Bilgi Çağında Savaş

Abdullah Atalar
Bilkent Üniversitesi

AFCEA
12 Şubat 1998

Konuşma Planı

- Bilgi emniyeti
- Temel kavramlar
- Kullanılan silahlar
- Saldırı örnekleri
- Alınabilecek tedbirler

Bilginin Kıymetli Olduğu Yerler

- Bankalar, finans kuruluşları
- Bakanlıklar, üniversiteler
- Haberleşme sistemleri
- Ulaşım sistemleri (hava trafik, tren, metro)
- Askeri sistemler

"Bilgi emniyeti" ne demek?

- Döküman, istatistik, patentlenmemiş bir fikir, veya ticari sır gibi bir bilginin gizli tutulabilmesi
- Bir sistemi çalıştıran yazılımın beklenen fonksiyonu her zaman yapabilmesi ve güvenli olması

Bilgi Emniyetinin Önemli Olduğu Sistemler (1)

- Tek kullanıcılı masa üstü bilgisayarlar
- Çok kullanıcılı genel amaçlı bilgisayar sistemleri
- Bilgisayarla kontrol edilen telefon santralı gibi haberleşme sistemleri
- Elektrik enerji veya hava trafik kontrol merkezi gibi hayati öneme sahip sistemler

Bilgi Emniyetinin Önemli Olduğu Sistemler (2)

- Bilgisayarla kontrol edilen uçak, gemi gibi taşıtlar
- Bilgisayar kontrollü silah sistemleri

Tehlikeler

- Bilginin çalınması
- Bilginin değiştirilmesi
- Bilginin yokedilmesi
- Sistemin fonksiyonunu yapmaması
- Sistemin istenmeyen şeyler yapması

Temel Kavramlar

Bilgi emniyeti bilgisayarlarda nasıl sağlanır?

- Şifreleme
- Hiyerarşik erişim hakları
- Yedekleme
- Yazılım güvenliği

Basit Şifreleme Metodları (1)

- Sezar şifresi (anahtar bir sayı)

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

Anahtar sayı = 3

d e f g h i j k l m n o p q r s t u v w x y z a b c

Bütün olasılıklar denenerek kolayca kırılabilir

Basit Şifreleme Metodları (2)

- Vigenere (tekrarlanan anahtar) şifresi

l o n d o n c a l l i n g m o s c o w
v i g e n e r e v i g e n e r e v i g
22 9 7 5 14 5 18 5 22 9 7 5 14 5 18 5 22 9 7
h x u i c s u f h u p s u r g x y w d

Kırmak için: A. Sinkov, *Elementary Cryptanalysis*. Math. Assoc. Am. 1966.

Basit Şifreleme Metodları (3)

- Agustus şifresi

l	o	n	d	o	n	c	a	l	l	i	n	g	m	o	s	c	o		
t	o	b	e	o	r	n	o	t	t	o	b	e	t	h	a	t	i		
20	15	2	5	15	18	14	15	20	20	15	2	5	20	8	1	20	9		
f	d	p	i	d	f	q	p	f	f	x	p	l	g	w	t	w	x		

e 13 t 9.0 o 8.2 a 7.8 n 7.3 i 6.8 r 6.6 s 6.5 h 5.9
d 4.1 l 3.6 c 2.9 f 2.9 u 2.8 m 2.6 p 2.2 y 1.5 w 1.5
g 1.4 b 1.3 v 1.0 k 0.4 x 0.3 j 0.2 q 0.1 z 0.1 z 0.00
th he an in er re es on ea ti the and tha ent ion tio for nde

Basit Şifreleme Metodları (4)

- Vernam şifresi. Şifrelenecek kayıt uzunluğunda bir anahtar lazım.

Anahtarın rasgele olması ve gizli olarak daha evvelden taşınması gerekir.

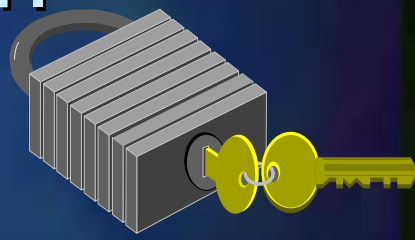
Eğer anahtar bir kere kullanılırsa teorik olarak kırmak imkansız.

