CSE 101
Slide Set 15

Doç. Dr. Mehmet Göktürk

Department of Computer Engineering

1

Elektronik Güvenlik

A- İletişim güvenliği

B- Bilgisayar Güvenliği

1. Bilgiye yalnızca yetkili kişilerin erişmesini sağlamak
2. Yetkisi olmayan kişilerin veriler üzerinde, yaratma, değiştirme ve silme işlemleri yapmasını engellemek
3. Yetkili kullanıcıların verilere erişmesinde problem yaratmamak
4. Kaynakların doğru ve yerli yerinde kullanılmasını sağlamak

2

Güvenlik Bileşenleri

- **Fiziksel Güvenlik:** Kilitler, kapılar, yaka kartları, giriş kontrol sistemleri.
- **Çalışan Güvenliği:** Çalışanların güvenlik soruşturması, şahıs güvenlik belgeleri.
- **İdari Güvenlik:** Güvenliğinde zayıf noktaların bulunup bulunmadığı süreçler.
- **Veri Güvenliği:** Gizli verilerin çoğaltılmasının engellenmesi.
- **Online Güvenlik:** Online verilere erişimin kontrol altında tutulması.

3

Güvenlik Riskleri

- **Yetkisiz Erişim:** Bu risk yetkisi olman bir kişi bilgisayar sistemine erişim hakkı kazanması riskidir. Ya da sistemi sadece belirli bir iş amacıyla kullanma hakkı olan bir kişi, hakkı olmayan biçimde sistemi kullanmaya çalışabilir.
- **Yerleşme:** Sisteme saldıran bir saldırgan, daha sonra saldırılarda bulunabilmek amacıyla, sistemde heniz farkedilmeyen bir yapı bırakabilir. (Truva atları bu gruba girer)
- **İletişim Dinleme:** Saldırgan, hedef bilgisayara girmeden de hedef bilgisayar hakkında iletişimleri dinlemek yoluyla, yetkisi olmadığı bilgilere erişebilir.
- **Kandırma:** Saldırgan, iletişim süreci sırasında verilerle oynayarak, gizli bilgilere yetkisi varmış gibi ulaşabilir. Örneğin, sokakta korsan bir bankamatik inşa ederek kişilerin ATM şifrelerinin toplandığı görülmüştür.
- **Hizmetin Reddedilmesi:** Saldırgan, yetkili olan normal kullanıcıların sisteme erişimini engeller.
- **İnkar:** Elektronik bir işlem sonucunda saldırgan işlemi yaptığını (ya da yapmadığını) inkar eder. (Kredi kartı ile online alışveriş yaptıktan sonra inkar edebilir).

4

Temel Güvenlik Önlemleri

- **Tanıma Servisleri:** Bu servisler kimlik doğrulama görevini yerine getirirler. Erişim yapanın yetkilendirilme amacıyla tanınması ya da eldeki verinin sahibinin doğrulanması olarak iki ana alt grupta incelenir.
- **Erişim Servisleri:** Bu servisler kaynakların yetkisiz erişime karşı korunlmalarını sağlar.
- **Gizlilik Servisleri:** Bu servisler, gizli kalması gereken bilgilerin, yetkisi olmayan ellere geçmesini engelleyen servislerdir.
- **Veri Bütünlüğü Servisleri:** Veriler üzerinde değişiklik yapılmasını engellemek amacıyla oluşturulmuş servislerdir. (Örneğin notunu değiştirmeye çalışan öğrenci vb)
- **İnkar Edememe Servisleri:** Bu servisler, elektronik işlemlerden sonra taraflardan birinin yapılan işlemi inkar edememesini sağlarlar.

5

Şifreleme

BUNLARI HAFIFE ALMAYALIM !!!

- Gerçek hayatta verileri korumak amacıyla geliştirilmiş pek çok güvenlik yöntemi vardır.
- Klasik yollarla tanıma ve kimlik doğrulama, uzun yıllardan beri kullanılagelmiş basit ama etkin bir yöntemdir.
- Bu klasik yöntemlerde, resimli kimlik kartları, parolalar, kilitler, anahtarlar hatta bekçiler, bekçi köpekleri kullanılabilir.
- Gizlilik ise, mühürlü zarflarla ya da gizli odalarda karşılıklı görüşerek ya da gizli iletişim hatları ile sağlanır.

