şifreleme olarak kabul edilir.**
- **Bankacılık ve Dökümantasyon (PDF) şifrelemelerinde yaygın olarak kullanılır.**

Simetrik Şifreleme Algoritmaları – MD5

- MD5 (Message-Digest algorithm 5) Ron Rivest tarafından 1991 yılında geliştirilmiş bir tek yönlü şifreleme algoritmasıdır.
- Veri bütünlüğünü test etmek için kullanılan, bir şifreleme algoritmasıdır.
- Bu algoritma girdinin büyüklüğünden bağımsız olarak 128-bit'lik bir çıktı üretir ve girdideki en ufak bir bit değişikliği bile çıktıının tamamen değişmesine sebep olur.
- MD5'in en çok kullanıldığı yerlerden biri, bir verinin (dosyanın) doğru transfer edilip edilmediği veya değiştirilip değiştirilmemişinin kontrol edilmesidir.

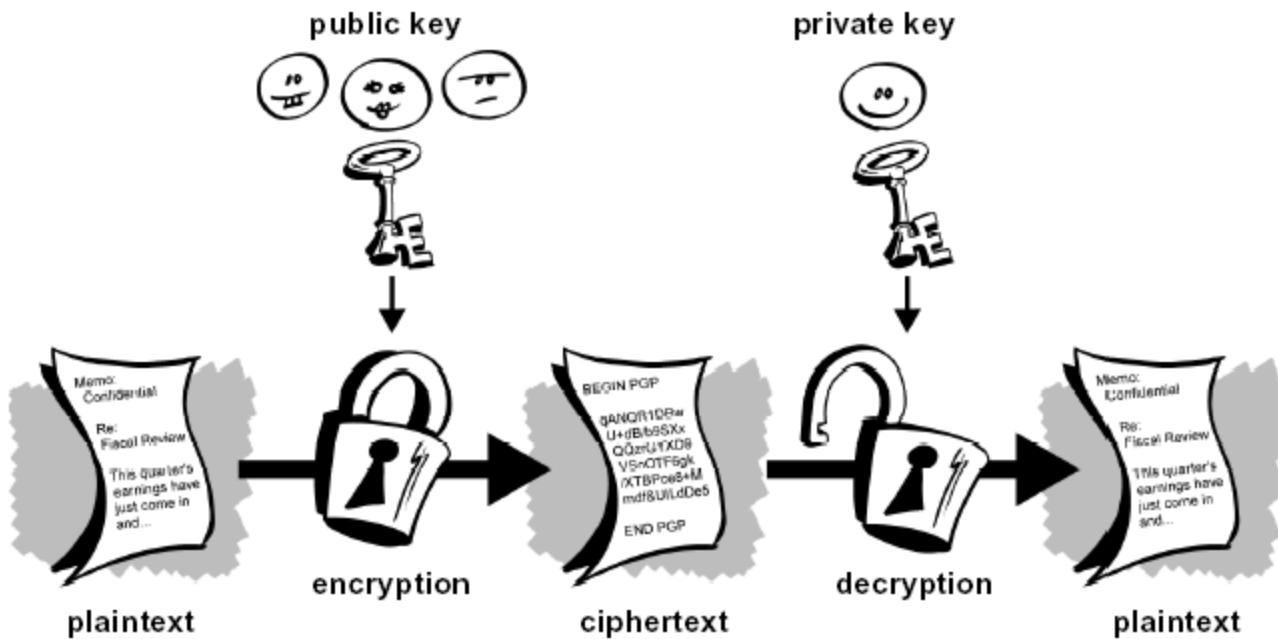
Simetrik Şifreleme Algoritmaları – SHA

- SHA (Secure Hash Algorithm – Güvenli Özetteleme Algoritması), Amerika'nın ulusal güvenlik kurumu olan NSA tarafından tasarlanmıştır.
- SHA-1, uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir.
- Bu işlem sırasında, ilk önce mesajı 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar.
- SHA-1 çalışma prensibi olarak R. Rivest tarafından tasarlanan MD5 özet fonksiyonuna benzer.
- 160 bitlik mesaj özeti üreten SHA-1 çakışmalara karşı 80 bitlik güvenlik sağlar.

Asimetrik Şifreleme Algoritmaları

- 1976 yılında Stanford Universitesinden Diffie ve Hellman adlı araştırmacılar iki farklı anahtara dayalı şifreleme sistemi önermiştir.
- Bu sistemde bir tane şifreleme için (public key) ve bundan farklı olarak bir tanede şifre çözmek için(private key) anahtar bulunur.
- private key, public key' den elde edilemez.
- Asimetrik şifreleme algoritmalarında çok büyük asal sayılar kullanılmaktadır.

Asimetrik Şifreleme Algoritmaları



Asimetrik Şifreleme Algoritmaları

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

Asimetrik Şifreleme Algoritmalarının Avantajları

- Asimetrik şifrelemenin kırılması simetrik şifrelemeye göre daha zordur.
- Bu yöntem private-key' lerin karşılıklı aktarılmasını gerektirmez.
 - Böylece simetrik şifrelemedeki anahtar dağıtım problemi çözülmüş olur.
- Public Keylerin bize şifreli mesaj göndermek isteyenler tarafından bilinmesi gereğinden bu anahtarlar internette bir sunucu ile rahatça dağıtılmaktadır.
- İki anahtarla şifrelemeden dolayı inkar edememeyi sağlayan sayısal imza gibi yeni yöntemler geliştirilmiştir.

Asimetrik Şifreleme Algoritmalarının Dezavantajları

- Anahtarları kullanarak bilgileri çözme işlemlerinde CPU zamanının çok fazla olması.
- Bu zaman ileti uzunluğu ile üssel olarak artmaktadır.

Asimetrik Şifreleme Algoritmaları – Diffie Helman

- 1976 yılında Diffie ve Helman tarafından bulunmuş ilk asimetrik şifreleme algoritmasıdır.
- DH iki katılımcının öncesinde herhangi bir bilgi alışverişi yapmadan güvenli olmayan bir kanal vasıtasyyla (güvenli bir şekilde) ortak bir şifrede karar kılmalarına yarayan bir protokoldür.
- Algoritma anahtar değişimi ile asıl amacı, iki kullanıcının bir anahtarı güvenli bir şekilde birbirlerine iletmeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır.
- Diffie–Hellman algoritması oluşturularak simetrik şifreleme algoritmaları için büyük problemi olan gizli anahtarı koruma ve dağıtım büyük ölçüde aşılmıştır.
- Bununla birlikte Diffie-hellman algoritması sadece ortak gizli anahtarı belirlemekte kullanılmaktadır.

Asimetrik Şifreleme Algoritmaları - RSA

- Dünyada en yaygın biçimde kullanılan asimetrik algoritma, ismini mucitlerinin baş harflerinden (Ronald L.Rivest, Adi Shamir ve Leonard Adleman) almıştır.
- Büyük sayıların moduler aritmetığıne dayalı çok basit bir prensibi vardır.
- Anahtarlar, iki büyük asal sayıdan üretilir.
- Dolayısıyla, algoritmanın güvenliği büyük sayı üretme problemine dayalıdır

Asimetrik Şifreleme Algoritmaları - DSA

- DSA (Digital Signature Algorithm) , NIST tarafından sayısal imza standarı olarak yayınlanmıştır.
- Amerika Birleşik Devletleri tarafından kullanılan dijital doğrulama standartlarının bir parçasıdır.
- DSA “discrete logarithm” problemine dayanır ve Schnorr ve ElGamar tarafından geliştirilen algoritmalarla benzer yapıdadır.
- RSA ’dan farkı sadece imzalama amaçlı kullanılabilmesi, şifreleme yapılamamasıdır.

Asimetrik Şifreleme Algoritmaları – Eliptik Eğri Algoritması (ECC)

- ECC şifreleme algoritmasının en büyük özelliği diğer açık anahtar şifreleme sistemlerinin güvenliğini daha düşük anahtar değerleriyle sağlayabilmesidir.
- 1024-bitlik anahtar kullanan RSA şifreleme algoritmasının sağladığı güvenlik gücünü, 160-bit anahtar kullanan ECC sağlayabilmektedir.
- Bu açık anahtarlı algoritmalar içinde çok önemli bir avantajdır.
- Yeni gelişen teknolojiyle birlikte kablosuz ağların kullanımını geniş anahtar değerlerine sahip şifreleme algoritmalarının kullanımını zorlaştırmıştır.
- ECC daha düşük anahtar değerlerini kullanması ve aynı güvenlik seviyesini sağlaması sayesinde kablosuz ağlarda kullanımına çok uygundur.

Şifreleme Algoritmaları

- Günümüzde simetrik ve asimetrik şifreleme algoritmalarını birlikte kullanarak hem yüksek derecede güvenlik hem de yüksek hızlı sistemler şifrelenebilmektedir.
- Bu gibi sistemlere melez sistem adı verilir.
- Anahtar şifreleme, anahtar anlaşma ve sayısal imza işlemleri genellikle asimetrik şifrelemeyle, yığın veri işlemleri ve imzasız veri bütünlüğü korumaysa simetriklerle gerçekleştirilir.

İletişim Protokollerini Kullanan Saldırılar

IP Adresi- Internet Protocol Address

- IP adresi (internet protokol adresi), TCP/IP(iletişim kontrol protokolü/internet protokolü) standardını kullanan bir ağdaki cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve veri haberleşmesinde bulunmak için kullandıkları noktalarla ayrılan 4 sayıdan oluşmaktadır.
- İnternette trafigin işlemesi bu IP adreslerine bağlıdır.
- Çoğu kullanıcının IP adresi dinamiktir, yani servis sağlayıcınızda o an boş bulunan IP adresi atanır. Bu yüzden her bağlantıda IP adresinizin son numarası değişir.

IP Protokol Türleri

- Bugün halen kullanılmakta ve test edilmekte olan 2 tür internet protokolü bulunmaktadır.
 - IPv4:Günümüzde kullanılmakta olan standart internet protokolüdür ve 32 britten oluşur.
 - IPv6:Artan ağ kullanıcısı sayısına bağlı olarak daha büyük bir ip adresine ihtiyaç duyulmuştur.Bu ihtiyacı karşılamak ve IPv4'ün eksikliklerini gidermek amacıyla 128 britten oluşan IPv6 geliştirilmiştir.

IP Adreslerinin Dağıtımı

- IP adresleri IANA başkanlığında RIR(Regional Internet Registry) olarak adlandırılan organizasyonlar tarafından dağıtilır.
- Tüm dünyaya IP dağıtan beş farklı RIR vardır.
- Bunlar bölgelere göre IP dağıtım işlemlerini üstlenmişlerdir.
- Sıradan Internet kullanıcılarına (son kullanıcılarla) IP dağıtım işlemi hizmet aldıkları ISS(Internet servis sağlayıcısı) tarafından yapılır.
- Bazı ISS'ler sabit IP adresi verebilirken bazı ISS'ler değişken IP adresi ataması yapar.

IP Sahteciliği (IP Spoofing)

- Internetin çalışmasını sağlayan TCP/IP protokol ailesi geliştirilirken güvenlik temel amaç olmadığı için olabildiğince esnek davranışlı olmuştur.
- Bu esneklik IP adreslerinin aldatılabilir(spoofed) olmasını sağlamıştır.
- Spoofing IP paketlerinin yanlış kaynak adres kullanılarak gönderilmesidir.
- Bu işlem:
 - Saldırıda bulunan kişinin IP adresini gizlemesi, başka bir taraf ya da kişiyi saldırısı yapan olarak göstermesi.
 - Güvenilir bir kullanıcı gibi görünmesi yanında network trafigini dinleme ya da ele geçirme
 - Ortadaki adam saldırısı gibi saldıruları gerçekleştirmek için kullanılır.

IP Sahteciliği (IP Spoofing)

- Genel korunma yöntemleri şu şekilde sayılabilir.
 - Kaynak IP yanında Hedef IP ve MAC kontrolünün yapılması
 - Yönlendiricilerde, kaynak yönlendirme fonksiyonunu pasif hale alınması
 - İç ağın İnternete açıldığı yerde güvenlik duvarı kurulması
 - Paket Filtreleme
 - Şifreleme Yöntemleri

TCP SYN Paketi Akışı Saldırıları

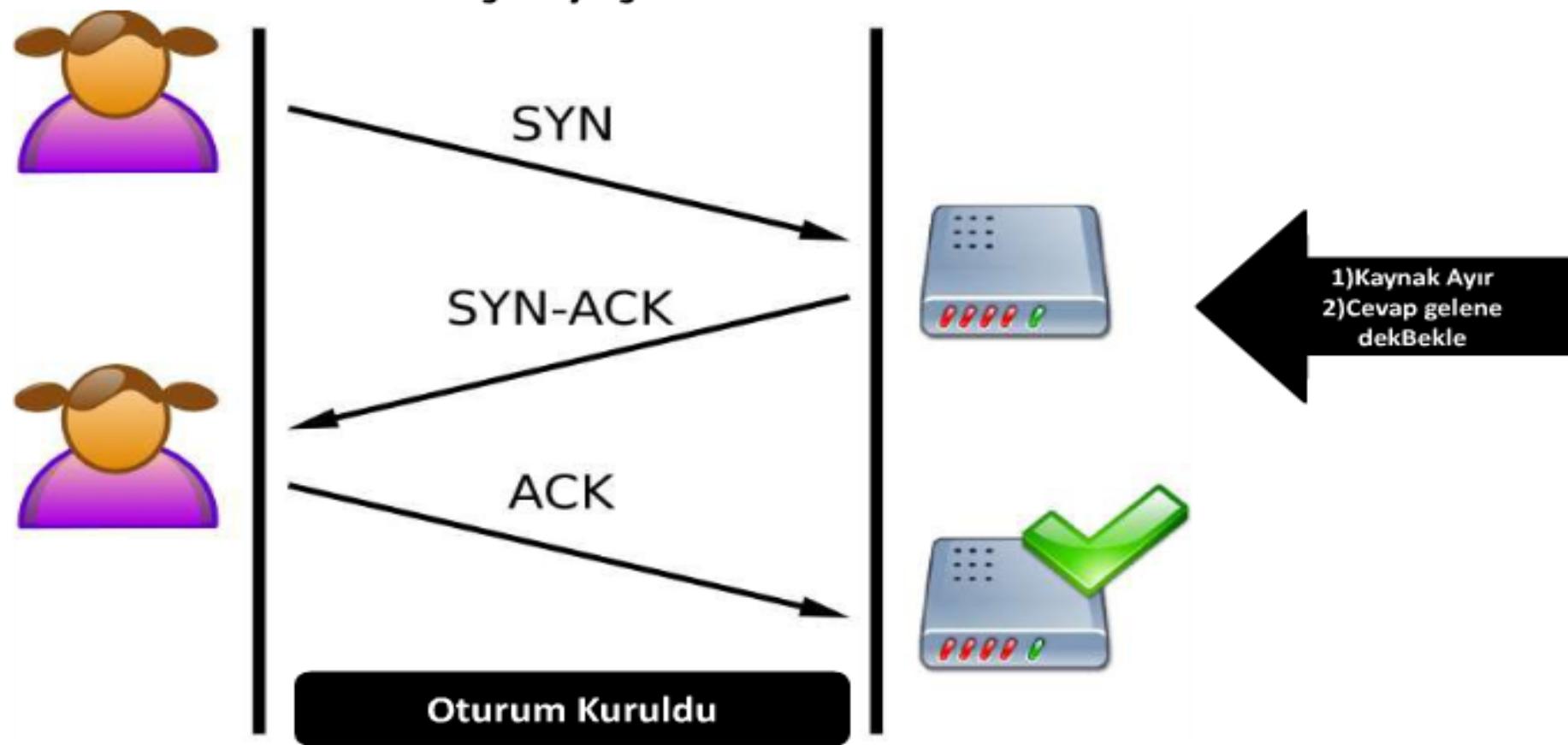
- Genelde TCP/IP servislerini devre dışı bırakmak için kullanılan bir saldırı türüdür.
- TCP bağlantı temelli bir protokoldür.
- Birbiriyle iletişim kuran iki bilgisayar, paketlerini önceden kurulmuş bir hat üzerinden aktarırlar.
- Bunun için iletişimimin başlaması esnasında 3 yönlü el sıkışma kuralıyla hat kurulur.

TCP SYN Paketi Akışı Saldırıları

- Bir TCP bağlantısının başında istekte bulunan uygulama SYN paketi gönderir.
- Buna cevaben alıcı site SYN-ACK paketi göndererek isteği aldığı onaylar.
- Son olarak istekte bulunan uygulama ACK göndererek hattın kurulmasını sağlar.

SYN Flood Saldırıları

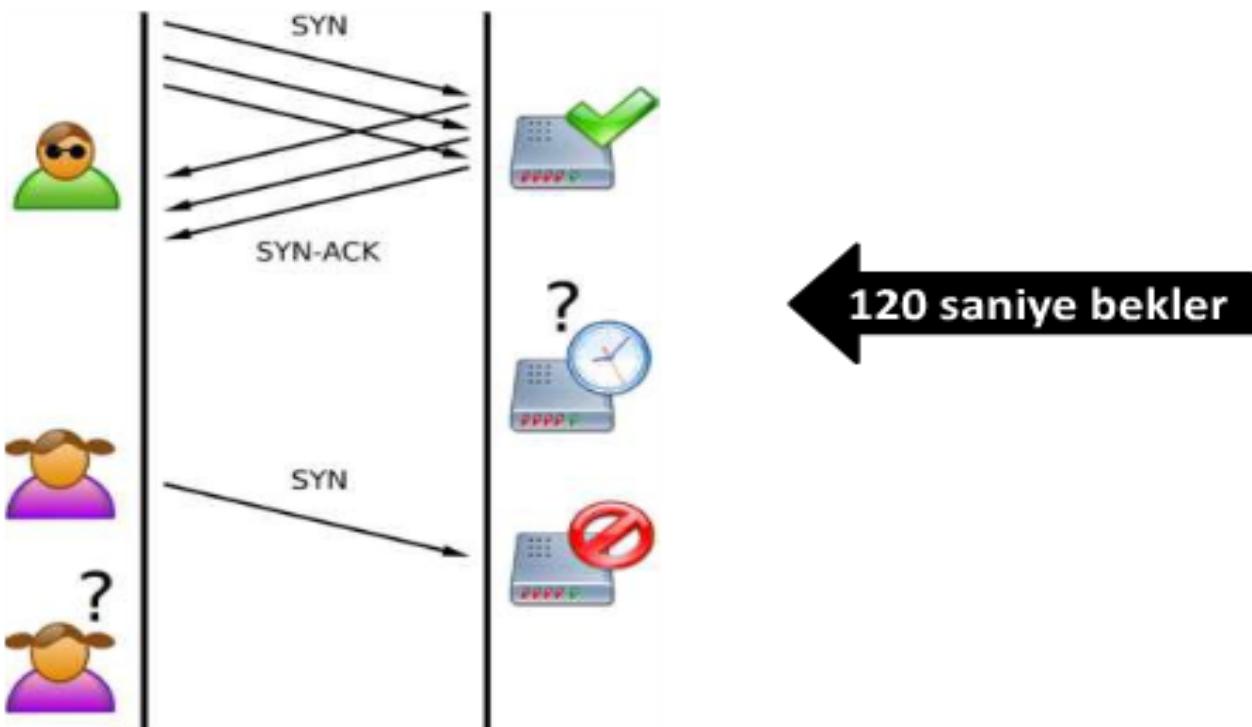
- Normal TCP İşleyışı



TCP SYN Paketi Akışı Saldırıları

- Flood kısa zamanda fazla sayıda bağlantı kurarak siteye zarar verme demektir.
- Bu saldırının türünde saldırıcı, internet üzerinde kullanılmayan IP adreslerini kullanarak birçok SYN paketini hedef makineye yollar.
- Hedef makine, alınan her SYN paketi için kaynak ayırrı ve bir onay paketini(SYN-ACK), SYN paketinin geldiği IP adresine yollar.
- Hedef makine, kullanılmayan IP adresinden yanıt alamayacağı için SYN-ACK paketini defalarca tekrarlar. Saldırıcı bu yöntemi üst üste uyguladığında hedef makine ayırdığı kaynaklardan ötürü yeni bir bağlantıyı kaldırıramaz duruma gelir ve bu sebepten makineye bağlanılamaz.

SYN Flood



- Bir SYN paketi ortalama 65 Byte
- 8Mb ADSL sahibi bir kullanıcı saniyede $16.000/4$ SYN paketi üretebilir, 100 ADSL kullanıcısı?

IP Servis Durdurma Saldırıları

- Bu saldırının türünde (smurf), saldırıcı hedef bilgisayardan ping isteği içinde bulunur.
- Ancak ping paketi, hedef makinenin IP'sinden gelmiş gibi görünecek şekilde hazırlanmıştır.
- Bu durumda ağ üzerindeki bütün makineler, hedef makineye ping atar.
- Hedef makine bu trafiği karşılayamaz ve bağlantı kesilir.

IP Parçalama Saldırıları

- MTU (Maximum Transfer Unit) Nedir?
 - MTU değeri bir ağa girişteki maksimum kapasiteyi belirmektedir.
 - Örneğin Ethernet ağları için MTU değeri 1500 byte, FDDI için 4500 byte'dır. Bu da ethernet ağa giren bir paketin boyutunun maksimum 1500 byte, FDDI ağa giren bir paketin boyutu en fazla 4500 byte olabileceğini gösterir.
 - MTU değerleri farklı iki ağ arasında geçişlerde eğer ilk ortamın MTU değeri daha büyükse IP paketlerinde yeni girilecek ortama göre parçalama işlemi yapılır.