L O N D O N C A L L I N G

01011 01110 01101 00011 01110 01101 00010 00000 01011 01011 01000 01101 00110
01001 10010 11101 01110 00100 01010 00110 01001 10110 11101 00010 01011 01001
00010 11100 10000 01101 01010 00111 00100 01001 11101 10110 01010 00110 01111

DES (Data Encription Standard)

- Açık ve simetrik bir algoritma
- 64 bitlik blokları 56 bitlik bir anahtarla şifreler. Aynı anahtarla deşifrelenir.



ftp.uu.net:bsd-sources/usr.bin/des/

Cryptography: An Introduction to Computer Security, Seberry and Pieprzyk, Prentice Hall Australia. (İçinde C programı var)

Birkaç milyon dolarlık bir bilgisayarla birkaç saatte kırılabilir.

Modern Kriptolama

- Aleni anahtar (D) + gizli anahtar (E)

Orijinal (T), şifrelenmiş (C)

C = T^E mod N

T = C^D mod N

M. Hellman, *The mathematics of public key cryptography. Scientific American*, 130-139, 1979.

PGP (Pretty good privacy)

- Açık ve asimetrik bir algoritma. Aleni ve gizli anahtar
- İki kere kullanılırsa gizliliği ve imzalamayı sağlar
- Büyük sayıların asal çarpanlarına ayırmanın zor olduğu prensibine dayanır

Birçok şifre kolay kırılabiliyor

- Accessdata

  (87 East 600 South, Orem, UT 84058)

WordPerfect, Lotus 1-2-3, Quatro-Pro, MS Excel ve Paradox'la şifrelenmiş fakat anahtarı kaybolmuş dosyaları açan bir paket satıyor: $185.

Eğer parola 10 karakterden azsa bedava demo paketi kullanılabilir.

Hiyerarşik Erişim Hakları

UNIX, Windows-NT gibi çok kullanıcılı işletim sistemlerinde

- Süper kullanıcı: bütün erişim haklarına sahip
- Grup hakları: grubun sahip olduğu hakları kullanabilir
- Normal kullanıcı: sadece kendine ait veya genel kullanıma açık dosyalara girebilir

UNIX Şifre Komutu

- UNIX **`crypt`** komutu Amerika dışına satılan bilgisayarlara konmuyor.
- Bu komutla şifrelenmiş bir şifreli kütük kırılabilir mi?

  cbw (Crypt Breakers Workbench) isimli programı kullanarak, hemen.

  ftp.uu.net:usenet/comp.sources.unix/volume10/cbw/

Şifre Kırma Zamanları

Saldirgan tipi	Bütçe (dolar)	Araç	40-bitlik anahtari kirmak için gerekli zaman	Emniyet için gerekli anahtar uzunlugu
Yalniz saldirgan	0	Çalinmis bilgisayar zamani	1 hafta	45
	400	FPGA	5 saat	50
Küçük sirket	10,000	FPGA	12 dakika	55
Orta büyüklükte sirket	300,000	ASIC	20 saniye	60
Büyük sirket	10Milyon	ASIC	0.02 saniye	70
Devlet	300 Milyon	ASIC	0.0005 saniye	75

Bilgi emniyeti için yedekleme

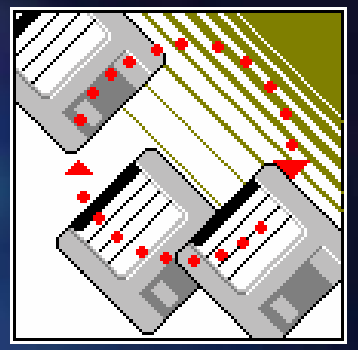
- Bilgilere saldırı olduğunda orijinale dönebilmek için gerekli
- 0. gün yedeklemesi, dışarıdan saldırı gelme ihtimali olmadan önce yapılmalı
- Uzun zaman saklanmalı

Yazılım Güvenliği

- Kullanılan işletim sisteminin ve uygulama yazılımlarının bilgi güvenliği açısından sağlamlığı

KULLANILAN SİLAHLAR

Bilgisayar Virüsleri (1)



- Başka bir programın içine kopyalanmış bir program parçası.
- Ancak o program çalıştırılırsa virüs harekete geçer.
- Kendini başka programlara kopyalar ve yayılır.

ATT'nin telefon santralı bilgisayarları 15 Ocak 1990'da bir virüs yüzünden kapanmıştı.

