Bilgi Sistemleri ve Güvenliği

Bilgi Güvenliğinin en temel unsurları : Gizlilik, Kullanılabilirlik, Kimlik Kanıtlama, Bütünlük, İnkar Edememe

Güvenlik Protokolleri :

Katmanlarına Göre Güvenlik Protokolleri :

Uygulama Katmanındaki güvenlik protokolleri : Kerberos, S/MIME, PGP

Ulaşım Katmanındaki Güvenlik Protokolleri : SSL, SSH, PCT, TLS

Internet Katmanındaki Güvenlik Protokolleri : IPSec, IKMP

Güvenlik Düzeyleri 6 ya ayrılabilir. Bunlar;

1. Kayıt Alanı Düzeyinde Koruma
2. Veri Kaydı Düzeyinde Koruma
3. Uygulama programı düzeyinde sorgulama/koruma
4. Bilgisayara bağlanmayı sorgulama
5. Ağ kaynaklarını koruma
6. Ağa girişi sorgulama/koruma

1 ve 2 numaralı düzeyler en sıkı korumayı sağlar ve iyi bir şifreleme ve anahtarı olmalı

3 ve 4 numaralı düzeyler birbirine benzer program girişi ve pc girişi denetimi sağlarlar.

Bir ağda korunacak varlıklar:

1. Veriler
2. Kaynaklar
3. Saygınlık

1.Sırada olan veriler güvenlik ile ilgili 3 özelliğe sahip olmalıdır.

1. Gizlilik

2. Bütünlük

3. Kullanıma Hazırlık

İnternetteki veri transferi ile ilgili güvenlik sorunları

1. Engelleme
2. Dinleme
3. Değiştirme
4. Oluşturma(Üretim)

IP Saldırıları : Land, TearDrop, Boink, Smurf, Suffer3

İşletim sistemlerine olan saldırılar exploit olarak adlandırılır

Uygulama Katmanı Saldırıları :

1. DNS, SMTP, NFS saldırıları
2. url
3. java, activex, uzaktan giriş

Sistem Güvenlik Seviyeleri :

D Seviyesi

D1 Seviyesi: En düşük güvenlik olanaklarını sunar.

Donanım elemanları için güvenlik yoktur.

Kolaylıkla ele geçirilebilir.

MS-DOS, MS-Windows 3.1/95/98 ve macos bu sınıftadır

C Seviyesi

C1 ve C2 diye iki ayrılır.

Kullanıcı için hesap tutma ve izleme yapılır.

C1 Seviyesi :

Dışarıdan gelecek saldırılar için koruma mekanizması yoktur.

UNIX ve IBM

C2 Seviyesi :

C1 seviyesine göre daha güvenlidir.

B Seviyesi

3 alt güvenlik seviyesine ayrılır

Zorunlu erişim denetimi kullanır.

Her nesnenin güvenlik seviyeleri tanımlanır.

A Seviyesi

A1 tek seviyesini içerir.

En üst güvenliği sunan seviyedir.

Donanım ve yazılım için kontrol ve doğrulama

Daha önce bahsedilen güvenlik seviyelerindeki tüm bileşenleri içerir



Wireshark: pc ye gelen paketleri yakalar. Ethernet kartı veya modem kartlarında tüm tcp/ip mesajlarını analiz eder.

Amaçları:

* Şebeke problemlerinde sorun çözme
* Güvenlik problemlerini sınamak
* Uygulamaya konan protokollerde oluşan hataları onarmak veya arındırmak
* Ağ problemlerinin içindeki bilgileri öğrenebilmek

amacıyla kullanılır.

Tutulan bilgileri kaydeder. Çeşitli kriterlerde paket arar ve filtreler.