IP Parçalama Saldırıları

- Parçalanmış paketlerin hedefe ulaştığında doğru sırada birleştirilmesi gereklidir.
- Paketler hedefe ulaştığında tekrar birleştirilip orijinalinin elde edilmesi için her pakette bulunması gereken bazı alanlar vardır.
 - Fragmentation ID (IP ID): Bir IP datagramına ait parçalanmış tüm paketlerde bu değer aynı olmalıdır.
 - Parçalanmış her paket datagramın hangi kısmını taşıdığını (Offset Değeri ve Sırasını) bilmelidir. Kendisinden sonra ek parça paket varsa bu alan **flags[+]**, paketin kendisi son paket ise değer **flags[none]** olur.
 - Parçalanmış her paket taşıdığı veri boyutunu ve hangi byte'dan itibaren taşıdığını bilmelidir.

IP Parçalama Saldırıları

- Öncelikle paket parçalamanın olağan bir durumdur. İyi niyetlerle düşünülmüş bu özellik bugüne kadar çeşitli ciddi güvenlik sorunlarına sebep olmuştur.
- Parçalanmış paketlerin sadece birincisinde protokol bilgisi bulunmaktadır. Güvenlik duvarları protokole göre paketleri alır ya da reddeder. Bu durumda sadece ilk paket alınacak yada reddedilecek ama diğer paketler sisteme girebilecektir.

UDP Portlarından Saldırılar

- UDP, TCP / IP protokol grubunun iki aktarım katmanı protokolünden birisidir.
- TCP/IP ailesinin iletim katmanında yer alır.
- UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir, gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur.



UDP Portlarından Saldırılar

- Bir bilgisayar üzerinde veya birkaç bilgisayar arasında, UDP portlarına yönltilecek yoğun paket akışıyla gerçekleştirilen bu saldırılar, tek bir bilgisayar üzerinde gerçekleştiriliyorken bu bilgisayarın performansının düşmesine, birden fazla bilgisayar arasında gerçekleştiriliyorken ise, ağın performansının düşmesine sebep olacaktır.
- Birbiriyle haberleşmekte olan iki UDP servisinden birisi veya her ikisi üreteceği yoğun paket akışıyla, karşısındaki bilgisayarın servisini kilitlemeyi, bilgisayarın performansını kötüleştirmeyi başarabilir.
- UDP servisleri bağlantı temelli olmadıklarından, herhangi bir el sıkışma mekanizması ya da bazı kontrol bilgilerinin karşılıklı değerlendirilmesi gerekmeden, bu tür saldırılara açıktır.

UDP Portlarından Saldırılar

- Örneğin 7 numaralı portu kullanan UDP echo servisi, karşısındaki bilgisayardan (istemci) aldığı bilgileri olduğu gibi geri gönderir.
- 19 numaralı port üzerinden servis veren UDP chargen servisi ise, istemci bilgisayardan her paket alanında, rastgele sayıdaki verilerden oluşan paketi geri gönderir.
- Bu iki servise ilişkin UDP portlarının aynı bilgisayar üzerinde veya değişik bilgisayarlar arasında birbirine bağlanması, sonsuz bir trafigin oluşmasına sebep olacaktır.
- Bu hem servisi veren bilgisayarı hem de trafigin aktığı ağı etkileyecektir.

UDP Portlarından Saldırılar

- Böyle bir saldırı sonucunda doğabilecek sonuçlar şunlardır:
 - Saldırının yönetildiği servisler kilitlenebilir.
 - Bu servisleri veren bilgisayarların performansı düşebilir
 - Servisleri veren bilgisayarların bulunduğu ağın trafiğini arttırmır.
- Bu saldırı tipinden korunmak için alınabilecek önlemlerin başında saldırıda kullanılan servisleri bilgisayarın üzerinden kaldırmak gelir.

UDP Portlarından Saldırılar

- Bu yaklaşımı kullanırken iptal edilecek servislerin ne kadar gerekli olduğu da önemlidir.
- Bu saldırınlarda en çok kullanılan UDP servisleri chargen ve echo servisleridir. Bu servisler neredeyse hiç kullanılmazlar. Dolayısıyla bu servislerin iptal edilmesi ya da güvenlik duvarı üzerinden filtrelenmesi, normal çalışmayı etkilemeyecektir.
- Saldırıların daha çok hangi servislere yapıldığının tespiti için ağa saldırıları kontrol edip raporlayan programların kurulması faydalı olacaktır.

ARP Saldırıları

- ARP (Address Resolution Protocol- Adres Çözümleme Protokolü) IP adreslerini fiziksel adrese dönüştürmek için kullanılır.
- Bir paketin bir bilgisayardan çıktığında nereye gideceğini IP numarası değil gideceği bilgisayarın fiziksel adresi (MAC) belirler.
- Bu adres de paketin gideceği IP numarası kullanılarak elde edilir.

ARP Saldırıları

- Ardından paket yönlendirilir.
- ARP adres çözümlemek istediği zaman tüm ağa bir ARP istek mesajı gönderir ve bu IP adresini gören yada bu IP adresine giden yol üzerinde bulunan makine bu isteğe cevap verir ve kendi fiziksel adresini gönderir.
- ARP isteğinde bulunan makine bu adresi alarak verileri bu makineye gönderir.

ARP Saldırıları

- Protokol adreslerinin fiziksel adreslere çevrilmesi işine adres çözümleme (address resolution) denilir.
- Çevrilen adres “çözülen” (resolved) olarak adlandırılır.
- Bir bilgisayar diğer bir bilgisayarın adresini ancak ikisi de fiziksel olarak aynı ağ üzerinde ise bulacaktır.
- Farlı ağlardaki bilgisayarlar birbirlerinin adreslerini çözemezler.

ARP Saldırıları

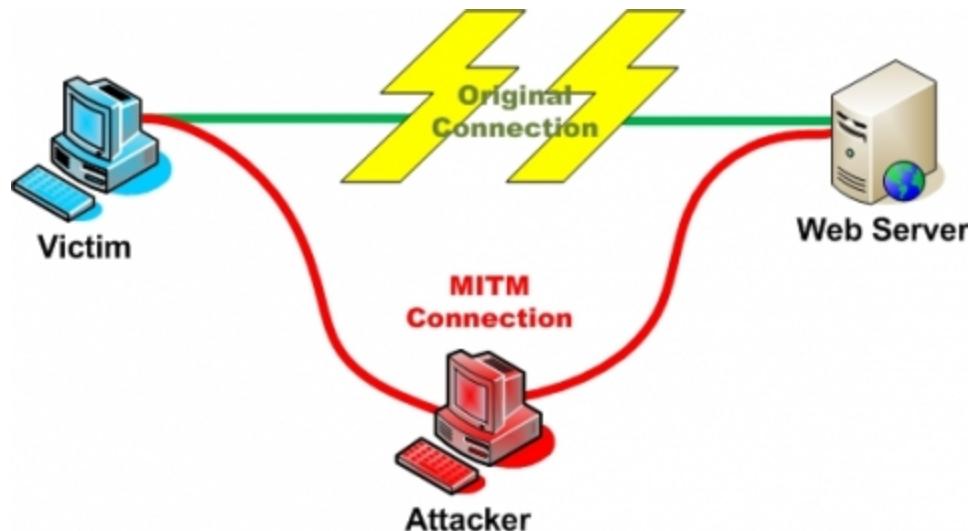
- ARP'de iki temel mesaj vardır. Birisi istek (request) diğeri cevap (response) mesajlarıdır.
- İstek mesajı IP adresi içerir ve karşılık gelen fiziksel adresi ister.
- Cevap ise hem IP hem de aranan fiziksel adresi içerir.
- ARP istekleri broadcast mesajlardır. Cevaplar ise broadcast değil unicasttır.
- Sonuç olarak
 - Ağ üzerinde iki bilgisayarın veri iletişiminde bulunabilmesi için hedef bilgisayar MAC adresini bilmesi gereklidir.
 - Veriyi göndermek isteyen bilgisayar hedef bilgisayarın MAC adresini öğrenmek amacıyla adres çözümleme protokolünü (ARP) kullanır.

ARP Saldırıları

- ARP sahtekarlığı (ARP spoofing, ARP flooding, ARP poisoning) saldırısı lokal ağlarda gerçekleştirilebilen bir saldırıdır. Bu saldırısı, üç şekilde gerçekleştirilmektedir:
 - **MAC Flooding:** Hedef bilgisayarın ARP tablosunun yanlış bilgilerle dolmasını sağlayarak, hedef bilgisayarın göndereceği paketlerin saldırının istediği adreslere gitmesini sağlamaktır.

ARP Saldırıları

- **Man in the Middle:** Bu saldırısında saldırgan, sahte ARP (spoofed ARP) çerçevelerinin içerişine kendi bilgisayarının MAC adresini yazmak suretiyle hedef bilgisayardan çıkan tüm paketlerin kendi bilgisayarı üzerinden geçmesini sağlar.
- Böylece kullanıcının hangi sitelere girdiğinden tutunda, gönderdiği aldığı maillere, şifrelere vs. kadar bilgileri alabilir.



ARP Saldırıları

- **Denial of Service:** Bu saldırının amacı, hedef bilgisayardan dışarı çıkacak olan paketleri dinlemek değil, hedef bilgisayara servis dışı bırakma (DoS) saldırısı yapmaktadır.
- Saldırgan tüm ağda yer alan bilgisayarlara sahte ARP mesajları yollar.
- Bu mesajların içerisinde de hedef bilgisayarın MAC adresini yazar.
- Böylece ağda yer alan tüm bilgisayarlar paketlerini hedef bilgisayara yollar. Bu da hedef bilgisayarın ethernet bağlantısının limitinin dolmasına sebep olur.

ARP Saldırıları

- ARP saldırılarından korunabilmek için alınabilecek önlemler şunlardır.
 - Statik veya Dinamik ARP koruması kullanımı
 - ARP sınırlama

YMH321 Bilgi Sistemleri ve Güvenliği

Steganografi

Prof. Dr. Resul DAŞ

Bölüm - 6

1

Prof. Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

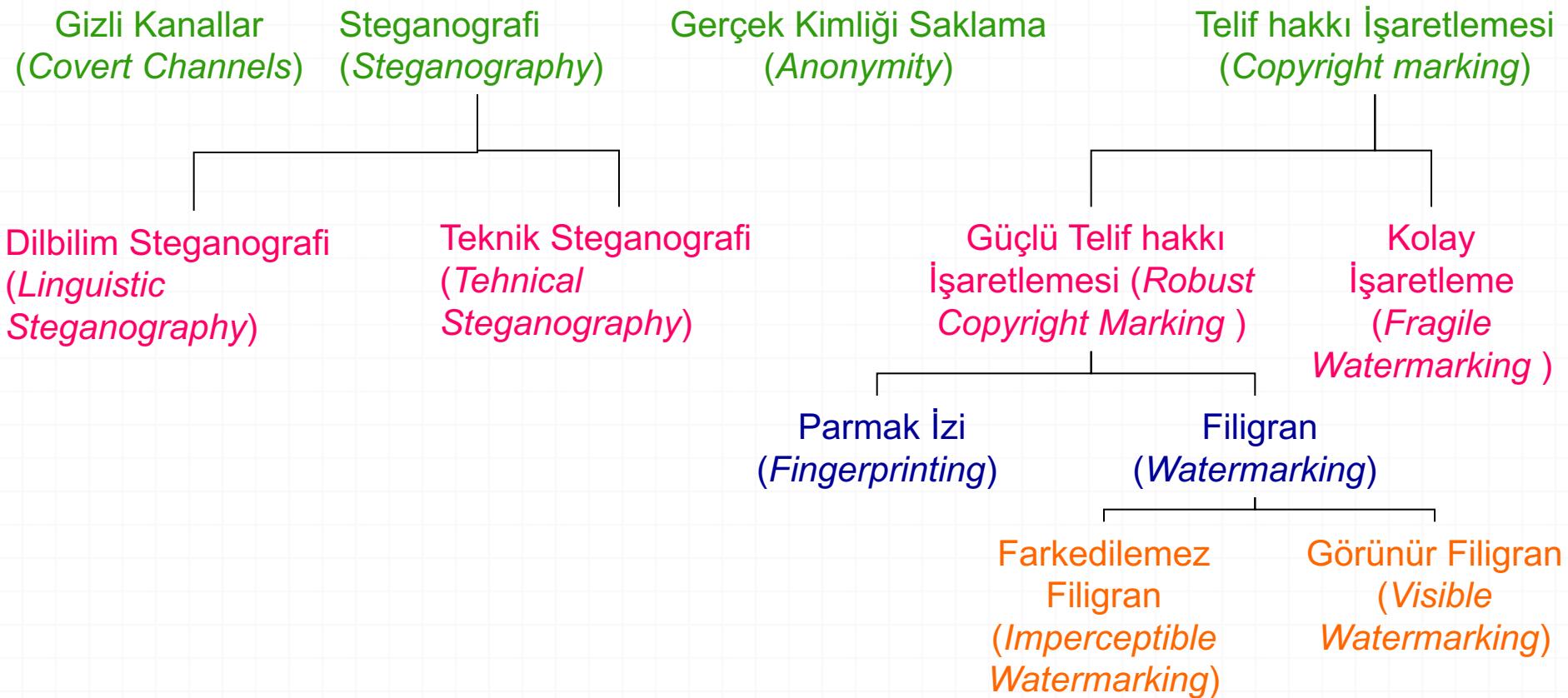
Konu Başlıklarısı

- Metin Steganografi
- Resim Steganografi
- Ses Steganografi

Bilgi Gizleme

- Bilgi gizleme bir mesajın yada bilginin, herhangi bir masum görünüşlü ortam içine saklanarak bir diğer kişiye iletilmesidir.
- Bilgi gizleme bilgisayar ortamındaki encapsulation işlemine benzer bir durumdur.
 - Encapsulation (Kapsülleme)
 - Bir modülün yaptığı işlemlerin bir kısmını, bu işlemleri nasıl gerçekleştirdiği bilgisini dışarıdan bilinçli olarak saklamaktır.
 - Encapsulation'ın asıl amacı içeriği saklamak değil kontrolsüz ve gereksiz erişimi engellemek, dış öğeleri, içeriğe standart, önceden tanımlı arayüzler aracılığıyla ulaşımı zorlamaktır.

Bilgi Gizleme



Gizli Kanallar (Covert Channels)

İki kişi arasında gizli bilgilerin eldeğiştirmesi için iletişimi sağlayan kanaldır. Gizli kanal kurulması iki kişinin karşılıklı anlaşmasını gerektirmektedir.

Gizli Kanalların amaçları:

- İletişimimizdeki veriyi saklamaya çalışmak
- İletişiminin amacını saklamak

Gizli Kanallar (Covert Channels)

Böylece;

- Gerçek veri transferi, dikkatsiz gözlere zararsız ve kanuna uygunmuş gibi gözükecektir.
- Veriyi karıştırmak için ayrı bir şifreleme yapılmasına gerek kalmayacaktır.

Gizli Kanallar (Covert Channels)

- Gizli Kanallar çeşitli alanlarda kullanılmaktadır. Bunlar;
- Dosya tabanlı steganografi
 - Görüntü, ses ve text dosyaları
- Ağ paket steganografisi
 - Veriler IP paketleri içine gizlenmektedir.
- Protokol Kapsüllenmesi
 - SSL (Secure Sockets Layer) üzerinde TCP paketleri içerisine
 - SSH (Secure Shell) üzerinde TCP paketleri içerisine

Gerçek Kimliği Saklama (Anonymity)

- Veri gönderimi sırasında gerçek kimliği saklayarak bilginin bilinmeyen yada anlaşılamayan biri üzerinden gidiyor olduğunu izlenimi verilerek te bilgi zarar görmeden gönderilebilmektedir.
- Fakat ağlar üzerinde bilinmeyen kullanıcı olayı ağ yöneticilerinin daha fazla dikkatini çekmekte ve bilgi güvenliği tehlikeye girmektedir.
- Bu yüzden sadece çok gerektiği durumlarda kullanılması uygundur.

Steganografi (Steganography)

- Bu yaklaşım, bir nesnenin içerisinde bir verinin gizlenmesi olarak tanımlanabilir.
- Ses, sayısal resim, video görüntüleri üzerine veri saklanabilir.
- Bu veriler metin dosyası olabileceği gibi, herhangi bir görüntü içeresine başka bir görüntüyü gizlemekte olasıdır.

Steganografi

- Bu yaklaşımda içine bilgi gizlenen ortam cover-data (örtü verisi), ve oluşan ortama da stego-text veya stego-object denilmektedir.
- Bir stego-key (stego-anahtarı), bilginin saklaması işlemini kontrol etmek için ve gömülü bilginin elde edilmesini zorlaştırmak için kullanılmaktadır.

Steganografi



Steganografi kendi içinde iki kısma ayrılmaktadır.

Steganografi
(Steganography)

Dilbilim Steganografi
(Linguistic Steganography)

Teknik Steganografi
(Technical Steganography)

Dilbilim Steganografi (Linguistic Steganography)

- Dilbilim steganografi, taşıyıcı verinin text olduğu steganografi koludur.
- Burada veriyi gizlemek için text üzerinde değişiklikler yapılmaktadır.
- Bu değişiklikler şu şekilde yapılabilir. Değişiklik yapmanın çeşitli yolları vardır.
- Bunlardan bazıları;
 - grafik kullanılarak yapılabilir
 - text'in yapısı değiştirilerek yapılabilir
 - yada amacı sadece veriyi saklamak olan yeni bir text yaratılabilir

Linguistic Steganography

Dilbilim Steganografi'de kullanılan yöntemler şunlardır:

- Açık kodlar
 - Gizli mesaj, açıkça okunabilir fakat zararsız bir mesaj haline gelir.
 - Bu işlem; maskeleme, boş şifreler ve ızgaralama ile yapılmaktadır.
- Şemagramlar
 - Gizli mesaj, açık metinin ufak fakat gizli bir detayının içine gizlenmektedir.
 - Bunun için grafiksel değişiklikler yapılmaktadır.
 - Kullanılan yöntemler; farklı yazı tipleri kullanmak, eski dactilo yazılarını kullanmak, resimler içinde boşluklar kullanmak vb.

Teknik Steganografi (Technical Steganography)

Teknik Steganografi bir çok konuya içine almaktadır.

- Bunları bazı başlıklar altında toplayabiliriz;
 - Görünmez mürekkep: Geleneksel haline gelmiş olan görünmez mürekkeple yazma yöntemidir.
 - Gizli yerler: Kimsenin göremeyeceği gizli yerlere saklama (bavul, kasa vb.)
 - Microdot'lar: Bilgiyi noktalar halinde sayfaya gizleme
 - Bilgisayar tabanlı yöntemler: Text, ses, görüntü, resim dosyalarını kullanarak veri gizleme yöntemleridir.

Steganografinin Kullanım Alanları

- Metin Steganografi (Text Steganography)
- Görüntü Steganografi (Image Steganography)
- Ses Steganografi (Audio Steganography)

Metin Steganografi

- Metin Steganografi taşıyıcı ortamın text olduğu Steganografi alanıdır.
- Metin steganografi genelde uygulanması zor bir veri gizleme şeklidir.
- Metin Steganografi'de saklanacak veri miktarı azdır.
- Bunun nedeni taşıyıcı text'in içindeki gereksiz alanların ve boşlukların miktarının az olmasıdır.
- Metin tabanlı gizleme yöntemlerinin hepsi, gizli mesajı geri çözebilmek için ya orijinal metne, yada orijinal metnin biçimlendirme bilgisine ihtiyaç duyar.

Metin Steganografi

Metin Steganografi veri saklanacak yerlerin özelliklerine göre aşağıdaki yöntemleri kullanır.

1. Açık Alan Yöntemleri (Open Space Methods)
2. Yazımsal Yöntemler
3. Anlamsal Yöntemler

1- Açık Alan Yöntemleri (Open Space Methods)

- Bu yöntemler, anormal gözükmeyen iki kelime arasında extra boşluklar, satır sonu boşlukları ile çalışmaktadır.
- Bununla birlikte Açık Alan Yöntemleri'nin ASCII kodları ile kullanılması daha uygundur.

Açık Alan Yöntemleri

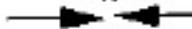
- Açık alan yöntemleri de kendi içerisinde 5 farklı uygulama tipine sahiptir.
 - Cümle içi boşluk bırakma
 - Satır kaydırma
 - Satır sonu boşluk bırakma
 - Sağ hizalama
 - Gelecek kodlaması

a) Cümle İçi Boşluk Bırakma

- Cümle içi boşluk bırakma yöntemi;
 - İngilizce dil yapısında, bir noktadan sonra tek bir boşluk bırakarak “0”ı saklar.
 - Çift boşluk eklemek ise “1”i saklar.
 - Bu işlem işe yarar, ancak çok küçük bir veriyi saklamak için çok büyük veriye ihtiyaç duyar.
 - Bununla birlikte bir çok kelime işleme programı da çift boşlukları otomatik olarak temizler.

Now | is | the | time | for | all | men/women | to ...

Now | is | the | time | for | all | men/women | to ...



(a)

Now is the time for all men/women to ...

Now is the time for all men/women to ...

(b)

- (a) Üst satır'da "for" kelimesinden önce bir boşluk eklenmektedir, alt satırda for ile all arasında daha fazla boşluk vardır.
- (b) Dikey çizgiler olmadan text'in nasıl gözüktüğü

b) Satır Kaydırma Kodlaması

- Bu yöntemde text satırları düşey olarak kaydırılarak gömülecek mesajın kodlanması sağlanır.
- Gömülülmüş kelime yine text dosyası yada bitmap dosya olarak açılabilir.