Bilgisayar Virüsleri (2)

- Virüs tarama programları yoluyla tesbit edilebilir.
- Bilinen virüslerin kod parçalarını kütüklerde arayarak bulur.

Bilgisayar Solucanı (worm)

- Yalnız başına bir program
- Bilgisayar ağları üzerinden başka bilgisayarlara atlayarak çoğalır
- Sistemin kaynaklarını harcayıp performansı düşürebilir. Daha önemli hasarlar da yapabilir.

Kasım 1988'de bir bilgisayar solucanı Internet yoluyla 60,000 bilgisayara yayıldı.

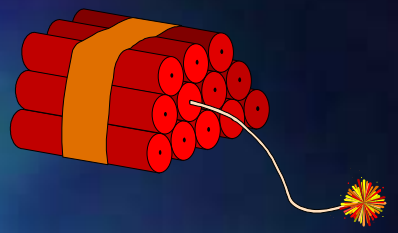
Truva Atı

- Bir başka programın içine saklanmış program parçası. Gizli bir fonksiyonu yerine getirir. Kullanıcının erişim haklarını kullanır.

Örnek: Sisteme girişte parolayı soran komutları taklit eden bir yazılım.

UNIX sistemindeki emniyet boşluklarını bulan SATAN isimli bedava bir programın içine bir Truva atı kolayca yerleştirilebilir: Boşlukları e-posta ile istediğine yollayabilir.

Mantık Bombası



- Bir programın içine yerleştirilmiş ve önceden programlanmış durum ve şartlarda çalışmaya başlayan program parçası.
- Genellikle programı yazanlar tarafından içine konur.
- Mantık bombasının ateşlenmesi dışarıdan da yapılabilir.

Tuzak Kapısı (arka kapı)

Programı yazanlar tarafından içine konmuş,

normal emniyet mekanizmalarını kısa devre yapan ve

bunu bilenlerin sistemin içine kolayca girmesini sağlayan program parçaları.

Tuzak Kapısı (örnek)

- Windows NT sisteminin süper kullanıcı anahtarını kaybederseniz
- Microsoft' göre diskleri formatlayıp sistemi tekrar yüklemekten başka çare yoktur.
- Oysa birkaç firma bu durumlarda size yardım edebiliyor!
- Winternals Software: NT Locksmith
- Mirider: NT Access

Tuzak Kapısı Bırakma Sebepleri

- Yazılım bakımında kolaylık
- Lisans şartlarına uygunluğu sağlamak
- Yanlışlıkla
- Kötü niyet

Tuzak Kapısı Tesbit Edilebilir mi?

- Yazılımın source kodunu inceleyerek, evet.
- Source kodu bulunmayan bir sistem için pratik bir yol yok.

Parola Kırmak

- Tipik parolalar: Eşlerin, çocukların isimleri, plaka numaraları, doğum tarihleri gibi tahmin edilmesi kolay parolalar.
- Şifrelenmiş parola dosyasını eline geçiren bir kişi parola kırma programları kullanarak zayıf parolaları kırabilir.

Parola Örnekleri

Örnek kötü bir parola: **`tneuqole5`**

Parola kırma programları sözlükte bulunan bütün kelimeleri, onların tersten yazılmışlarını, sonuna veya başına bir sayı getirilmişlerini deneyerek birçok parolayı kırabilir.

Örnek iyi bir parola: **`4G&tt(:Wb_ %C`**

Parola Koklamak (sniffing)

- Bilgisayar ağından geçen paketler incelenirse bir terminalde girilen parolalar öğrenilebilir.
- telnet veya ftp yapıldığında parolanız ağa bağlı biri tarafından gözlenebilir.
- UNIX X-windows sistemiyle çalışan bir sistemde bir kullanıcının ekranı başka bir kullanıcı tarafından gözlenebilir.

Parola Koklamak (sniffing)

- Eğer şifreli paket sistemi kullanılırsa önlenebilir
- telnet ve ftp gibi işlemleri kritik bilgiler içeren hesaplar için yapmamak gerekir
- UNIX'de uygun önlemler alarak ekranların başkaları tarafından görülmesini önlemek mümkündür

İçeriden Tehditler (1)

- Bilgisiz kullanıcılar:

Giriş haklarını doğru ayarlamadıkları için başkaları bilgilere problemsiz erişebilir.