Wireshark kullanım örnekleri : Ağ trafik tespiti, Veri madenciliği, Saldırı tespiti…

Wireshark en çok kullanılan filtreler :

Filter -> Tip = Tanım

1. IP Filtreler

ip.addr -> IPv4 adresi = Soruce (Kaynak) veya Destination (Hedef) kaynak

ip.src -> IPv4 adresi = Soruce (Kaynak) adres

ip.dst -> IPv4 adresi = Destination (Hedef) 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.versiyon -> 8 bit integer = IP versiyonu

1. Ethernet Filtreleri

eth.addr -> 6 bit mac adres = Soruce (Kaynak) veya Destination (Hedef) adres

eth.src -> 6 bit mac adres = Soruce (Kaynak) adres

eth.dst -> 16 bit integer = Destination (Hedef) adres

eth.len = uzunluk, eth.type = tip

1. TCP Filtreleri

tcp.ack -> 32 bit integer = acknowledgement(kabul,alındı) numarası

**IEEE 802.16 ve WiMAX**

IEEE 802.16 : Telsiz kentsel alan ağı standardı

ViMAX (Worldwide Interoperability for Microwave ACCess ): 802.16 standartını destekleyen uç birimlere telsiz alanda yüksek band genişliği sağlamayı amaçlayan forum standartı.

* 70 Mbps
* Kapsama alanı 50-70 km
* Veri, ses, görüntü

İletişim Türleri:

* Baz İstasyonu(BS) -> Kullanıcı İstasyonu (SS) : Downlink
* Kullanıcı İstasyonu (SS) -> Baz İstasyonu(BS) : Uplink
* Baz İstasyonu(BS) - Kullanıcı İstasyonu (SS) ları arası Tek noktadan çok noktaya PMP
* Kullanıcı istasyonları arası Ağ yapısı (Mesh)
  1. **güvenlik Standardı :**

5 kavrama dayalı bir yapı

1. Veri şifreleme
2. Anahtar Yönetimi
3. Güvenlik Birimi Oluşturulması
4. Bağlantıların güvenlik birimine iletilmesi
5. Kriptografik süreç

WiMAX Ağ(Mesh) yapısında Güvenlik

SS’ler BS olmadan birbirleriyle haberleşebilir à Mesh yapının en önemli özelliği BS’nin kapsama alanında artış olur.

Ağda bir düğüm çöktüğünde yada BS çöktüğünde tüm iletişim kesilmez .

Linux:

Linus Torvaldos 1991 de öğrenci iken buldu.

Linux Nedir:

Unix bir işletim sistemi ailesine verilen ortak bir isimdir.

Linux (resmi olarak olmasa da ), OpenBSD, FreeBSD, Irix, Solaris, Aix... çeşitli Unix türevleridir.

* Çok işlemci desteği var
* TCP/IP desteği
* Çok görevli

Neden LINUX

§Hız §Maliyet §Yaygınlık §Güvenlik §Sağlamlık

NOT \* Veri şifreleme yöntemi:DES yetersiz

NOT \* 802.16 standardındaki 2 düzeyli yapı,802.11’e göre geliştirilmeye daha elverişli bir altyapı oluşturmakta.

E-Posta Güvenliğine Yönelik Tehditler

o Gizlilik Adımındaki Eksiklik o Brute Force o Fake Mail o Phishing

o Keylogger-Trojan o Uygulama Zaafları o Sosyal Mühendislik o XSRF-CSRF-XSS

Bir malware (Zararlı Yazılım) genellikle temel olarak 2 kısımdan oluşur

Bunlar “server-sunucu” ve “client-istemci”tir.

Ağ üzerinden yapılan saldırı türleri:

**1)  İfşaat-Açığa Çıkarma (Disclosure):** mesaj içeriğinin herhangi birisine verilmesi

**2)  Trafik Analizi:** ağdaki trafik akışının analiz edilmesi.

**3)  Gerçeği Gizleme (Masquerade):** hileli bir kaynaktan ağa mesaj ekleme.

**4)  İçerik Değiştirme (Content Modification):** Ekleme, silme… ile mesajın değiştirilmesi

**5)  Sıra Değiştirme (Sequence Modification):** Ekleme, silme…sırasında değişiklik yapmak.

**6)  Zamanlamayı Değiştirme (Timing Modification):** Mesajları geciktirme, yeniden yollama.

**7)  İnkarcılık (Repudation):** gönderilen mesajın kaynak tarafından inkar edilmesi.

Şifreleme Algoritmaları

1. Simetrik şifreleme algoritmaları

Bu algoritmada şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır.