6

Basit Şifreleme Yöntemi

Başlangıç parola kelimesi: **PRINCIPAL**

Formül: **C= aP + s (mod k)**

(a=katsayı, P= her karakterin rakamsal değeri,

s=doğrama katsayısı, k=alfabedeki harflerin sayısı,C=şifrelenmiş karakter)

şifrelenmiş çıktı1 (a=1, s=3 ,k=27)=> **sulqflsdo**

şifrelenmiş çıktı2 (a=2, s=4, k=27)=> **imvejvifa**

7

Şifreleme

- Bu yöntem aracılığı ile sözlükte var olan bir kelime, kolayca tahmin edilemeyen, ve tekrar aynı kelimeye geriye ulaşılmasına olanak vermeyen bir formül ile işlenir. Bu formül genellikle **mod** fonksiyonları içerir.
- Şifrelenmemiş metne İngilizce'de "plaintext", şifre sonucunda elde edilene de "ciphertext" adı verilir.

Veri tabanları örneği

8

"Anahtar" tabanlı şifreleme

- Bu sanal anahtar, aynen gerçek fiziksel anahtarda olduğu gibi, verilere yalnıza anahtar sahiplerinn erişmesini sağlar.
- Anahtarı olmayanlar verilere erişemez.
- Bu yöntemde bilgi anahtar yardımı ile kodlanmıştır.
- Ancak anahtar sahipleri, ellerinde bulunan sanal anahtar aracılığıyla sözkonusu bilgiye erişebilir

9

DES (Digital Encryption Standard)

- DES sisteminde, veri alışverişi yapmak isteyen varlıklar (insan ya da cihaz) arasında gizli bir anahtar kod üzerinde önceden anlaşılır.
- Bu anahtar yardımıyla gizli dolaşan verileri, vardıkları yerde anahtar aracılığı ile çözmek olasıdır.
- Bu yöntem, az sayıdaki kullanıcı arasında kolay ve etkin olarak kullanılabilmesine karşın günümüzün büyük firmalarında ciddi sorunları beraberinde getirebilir.

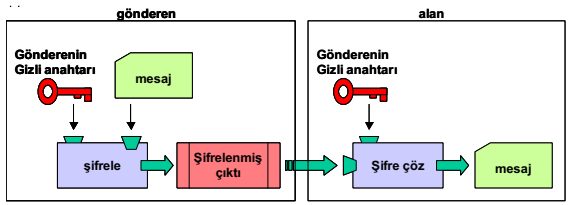
10

RSA

- Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman @ MIT; 1977
- RSA açık-anahtar şifreleme sistemi ise birbiriyle eşli tasarlanmış iki anahtar kullanır.
- Herkes tarafından öğrenilebilen "açık anahtar" ve yalnızca mesaj gönderici tarafından bilinen "gizli anahtar.
- Bu yöntemde hem iletişim veri gizliliği sağlanmış hem de gönderenin kimliği kesinlikle doğrulanmış olur.

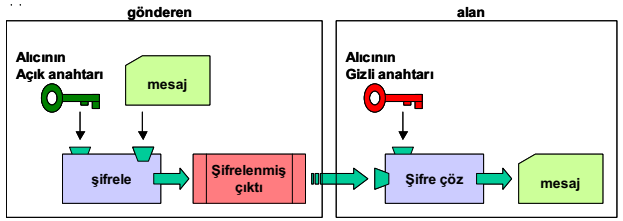
11

Simetrik Şifreleme



12

Asimetrik Şifreleme



13

Sayısal İmza

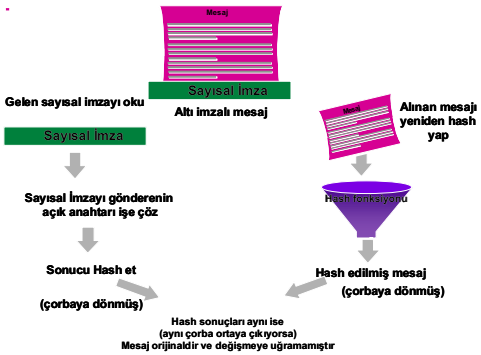
- Sayısal imza, bir elektronik mesajı ya da dökümanı yaratan ve gönderenin kimliğinin doğrulanması, mesaj ya da dökümanın yazıldığı ve imzalandığı andan sonra değişikliğe uğramadığını kanıtlamak amacıyla kullanılan elektronik işaretleme yöntemine verilen isimdir.
- Başlıca sayısal imza algoritmaları arasında RSA(RC4), DSS/DSA, SHA, MD2, MD5 sayılabilir