This is a method of altering a document by vertically shifting the locations of text lines to uniquely encode the document. This method provides the highest reliability for detection of the embedded code in images degraded by noise. To demonstrate that this technique is not visible to the casual reader, we have applied line-shift encoding to this paragraph.

Burada ikinci satır 1/300 inch yukarıya kaydırılmıştır.

Prof. Dr. Resul DAŞ

22 / 43

c) Satır Sonu Boşluk Bırakma

- Satır sonu boşluğu yöntemi, her satırın sonundaki boşluktan faydalananır.
- Veri, tüm satırlarında daha önceden belirlenen sayıda boşluklar bırakarak gizlenir.
- Örneğin, iki boşluk bir bit, dört boşluk iki bit, sekiz boşluk dört bit vb. gizler.
- Bu yöntem, iç boşluk metodundan daha iyi çalışır çünkü satır sonundaki boşluk sayısı arttırılarak daha fazla veri gizlenebilir.

d) Sağ Hizalama

- Metinlerin sağa hizalanması da metin dosyalarında veri saklanmasında kullanılabilir.
- Kelimeler arasındaki boşluklar hesaplanıp kontrol edilerek, masum metin dosyalarına veri gizlenebilir.
- Kelimeler arasındaki tek boşluk “0”ı, çift boşluk “1”i temsil eder.

Sağ Hizalama

- Ancak bu yöntem, normal bir boşluk ile gizlenmiş bir boşluk arasındaki farkı anlamak imkansız olduğu için çözme işlemini zorlaştırır.
- Bu amaçla, Manchester kodlamasını temel olan başka bir teknik kullanılır.
- “01” “1” olarak, “10” “0” olarak yorumlanır. Bununla birlikte “00” ve “11” ise null boşluk bitlerini gösterir.

e) Gelecek Kodlaması

- Bu yöntemde, b, d, T gibi harflerin yatay/düsey uzunlukları gibi bazı metin özelliklerini değiştirerek, biçimlendirilmiş metin içine gizli mesajları saklamayla ilgilenir.
- Bu yöntem, her biçimlenmiş metnin, gizli mesaj saklamak için kullanılabilcek çok sayıda özelliği olmasından dolayı, uzak ara durdurulması en zor yöntemdir.

:S AND

1

Incremental Mod

(a)

:S AND

1

Incremental Mod

(b)

:S AND

1

Incremental Mod

(c)

- (a) Herhangi bir kodlama yapılmamış orijinal metin.
- (b) Sadece seçilen karakterler üzerinde yapılmış gelecek kodlaması.
- (c) Gelecek kodlamasının abartılmış gösterimi

2- Yazımsal Yöntemler (Syntactic Methods)

- Bu yöntem, dökümanı kodlamak için noktalama işaretlerini kullanır.
- Örneğin aşağıdaki iki cümle de ilk bakışta aynıymış gibi gözükmeaktır, fakat dikkatlice bakıldığında ilk cümlenin fazladan bir ; işaretinin içerdığı görülür.
- Bu yapıların biri “1”, diğeride “0” olarak belirlenir ve kodlama işlemi bu şekilde yapılır.
 - “bread, butter, and milk”
 - “bread, butter and milk”

3- Anlamsal Yöntemler (Semantic Methods)

- Bu yöntem W. Bender tarafından ortaya atılmıştır.
- Bu yöntemde eşanlamlı kelimelere birincil ve ikincil değerler atanmaktadır.
- Sonra bu değerler “1” ve “0” olarak binary’e dönüştürülür.
 - Örneğin “*big*” kelimesi birincil, “*large*” kelimesi de ikincil olarak işaretlenmiş olsun.
 - Birincil “1”, ikincil de “0” olarak binary’e çevrilir.

Görüntü Steganografi

Bilgilerin görüntü dosyaları içerisine saklanmasıının çeşitli yöntemleri vardır. Bunlar:

1. En önemsiz bite ekleme
2. Maskeleme ve filtreleme
3. Algoritmalar ve dönüşümler

1- En Önemsiz Bite Ekleme (Least Significant Bit Insertion)

- En önemsiz bite ekleme yöntemi yaygın olarak kullanılan ve uygulaması basit bir yöntemdir.
- Fakat yöntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya çıkmaktadır.
- 0-255 arası 1 byte ile temsil edilen gri-seviye (gray-scale) görüntüler vardır.
- Renkli dijital görüntüler 24 bit yada 8 bit olabilir.

24 bit görüntüler

- 24 bitlik bir görüntü bir pixel başına 3 byte kullanmaktadır.
- Her pixel için renk üç ana renkten elde edilir.
 - Kırmızı (red), Yeşil (green), Mavi (blue)
- Her byte'ta son biti değiştirmek suretiyle her pixel'de 3 bitlik bilgi saklayabiliriz.
- Yani 24 bitlik 1024x768 resim, bilgi saklamak için kullanılabilir 2.359.296 bit (294.912 byte)'e sahiptir.
- Eğer gizlemek istediğimiz mesajı resmin içine gömmeden önce sıkıştırırsak çok daha fazla sayıda bilgiyi gizleyebiliriz.

8 bit görüntüler

- 8 bitlik görüntüler pixel başına 1 byte kullanmaktadır.
- 8 bitlik görüntüler renk sınırlaması yüzünden pek iyi bir sonuç vermezler.
- Saklanacak bilgi, saklama ortamını çok fazla değiştirmeyecek şekilde dikkatlice seçilmelidir.
- Orijinal görüntüde son bite ekleme işlemi yapıldığında, renk girişi göstergeleri değişmektedir.
- 8 bitlik görüntülerde 4 basit renk kullanılmaktadır. Bunlar; beyaz, kırmızı, mavi ve yeşildir.
 - Bu renklerin renk paletinde karşılık gelen girişleri ise sırasıyla şöyledir:
 - 0 (00), 1 (01), 2 (10), 3 (11)

Gri-seviye görüntüler

- Bununla 0 (siyah) ile 255 (beyaz) arasında tam sayılar elde edilebilir. Bu sayılar arasındaki değerler gri'dir ve bundan dolayı bir resime ait tam sayı "gri ton seviye" (gray level) olarak isimlendirilir.
- İkili sayı sistemine göre 10110111 sayısını ele alalım. Bu sayı onluk düzende 183 sayısının karşılığıdır.
- Sondaki bit'in 1 veya 0 olması bu değeri çok fazla değiştirmeyecektir.
- Sondaki bit değerimiz eğer 0 olsaydı bu değer 182 olacak ve renk üzerinde gözle görülecek büyük bir değişikliğe neden olmayacağından emin oluyoruz.

2- Maskeleme ve Filtreleme (Masking and Filtering)

- Maskeleme vefiltreleme teknikleri genellikle 24 bit ve gri-seviye görüntüler üzerinde işaretleme (marking) ve filigran yapılarak uygulanmaktadır.
- İşaretleme yada filigran tekniklerinin görüntülere sıkça uygulanması nedeniyle, görüntünün değişmesi korkusu olmadan uygulanabilmektedir.
- Teknik olarak filigran bir steganografik biçim değildir.

Algoritmalar ve Dönüşümler (Algorithms and Transformations)

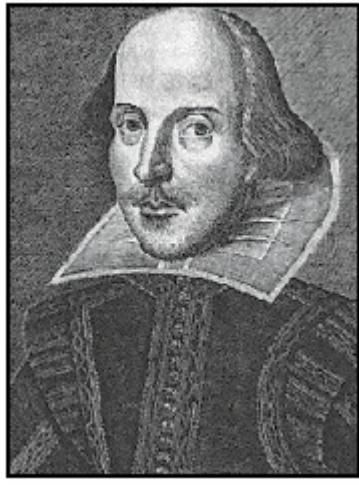
- Son bite ekleme yöntemi bilgi gizlemek için oldukça kolay ve hızlı bir yöntemdir, fakat görüntüye uygulanan işlemler yada kayıplı sıkıştırmalar sonucunda bilgi zarar görebilmektedir.
- Yüksek kalitedeki resimlerin sıkıştırılarak örneğin jpeg formatı kullanılarak internet üzerinden gönderilmesi daha uygundur. Bunun için gizlenen bilginin kaybolmaması ve görüntünün sıkıştırılmasını sağlayan bazı yöntemler ve steganografik araçlar ortaya çıkarılmıştır.

Algoritmalar ve Dönüşümler (Algorithms and Transformations)

Hem sıkıştırma hemde bilgi gizleme işlemlerini
yapan

- Jpeg- jsteg
- Stego-Dos
- Picture-Mark
- SureSign
- S-Tools

Algoritmalar ve Dönüşümler (Algorithms and Transformations)



Orjinal resim



Stego-Dos kullanılarak içine veri
gömülmüş resim

Ses Steganografi

İnsan işitme sistemi (Human auditory system-HAS) aralığı yüzünden, ses sinyalleri içerisinde bilgi gizleme oldukça uğraş gerektiren bir konudur.

HAS 1/1.000'den daha büyük frekans aralığını farkedebilir. Aynı zamanda HAS nereden geldiği belli olmayan gürültülere de oldukça duyarlıdır.

Ses Steganografi

Ses sinyalleri üzerinde uğraşırken ses dosyalarının hangi karakteristiklere sahip olduğunu bilmemiz gerekmektedir. İki ana özelliğe sahiptirler:

- Basit niceleme (quantisation) metodu: Yüksek kaliteli dijital seslerin 16-bit doğrusal niceleme ile ifadesinde en çok kullanılan yöntemdir. WAV(Windows Audio-Visual) ve AIFF(Audio Interchange File Format). Bazı sinyal bozulmaları bu formatta ortaya çıkabilir.
- Geçici seçme oranı: Ses için en çok kullanılan oranlar 8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz ve 44.1 kHz ‘dir. Bu değer frekans aralığının kullanılabilecek en üst seviyesidir.

Sonuç



Sorular



Kaynaklar

- [1] IEEE Std 802.16-2004--IEEE standard for local and metropolitan areanetworks, part 16: "**Air Interface for Fixed Broadband Wireless Access Systems**".
- [2] David Johnston ve Jesse Walker--INTEL: "**Overview of IEEE 802.16 Security**"
- [3] Kitti Wongthavarawat--Thai Computer Emergency Response Team (ThaiCERT) National Electronics and Computer Technology Center,Thailand: "**IEEE 802.16 WiMax Security**"
- [4] Loutfi Nuaymi, Patrick Maillé, Francis Dupont, Raphaël Didier--École Nationale Supérieure des Télécommunications de Bretagne:"**Security issues in WiMAX/IEEE 802.16 BWA System**"
- [5] Yun Zhou ve Yuguang Fang--Department of Electrical and Computer Engineering,University of Florida, Gainesville:"**Security of 802.16 in Mesh Mode**"

YMT311 Bilgi Sistemleri ve Güvenliği

Yazılım Güvenliği

Bölüm - 7

Prof.Dr. Resul DAŞ

Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarları

- Yazılım ve Güvenlik
- Yazılım Geliştirmede Tehdit Modelleme
- Tehdit Modellemenin Faydaları
- Akış Diyagramı
- Risk Hesaplaması DREAD Kavramı
- Örnek Saldırı Senaryusu
- Tehditlerin Azaltılması

Yazılım Güvenliğine Genel Bakış

- **Yazılım güvenliği** genel olarak; yazılımların **tersine mühendislik** yöntemleri ve araçları ile (*debugger, disassemblers, vb.*) algoritmalarının ortaya çıkartılması veya değiştirilmesini engellemeyi amaçlayan yöntemler bütünüdür.
- Yazılım güvenliğinin ele aldığı temel sorunlar, kodların açığa çıkmasını ve değiştirilmesini (*debugging, tracing ya da disassembly ile*) ve tersine mühendislik araçlarını (*debugger, disassemblers, vb.*) engellemek şeklinde özetlenebilir.
- Tersine mühendislik için kullanılan araçları da kısaca tanıyacak olursak:
 - **Debugger:** Derlenmiş bir programın, çalışma anında assembly kodlarına dönüştürülmesi ve üzerinde değişiklik yapılmasını sağlayan araçlardır. En yaygın tersine mühendislik aracıdır. Çok çeşitli tersine mühendislerin en sevdiği araçtır.
 - **Disassemblers:** Derlenmiş bir programın, çalıştırılmadan çözümlenmesini (*assembly kodlarına dönüştürme*) sağlayan tersine mühendislik aracıdır. Uygulama algoritmalarının ve denetim mekanizmalarının kavranarak çözümlenmesi amacıyla sıkça kullanılmaktadır.
- Özetleyecek olursak; yazılım güvenliğini ortaya çıkarılan sorun tersine mühendislik araç ve yöntemlerinin kötüye kullanılmasıdır. Buna karşı yöntem geliştirmek çok fazla bilgi ve tecrübe gerektirdiğinden sıradan bir yazılımcı ya da programcılar tarafından engellenmesi de mümkün değildir.

Yazılım Güvenliğinde Etkileşim

- Gelişen bilgisayar ve yazılım teknolojileri yazılım güvenliğini daha da karmaşık hale getirmiştir.
- Dün, işletim sistemleri ve programlarımız sadece donanım ile etkileşim halinde iken bugün işletim sistemleri, işletim sistemi bileşenleri, kullanıcı bileşenleri, 3. parti bileşenler vs. ile etkileşimlidir.
- Etkileşim beraberinde güvenlik sorunlarını da getirmektedir.
- Böylesi karmaşık problemlerin çözümlenmesi için problemde soyutlama yapılarak, saldırıyla en fazla maruz kalacak nesne (*base object*) tespit edilerek korunması sağlanır.
- Bu yaklaşım ise çoğu zaman etkileşimli bileşenlerin korunmasını göz ardı etmeyi gerektirir.

Yazılım ve Güvenlik

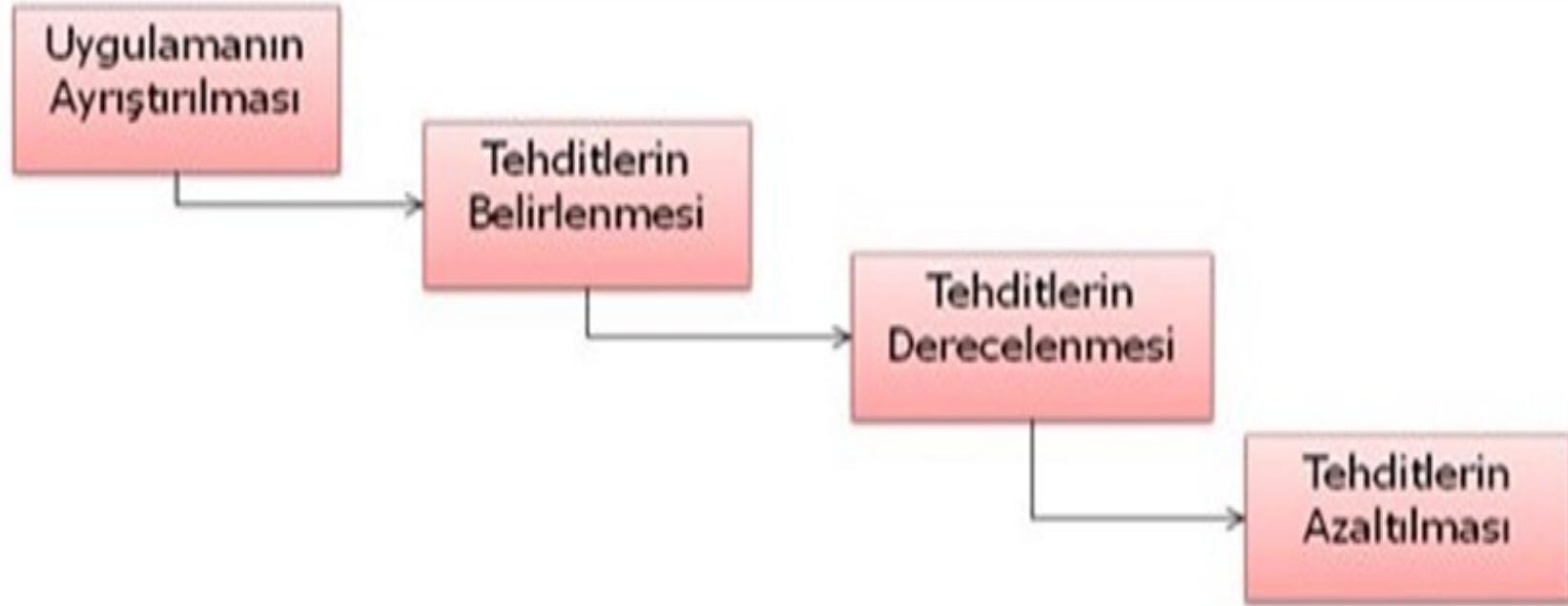
- Güvenliğin En Zayıf Halkası Çalışabilirler (*Programlar*)
- **Code:** Uygulamaların kodlarının bulunduğu bölümdür. Programların çalışabilir kodları burada bulunur. En fazla saldırıya maruz kalan bölümdür. Üzerinde değişiklik yapılması çok da kolay değildir. Temel assembly bilgisinden daha fazlasını gerektirir.
- **Import:** Uygulamaların diğer bileşenleriyle ve işletim sistemleriyle bütünleşme noktalarıdır. Programların çalışmasına doğrudan etkisi vardır. Ulaşılması ve değiştirilmesi oldukça kolay olduğundan saldırganlar tarafından sıkça kullanılmaktadır. Bölümün bir özelliği de, uygulamanın çalışmasına yönelik bilgiler bulundurmasıdır. Buradaki bilgiler normal kullanıcılar ya da program geliştiriciler için önemli gibi görünmesede, saldırgan için değerli bilgiler içerir. Bu bakımdan da saldırganlar için yüksek önceliğe sahiptir. Genel olarak bu bölüme yapılan saldırılar:
 - Bütünleşme adresleri üzerinde değişiklikler,
 - Saldırgan tarafından hazırlanan bileşenlerin uygulama etkileşimine dahil edilmesi,
 - Uygulama kodlarının ve verilerinin daha belleğe yüklenme sırasında değiştirilmesi ya da yönlendirilmesi,
 - Bütünleşmesi beklenen bileşenler yerine saldırgan tarafından hazırlanan bileşenleri ikame edilmesi, vb. yöntemler sayılabilir.
- **Resource:** Uygulama iç verilerinin tutulduğu ve ihtiyaç duyulduğunda karşılandığı bölümdür. Programların çalışmasına dolaylı etkisi vardır. Ulaşılması ve değiştirilmesi oldukça kolaydır, ancak doğrudan çalışabilir olmadığından saldırganlar için daha düşük önceliğe sahiptir. Uygulama iç verileri (*resimler, sesler, ikonlar, vb.*) burada bulunduğuandan başkaları tarafından da kolayca kopya edilebilir. Herhangi bir program üzerinden kopya edilen resimler, sesler ya da ikonlar dezersiz gibi görünmesede ülkemizde de patente konu olduğundan dikkatle korunması gerekmekir. Bu bölüm üzerinden saldırı yapmak daha fazla tecrübe gerektirdiğinden uzman saldırganlar tarafından tercih edilir.

Yazılım Geliştirmede Tehdit Modelleme

- Tehdit modelleme, organizasyonların yüksek düzeyli güvenlik risklerini anlamalarına yardımcı olan, güvenlik tabanlı bir analizdir.
- Tehdit modellemede amaç,
 - tehditlerin saptanması,
 - hangi tehditlerin azaltılmasının gerektiği
 - tehdit azaltma işleminde hangi yöntemlerin uygulanacağının belirlenmesidir.
- Risklerin azaltılması için tehdit modelleme kapsamında uygulanacak olan tehdit değerlendirmesi güvenli sistemler inşa etmek için olmazsa olmaz bir süreçtir.
- Bir organizasyonun ya da bir kurumun herhangi bir uygulama geliştirirken neden tehdit modellemeye gitmesi gerektiği şu maddelerle sıralanabilir:

Tehdit Modellemenin Faydaları

- **Uygulamanın daha iyi anlaşılması:** Uygulamanızın özelliklerinin analizi için zaman harcamak zorunda kalmanız, uygulamanızın ve parçalarının nasıl çalıştığı konusunda size daha geniş bir bakış açısı sağlayacaktır.
- **Tehditlerin belirlenmesi:** Herhangi bir yazılımsal süreç başlamadan, başka bir deyişle uygulama kodlanması başlamadan, sisteminizi ilgilendiren tehditlerin belirlenmesini sağlayacaktır.
- **Kod hatalarının kolayca belirlenmesi:** Kod hatalarının birçoğu tehdit modellemede ortaya çıkacaktır.
- **Proje takımının yeni üyelerinin uygulamaya uyumu:** Yeni işe başlayan birinin yüzde yüz performansla çalışmaya başlaması ve proje takımına uyum sağlaması için her zaman belirli bir sürenin geçmesi gerekmektedir. Tehdit modellemenin bütün uygulamayı gösterecek sistemli ve yapısal bir modelleme olması, yeni işe başlayan çalışanların uygulamayı hızlı bir şekilde öğrenmesini sağlayacaktır.
- **Testçiler için faydaları:** Testçilere hangi tehditlere göre test araçları hazırlamaları gereği hususunda katkı sağlayacaktır.
- **Diğer proje takımları için faydaları:** Sizin ürününüzle alakalı proje geliştiren diğer ürün geliştirme takımları, sizin oluşturduğunuz tehdit modellemeyi incelemelidirler. Bu sayede, diğer takımlar yeni bir tehdit modelleme oluşturmak zorunda kalmayacaktır ve uygulamanın tümünü görmek manasında proje hız kazanacaktır.