Simetrik şifrelemenin en önemli avantajlarından birisi oldukça hızlı olmasıdır.

o Kuvvetli Yönleri;  
n Algoritmalar olabildiğince hızlıdır.

n Donanımla birlikte kullanılabilir.

n Güvenlidir.

o Zayıf Yönleri;  
n Güvenli anahtar dağıtımı zordur.

n Kapasite sorunu vardır.

n Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

Simetrik algoritmalar blok şifreleme ve dizi şifreleme algoritmaları olarak ikiye ayrılmaktadır.

Blok Şifreleme Algoritmaları veriyi bloklar halinde işlemektedir.

Simetrik Şifreleme Algoritmaları - DES

DES (Data Encryption Standard) : DES yapısı itibari 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. DES, IBM tarafından geliştirilmiştir. 1975 yılında “Federal Register” tarafından yayınlanmıştır. DES 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler. DES’in en büyük dezavantajı anahtar uzunluğunun 56 bit olmasıdır.

Simetrik Şifreleme Algoritmaları – AES 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.

1. Asimetrik şifreleme algoritmaları

o Kuvvetli Yönleri;

n Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.

n Anahtarı kullanıcı belirleyebilir.

o Zayıf Yönleri;

n Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması.

n Anahtar uzunlukları bazen sorun çıkarabiliyor olması.

Asimetrik şifrelemenin kırılması simetrik şifrelemeye göre daha zordur.

----

IP Protokol Türleri

IPv4:Günümüzde kullanılmakta olan standart internet protokolüdür ve 32 bitten 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 bitten oluşan IPv6 geliştirilmiştir.

IP adresleri IANA başkanlığında RIR(Regional Internet Registry) olarak adlandırılan organizasyonlar tarafından dağıtılır.

o Tüm dünyaya IP dağıtan beş farklı RIR vardır.

§ **Kriptografi** :Bilgiyi şifreli hale dönüştürme işlemidir.

§ **Kriptoanaliz** :Bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek, şifreli mesajın açık halini elde etmeye çalışan kriptoloji disiplinidir.

§ **Sezar Şifreleme**§ Şifrelenecek metin alfabede kendinden sonra gelecek 3. harfle yer

değiştirerek oluşturulmaktadır.

§ EBCED HESABI

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

Pigpen (Mason) Şifrelemesi demek.

§ **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.

§ **PROMİS** (Dava Yönetim Sistemi)

§ Bu sistem ile; Birçok ülkenin banka sisteminin kilitlenebileceğI, Kontrollü mali krizler çıkarılabileceğI, Uluslar arası ihalelere girecek şirketlerin dinlendiği İddia edilmektedir.

§ **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.

§ **Steganografi :** Eski Yunanca'da "gizlenmiş yazı" anlamına gelen bilgiyi gizleme

bilimidir. Resim, Ses ve Video ortamlarına bilgiler gizlenebilir.

§ 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.

**1** byte **8 bit**'e eşittir

800x600 ebatında bir resimde 480.000 adet piksel bulunur.

480.000 x 3 bit = 1.440.000 bit

(gizlenecek olan veri için kalan yer) 1.440.000 bit = 175,7 KiloByte

NOT: En iyi bilinen hash fonksiyonları MD-4, MD-5 ve SHA'dır.

**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 = 32 tane

**SHA-1(Secure Hash Algorithm)**

Tek yönlü (açık anahtarlı) şifreleme tekniğidir.Verileri 160 bit

uzunluğunda özetler. Web alanında geniş kullanımı vardır. SHA-2 adı altında hazırlanmış 224, 256, 384, 512 bit uzunluğunda özetler üreten çeşitleri vardır.

**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.

**RSA Açık Anahtar Algoritması**

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 anahtarı kullanan biri herhangi bir mesajı şifreleyebilir.