- Bilgisiz sistem yöneticileri:

İşlerini kolaylaştırmak için bazı kurallara uymayabilirler.

Örnekler: NFS, güvenilir bilgisayar listeleri

İçeriden Tehditler (2)

- Kırılmış veya elegeçmiş parolalar. Giriş hakkı olmayan kişiler girme hakkı elde eder.
- Art niyeti olmadığı halde açık kapısı olan sisteme yüklü yazılımlar. Bunların zayıf noktaları kullanılarak girme hakkı sağlanabilir.

Netscape, Internet Explorer http://www.nlc.net.au/~john/

İçeriden Tehditler (3)

- Sisteme daha önceden yüklenmiş art niyetli programlar. Bunların yardımıyla erişim hakları elde edilebilir.
- Çok kullanıcılı sistemlerde artık kullanılmayan bellek bölgelerini tarayan programlar. Bir başka kullanıcının bellekte bıraktığı bilgilere ulaşılabilir.

İçeriden Tehditler (4)

- Artık kullanılmayan disk bölgelerini tarayan programlar.

Başka bir kullanıcı tarafından kullanılan disk bölgesi silindiğinde aslında bilgilerin hepsi silinmez

Erase Unerase

Dışarıdan Tehditler

- NFS, NIS gibi servislerin zayıf tarafları
- sendmail gibi e-posta programlarının zayıflıkları

Sisteme dışarıdan gelen bir e-posta süper kullanıcının erişim haklarıyla çalışan bir kod çalıştırabilir.

IP Numarası Kandırmacası

- Internet'e bağlı her bilgisayarın bir numarası vardır.
- Bir saldırgan kendi bilgisayarının numarası yerine başka bir bilgisayarın numarasını kullanabilir.
- Sanki yerel ağ içerisindeymiş gibi davranıp erişim hakları elde edebilir.

Bilgisayar Servislerine Saldırı

- E-posta bombardımanı.
- Bir bilgisayar, saldırganın yazdığı bir program vasıtası ile bir başka bilgisayara çok sayıda e-posta yollayabilir.
- Bombardımana tutulan bir bilgisayar normal çalışmasını yapamaz. Diski sonuna kadar dolabilir.

Bilgisayar Ağı

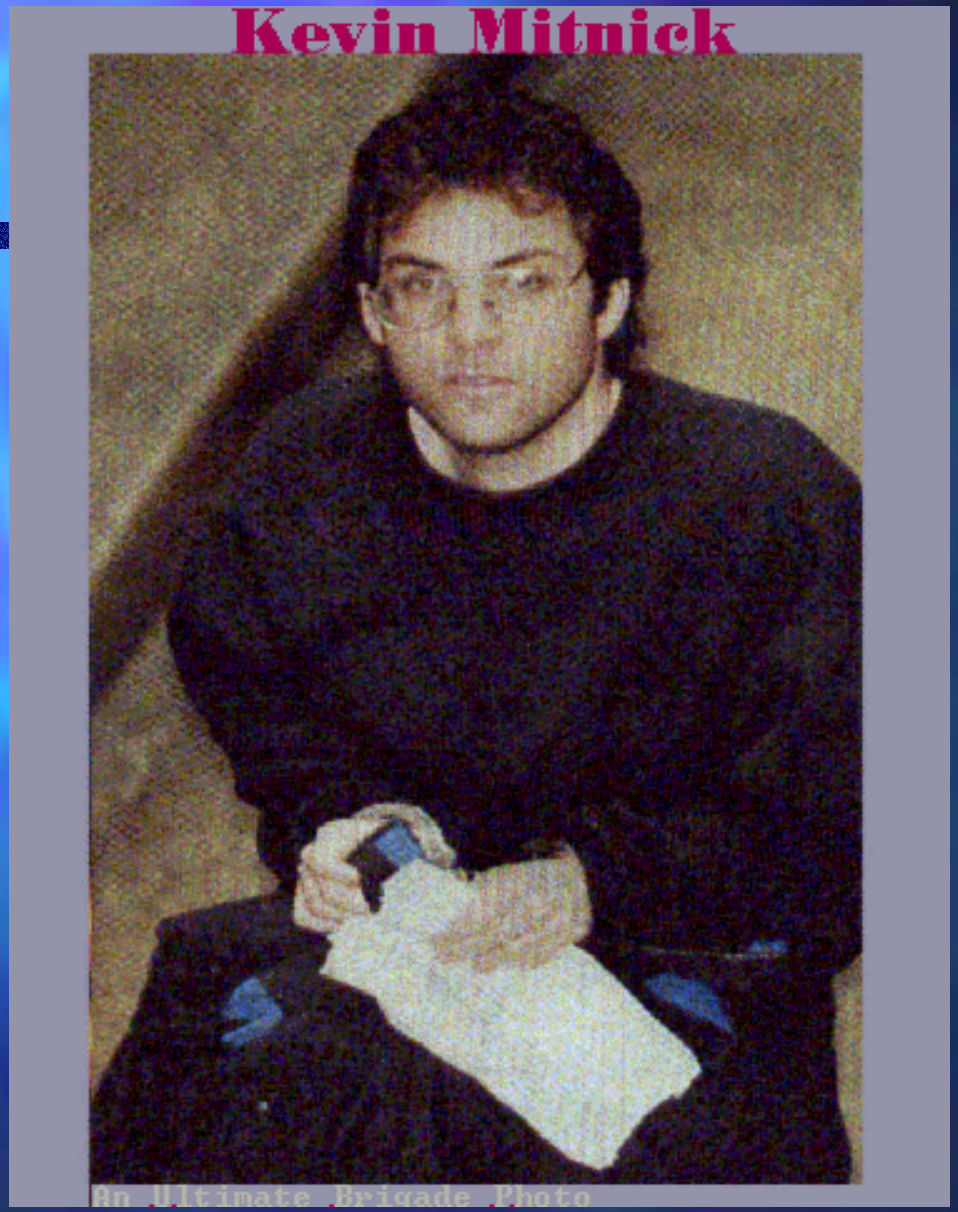
- Router, gateway gibi cihazlar da aslında birer bilgisayardır.
- Ağ güvenliği açısından en önemli cihazlardır.
- Genellikle bunların parolaları ya hiç olmaz ya da satıcısından geldiği gibi bırakılır!