Şekil-1 Tehdit Modelleme Döngüsü

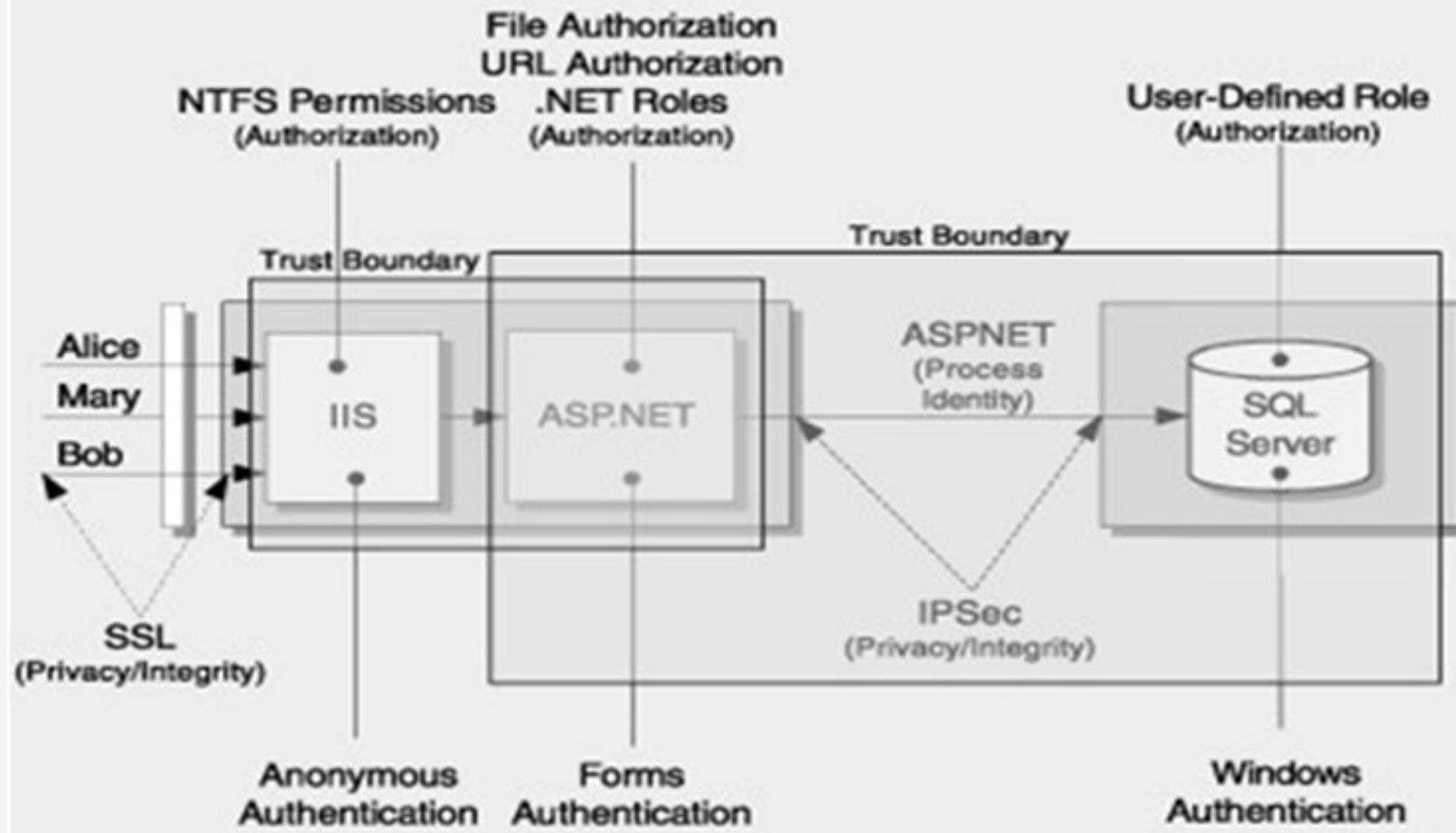
Uygulamanın Ayrıştırılması

- Açıklık tabanlı güvenlik profilinin oluşturulması için uygulama alt parçalara ayrılır.
- Güvenlik çemberi, akış diagramları, giriş noktaları, ayrıcalıklı kod parçacıklarının belirlenmesi ve güvenlik profilinin oluşturulması bu adımda gerçekleştirilir.
- Uygulamanız hakkında ne kadar detaylı bilgiye sahipseniz, tehditleri bulma olasılığınız o kadar yüksek olacaktır.

Uygulama Ayrıştırma		
Güvenlik Profili		Güvenlik Çemberi
Girdi Geçerleme	Oturum Yönetimi	Akış Diagramları
Kimlik Denetleme	Kriptografi	Giriş Noktaları
Yetkilendirme	Parametre Değiştirme	Ayrıcalıklı Kod
Yapıllandırma Yönetimi	Hata Yönetimi	
Kritik Veri	Denetleme ve Kayıt	

Güvenlik Çemberinin Belirlenmesi

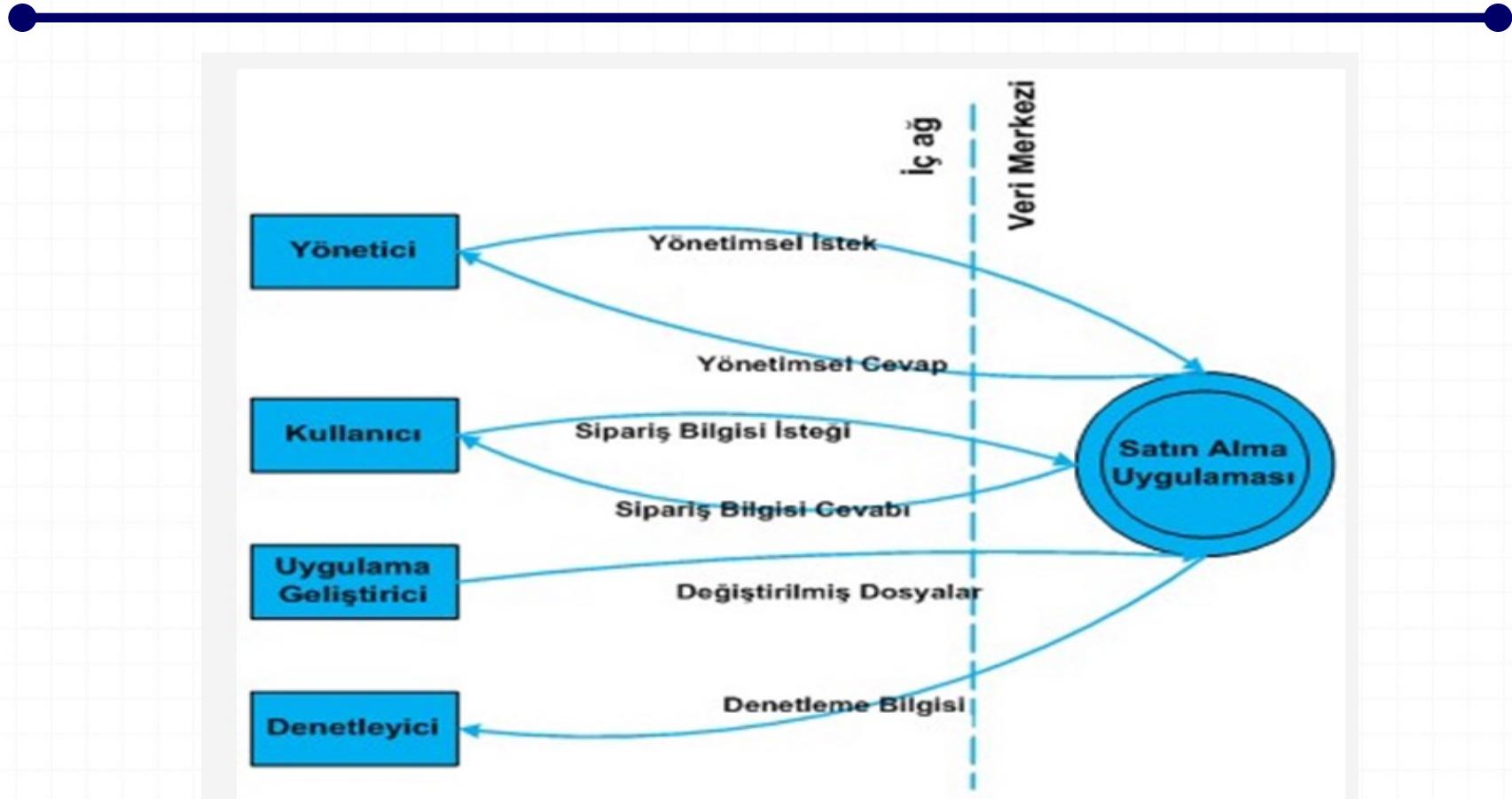
- Bütün varlıklarınızı çevreleyen güvenlik çemberlerinin belirlenmesi bu süreçte yapılır.
- Her bir alt sistem için, veri akışı veya kullanıcı girdisinin güvenliğinin belirlenmesi ve bu veri akışlarının ve kullanıcı girdilerinin nasıl yetkilendirildiği ve kimlik denetlemeye tabi tutulduğu belirlenir.
- Bununla beraber, dışardan çağrıdığınız kod parçasının güvenli olup olmadığını da incelenir.
- Güvenlik çemberinden genel kasıt şudur: O çemberin içindeki bütün giriş noktaları güvenli bir şekilde korunuyordur ve o çemberden geçen bütün veri girdi geçerlemeye tabi tutulmuştur.
- Ayrıca sunucu güvenlik ilişkilerinin de belirlenmesi gerekmektedir.
- Bir sunucu yetkilendirme ve kimlik denetleme gibi süreçleri başka bir sunucudan mı alıyor yoksa kendi mi bu mekanizmaları sağlıyor gibi soruların cevaplanması gerekmektedir.
- Aşağıdaki web uygulaması, ASP.NET Web uygulaması process account'ı güvenli olarak kabul ediyor ve veri tabanı sunucusuna bu güvenli hesap üzerinden ulaşıyor. Veri tabanı sunucu ise, uygulamaya yetkilendirme ve kimlik denetleme sürecinde güveniyor ve yalnızca doğrulanmış veriyi yetkilendirilmiş kullanıcıya dönüyor.



Akış Diagramlarının Belirlenmesi

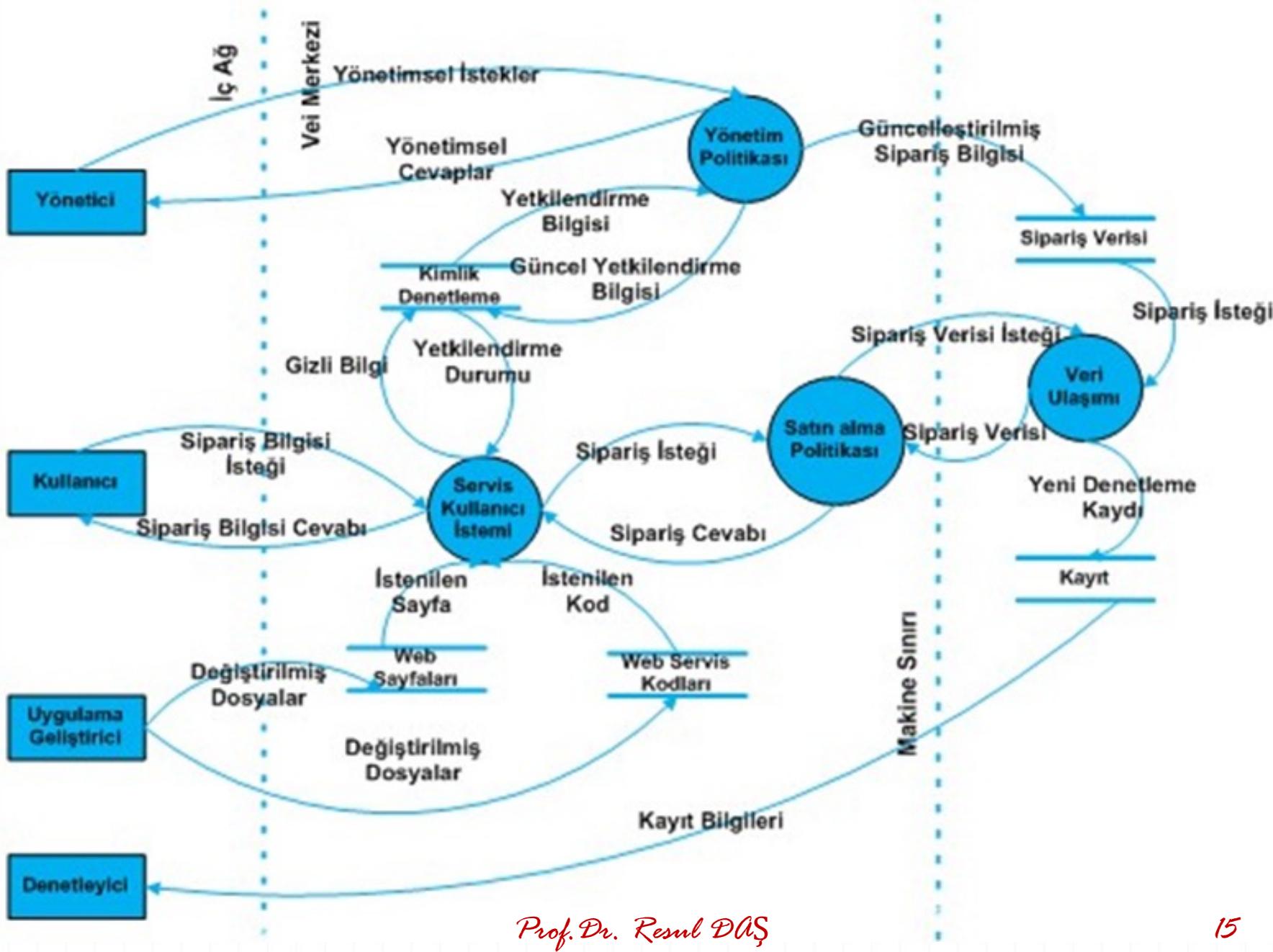
- Uygulama öncelikle bütünü kapsayacak şekilde, akış diagramı halinde gösterilir.
- Sonra uygulama parçalara bölünür ve her parça da büyülüğüne göre parçalara bölmeye devam eder ve akış diagramı halinde gösterilir.
- Örnek bir uygulama olarak basit bir satın alma uygulamasını ele alabiliriz.
- Bu uygulamada, yöneticilerin, kullanıcıların, uygulamayı geliştiricilerin ve denetleyicilerin olduğunu varsayıyalım.
- Yönetici uygulama yönetimiyle ilgili işlerden sorumlu kimse, kullanıcı sipariş bilgilerine bakabilen kimse, uygulama geliştirici uygulamayı geliştiren kimse ve denetleyici denetleme bilgilerini okuyan kimse olarak görev paylaşımında bulunmuş olsunlar.
- Bu uygulamanın öncelikle bütün uygulamayı temsil eden içerik diagramı aşağıda gösterilmiştir.

Akış Diyagramı



İçerik Diagramı

- İçerik diagramı hazırlanırken şu hususlara dikkat edilmelidir:
 - Olabildiğince yüzeysel bilgileri içermelidir. İçsel ve detaylı fonksiyonların incelenmesinden kaçınılmalıdır. Önemli olan kapsamın belirlenmesidir, detaylı fonksiyonların belirlenmesi değil.
 - Sistemin cevap vermek zorunda olduğu istekler bu diagramda belirlenir. Mesela, bir satın alma uygulaması, sipariş bilgisinin görüntülenmesi isteğiyle karşı karşıya kalabilir.
 - Uygulamanın bu isteklere nasıl cevap vereceği de bu diagramda gösterilir.
 - Her bir istekle ve cevapla alakalı olan veri kaynakları belirlenir.
 - Her cevabın muhatabı bu diagramda belirlenir.



İçerik Diyagramı

■ Giriş Noktalarının Belirlenmesi

- Şunu hiçbir zaman unutmamak gereklidir ki, sisteminizin giriş noktaları aynı zamanda saldırganlar için de giriş noktası manasındadır.
- Öyleyse bu noktaların en iyi şekilde korunması gerekmektedir.
- Örneğin, giriş noktalarınız HTTP isteklerini dinleyen web uygulaması içeriyor olabilir.
- Normalde bu uygulama, son kullanıcıların kullanımına açılmış olan giriş noktalarıdır.
- Ne var ki saldırganlar da bu noktaları kullanacaklardır.
- Sisteminizdeki bütün giriş noktalarını bilmek zorundasınız. Her bir giriş noktası için, yetkilendirme ve kimlik denetleme süreçleri en iyi şekilde belirlenmelidir.
- Mantıksal giriş noktaları şunları kapsayabilir: Web sayfaları, web servisleri için servis arayüzleri, mesaj kuyrukları vb... Fizikselli giriş noktaları ise portlar ve soketlerdir.

■ Ayrıcalıklı Kod Parçalarının Belirlenmesi

- Ayrıcalıklı kod parçaları, hassasiyeti yüksek veri kaynaklarına ulaşıkları ve ayrıcalıklı işlemler yapabildikleri için, dikkatlice ele alınmalıdır.
- Hassasiyeti yüksek veri kaynağı olarak şu kaynaklar sıralanabilir:
- DNS sunucları, dizin servisleri, çevresel değişkenler, olay günlükleri, dosya sistemleri, mesaj kuyrukları, performans sayaçları, yazıcılar, register sunucuları, soketler, Wen sunucuları vb.
- Ayrıcalıklı kod parçasının güvensiz ya da potansiyel kötü niyetli bir yazılım tarafından kullanılmayağına emin olunmalıdır.

İçerik Diyagramı

- Güvenlik Profilinin Oluşturulması için cevaplanacak sorular
- **Girdi Geçerleme**
 - Uygulamanız kapsamındaki bütün girdiler geçerlendi mi?
 - Saldırgan uygulamanıza kötü niyetli veri enjekte edebilir mi?
 - Veri ayrı güvenlik çemberlerinden geçerken, geçerlemeye tabi tutuluyor mu?
 - Veri tabanındaki veri güvenilir mi?
- **Kimlik Denetleme**
 - Şifre ve kullanıcı gibi gizli veriler ağ üzerinden geçerken güvenliği sağlanıyor mu?
 - Sıkı kullanıcı hesabı politikaları kullanılıyor mu?
 - Kullanıcılar güvenlik düzeyi yüksek şifre almaya zorlanıyorlar mı?
 - Kullanıcı şifreleri için şifre doğrulama uygulamaları kullanılıyor mu?
- **Yetkilendirme**
 - Giriş noktaları için hangi önlemler alındı?
 - Veri tabanında yetkilendirme nasıl şart koşuluyor?
 - Bağlantı kopmasında ya da hata anında uygulama güvenliği sağlanıyor mu?
- **Yapilandırma Yönetimi**
 - Uygulamanız hangi yönetimsel arayüzleri içeriyor?
 - Bu arayüzlerin güvenliği nasıl sağlanıyor?
 - Uzaktan yönetici yetkilendirmesi nasıl正在被修改?
 - Hangi yapılandırma bilgileri saklanıyor ve bunların güvenliği nasıl sağlanıyor?
- **Kritik Veri**
 - Uygulama kapsamında hangi kritik bilgiler işlenmektedir?
 - Bu gizli bilgiler olduğu yerde ve ağ üzerinde nasıl korunuyor?
 - Nasıl bir şifreleme teknigi kullanılıyor ve şifreleme anahtarları nerede tutuluyor?

Güvenlik Profilinin Oluşturulması

■ Oturum Yönetimi

- Oturum tanımlama bilgileri nasıl tutuluyor?
- Oturum bilgilerinin çalınmaması için ne gibi tedbirler alınıyor?
- Oturum bilgileri ağ üzerinden geçerken güvenliği nasıl sağlanıyor?

■ Kriptografi

- Hangi şifreleme algoritmaları ve yöntemleri kullanılmaktadır?
- Şifreleme anahtarları ne kadar süredir kullanılmakta ve bunların güvenliği nasıl sağlanmaktadır?
- Uygulamanın kullandığı kendi şifreleme tekniği var mı?,
- Şifreleme anahtarları ne kadar sürede bir değiştirilmektedir?

■ Parametre Değiştirme

- Uygulama oynanmış parametreyi tespit edebiliyor mu?
- Form alanlarındaki, HTTP başlıklarındaki, oturum tanımlama bilgilerindeki parametreleri geçerliyor mu?

■ Hata Yönetimi

- Uygulama hata durumlarının nasıl üstesinden geliyor?
- Hata bilgileri kullanıcıya iletiliyor mu?
- Bu hata bilgilerinde sistemin kritik bilgilerini içeren uyarılar bulunuyor mu?

■ Denetleme ve Kayıt

- Uygulamanız bütün sunucu ve katmanlarda denetleme ve kayıt mekanizmasına sahip mi?
- Kayıt dosyalarının güvenliği nasıl sağlanıyor?