**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.

**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) üstünde TCP paketleri içerisine

§ SSH (Secure Shell) üstünde TCP paketleri içerisine

**NOT**: 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 kendi içinde iki kısma ayrılır :

1. Dilbilim Steganografisi
2. Teknik Steganografisi

**Dilbilim Steganografi** : Taşıyıcı veri texttir. Veriyi gizlemek için text üzerinden değişiklikle yapılır. Bunlar Grafik Kullanılarak, textin yapısını değiştirilerek yada amacı veriyi saklamak olan yeni text yaratmak.

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 daktilo yazılarını kullanmak, resimler içinde boşluklar kullanmak vb.

**Teknik Steganografi :**

Teknik Steganografi bir çok konuyu içine almaktadır.

Bunları bazı başlıklar altında toplayabiliriz;

1. Görünmez mürekkep: Geleneksel haline gelmiş olan görünmez mürekkeple yazma yöntemidir.
2. Gizli yerler: Kimsenin göremeyeceği gizli yerlere saklama (bavul, kasa vb.)
3. Microdot’lar: Bilgiyi noktalar halinde sayfaya gizleme
4. Bilgisayar tabanlı yöntemler: Text, ses, görüntü, resim

dosyalarını kullanarak veri gizleme yöntemleridir.

**Metin Steganografi**

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

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 de kendi içerisinde 5 farklı uygulama tipine sahiptir.

§ Cümle içi boşluk bırakma § Satır kaydırma  
§ Satır sonu boşluk bırakma § Sağ hizalama

§ Gelecek kodlaması

**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.

Yani iki kelime arasına eklenen boşluğa veri girilir.

**Satır Kaydırma Kodlaması**

§Bu yöntemde text satırları düşey olarak kaydırılarak gömülecek mesajın kodlanması sağlanır.

§Gömülmüş kelime yine text dosyası yada bitmap dosya olarak açılabilir.

Yani iki satır arasında olan boşluğa veri eklenir

**Satır Sonu Boşluk Bırakma**

§Satır sonu boşluğu yöntemi, her satırın sonundaki boşluktan faydalanır.

§Veri, tüm satır sonlarında 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.

**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.

§ 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.

**Gelecek Kodlaması**

§Bu yöntemde, b, d, T gibi harflerin yatay/düşey uzunlukları gibi bazı metin özelliklerini değiştirerek, biçimlendirilmiş metin içine gizli mesajları saklamayla ilgilenir.

§Bu yöntem, her biçimlenmiş metnin, gizli mesaj saklamak için kullanılabilecek çok sayıda özelliği olmasından dolayı, uzak ara durdurulması en zor yöntemdir.

1. Yazımsal Yöntemler: Cümle içine ekstradan bir virgül vs konarak veri gizlenir.
2. Anlamsal Yöntemler: W.Bender tarafından bulunmuştur. Eş anlamlı kelimelerle gizlenir.

**Görüntü Steganografi**

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

En önemsiz bite ekleme

§ 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 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 bitlik görüntüler pixel başına 1 byte kullanmaktadırlar.

§ 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)

§ 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 olacak ve renk üzerinde gözle görülecek değişikliğe neden olmayacaktır.

Maskeleme ve filtreleme

§ Maskeleme ve filtreleme 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

§ 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.

Hem sıkıştırma hemde bilgi gizleme işlemlerini yapan

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

**Ses Steganografi**

İnsan işitme sistemi (Human auditory system-HAS) aralığı yüzünden, ses sinyalleri içerisine 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 sinyalleri üzerinde uğraşırken ses dosyalarının hangi karakteristiklere sahip olduklarını 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 AIIF(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.

**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 çalıştırmak (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.

**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.

**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.

Rootkitin girdiği bilgisayarınız tamamen dışarıdan kontrol edilebilir hale gelecektir.

Kusursuz bilgi vermek. §“yanlış pozitif” §“yanlış negatif”

Anomali Modeli:

§Beklenmeyen davranışın olası bir sızmanın kanıtı olacağı varsayımı kullanılır.