Bilkent'teki routerların parolası neydi acaba?

Kriptoanaliz Metodları

- Kaba kuvvet: Bütün anahtar olasılıklarını denemek
- Şifrelenmemiş mesajın bir kısmını elde ederek veya tahmin ederek şifreyi kırmaya çalışmak
- Değişik mesajları aynı anahtarla şifreleyerek şifreleme metodunu bulmaya çalışmak
- Differansiyel kriptoanaliz: İstatistik dengesizlikleri kullanarak anahtarı kırmaya çalışmak (kappa testi)

SALDIRI ÖRNEKLERİ


Kevin Mitnick
An Ultimate Brigade Photo

Kevin Mitnick'in Saldırısına Uğrayan Bilgisayar Sistemleri (1)

- 1980 - US Leasing (kiralama)
- 1982 - University of Southern California
- 1984 - TRW (elektronik donanım)
- 1984 - Pacific Bell (telefon şirketi)

  İstediği numarayı evine bağlayabiliyor, para ödemeden konuşabiliyor, istediği hattı dinleyebiliyordu.
- 1985 - National Security Agency
- 1987 - Santa Cruz Operations (yazılım)

Kevin Mitnick'in Saldırısına Uğrayan Bilgisayar Sistemleri (2)

- 1988 - Jet Propulsion Lab (uzay araş.)
- 1988 - DEC (bilgisayar şirketi)
- 1994 - California Dept. of Motor Vehicles (sürücü ehliyeti veren kurum)
- 1994 - Netcom (kredi kartı sistemi)
- 1994 - Tsutomu Shimomura (dünyanın en usta bilgisayar güvenliği uzmanlarından)

Roma Laboratuvar'ına Saldırı

- 1994 Mart ve Nisan
- İngiltere'den saldırı: 150 kere girilmiş
- İzini kaybettirmek için Güney Amerika üzerinden dolaşmış
- Önemli bilgilerin kopyalarını almış
- NASA ve Wright-Patterson Air Force Base bilgisayarlarına atlamış

Naval Research Lab'a Saldırı

- 1995 ve 1996
- Arjantin'den saldırı
- Önce bir üniversite bilgisayarına giriyor
- Oradan Naval Research Lab'a
- Oradan NASA'ya
- Oradan Los Alamos Research Lab'a giriyor

Microsoft'tan Bir Örnek

- Microsoft'un Seattle'daki sistemlerine giren saldırganlar Windows NT'nin source kodlarını çalarak Internet'te yayınladılar.