Tehditlerin Belirlenmesi

- Uygulama ayırtırıldıktan sonra, her bir bileşen tehdit modelleme için potansiyel tehdit olarak ele alınır.
- Burada amaç her şeyin nasıl çalıştığını görmekten ziyade, uygulamanın bileşenlerini anlamak ve bu bileşenler arasında veri alışverişinin nasıl yapıldığını görmektir.
- Bileşenler genel olarak tehdit hedefleri olarak adlandırılır.
- Belirlenen tehditlerin azaltılması için öncelikle tehditlerin sınıflandırılması gerekmektedir.
- Bunun için STRIDE sınıflandırma modeli kullanılabilir.
- STRIDE modeli aşağıda belirtilmiştir:

Tehditlerin Belirlenmesi

- **Kimlik Yanıltması (Spoofing Identity):** Yanıltma tehditleri saldırganların başka bir kullanıcı gibi davranışları ya da geçerli bir sunucu gibi davranışarak diğer sunucuları yanıltma amacı güder. Kimlik yanıltmaya örnek olarak, yasa dışı olarak başka bir kullanıcının şifre ve kullanıcı ismi gibi gizli bilgilerine ulaşmayı ve bu bilgileri kullanmayı gösterebiliriz.
- **Verinin Değiştirilmesi (Tampering with Data):** Bu işlem verinin kötü niyetli bir şekilde değiştirilmesi manasına gelir. İnternet üzerinden akan verinin değiştirilmesi buna örnek olarak gösterilebilir.
- **Inkar (Repudiation):** Bu tip tehditler, bazen saldırganın gerçekleştirdiği ama bunu inkâr edebileceği tehditler olarak görülür. İnkâr tipi tehditler kredi kartı gibi işlemlerde kendini gösterir. Kullanıcı bazı alımlarda bulunur ve sonra yapmadığını iddia eder. Başka bir örnek de e-posta örneği olabilir. Size gelen bir maili, karşı taraf ben atmadım diye inkâra başvurabilir.
- **Bilginin Açığa Çıkarılması (Information Disclosure):** Bu tip tehditler, bazı bilgilerin onları görmemesi gereken kullanıcılar tarafından görünmesini kapsar. Örnek olarak, bir kullanıcının okumaması gereken bir dosyaya erişim hakkı olması ya da bir saldırganın ağ trafigini dinleyip bazı bilgileri elde etmesidir.
- **Hizmet Dışı Bırakma (Denial of Service):** Hizmet dışı bırakma atakları sistemlerin kullanılmaz hale gelmesini sağlayan ataklardır. Web sunucusunun kullanılmaz hale gelmesi bu tip ataklara örnek olarak gösterilebilir. Sistemlerin güvenirliliği ve sürekliliği sağlamaları adına bu tip ataklara önlem almaları gerekmektedir.
- **Yetki Kazanma (Elevation of Privilege):** Bu tür ataklarda, yetkisiz bir kullanıcı sistemi kullanmak üzere yetki kazanır ve bütün sisteme zarar vermek ya da kontrolü altına almak için sisteme giriş yapar.

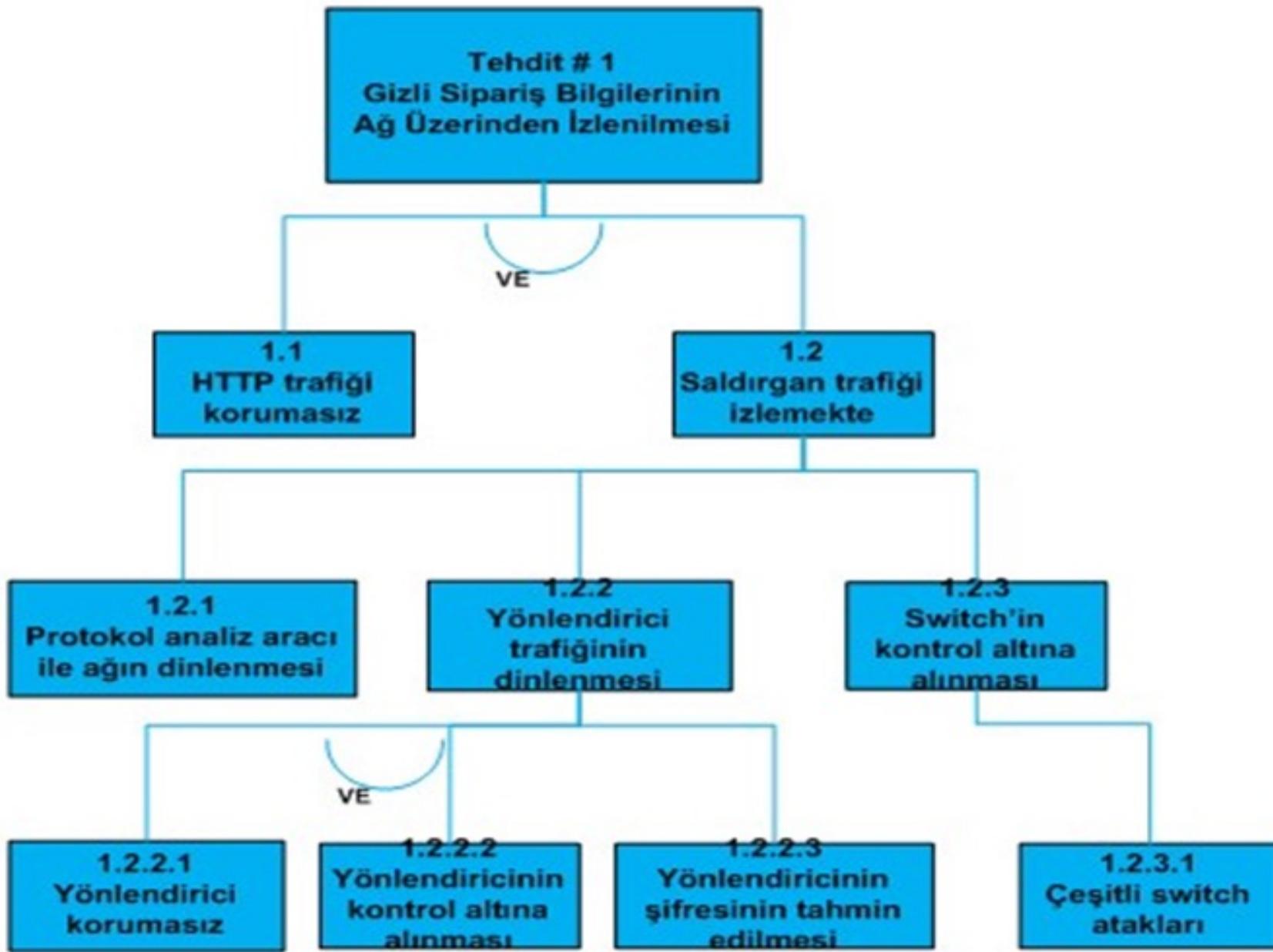
Örnek Saldırı

- Bu sınıflandırmaya dayalı olarak, örnek satın alma uygulamasında örnek bir tehdit üzerinde durabiliriz.
- Bu tehdit şekilde gösterilmiştir. Burada dikkat edilmesi gereken husus, bir kullanıcının başka bir kullanıcıya ait sipariş bilgilerini görmemesi gerektidir.
- Öyleyse, bilginin çalınmasına ya da başka kullanıcılar tarafından görüntülenmesine engel olunmalıdır.
- Bu tehdit bilginin açığa çıkarılması tehdit grubuna örnek bir tehdittir.
- Bir saldırganın bu veriyi görmesinin birçok yolu olabilir.
- Fakat en basit haliyle, saldırgan ağ trafigini, protokollerini analiz eden bir araçla dinliyor olabilir; ya da ağda bir yönlendiriciyi kontrol altına almış olabilir.



Tehdit Ağaçları

- Tehdit ağaçlarının arkasındaki ana fikir bütün sistem tehdit hedeflerinden bir araya getirilmiş bir sistemler bütünüdür ve her tehdit hedefi bazı açıklıklara sahip olabilir.
- Bu açıklıklar da bütün sistemin saldırganlar tarafından kullanılması manasına gelebilir.
- Tehdit ağaçları, bir saldırganın sistemi ele geçirebilmek için izleyebileceği yolları çizen yapısal ağaçlardır.
- Uygulama ayrıştırması işlemi gerçekleştikten sonra, her bir bileşen için tehditlerin belirlenmesi süreci başlar.
- Tehditler belirlendikten sonra ise bu tehditlerin nasıl ortaya çıkabileceği tehdit ağaçlarıyla belirlenir.
- Yukarıda verilen tehdit örneği için, belirlenen tehdit aғacı aşağıdaki gibi olabilir.
- Tehdit ağaçının en başındaki kutu, tehdit kutusu olarak adlandırılır ve altındaki kutular tehditin gerçekleşmesi için gereken adımları temsil eder.
- Bu örnek tehditte, tehditin gerçellenmesi için, HTTP trafigi korumasız olmalı ve saldırgan trafigi dinliyor olmalı.
- Saldırganın trafigi dinlemesi için, ağ trafigini dinliyor olması ya da yönlendirici üzerinden geçen veriyi dinliyor olması gereklidir.
- Yönlendirici dinleme senaryosunun gerçek olması için, ya hedef yönlendirici korumasız olmalı ve kontrol altına alınması gerekiyor ya da yönlendiricinin şifresinin bilinmesi gerekiyor.



Tehditlerin Derecelendirilmesi

- Tehdit ağaçları oluşturulduktan ve tehditler anlaşıldıktan sonra, belirlenen bu tehditlerin derecelendirmesi gerekmektedir.
- Derecelendirmeli amaç, öncelikle hangi tehdit üzerinde duracağımıza karar vermek ve bir sıralama oluşturmaktır.
- Uygulamamız için en büyük tehditin ilk önce giderilmesi mantıklı bir yaklaşım olacaktır.
- Derecelendirme yaparken bazı derecelendirme yöntemleri kullanılabilir.
- Bu derecelendirme yöntemlerinden DREAD adlı yöntemi örnek satın alma uygulamamız için kullanacağız.

DREAD Modeli

- **Zarar Potansiyeli (Damage Potential):** Tehdidin gerçekleşmesi durumunda, zarar ne kadar büyülükté olacaktır. En kötü durum 10 ile gösterilebilecekken, en hafif durum 0 ile gösterilebilir. Yetki tehditleri genellikle 10 ile gösterilir. Tıbbi, mali, ya da askeri veri içeren uygulamalar içi zarar potansiyeli yüksek kabul edilir.
- **Uygulanabilirlik (Reproducibility):** Potansiyal bir saldırının başarıya ulaşma şansını belirlemeye çalışır. Belirli bir tehditin, saldırgan için başarılı bir saldırı olma kolaylığının incelenmesini ön görür.
- **Sömürülebilirlik (Exploitability):** Bu tehdit kapsamında bir atağı gerçekletemek için ne kadar tecrübe ve çaba gerekmektedir. Örneğin, acemi bir kullanıcı, normal ev bilgisayarı ile tehdite bir atak uyguluyabiliyorsa bu ciddi bir durumdur ve bu tehdit sömürülebilirlik manasında 10 alabilir.
- **Etkilenen Kullanıcılar (Affected User):** Eğer bu tehdit bir saldırıyla dönüştürülür ve saldırı başarılı olursa ne kadar kullanıcının bundan zarar göreceği araştırılır. Mesela, bir sunucuya alakalı bir tehdit, birçok kişiyi ilgilendireceğinden yüksek önem arz eder.
- **Keşfedilebilirlik (Discoverability):** Açıklığın kolay ya da zor bulunabileceğinin ya da keşfedilebileceğinin değerlendirimesi yapılır.

DREAD Hesabı

- Bu değerlendirme kriterine göre, yukarıda verdiğimiz örnek tehdidin değerlendirmesi şu şekilde olabilir:
- *Tehdit #1:* Kasıtlı kullanıcı başka bir kullanıcının sipariş bilgilerini ağ üzerinden dinler.
 - **8** Zarar Potansiyali: Başkasının gizli sipariş bilgilerini okuyabilmek ciddi bir sorun.
 - **10** Uygulanabilirlik: Tamamen uygulanabilir.
 - **7** Sömürülebilirlik: Ağ üzerinde yer edinmeli ve ağın dinlemeli.
 - **10** Etkilenen Kullanıcılar: Yöneticiler dâhil herkes etkilenebilir.
 - **10** Keşfedilebilirlik: Bu açıklığın kolayca bulunacağını varsayıyalım.

DREAD ile ölçülen risk oranı = (8+10+7+10+10)/5 = 9

Tehditlerin Azaltılması

- Tehditler belirlendikten ve önem sırasına göre sıralandıktan sonra her tehdit için ne yapılması gereki̇ği kararlaştırılmalı. Bu karar dört farklı şekilde olabilir:
- **Herhangi bir tedbir almama:** Bu yöntem genellikle doğru olmayan bir yöntemdir. En sonunda uygulamanın içerisindeki bu açıklık başınızı ağrıtabilir ve önlem almak zorunda kalabilirsiniz. Daha sonradan alacağınız önlem çok daha pahaliya size mal olabilir.
- **Kullanıcıyı uyar:** Diğer bir yol ise, kullanıcının bu hususta bilgilendirilmesi ve uygulamanın o özelli̇ğini kullanıp kullanmayacağından kendisine bırakılmasıdır. Buna örnek olarak Microsoft Internet Bilgi Servisi (IIS) verilebilir. Bu sistem, yöneticiyi eğer SSL/TLS kullanmazsa kullanıcı bilgilerinin şifresiz bir şekilde ağȧda gezeceğini belirtir. Bu yöntem de birçok durumda problemlı bir yöntemdir. Kullanıcıların çoğu nasıl seçim yapacaklarını bilmezler. Aslında çoğu zaman, kullanıcının karşısına çıkan seçenek, kullanıcı için anlaşılması zor bir seçenektedir. Diğer bir durum ise, kullanıcılar genellikle hazır ayarları kabul ederler ya da uyarıları görmezden gelirler.
- **Problemi ortadan kaldırır:** Problemi çözmek için yeterli zamanınız yoksa kısaca tehdit altında olduğunu düşündüğünüz özelli̇ge sahip parçayı sistemden çıkarmanız yeterlidir.
- **Problemi çöz:** En kesin ve gerçekçi çözüm budur. Teknolojiyi kullanarak, problemi azaltma ya da tamamen çözme yoluna gidilmelidir. Bu yöntem aynı zamanda en zor yöntemdir. Tasarımcılar, geliştiriciler, testçiler ve güvenlik ekibi için daha fazla iş yükü ve daha fazla maliyet demektir.

Güvenli Yazılım Geliştirme ve En Tehlikeli 25 Hata

Sıra	Puan	ID	İsim
[1]	93.8	CWE-89	SQL Komutlarında kullanılan özel elemanların uygunsuz nötrleştirilmesi ('SQL Injection')
[2]	83.3	CWE-78	İşletim sistemi komutlarında kullanılan özel elemanların uygunsuz nötrleştirilmesi ('OS Command Injection')
[3]	79.0	CWE-120	Girdi boyutunu kontrole etmeden ara bellek kopyalama ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Web sayfası oluşturulurken girdilerin uygunsuz nötrleştirilmesi ('Cross-site Scripting')
[5]	76.9	CWE-306	Kimlik Doğrulama gerektirmeyen kritik fonksiyonlar
[6]	76.8	CWE-862	Yetkilendirme eksikliği
[7]	75.0	CWE-798	Kaynak kod içine gömülü hard-coded kimlik doğrulama
[8]	75.0	CWE-311	Hassas verilerde şifreleme eksikliği
[9]	74.0	CWE-434	Sınırlanılmamış tehlikeli türde dosya yüklenmesi
[10]	73.8	CWE-807	Güvenilmeyen girdilere dayalı güvenlik kararları
[11]	73.1	CWE-250	Gereksiz haklarla uygulama çalışma
[12]	70.1	CWE-352	Siteler arası istek sahteciliği (CSRF)

Güvenli Yazılım Geliştirme ve En Tehlikeli 25 Hata

[13]	69.3	CWE-22	Kısıtlanmış dizine erişime sebep olan uygunsuz dosya yolu sınırlaması ('Path Traversal')
[14]	68.5	CWE-494	Bütünlük kontrolü yapılmadan kod indirilmesi
[15]	67.8	CWE-863	Hatalı yetkilendirme
[16]	66.0	CWE-829	Güvenilmeyen kontrol alanından fonksiyonellik dahil edilmesi
[17]	65.5	CWE-732	Kritik kaynağı hatalı izin tahsis'i
[18]	64.6	CWE-676	Muhtemelen tehlikeli fonksiyonların kullanılması
[19]	64.1	CWE-327	Kırılmış veya riskli şifreleme algoritmalarının kullanılması
[20]	62.4	CWE-131	Ara bellek boyutunun hatalı hesaplanması
[21]	61.5	CWE-307	Kimlik doğrulama teşebbüslerinin uygunsuz sınırlandırılması
[22]	61.1	CWE-601	Güvenilmeyen siteye URL yönlendirilmesi ('Open Redirect')
[23]	61.0	CWE-134	Kontrol edilmeyen metin formatı
[24]	60.3	CWE-190	Tamsayı Taşması veya Sarımı (Integer overflow or wraparound)
[25]	59.9	CWE-759	Tuzlanmamış kriptografik özet kullanılması

Risk Azaltma Konuları

ID	Name
<u>M1</u>	Tüm girdileriniz üzerinde kontrol mekanizması kurup devam ettiriniz.
<u>M2</u>	Tüm çıktılarınız üzerinde kontrol mekanizması kurup devam ettiriniz.
<u>M3</u>	Uygulama ortamınızı izole ediniz.
<u>M4</u>	Harici bileşenlerin suistimal edilebileceğini ve kaynak kodunuzun herkes tarafından okunabileceğini varsayıñ.
<u>M5</u>	Kendi yöntemlerinizi geliştirmek yerine, sektör tarafından kabul görmüş güvenlik öğelerini kullanın.
<u>GP1</u>	(genel) Açıklıklardan kaçınmanızı kolaylaştıracak kütüphane ve çerçeveleri kullanın.
<u>GP2</u>	(genel) Tüm yazılım geliştirme döngünüze güvenliği entegre edin.
<u>GP3</u>	(genel) Kapsamlı bir şekilde açıklıkları bulmak ve önlemek için geniş çeşitlilikte metodlar uygulayın.
<u>GP4</u>	(genel) İzole ortam kullanan istemcilere müsade edin.

Sonuç

- Alınması gereken en temel önlemler, risklere karşı sürekli uyanık olmak, bu çalışmada açıklanan saldırıcı tekniklerine karşı uyanık olmak, yeni gelişmeler ışığında gerekli güncellemeleri yaparak saldırılardan etkilenme olasılığını en aza indirmek olarak belirtilebilir. Güvenliğin statik değil dinamik bir süreç sahip olduğu, koruma ve sağlamlaştırma ile başladığını, bir hazırlık işlemine ihtiyaç duyulduğu, saldırıların tespit edilmesinden sonra hızlıca müdahale edilmesi gerektiği ve sistemde her zaman iyileştirme yapılması gerektiği unutulmamalıdır.

Sorular



YMT311 Bilgi Sistemleri ve Güvenliği

Sızma Belirleme ve Testleri

Bölüm - 8

Prof.Dr. Resul DAŞ

Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarları

- Giriş
- Temel İlkeler
- Temel Sızma Belirleme (Pentest)
- Sızma Belirleme Modelleri
- Mimari
- Sızma Belirleme Sistemlerinin Örgütlenmesi
- Sızmaya Tepki

Giriş

- Bilişim güvenliğinin en önemli konularından biri sizma testleri olmaktadır. Kimi zaman bir zorunluluk, kimi zaman güvenliğe olan gerçek ihtiyaç kurum, kuruluş ve firmaları güvenliklerini sizma testleri yapmaya zorlamaktadır.

Temel İlkeler

- Bir sistemdeki kullanıcıların ve süreçlerin hareketleri, genellikle istatistiksel öngörülen bir örüntüye dayanır.
- Bir sistemdeki kullanıcıların ve süreçlerin, hareketleri, sistemin güvenlik politikasını altüst edecek komut veya komutlar dizini içermez.
- Bir sistemdeki kullanıcıların ve süreçlerin hareketleri, sistemde olan ve süreçlerin hareketlerine kısıtlamalar (olumlu veya olumsuz) getiren belirtimler kümese uyur.

Temel Sızma Belirleme

- Teknolojik gelişmeler arttıkça, sistemlere karşı saldırılar da otomatikleşmeye başlamıştır.
- Otomatik olarak saldırı gerçekleştirmeye amacıyla sahip araçlara “saldırı aracı” denmektedir.

Temel Sızma Belirleme

Rootkit nedir?

Çalışan süreçleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdürden bir program veya programlar grubudur. Amacı yayılmak değil bulunduğu sistemde varlığını gizlemektir.

Temel Sızma Belirleme

- Rootkit nasıl kurulur/bulaşır?

Tipine bağlı olmakla birlikte genelde erişim yetkiniz dahilinde sisteminize kurabileceğiniz rootkit'ler bulmanız mümkündür. Bunun dışında güvenilir bir kaynaktan geldiğine inandığınız bir programı haddinden fazla yetki ile çalıştırırmak (Ör: root veya **root yetkili** bir **wheel** grubu üyesi) zararlı bir rootkit'in sisteme kurulmasına sebep olur. Aynı şekilde çok kullanıcılı bir sistemde kernel vs açıkları kullanılarak sistemde root yetkisi kazanıp rootkit kurulması en yaygın görülen bulaşma şeklidir.

Temel Sızma Belirleme

■ Rootkit nasıl temizlenir?