14

Sayısal imza ile bir mesajın imzalanması

15

Sayısal imzalı belgenin okunması



16

Sayısal Sertifika

- Sayısal sertifikalar bir anlamda sanal parmak izleri olarak adlandırılabilir.
- Bu sanal parmak izleri, br nesne ya da kişiyi tanıma amacıyla kullanılır.
- Sayısal sertifika, sayısal imza ile birlikte birtakım ilave bilgilerin bir araya getirilmesi ile oluşturulur.
- Sayısal imza, kişi ya da nesneye ait değil, sertifikayi veren yetkili sertifika sağlayıcı kuruluşun (CA-Certificate Authority) imzasıdır.
- Sayısal sertifikayı kullanan ve kabul edenler bu yetkili kuruluşa belirli bir güven duyduklarını peşinen kabul ederler.

Sayısal Sertifika İçeriği

- Sertifika sahibinin ismi
- Elektronik posta adresi
- Açık anahtar
- Sertifikanın geçerlilik süresi
- Sertifika sağlayıcı kuruluşun adı (Verisign)
- Sertifika sağlayıcının imzası (diğer öğelerle birlikte mühürlenmiş)

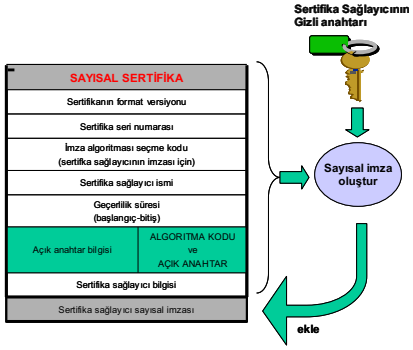
Sayısal Sertifika Dağıtımı

- Sertifikaya ekli imza
- Sertifika Dizin Servisi

Sayısal Sertifikaların İptali

- Onay kurumuna güven esastır

Sayısal Sertifika



21

TANIMA VE YETKİLENDİRME PROTOKOLLERİ

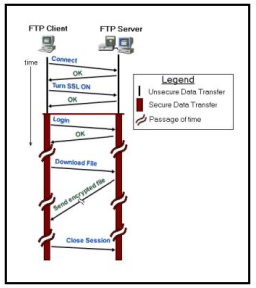
- Parola ve PIN (Personal Identification Number) Yaklaşımı, başlıca olası sorunlar?
  - **Öğrenme:** Parola saldırgan tarafından öğrenilebilir. Parolalar bazı kişiler tarafından küçük kağıtlara ya da dokümanlara yazılmış olabilir. Ağızdan söylenmiş ya da duyulmuş olabilir.
  - **Tahmin:** Kolayca tahmin edilebilen parolalar öğrenilebilir. Örneğin takma isimler, çocuk isimleri,doğum yılları vb. Parola olarak kullanıldığında bulunma tehdidi ile karşı karşıyadır. Hollywood filimlerinde genellikle bu yöntem çok gözlenir. Bazı saldırganlar, sözlük programları yardımıyla otomatik olarak sözlükteki bütün sözcükleri denerler.
  - **Dinleme:** Elektronik iletişim dinlenerek, parola elde edilebilir. Bazı durumlarda çok gelişmiş dinleme sistemleri kullanmak gerekir.
  - **Yeniden Verme:** Şifrelenmiş parolalar, saldırgan tarafından elde edilir. Daha sonra saldırı anında şifrelenmiş parolalar (aslını bilmese de) sisteme verilir ve sistem bunları kabul ediyor olabilir.
  - **Sunucuya Erişme:** Saldırgan parolaların saklandığı sunucuyu ele geçirmiş ve parolaları kaynağından elde etmiş olabilir.

22

SSL ?

23

Sorularınız?...



24