Microsoft utandığı için böyle bir olayın varlığını inkar etti.

Bilkent'ten Bir Örnek

- Orta Okulun bilgisayarına girerek giriş WEB sayfasına yanan bir Türk bayrağı kondu.
- Bilgisayarın şifresi çok basitti.
- Giren saldırganın IP numarasından Yunanistan'dan kaynaklandığı bulundu.
- Şifre değiştirildi.

Bilkent'ten Bir Başka Örnek

- XX bölümünün hocaları sınav sorularını UNIX in zayıf noktaları olduğunu bildikleri için sistemde saklamazlar.
- Kendi PC'lerinde hazırladıkları soruları ağ yazıcısından bastırmak için UNIX'e bir anlık kopyalayıp bastırdıktan sonra kütüğü hemen silerler.

Örnek (devam)

- XX Bölümü ikinci sınıf öğrencisi sınav sorularını bulmak için saldırı yapar.
- Parola koklayarak bir kullanıcının hesabına girer.
- Süper kullanıcının parolasını kırmak için *elm* programının bir açık kapısını kullanır.

Örnek (devam)

- Hocaların hesaplarına konan yeni kütüklerin anında bir kopyasını kendi hesabına yapan bir program yazar.
- Devamlı çalışan bu programın ismini dikkat çekmemek için *sendmail* koyar.
- İzini kaybettirmek için başka bölümdeki bir hocanın zayıf parolasını parola kırma programı ile kırar.

Örnek (devam)

- Gece geç saatlerde modemle o hocanın hesabını kullanarak sisteme girip avını kontrol eder.
- Her girişte iz bırakmamak için sistemdeki *log*'ları silen bir program kullanır.
- UNIX'in normal log'larının dışında da log tutulduğu için farkına varılır.

Örnek (devam)

- Tuzaklar hazırlanır. Girince neler yaptığı anlaşılır.
- Ancak iç hat modemle girdiği için izini kaybettirir. (Eski santralın log özelliği yoktu.)
- İkinci sınıf öğrencilerinden UNIX'i iyi bilenler izlemeye alınır.

Örnek (devam)

- Bunlardan modemle girmeyi bilen, notları iyi olmayan ve sabıkalı bir öğrenciden şüphelenilir.
- Birisinin bölüm bilgisayarlarına saldırı yaptığı bilgisi kendine duyurulur.
- O gece saldırı hesabı sistemden silinir.
- Şüpheli öğrenci aynı gece İstanbul yolunda otobüstedir...

Tipik saldırı stratejileri

- İz kaybettirmek için bilgisayardan bilgisayara hoplamak
- Bu bilgisayarlarda daha evvelden kırdıkları parolalarla masum kullanıcıların hesaplarını kullanmak

ALINABİLECEK TEDBİRLER

Bilgi emniyeti/ kullanım kolaylığı

- Bilgi emniyetini artırmak için kullanım kolaylıklarını azaltmak lazım
- Kullanım kolaylığı ve açıklığın çok olması gereken yerlerde bilgi emniyeti sağlamak zor

Genel Tedbirler (1)

- Bilgi güvenliğinden sorumlu personel
- Ayrılan personelin hesabını kapatmak
- Parolaları kuralına uygun seçmek ve seçtirmek
- Ağa bağlı bütün bilgisayarlara erişim ve kontrol hakkına sahip olmak
- Güvenilmeyecek yazılımları kullanmamak

Genel Tedbirler (2)

- Sistemdeki standart ve ek *log* ları sık sık kontrol etmek
- Anlam verilemeyen şeyleri sebebi bulununcaya kadar incelemek
- Kullanım kolaylığı sağlayan ancak bilgi güvenliğini tehlikeye atan yöntemlerden kaçınmak

Genel Tedbirler (3)

- Detay gibi görünen şeylere dikkat etmek
- Önemli bilgi kütüklerinin 0. gün yedeğini alarak zaman zaman karşılaştırmak
- Bilgi güvenliği ile ilgili son gelişmeleri takip edip en son güvenlik *yama* larını kullanmak

Genel Tedbirler (4)