Rootkit çalışırken altında çalıştıracağınız her program rootkit'in yetenekleri doğrultusunda onun verdiği bilgiler ile sistemden aldığı bilgileri ayırd edemez. Dolayısıyla gerçekte hangi dosyaları değiştirdiği, kernele hangi modülü yüklediği, dosya sisteminin neresinde kayıtlı olduğu, hangi ağ servisi üzerinde "sniffer" şeklinde dinleme yaparak uygun komutla harekete geçeceğini tespit etmek kolay değildir. Dolayısıyla rootkit bulaşmış bir sistemin en güzel temizliği içinden hiçbir BINARY dosya alınmadan sadece verilerin alınarak tamamen baştan kurulmasıdır.

Temel Sızma Belirleme

- Rootkit nasıl tespit edilir?

Belli zamanlarda en temel komutların ve muhtemel rootkit bulaşma noktalarının "**hash**" değerlerinin saklanarak bunların daha sonra kontrol edilmesi gibi metodlar olmasına rağmen yukarıda belirttiğim gibi rootkit bulaşmış bir sistemin vereceği bilginin gerçekliği bulaşan rootkit'in yeteneğine bağlıdır. Yine de sistemi bir CD ile açarak bu kontrolleri yapan programlar olduğu gibi bu "hash" alma ve kontrol etme işlemi CD ile açıldıktan sonra elle de yapılabilir.

Temel Sızma Belirleme

- Rootkit'ten nasıl korunulur?
- Linux ve türevleri için konuşursak kullanılan dağıtımın resmi paket dağıtım sistemi dışına çıkmamak pek çok sorunu çözecektir. Bu paket dağıtım sistemlerinin ele geçirilmesi veya zehirlenmesi ihtimali her zaman mevcut olacaktır.
- Genel kaide olarak dağıtımın resmi paket depoları ile kullanılacak programın resmi internet sitesinden alacağınız kaynak kodlar sizi bir derece koruyacaktır.
- Eğer diğer insanların erişimine açık bir sistem kullanıyorsanız güncellemeleri zamanında yapmak ve sık sık kontrol etmek de unutulmaması gereken bir işlemidir.

Temel Sızma Belirleme

■ Rootkit'in zararı nedir?

Rootkitin girdiği bilgisayarınız tamamen dışarıdan kontrol edilebilir hale gelecektir. Tipine bağlı olarak ayrı bir "güvenlik duvarı" bile size koruyamayabilir. (İçeriden dışarıya sanki bir web sitesi açar gibi karşı tarafa bağlanan rootkitler). Aynı bilgisayarda yüklü bir güvenlik duvarı ise muhtemelen rootkitin yeteneği ile ters orantılı olarak sizi koruyabilir.

Temel Sızma Belirleme

- Sisteme sizan kötü niyetli kişiler, Rootkit, Trojan veya özel geliştirilmiş araçlar kullanarak sistem kayıtları değiştirilebilir. Böylece hedef bir sistem için veri toplama aşamasıyla başlayan saldırı planı, izleri silme ile sona ermiş olur.
- Ağ dinleme programına ek olarak programın varlığının sistemden gizlenmesi için bazı sistem komutlarının değiştirilmiş versiyonları da sisteme kurulur.
- *netstat, ps, ls, du, ifconfig, login, ...v.b.*

Temel Sızma Belirleme

- Saldırı araçları temel olarak sızma belirlemenin doğasını etkilemez.
- Bütün izler temizlenemez.
- Genel olarak sistemin zarar görebilecek özelliklerinden yararlanmak için komutların normal kullanımlarının dışında anormal olarak kullanılması gereklidir.

Temel Sızma Belirleme

- Güvenlik ihlalleri ancak anormallikler takip edilerek belirlenebilir.
- Bu anormallikler;
 - Olağanın dışında hareket etme (anomali belirleme)
 - İçeri sızmayı sağlayan süreç hareketleri (kural tabanlı belirleme)
 - Belirlirtimlerin dışında hareket eden yetkili programlar (belitim-tabanlı belirleme)

Temel Sızma Belirleme

- Bu belirleme işlemlerini yapabilen sistemlere Sızmaya Belirleme Sistemleri (SBS) denir.
- Amaçlar:
 - Geniş çeşitlilikte sızmaları tespit etmek. İçeriden veya dışarıdan gelebilecek sızmaları belirlemek.

Temel Sızma Belirleme

- Zaman ayarlamalı sızma belirlemek.
- Yapılan analizi en kolay anlaşılabilen şekilde sunmak.
- Kusursuz bilgi vermek.
 - “yanlış pozitif”
 - “yanlış negatif”

Sızma Belirleme Modelleri

- Sızma belirleme modeli bir dizi durumu veya hareketi sınıflandırarak, yada durum veya hareketleri tanımlayarak iyi (sızma yok) yada kötü (olasısızma) olarak belirtir.
- Pratikte bu modeller birbirleriyle içiçe geçmiş şekillerde de kullanılabilir.

Sızma Belirleme Modelleri

- Anomali Modeli:
 - Beklenmeyen davranışın olası bir sizmanın kanıtı olacağı varsayıımı kullanılır.
 - Anomali belirleme sistemleri sistemin tanım kümesindeki eylemleri davranışlarıyla ve beklenen davranışlarıyla karşılaştırarak tespitler yaparlar.

Anomali Belirleme

- Üç çeşit istatiksel yöntem tanımlanmıştır
 - Eşik metriği
 - İstatiksel momentler
 - Markov modelleri

Kural Tabanlı Sızma Belirleme

- Herhangi bir komut dizisinin önceden bilinen ve sistemin güvenlik politikasını ihlal edecek işlemler yapıp yapmadığını tespit eder ve potansiyel sızmaları raporlar.
- Sistemin zarar görebilecek yerlerinin ve buralara karşı yapılabilecek potansiyel saldırıların bilgisinin önceden bilinmesi gereklidir.
- Bu sistemler kural kümesinde bulunmayan saldırırlara müdahale edemezler.

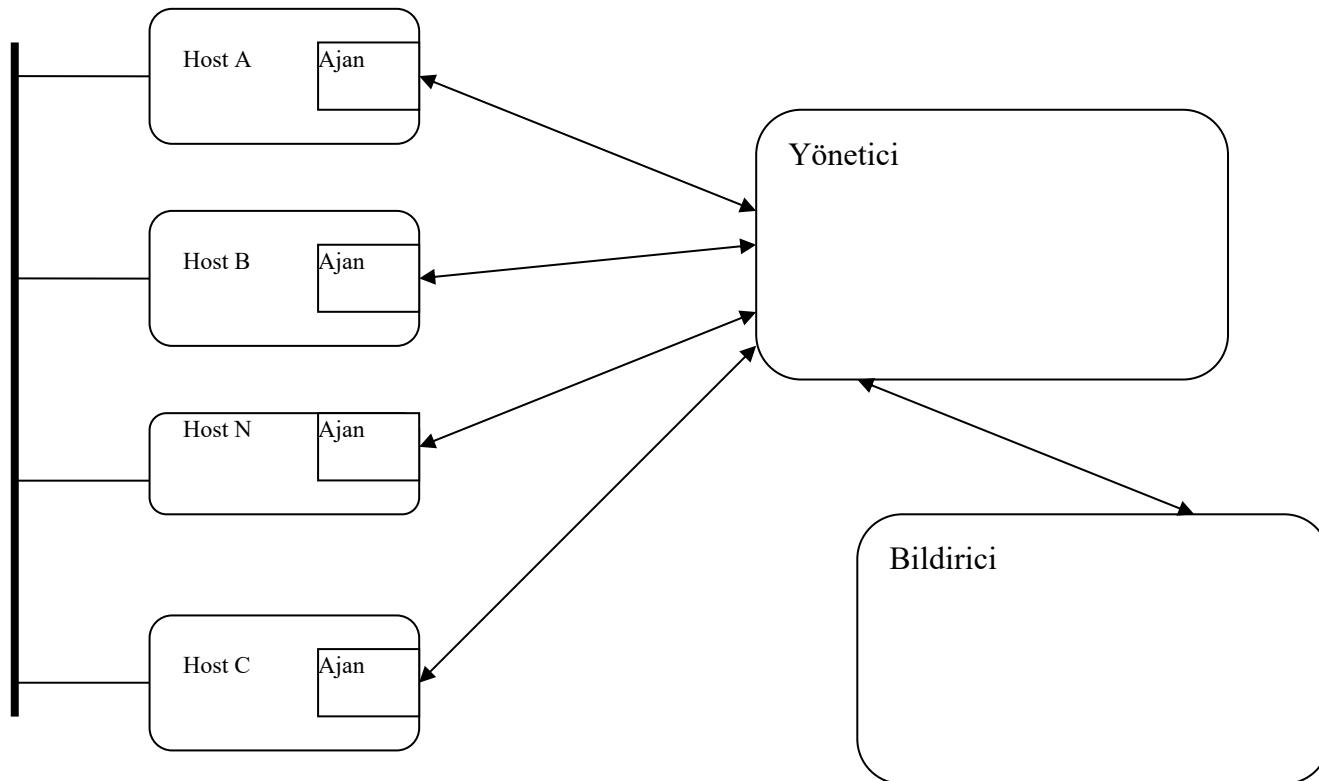
Belirtim Tabanlı Sızma Belirleme

- Bir dizi komutun bir programın yada sistemin çalışma şekline zarar verip vermediğini belirler.
- Sistemin güvenlik durumunu değiştirebilecek programların belirlenmesi ve kontrol edilmeleri gerekmektedir.

Belirtim Tabanlı Sızma Belirleme

- Yeni bir yaklaşım.
- Sistemde ne olabileceği şekillendirilir.
- Bilinmeyen saldırırlara karşı çözüm.
- Zor kısmı; belirtimlerinin çıkarılması gereken programları iyi seçme.

Mimari



Ajan

- Veri kaynaklarından bilgi toplar.
- Anında gönderme – Önislemeli gönderme
- Yönetici potansiyel bir saldırıldan şüphelenmesi halinde ajanların çalışma şekillerini değiştirmelerini sağlayabilir.
- Tek bir konak, birçok konak, ağ.

Ajan

- Konak Tabanlı Bilgi Toplama
 - Sistem ve uygulama kayıtları üzerinde çalışırlar.
 - Olabildiğince sade bir tasarım.
- Ağ Tabanlı Bilgi Toplama
 - Ağdaki çeşitli araçlardan ve yazılımlardan faydalanaırlar.
 - İçerik incelemesi
 - Yerlestirilme yerleri iyi seçilmeli

Yönetici

- Analiz motoru ile herhangi bir saldırısı veya saldırısı başlangıcı olup olmadığını kontrol eder.
- Bir veya birden fazla analiz modeli kullanabilir.
- Ayrı bir sistem üzerinde bulunur.
- Birçok yönetici üzerinde çalışıkları kural kümelerini ve profilleri değiştirebilme özelliğine sahiptir.

Bildirici

- Yöneticiden aldığı bilgilere göre hareket eder.
- Sistem yöneticisine bir saldırının yapılmakta olduğunun haber vermek.
- Saldırıya karşılık vermek.

Sızma Belirleme Sistemlerinin Örgütlenmesi

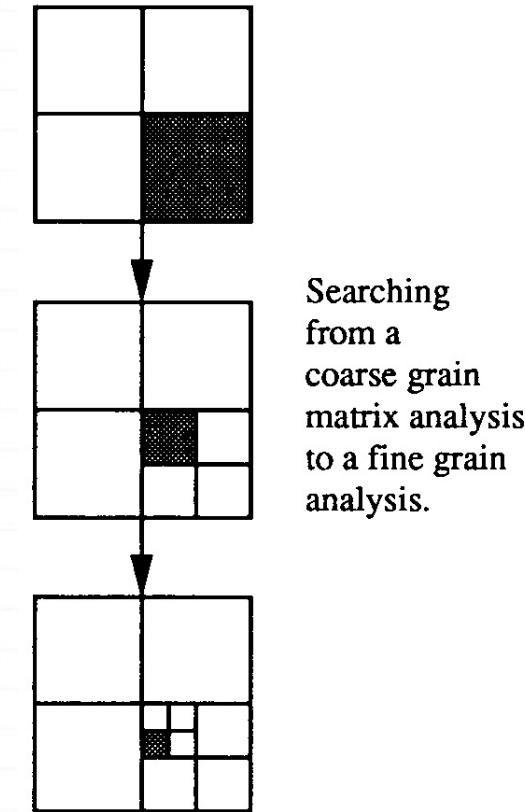
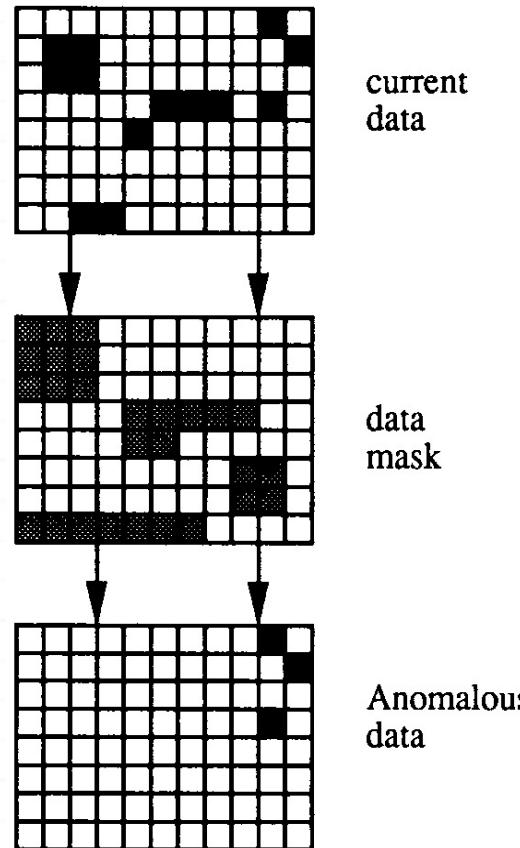
Üç temel yaklaşım var

- Ağ Trafigini İzlemek (NSM)
- Konakları ve Ağları Birlikte İzlemek (DIDS)
- Özerk Aracılar Kullanmak

Ağ Trafiğini Sızmalara Karşı İzlemek

- Kaynak, varış ve hizmet üçlüsü izlenir.
- Elde edilen bilgiler üç eksene yerleştirilerek bir matris oluşturulur.
- Beklenen değerler matrisi ile maskelenerek terslikler ortaya çıkarılır.
- Matrisler sıradüzeni ile aşım engellenir.
- *İmzalar* da yapıya eklenebilir.

Ağ Trafiğini Sızmalara Karşı İzlemek



Searching
from a
coarse grain
matrix analysis
to a fine grain
analysis.

Konakları ve Ağrı Birlikte İzlemek

- Konakların ve ağın izlenmesini içiçe koyarak ayrı ayrı izlemeyle belirlenemeyen saldıruları belirleyebilir.
- *Director* adında merkezi bir uzman sistem kullanır.
- Uzman sisteminin altı katmanlı bir yapısı vardır.
- DIDS üzerine kurulan GrIDS sıradüzensel bir yapıyla bu yaklaşımın geniş alan ağlarına uygulanmasını sağlar.

Özerk Aracılar

- *Director*, tekil hata noktası oluşturur.
- Bu yaklaşımda uzman sistem her bir ayrı bir izleme ile görevli aracı parçalara ayrılır.
- Parçalardan biri çalışmazsa diğerleri onun boşluğunu doldurabilir.
- Parçalardan birine yapılan saldırısı tüm ağın güvenliğini etkilemez.
- Yapısı gereği ölçülebilir.

Sızmaya Tepki

Sızmanın gerçekleştiği algılandıktan sonra korunan ağı en az hasarla eski durununa getirmek için sızmaya karşı tepkiler geliştirilmelidir.

- Engellemeye
- Sızma Yönetimi

Engelleme

İdeal şartlarda sızma denemeleri henüz başında engellenir.

- *Hapsetme*, saldırganları saldırılarının başarılı olduğuna inandırarak sınırlı bir alana sıkıştırmaktır. Hapiste gerçek dosya yapısına çok benzer bir dosya yapısı kullanılır, iyice kısıtlanmış saldırganın davranışları böylece gözlenebilir.
- Bu kavram, ayrıca, çok güvenlik seviyeli ağlarda da kullanılabilir.

Engelleme

- Bir başkaörnektesistem çağrılarında bir terslik olması durumunda sistem çağrıları özellikle geciktiriliyor.
- Normal kullanıcılar bundan etkilenmezken, saldırganlar kısa sürede iki saat aşıkın bekleme sürelerine erişiyorlar.

Sızma Yönetimi

- Bir sizma gerçekleştiğinde ağı korumak, korunan ağı eski durumuna getirmek ve ilkeler doğrultusunda tepkiler vermektedir.
- Altı aşamadanoluştugu düşünülebilir.

Sızma Yönetimi

- **Hazırlık** aşamasında henüz bir saldırı belirlenmemiştir. Gerekli ilkeleri ve düzenekleri kurma aşamasıdır.
- **Tanıma aşaması**, bundan sonra gelen aşamaları ateşleyen aşamadır.
- **Yakalama aşaması** hasarı en aza indirmek içindir.
- **Temizleme aşaması** saldırıyı durdur ve benzer saldırıları engelleyen aşamadır.
- **Kurtarma aşaması**, ağı eski durumuna getimek içindir.
- **Kovalama aşaması** saldırgana karşı alınacak tepkileri, saldırganın davranışlarının incelenmesini ve kazanılan bilgilerin ve derslerin kaydedilmesini içerir.

Sızma Yönetimi - Yakalama

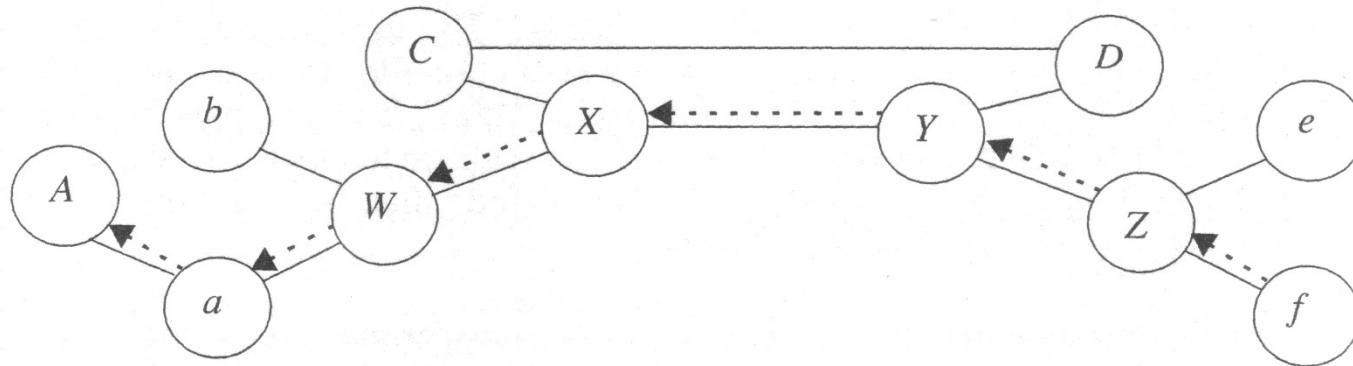
- Pasif izleme ve erişimi sınırlırmak olarak ikiye ayrılabilir.
- Pasif izleme, basitçe saldırgan davranışlarının kaydedilmesidir. Saldırgan davranışları hakkında bilgi verir.
- Erişimi sınırlırmak, saldırganın amacına ulaşmasını engellerken, ona en küçük alanı vermektedir.
 - Bal küpleri yaklaşımında saldırganın ilgisini çekecek sahte hedeflerle gerçek hedefe ulaşması engellenebilir. sistem bir saldırı belirlediğinde saldırganı küpe düşürmeye çalışır.

Sızma Yönetimi - Temizleme

- Saldırıyı durdurmak anlamına gelir. En basiti saldırganın sisteme tüm erişimini kesmektir. (Ağ kablosunu çıkarmak?)
- Sık kullanılan bir yaklaşım örtülerle olası hedeflerin etrafını sarmaktır. Örtüler çoğunlukla işletim sisteminin çekirdeğine gömülür.

Sızma Yönetimi - Temizleme

- Güvenlik duvarları saldırının bağlantısını hedefe gelmeden önce süzmek için kullanılabilir.
- IDIP (Intrusion Detection and Isolation Protocol) kullanılarak ağda bir sızma olduğunda komşu ağlara haber verilebilir. Böylece komşu ağlar da saldırının süzülmesine yardım edebilirler.



Sızma Yönetimi - Kovalama

- Saldırının yerini belirlemek gerekecektir. İki ayrı yaklaşım önerilebilir.
- İzbasma (Thumphprinting)
 - Olabildiğince az yer kaplamalı.
 - İki bağlantının içeriği farklısa farklı izleri olmalı.
 - İletişim hatalarından etkilenmemeli.
 - Toplanabilir olmalı.
 - Hesaplaması ve karşılaştırması ucuz olmalı.

Sızma Yönetimi - Kovalama

- IP başlığı işaretleme (IP header marking)
 - Paket seçimi gerekirci ya da rastgele olabilir. Rastgele seçim daha ekonomik ve güvenlidir.
 - Paket işaretleme içsel ya da genişletilebilir olabilir. İçsel işaretlemede başlığın boyu değişmez.

Sızma Yönetimi - Kovalama

- Karşı saldırısı yasal ya da teknik olabilir.
 - Yasal saldırısı uzun zaman gerektirir. Kanunlar yerli yerinde değil ve oldukça karışık. Ayrıcı yabancı ülkelerden saldırısı gelirse uluslararası kanunlar yetersiz.
 - Teknik saldırısı masumlara zarar verebilir. Saldırganlar masum bir ağı ele geçirdikten sonra orayı üs olarak kullanmış olabilirler.
 - Kendi ağımızdaki haberleşmeye zarar verebilir.
 - Paylaşılan bir ağıın her ne sebeple olursa olsun saldırısı için kullanılması etik değil.
 - Karşı saldırısı da saldırısı gibi dava edilebilir.