Üç çeşit istatiksel yöntem tanımlanmıştır

§Eşik metriği §İstatiksel momentler §Markov modelleri

Sızma Belirleme Sistemlerinin Örgütlenmesi

Üç temel yaklaşım var  
§ Ağ Trafiğini İzlemek § Konakları ve Ağları Birlikte İzlemek § Özerk Aracılar Kullanmak

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 durduran 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 sınırlandırmak olarak ikiye ayrılabilir.

§Pasif izleme, basitçe saldırgan davranışlarının kaydedilmesidir. Saldırgan davranışları hakkında bilgi verir.

§Erişimi sınırlandırmak, saldırganın amacına ulaşmasını engellerken, ona en küçük alanı vermektir.

§ 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 sistemye tüm erişimini kesmektir. (Ağ kablosunu çıkarmak?)

§  Sık kullanılan bir yaklaşım örtülerle olası hedeflerin etrafını sarmaktır. Örtüler çoğunlukla işletim sisteminin çekirdeğine gömülür. §  Güvenlik duvarları saldırganın 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 (Thumprinting)  
§ Olabildiğince az yer kaplamalı.  
§ İki bağlantının içeriği farklıysa farklı izleri olmalı. § İletişim hatalarından etkilenmemeli.  
§ Toplanabilir olmalı.  
§ Hesaplaması ve karşılaştırması ucuz olmalı.

§ 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.

§Karşı saldırı yasal ya da teknik olabilir.

§Yasal saldırı uzun zaman gerektirir. Kanunlar yerli yerinde değil ve oldukça karışık. Ayrıcı yabancı ülkelerden saldırı gelirse uluslararası kanunlar yetersiz.

§Teknik saldırı masumlara zarar verebilir. Saldırganlar masum bir ağı ele geçirdikten sonra orayı üs olarak kullanmış olabilirler.

§Kendi ağımızdaki haberleşmeye zarar verebilir.  
§Paylaşılan bir ağın her ne sebeple olursa olsun saldırı için

kullanılması etik değil.  
§Karşı saldırı da saldırı gibi dava edilebilir.

**Worms – Solucanlar** : Ağ üzerinden pc sızıp zarar veren virüs.

**Trojen Horses – Truva Atları** : Bir program ile pc girip arka planda çalışıp pc oldukça zorlar.

**Backdoors – Arka Kapılar** : Sisteme sızabilmesi için açık oluşturur. Port açarak sızma yapar.

**Browser Hijacking – Tarayıcı ele geçirme** : Sitelere sızıp kendi reklamlarını vs artırmak, bilgi artır

**Spyware – Casus** : İnternette girdiğiniz siteleri vs bilgileri alıp üreticisine gönderir.

**Phishing - Oltalama**: Genelde kart şifresi veya kredi kart bilgilerini ele geçirmek için kullanılır. Sahte mail vs gönderilerek kişiyi sahte web sitelerine yönlendirip bilgileri girmelerini sağlar ve bilgileri çalarlar.

**Sniffer – Koklayıcı** : Ağ üzerineki veri paketini yakalayıp içeriğini okurlar. Ağdaki hareketleri izler alır vs. Şifreler, ağ yetkisi vs ele geçirilir.

**Spoofer – Kandırıcı** :IP sahteciliği. Herhangi bir ip üzerinden TCP/IP paketleri gönderebilme işlemidir. İp sahteciliği edip gizlenme veya istediği kişi gibi görünebilme.

**Password Cracker – Şifre Kırıcılar** : atm, net, web vs ortamlarda şifreleri tüm olasılıkları deneyerek kırma yöntemi. Şifreleri tekrar tekrar deneyip bulmak.

Adli Bilişim Alanları :

* Veri Kurtarma
* Veri İmha Etme
* Veri Saklama
* Gizlenmiş Dosya Bulma
* Şifreleme (Kriptografi)
* Şifre Çözme
* Veri Dönüştürme

NOT : Snort saldırı tespit sistemidir