- Bilgi güvenliği konusunda kullanıcıları eğitmek
- Bu konuda uzman danışmanlar kullanmak
- Saldırganlara karşı caydırıcı kanuni ve disiplin tedbirlerini almak

Fiziksel Tedbirler

- Sisteme yetkisi olmayan kişilerin ulaşmasını önlemek
- Fiziksel girişlerin log'unu tutmak (girişlerde kartlı sistem kullanmak)
- Video kameralarıyla terminalleri kayıt altında tutmak
- Ağ kablolarının güvenliğini sağlamak

Yazılım Tedbirleri (1)

- Parolaları sık sık değiştirmek ve kullanıcıların da değiştirmesini zorlamak
- Sisteme elektronik giriş çıkışı (ağ bağlantısı) tek kapıdan yapmak
- Standart log tutan nöbetçilere ek olarak hiç kimsenin bilmediği yerlere nöbetçiler koyup ek log'lar tutturmak

Yazılım Tedbirleri (2)

- Saldırganların kullandığı parola kırma programlarını kullanarak parolaları test etmek
- Saldırganlar için tuzaklar hazırlamak

  sahte parola dosyası
- Bilgileri şifrelemek: Triple-DES, IDEA, RC2, RC4, PGP

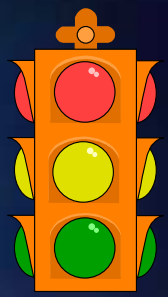
Yazılım/Donanım Tedbirleri

- Elektronik girişte geçilen kapı sayısını ve kontrol noktalarını artırmak
- Bir seferlik parola sistemini kullanmak (kullanıcılara verilen ufak akıllı kartlar parola üretiyor)
- Yangın duvarı kullanmak

Yangın Duvarı (Firewall)

- Yangının genişlemesini önleyen yangına dayanıklı duvar
- Yerel ağa Internet'ten, Internet'e de yerel ağdan erişimi sınırlayan donanım ve yazılım
- Büyük bir organizasyonda yerel ağları da birbirinden ayırabilir

Yangın Duvarı (Firewall)



- Trafik kontrol noktası: Burada herkes durdurulup kontrol ediliyor
- Paket filtrelemesi yapılıyor
- NFS, NIS gibi istekler kesin reddediliyor
- IP numarası kandırmacası önlenebilir

Yangın Duvarı (Firewall)

- ftp gibi istekler özel bir bilgisayara (proxy) yönlendiriliyor
- telnet de reddedilebilir
- Trafiğin log'u tutuluyor
- Yangın duvarı yazılımının güvenli olup olmadığı?...

Garantili Bilgi Güvenliği (1)

Bir bilgisayara fiziksel olarak dışardan ulaşabilmek için donanım (ethernet, RF girişi veya modem bağlantısı) varsa,

yazılım üreticisine tam güveniniz yoksa,

kullanılan işletim sistemin ve/veya diğer yazılımların source kodu yoksa,

bu bilgisayardaki bilgi güvenliği garanti edilemez!

Garantili Bilgi Güvenliği (2)

Kesin güvenliği sağlamak için en emin yol fiziksel bağlantıları kesmek (birçok kullanım kolaylığından vazgeçerek).

Bazı sistemlerde bu imkansız:

- Telefon santralı
- Askeri bir sayısal haberleşme sistemi

Garantili Bilgi Güvenliği (3)

- Kritik sistemleri ağa **hiç** bağlamamak (bu birçok durumda kabul edilemez olabilir)
- Kritik sistemler için yazılımların *source* koduna sahip olmak

SONUÇ

- Bilgisayarlarda bilgi güvenliği konusunda bilinçli, eğitimli ve uyanık olmak,
- Herşeyi kuralıyla yapmak,
- Konuya gereken önemi vermek,

şart.

- Bilgi savaşında güvenliği sağlamak zor ama **imkansız değil**.

Referans Kitaplar

- *Practical UNIX Security*, Simson Garfinkel, Gene Spafford
- *PGP: Pretty Good Privacy*, Simson Garfinkel
- *Internet Security Firewalls*, D. Brent Chapman, Elizabeth D. Zwicky

Referans Kitaplar

- *Computer Security Basics*, Deborah Russell, G. T. Gangemi
- *Computer Crime: A Crimefighter's Handbook*, David Icove, Karl Seger, William Von Storch
- *Firewalls and Internet Security*, W.R. Cheswick, S.M. Bellovin