Sonuç

- Bilgi Güvenliği ürün veya hizmet değildir.
- İnsan faktörü, teknoloji ve eğitim unsurları üçgeninde yönetilmesi zorunlu olan karmaşık süreçlerden oluşan, süreklilik arz eden bir süreçtir.
- Üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsedebilmek mümkün değildir.
- Yüksek seviyede E-Devlet güvenliğinden bahsedebilmek için **Kurumsal ve Bireysel** anlamda **Bilgi Güvenliğinin** gerekleri yerine getirilmelidir.

Sorular



Kaynaklar



YMH321 Bilgi Sistemleri ve Güvenliği

Güvenlik Araçları

Bölüm - 9

Prof. Dr. Resul DAŞ

Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarları

- Güvenlik Araçları
- Bilişim Suçları
- Bilgi ve Bilgi Güvenliği
- Sonuç
- Sorular
- Kaynaklar

Güvenlik Araçları

- Savunmadan çok “saldırı”ya yönelik araçlar.
- Amaç, saldırganlardan önce sistemdeki açıkları ortaya çıkarıp gereken önlemleri almak.

Nmap

- “Network Mapper”
- Ağ araştırması ve güvenlik denetlemesi yapan açık kaynaklı ücretsiz bir yazılım.
- Geniş ölçekli ağları taramak için tasarlanmıştır.
- Alışılışın dışında IP paketleri göndererek tarama yapar.

Nmap

- Ağdaki canlı bilgisayarlar
- Çalışan servisler (Uygulama adı ve versiyonu)
- Koşulan işletim sistemi
- Varsa kullanılan güvenlik duvarı



Nmap Görüşleri

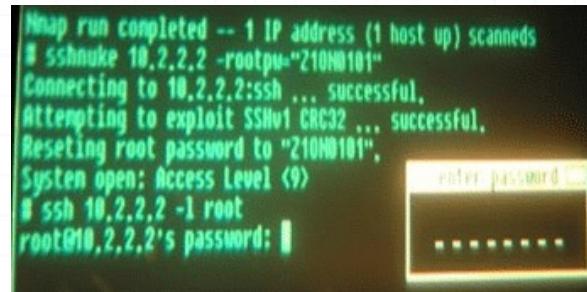
■ www.insecure.org/nmap

```
felix$# nmap -A -T4 felix apollo.sco.com www.insecure.org
Nmap 3.49 ( http://www.insecure.org/nmap/ ) at 2003-12-19 18:12 PST
Starting nmap 3.49 ( http://www.insecure.org/nmap/ ) at 2003-12-19 18:12 PST
Interesting ports on felix (127.0.0.1):
(The 1651 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 3.5p1 (protocol 1.99)
53/tcp    open  domain ISC Bind 9.2.1
111/tcp   open  rpcbind 2 (rpc #100000)
631/tcp   open  ipp   CUPS 1.1
953/tcp   open  rncd?
6000/tcp  open  X11   (access denied)
8080/tcp  open  http  Apache httpd 2.0.47 ((Unix) mod_perl/1.99_10 Perl/v5.6.1)
8081/tcp  open  http  Apache httpd 2.0.47 ((Unix) mod_perl/1.99_10 Perl/v5.6.1)
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 26.695 days (since Sun Nov 23 01:32:16 2003)

Interesting ports on apollo.sco.com (216.250.128.35):
(The 1650 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp   WU-FTPd 2.1WU(1)+SCO-2.6.1+-sec
22/tcp    open  ssh   SSH 1.2.22 (protocol 1.5)
139/tcp   open  smux?
457/tcp   open  http  NCSA httpd 1.3
615/tcp   open  http  NCSA httpd 1.5
1521/tcp  open  oracle?
13722/tcp open  inetd  inetd (failed to exec /usr/openv/netbackup/bin/bpjavamsvc; No such file or directory)
13782/tcp open  inetd  inetd (failed to exec /usr/openv/netbackup/bin/bpcd; No such file or directory)
13783/tcp open  inetd  inetd (failed to exec /usr/openv/bin/vopied; No such file or directory)
Device type: general purpose
Running: SCO UnixWare
OS details: SCO UnixWare 7.0.0 or OpenServer 5.0.4-5.0.6

Interesting ports on www.insecure.org (205.217.153.53):
(The 1654 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp  esmail smtpd
53/tcp    open  domain ISC Bind 9.2.1
80/tcp    open  http  Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 212.275 days (since Wed May 21 12:38:26 2003)

Nmap run completed -- 3 IP addresses (3 hosts up) scanned in 148.510 seconds
felix$
```





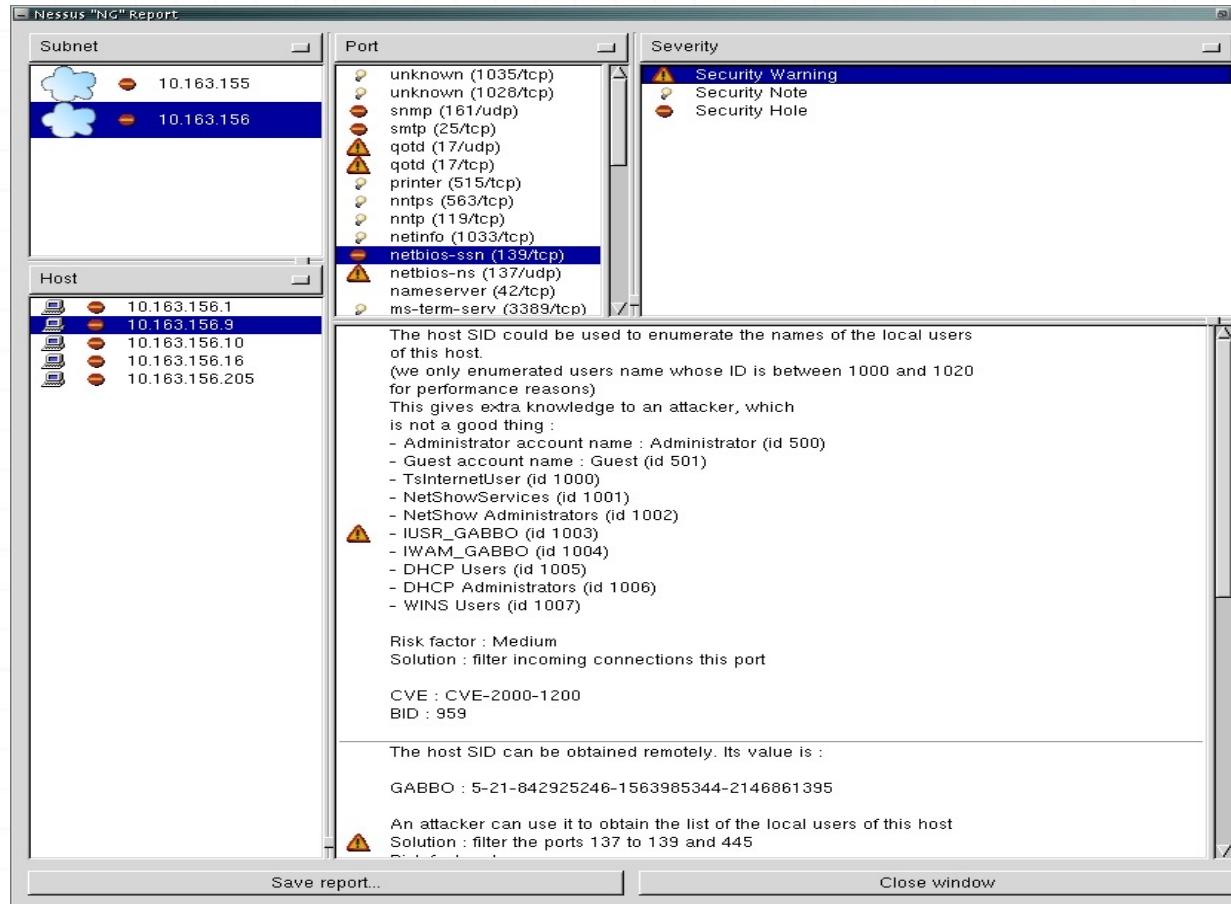
Nessus

- Güçlü, güncel ve ücretsiz bir uzaktan güvenlik taraması aracı.
- Diğerlerinden en büyük farkı bilinen kurallara bağlı olmaması. (Örnek: web sunucusu 1234 numaralı portta çalışsa bile nessus onu bulup güvenlik taraması yapabiliyor.)

Nessus

- Platform: Unix ve benzeri sistemler
Windows
- Çok çeşitli raporlama yetisi (HTML, XML, LaTeX, and ASCII)
- Uyumlu ek (plug-in) yazılımları ve GTK arayüzü ile kullanışlı
- www.nessus.org

Nessus Görüntüsü





Ethereal

- Unix ve windows üzerinde çalışabilen bir protokol analizi aracı.
- Canlı bir ağ üzerindeki verileri incelemek veya disk üzerine kaydetme amacıyla kullanılır.
- Her paket için ayrıntılı bilgi gösterebilen interaktif bir arayüzü vardır.

Ethereal

- Metin tabanlı versiyonu tethereal.
- Ücretsiz.

The screenshot shows a portion of a network capture in Ethereal. A specific TCP stream is selected, indicated by a blue border around its row. The stream details are as follows:

brunching.com	TCP	1028 > www [ACK]	Sec
brunching.com	HTTP	GET / HTTP/1.0	
.1.85			
.1.85			
brunch	— Contents of TCP stream —		
	GET / HTTP/1.0		
.1.85	Connection: Keep-Alive		
brunch	User-Agent: Mozilla/4.75 [en] (X11;		
.1.85	Host: www.brunching.com		
.1.85	Accept: image/gif, image/x-xbitmap,		
brunch	Accept-Encoding: gzip		
	Accept-Language: en		

www.ethereal.com

Snort



- Gerçek zamanlı trafik analizi ve paket kayıtlaması yapabilen ücretsiz bir ağ saldırısı belirleme sistemi.
- Protokol analizi, içerik araştırması ve eşlemesi yapabilir.
- Tampon taşıma, gizli port taramaları, CGI saldırıları, SMB yoklamaları, işletim sistemi belirleme saldırıları gibi birçok saldırısı veya yoklamayı belirleyebilir.

Snort

- Esnek bir kural yazma dili
- Modüler uyumlu ek yazılım mimarisi.
- Gerçek zamanlı alarm mekanizması.
(syslog, windows eventlog, winpopup, vb.)
- Arayüz yazılımı ACID.

www.snort.org

tcpdump

- Ağ inceleme ve veri yakalama amaçlı klasik bir sniffer.
- Metin tabanlı
- Ağ hareketlerini incelemeye kullanılır.
- Verilen deyimleri eşleyerek belirli bir ağ arayüzündeki paket başlıklarını gösterebilir.
- Nmap tcpdump altyapısını kullanır.
- www.tcpdump.org



DSniff

- Güçlü bir ağ denetleme ve giriş testi (penetration test) amcına yönelik araçlar takımı.
- dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf ve webspy araçları ağ üzerinde pasif bir şekilde kayda değer veri araştırmasında kullanılı. (şifre, e-posta, vb.)

DSniff

- arpspoof, dnsspoof ve macof normalde saldırganın ulaşamayacağı (2. katman) ağ bilgilerine ulaşmasını kolaylaştırır.
- sshmitm ve webmitm ssh ve https oturumlarında monkey-in-the-middle saldırılarında kullanılır.

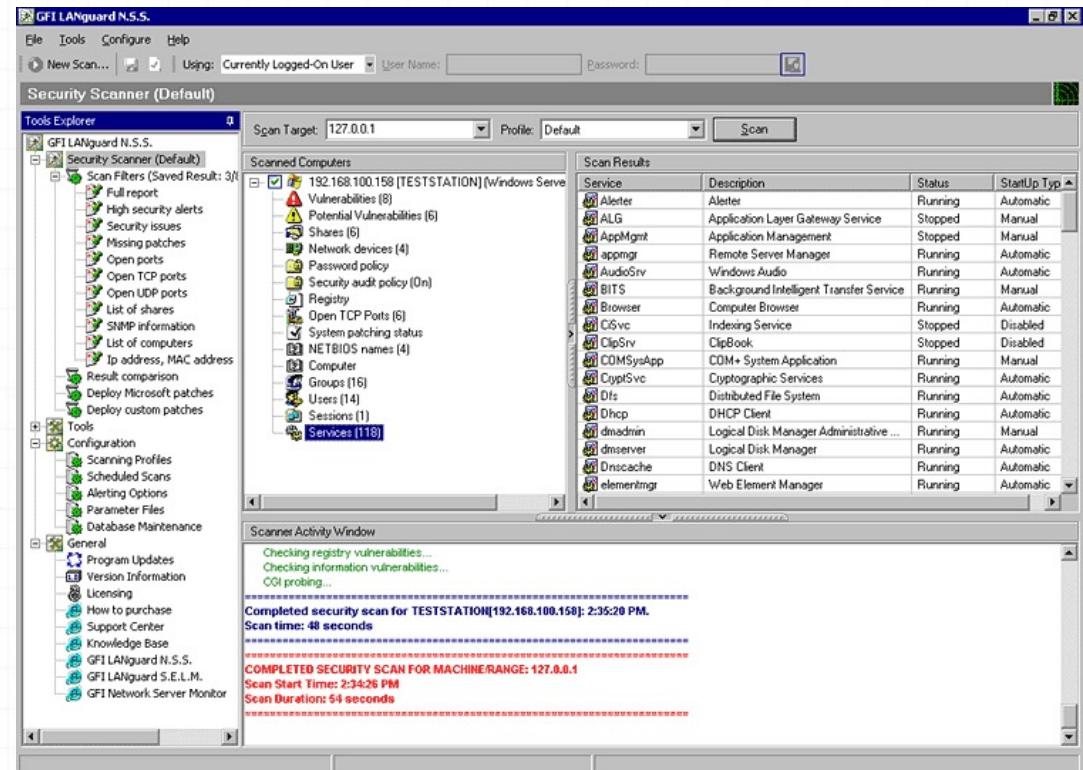
<http://naughty.monkey.org/~dugsong/dsniff/>

GFI LANguard

- Sistemdeki güvenlik hasar risk analizini otomatik olarak yapan bir araç.
- Windows üzerinde çalışır.
- Ağ taraması yapar.
- Her makinenin servis paket durumunu, yamanmamış güvenlik açıklarını, açık paylaşım alanlarını ve portlarını, çalışan uygulamalarını, vb. birçok bilgiyi raporlar.

GFI LANguard

- Ücretli bir yazılımdır.
(Windows tabanlı!)
- Deneme sürümü mevcut.
- www.gfi.com



Ettercap

- Anahtarlamalı yerel ağlar için kullanılan bir sniffer, araya girme ve kayıt yapma aracıdır.
- Şifreli olanlar da dahil birçok protokol için aktif ve pasif inceleme özelliği vardır.
- Kurulmuş bağlantılara veri enjeksiyonu yapma ve filtreleme özellikleri vardır.
- Ağ geometrisini çıkarma ve işletim sistemi tespitleri yapabilir.

John the Ripper

- Çok hızlı bir şifre kırcısı.
- Unix (11'i resmi olarak desteklenen birçok farklı mimarisinde), DOS, Win32, BeOS ve OpenVMS üzerinde çalışabilir.
- Geliştirilme amacı zayıf unix şifrelerini tespit etmek.
- Unix crypt(3) şifre özü, Kerberos AFS ve Windows NT/2000/XP LM özlerini kırabilir.
- Aynı zamanda sürekli güncellenen şifre veritabanı vardır.

ISS Internet Scanner

- Uygulama düzeyinde ağa bağlı araçlar üzerinde hasar risk analizi yapabilen ücretli bir yazılım.
- Ağdaki güvenlik açıklarını yakalamada çok iyi fakat çok pahalı bir yazılım. (ucuz + iyi = nessus)

www.iss.net

tripwire

- Bütünlük analizi yapan araçların büyükbabası.
- Dosya ve dizinlerin bütünlüklerinin bozulup bolulmadığını inceler.
- Herhangi bir değişim sonrası sistem yöneticilerini uyarır.
- Açık kaynak kodlu versiyonu Linux için www.tripwire.org da mevcut.
- Diğer sistemler için ücretli.

Güvenlik Araçları

- Ana kaynak:

www.insecure.org



Sonuç



Sorular



YMH321 Bilgi Sistemleri ve Güvenliği

Biyometrik Güvenlik Araçları

Bölüm - 10

Prof. Dr. Resul DAŞ

Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarları

- Güvenlik Araçları
- Bilişim Suçları
- Bilgi ve Bilgi Güvenliği
- Sonuç
- Sorular
- Kaynaklar

BİYOMETRİK GÜVENLİK SİSTEMLERİ

- Biyometrik tanıma, datayı kodlama veya şifreleme /deşifreleme için vücut özelliklerini kullanan bir süreçtir. Parmak izi, retina ve iris, avuç içi izi,yüz yapısı ve ses tanıma günümüzde sıkça araştırılan biyometrik tanıma teknikleridir. Bu özellikler her şahsa özel olduğu için biyometrik yöntemler hırsızlık ve dolandırıcılığa kısmen de internet üzerinde ticarete cevap olabilecektir.Bu yeni teknolojinin özelliği parola veya PIN numarası yerine çalınamayan kaybolmayan veya yeniden oluşturulamayan biyometrik özelliğin kullanılmasıdır. Bir endüstri uzmanına göre, Kullanıcının erişim haklarına sahip olabilmek için onun parmağını kesmedikçe, biyometrik tanıma erişim kontrolü için mükemmel bir yöntemdir.

BİYOMETRİK GÜVENLİK SİSTEMLERİ

- Tablo 8.1 'de ifade edildiği üzere biyometrik yöntemleri kullanmak için oldukça fazla seçenek bulunmaktadır. Tablo 8.1 'de verilmiş olan biyometrik yöntemler bugüne kadar kararlılığı test ve kabul edilmiş olan yöntemlerdir. Bunlar için daha doğru bir ifade kullanılması gerekirse bu yöntemler bilinen biyometrik yöntemlerdir. Bu yöntemlerin ötesinde halihazırda araştırma aşamasında olan bir çok biyometrik yöntemde bulunmaktadır. Bunlar arasında en dikkat çekici olanlarından birisi insanların kulak yapılarını algılayıp tanıyan sistemlerdir. Bu da göstermektedir ki insanların kendilerine has olan bütün uzuvları biyometrik tanımlayıcı olarak kullanılabilir. Bu da biyometrik sistemlerin ana amacını oluşturmaktadır.

BİYOMETRİK GÜVENLİK SİSTEMLERİ

Biyometrik Yöntem	Hata Oranı
Retina Tarama(ışığı ileten damarlar)	1:10.000.000
İris Tarama(göz rengini veren bölge)	1:131.000
Parmak İzi Tarama	1:500
El Geometrisi Tarama	1:500
İmza(Yazı Yazma) Tarama	1:50
Ses Tarama	1:50
Yüz Tarama	Veri Yok
Vascular Patterns	Veri Yok

Tablo 8.1. Biyometrik Yöntemlerin hata oranları

Biyometriğin Tarihçesi

- Bugünün biyometrik tanıma süreçleri geçmişteki bazı yaygın biyometrik tekniklerinden türetilmiştir. Doğal olarak en yaygın olan ve suçluların tespitinde, çalışanların lisanslarında kullanılan parmak izidir. Bu süreç, yazılı kopya üzerinden manuel olarak haftalarca süren bir inceleme sonucunda bazen de yanlış sonuçlar vererek gerçekleşirdi. Bilgisayar teknolojisinin gelişmesiyle, bazı kuruluşlar, arşivlerini elektronik olarak tutmaya ve parmak izi eşleştirme sürecini daha hızlı ve doğru olarak yapmaya başladılar. Parmak izi tanıma sürecinin sonraki adımı sadece kişileri tanımk değil aynı zamanda belirli yerlere erişimlerini denetlemektir. Bu teknik ile birlikte biyometrik tanıma koddaki bilginin çözümlenmesiyle, kişilerin belirli yerlere girişlerini sağlayacak biyometrik parola olarak kullanılmaya başlamıştır.

Biyometrik Tanıma Nasıl Çalışır?

- Tanıma, iletilen veya bir veritabanında saklanan bilginin anlaşılmasına yardım eden bir matematiksel süreçtir, ve bir kripto sistemini belirleyen üç ana faktör vardır, matematiksel süreç veya algoritmanın karmaşıklığı, mesajı anlamakta kullanılan tanıma özelliğinin uzunluğu, anahtar yönetimi olarak bilinen anahtarın emniyetli saklanması. 68 Dr.İ.SOĞUKPINAR G.Y.T.E. Bil.Müh.Böl. Algoritmanın karmaşıklığı, ters işlem ile doğrudan bağıntısı olması nedeniyle önemlidir. Bazıları tanımanın bu alanının kolayca kırılabileceğini düşünür, bununla birlikte kripto sistemleri saldırlıara karşı zayıf olan en az bu üç faktörü içerecek şekilde iyi tasarlanır.

Biyometrik Tanıma Nasıl Çalışır?

- Mesajı anlamakta kullanılan tanıma anahtarının uzunluğu, tanıma sürecinin ikinci en önemli parçasıdır. Daha kısa olan anahtarlar brute force saldırılara karşı daha zayıftır. Bunun anlamı bir kişinin hesaba girebilmek için bütün mümkün parola kombinasyonlarını denemesi demektir.
- Parola veya PIN numarası gibi biyometrik olmayan tanıma süreçlerinde, anahtarın uzunluğuna bağlı olarak enformasyon yetkisiz kişilerce erişilmeye karşı güvensizdir. Örneğin üç karakterlik bir şifre, mümkün olan permutasyonlar bakımından on karakter uzunlığundaki bir şifreye göre daha zayıftır. Mevcut bilgisayar gücü ile, 64 karakter uzunlığundaki bir anahtarın bulunabilmesi için gerekli permutasyonlarının hesabı dört yüz yıl alabilecektir. Biyometrik tanıma, personel tanımlayıcısı ile normal anahtar karakterlerinin yerlerini değiştiren bir standart karakter uyuşturma yapar. Bu biyometrik anahtar olmadan veriye erişilemez.

Biyometrik Tanıma Nasıl Çalışır?

- Anahtarların emniyetli olarak saklanması tanıma sürecinin en zayıf yönüdür. En kolay olarak gözüken saklama süreci en zor işlemidir çünkü parola veya PIN numarası kaybolabilir veya çalınabilir. İyi tanıma özelliği çok uzun olan ve hatırlanamayan parolaların, kağıtta akıllı kartlarda, veya disketlerde saklanarak yetkisiz kişilerin erişiminin önlenmesidir. Biyometrik tanıma sistemleri anahtarın kaybetme veya çalınma olmadan taşınmasını mümkün kılar.

Örüntü Tanıma Teknikleri

- Örüntü Tanıma, gereksiz detaylardan arındırılmış olan giriş datasından çıkartılan anlamlı özellikler yardımıyla teşhis sınıflarına ayrılan verinin sınıflandırılmasıdır.
- Görüntü, geçici mantıksal gibi değişik örüntü sınıfları mevcuttur. Geniş bir yorumlama ile örüntü tanımayı birçok akıllı faaliyette kullanabiliriz. Tek bir teorisi olmayan örüntü tanıma geniş çaptaki problemin çözümünde kullanılabilir. Bununla birlikte birkaç standart model aşağıda özetlenmiştir.

Örüntü Tanıma Teknikleri

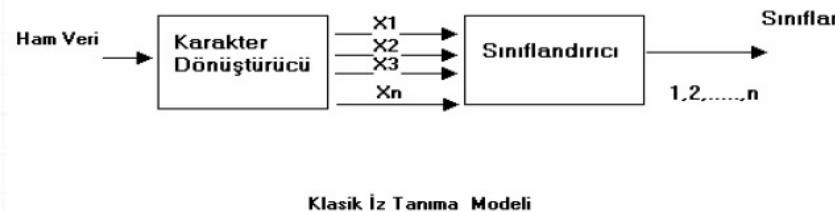
- İstatistiksel veya bulanık örüntü tanıma
- Sentetik veya yapısal örüntü tanıma
- Bilgi tabanlı örüntü tanıma(Yapay sinir ağları, Uzman sistemler)
- Burada istatistiksel yaklaşım ile kendimizi sınırlandıracağız.
Örüntü tanımayı, bir girişi bir sınıfı atayan sınıflandırma olarak
göreceğiz.. Problemi böyle sınırlamakla ihtiyaçlarımızı gören bazı
yararlı teknikleri geliştirecek ve aşağıdaki temel kavamlar
üzerinde yoğunlaşacağız:
- Sınıflandırma
- Özellikler
- Özellik vektörleri
- Standart sınıflandırma modelleri

Sınıflandırma Modeli

- Görsel örüntü ile çalıştığımızı ve Roman alfabetesinin 26 harfini temsil eden örüntüyü bildiğimizi kabul edelim. Buradan örüntü tanıma problemini, giriş verisini 26 sınıfından birisine atama olarak ifade edebiliriz.(Şekil 8-1) Genelde girişin sınıf 1 veya Sınıf 2 veya .. veya ...Sınıf c 'ye ait olduğu şeklinde kendimizi sınırlayacağız..



Şekil 8-1. Harflerden oluşan Görsel örüntü



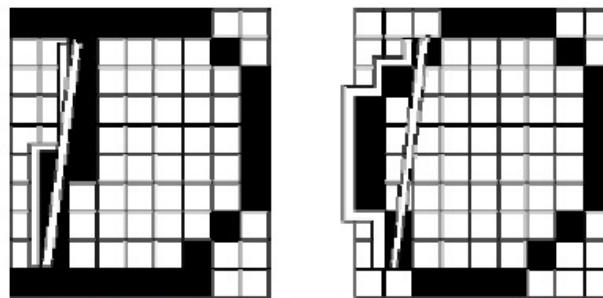
Şekil 8-2. Örüntü(iz) tanıma modeli

Sınıflandırma Modeli

- Daha ileriye giderek, görsel girişi sayısal hale getirmek için bir kamera kullandığımızı ve bir karakteri parlaklık değerlerinin dizisi olarak ayırttığımızı kabul edelim. Bilgisayar bu veriyi 70 Dr.İ.SOĞUKPINAR G.Y.T.E. Bil.Müh.Böl. nasıl sınıflandıracaktır. Belli bir yaklaşım, girişi, her bir sınıf için standart bir örüntü ile karşılaştırmak ve en iyi uyuşan sınıfı seçmektir. Bu yaklaşimdaki açık problem neyin karşılaşılacağı ve uyuşmanın mertebesini ölçmenin söyleneceğidir.(Şekil 8-2.) Aynı sınıfı ait olan girişlerin, farklı sınıflardaki örüntüler arasındaki farklılığa göre değişkenliği örüntü tanıma problemlerini böyle karmaşıklaştırır. Bu problemin üstesinden gelmenin bir yolu karakteristik özelliklerin araştırılmasıdır.

Özellikler

- Bir nesne veya bir olayı sınıflandırmanın tek yolu onun karakteristik özelliklerinin veya belirleyici niteliklerinin ölçülmesidir. Örneğin yazılı bir harfi sınıflandırmak için onun alan ve çevresini bilmek faydalı olacaktır. Onun alanının çevresinin karesine oranı ile onun sıkılığını ölçübilirdik. Onun yatay eksene göre üst ve altta kalan kısımlarının alanlarını karşılaştırarak simetrikliğini ölçübiliriz. (En iyi ölçmenin simetriklilik olduğu düşünülebilir.)
- Bazı özellikler önemli küçük farklara duyarlı olabilir. Örneğin Şekil 8-3'te gösterilen "D" harfini "O" dan ayırt etmek için sol tarafın düzluğu ölçülebilir, belki de düz çizgi farkının yay uzunluğuna oranı ölçülebilir. Açıkkası, çözülmesi gereken önemli bir özellik olan belirleyici niteliklerin tasarıımı bir bilimden çok sanattır.



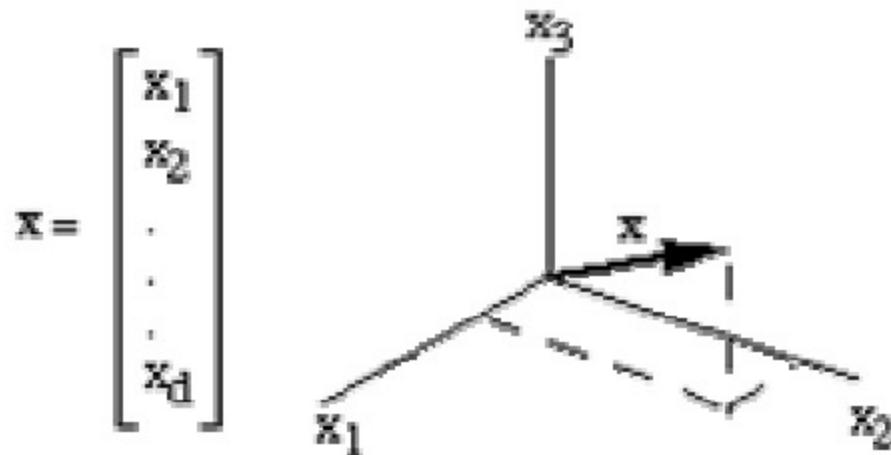
Şekil 8-3: D ve O harflerine ait görsel veri

Belirleyici Özellik Vektörleri

- Herhangi bir nesne veya olayı sınıflandırmak için sıkça belirleyici özelliklerin sabit bir kümesi elde edilir. Örneğin her zaman,,
- $x_1 = \text{alan}$
- $x_2 = \text{çevre}$
- ...
- $x_d = \text{yay uzunluğu} / \text{Düz çizdi uzaklığı}$ her zaman ölçülebilir.
- Bu durumda, belirleyici özellik kümesini, x belirleyici özellik vektörü olarak düşünebiliriz, burada
- x, d boyutlu bir sütun vektöridür. Şekil 8-4 de gösterilmiştir.

Belirleyici Özellik Vektörleri

- Benzer olarak, x 'i d boyutlu belirleyici özellik uzayında bir nokta olarak düşünebiliriz.



Şekil 8-4: Özellik vektörü

Standart Sınıflandırma Modelleri (Klasik Model)

- Aşağıdaki klasik model örüntü tanıma için önde gelir.
- Belirleyici özellik çıkartıcı olarak adlandırılan bir sistem veya program, bir özellik vektörü olan x 'in elemanlarına karşılık gelen belirleyici özellikleri x_1, x_2, \dots, x_d olan d sayısal kümesini belirlemek için ham veriyi işler. Sınıflandırıcı denilen bir sistem veya program, x 'i alır ve Sınıf 1 sınıf 2, ..., sınıf c 'den birine atar.

Standart Sınıflandırma Modelleri

(Klasik Model)

- Belirleyici özellik çıkartıcının tasarımları çoğunlukla probleme bağlıdır. İdeal belirleyici özellik çıkartıcı aynı sınıfındaki bütün örüntüler için aynı x özellik vektörünü, farklı sınıfındaki örüntüler için ise farklı özellik vektörünü üretmelidir. Pratikte, farklı girişler, belirleyici özellik çıkartıcı tarafından farklı özellik vektörü üretilmesin sağlanır, fakat sınıf içindeki değişkenliğin sınıf arasındakine göre küçük olmasını bekleriz.

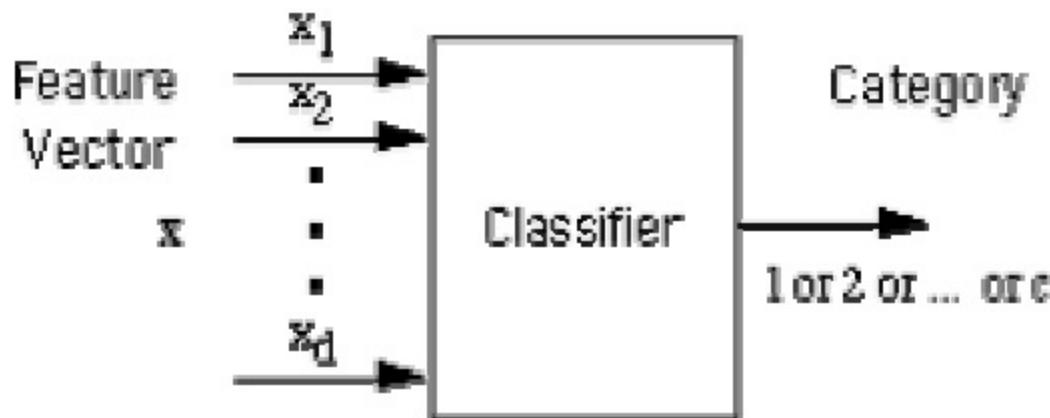
Standart Sınıflandırma Modelleri (Klasik Model)

- Bu noktada, belirleyici özellik çıkartıcının tasarımcısının yapabileceğinin en iyisi ile işini tamamladığını kabul ederiz, ve özellik vektörü örüntüleri ayırt etmek için gerekli olan bilgiyi içerir. Verilen belirleyici özellik kümelerinden sınıflandırıcıyı tasarlamak bizim işimizdir.

Basit Sınıflandırıcılar

Bir sınıflandırıcı tasarlama yaklaşımı için en az iki yol vardır:

- Makul bir çözümün varsayıımı ve onu probleme uydurulması
- Problemin matematik modelinin çıkartılması ve en iyi sınıflandırıcının üretimi



Şekil 8-5: Basit sınıflandırıcı

Basit Sınıflandırıcılar

Daha çok sezgisel olan ilk yöntem pratikte daha çok kullanılır, ve bizim ele alacağımız yaklaşımın Basit bir çözüm ile başlayacağız, karakteristiklerinin analizi, zayıf yönlerin belirlenmesi, ve sadece gerektiği şekilde karmaşıklaştırma.. Bu bölümde aşağıdaki kavramlar üzerinde duracağız:

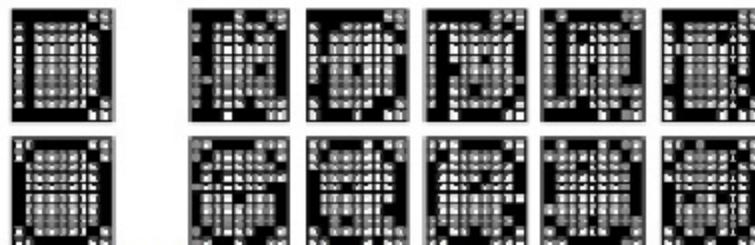
- Şablon Uyuşturma(Template matching)
- En az mesafe sınıflandırıcıları(Minimum-distance classifiers)
- Metrikler(Metrics)
- İç Çarpımlar(Inner products)
- Doğrusal farklılıkların anlaşılması(Linear discriminants)
- Karar sınırları(Decision boundaries)

Şablon Uyuşturma (Template Matching)

- Şablon uyuşturma örüntü sınıflandırma için doğal bir yaklaşımdır. Örneğin Şekil 8-6'da gösterilen gürültülü "D" ve "O" yu düşünelim. Gürültüsüz versiyon şablon olarak sol tarafta gösterilmiştir. Gürültülü örneklerin birisini sınıflandırmak için, onu iki şablon ile karşılaştırmak gereklidir. Bu işlem aşağıdaki yöntemlerden birisi ile yapılabilir:
- Uyuşmaların miktarını say(uyuşan siyahlar siyah, uyuşan beyazlar ise beyaz).
- En fazla sayıda uyuşan sınıfları ayıkla. Bu en fazla karşılıklı ilişki yaklaşımıdır.
- Uyuşmayanların miktarını say (Siyah yerde beyaz, beyaz yerde siyah olmalı). En az sayıda uyuşmayanların olduğu sınıfları ayıkla. Bu en az hata yaklaşımıdır.

Şablon Uyuşturma (Template Matching)

- Şablon uyuşturma , eğer farklılıklar sınıf içinde kalırsa iyi çalışır. Açıkça, bu örnekte karakterlerde öteleme, dönme, kırpma, çarpıklık, genişleme veya, büzülme gibi başka bozukluk olmadığı için yöntem çalışır. Yöntem bütün problemlerde çalışmamayacaktır fakat uygun olduğu zaman çok verimlidir. Aynı zamanda kullanışlı şekilde genelleştirilebilir.



Şekil 8-6: Şablon Uyuşturma

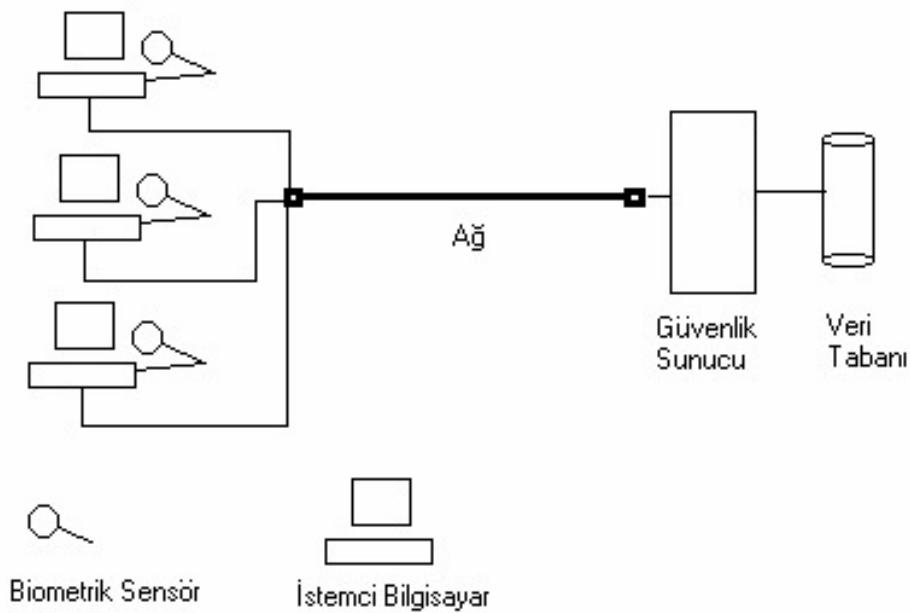
Biyometrik Sistemlerin Kuramsal Tasarım Yöntemleri

- Şimdiye kadar ki bölümlerde biyometrik yöntemlerin genel çalışma prensiplerinden öte bu tür sistemlerin çalışabilmeleri için nasıl bir fazladan donanıma ihtiyaç duyduklarını anlatıldı. Örneğin bir parmakizi tanıma sisteminde her istemci için bir CCD kamera içeren sensöre ihtiyaç vardı. Bahsedilen sensörlerin içeriklerinin farklımasına rağmen yaptıkları iş aynıdır. Bütün biyometrik sistemlerin kurulumu için istemci başına bir sensör gerekmektedir. Daha sonra buradan okutulan bilgiler tasarlanan sistemin mimarisine bağlı olarak işletilirler. Şekil 8-22'de bir biyometrik sisteme ait kuramsal çizim yer almaktadır.

Biyometrik Sistemlerin Kuramsal Tasarım Yöntemleri

Biyometrik sistemlerin tasarımı için uygulanan iki model vardır.

- On-line Model
- Off-line Model



On-line Model

- On-line model yapısında, kullanıcı okunması gereken biyometrik parametresini sisteme okutturur. Sistem almış olduğu biyometrik parametreleri eğer gerekliyse şifreleyerek ağ üzerinden güvenlik parametrelerinin tutulduğu sunucuya gönderir. Sunucu bu parametreleri veritabanı içerisindeki bilgilerle karşılaştırır. Eğer kullanıcı sisteme kayıtlı biriyse sisteme giriş izni gönderir. Kullanıcı tanımlanamadıysa sistem giriş izni vermez. Günümüzde on-line sistemler kullanılmaktadır.

On-line Model

- On-line bir sistemde önemli olan nokta biyometrik bilgileri okuyan sensörlerin sunucuya çok güvenli bir şekilde bağlanması gerekmektedir. Bunun için ya sensörler ve sunucu arasında güvenli bir yol tayin edilmelidir yada bilgiler yukarıda bahsedildiği üzere çok iyi şifrelenmiş olarak gönderilmelidir. Bilgilerin herhangi bir nedenden dolayı yetkisiz insanların eline geçmesi sistemin büyük bir zaafa uğramasına sebep olabilir. Öyleyse parametreler öyle bir şekilde şifrelenmeli ki bu parametreler bir şekilde elde edilse bile kullanılamamalılar

On-line Model

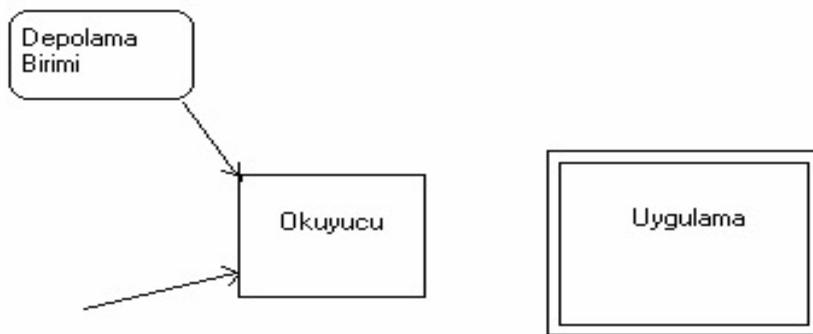


Off-line Model

- Off-line sistemlerde ,On-line sistemlerde olduğu gibi gerçek zaman bir doğrulama işlemi yapılmaz. Bunun için gerekli olan bir manyetik kart gibi aparatlar kullanmaktadır. Kullanıcıya ait olan bilgiler bu kart üzerinde tutulurlar. Kullanıcı sisteme girmek istediği zaman bu kartı kullanır. Bu tür sistemlerde güvenlik tamamen kullanıcının inisiyatifindedir. Kendisine verilmiş olan depolama aygıtını çok iyi korumak zorundadır. Tersi bir durumda sistemin güvenilirliğinden söz etmek gerçekçi olmayacağı.

Off-line Model

- Bu sebeplerden dolayı off-line bir sistem tasarlanırken güvenlik açısından üzerinde çok daha fazla düşünülmesi gereklidir.



Biyometrik Tanıma Teknikleri

Bu gün birçok biyometrik tanıma uygulaması vardır. Aşağıda bunların türleri verilmiştir.

- Parmak izi tanıma
- Optik Tanıma
- Yüz Yapısı Tanıma
- Ses Tanıma
- İmza Tanıma
- Yazma Ritmi Tanıma
- Toplardamar İzi Tanıma
- Avuç içi izi
- Kulak Şeklinden tanıma

Sonuç



Sorular



Kaynaklar

