



Dođrulama Protokolleri

Dr. Fatih KALEMKUŐ
Kafkas Üniversitesi



Konular

- Şifrelemenin Temelleri
- Protokol Türleri
- Güvenlik Özellikleri
- Kusur ve Saldırıların Sınıflandırılması
- Protokollerin Belirlenmesi
- Özelliklerin Belirlenmesi
- Protokol Analizleri



Şifrelemenin Temelleri

- Genel ilkeler
 - Sender, receiver, plaintext, ciphertext, encryption, decryption, etc.
- Simetrik anahtar (veya gizli anahtar) şifreleme
- Açık anahtar (veya asimetric) şifreleme
- Tek yönlü hash (karma) algoritmaları



Şifrelemenin Temelleri

- Gönderici (Sender) – Gönderen kişi
- Alıcı (Receiver) – Alan kişi
- Düz metin (Plaintext) – gönderilecek metin,
 - Gösterim: P ya da M
- Şifreli metin (Ciphertext) – P ya da M kodlaması
 - Gösterim: C



Şifrelemenin Temelleri

- Şifreleme (Encryption) – Bir mesajın içeriğinin gizlenmesi süreci
 - Gösterim: $E(M) = C$
- Şifre çözme (Decryption) – M'yi kurtarmak için C'nin kodunu çözme işlemi
 - Gösterim: $D(C) = M$
- Temel kimlik: $D(E(M)) = M$



Şifrelemenin Temelleri

- Kriptografi – mesajların güvenliğini sağlama sanatı ve bilimi
- Kriptografik algoritma– şifreleme ve şifre çözmek için kullanılan işlev
 - Kısıtlanmış (gizli) veya Kısıtlanmamış (yayınlanmış) ← odak noktamız
 - Kısıtlanmamış – K . E_K ve D_K anahtarına dayalıdır. Şifreleme ve şifre çözme anahtarı farklı olabilir.



Şifrelemenin Temelleri

- Simetrik anahtar şifrelemesi– şifreleme anahtarı, şifre çözme anahtarından hesaplanabilir veya tam tersi
 - Özel durum: İki anahtarda aynıdır.
 - **Anahtar(lar) gizli tutulmalıdır!!**
- Açık anahtar şifreleme– şifreleme anahtarı herkese açıkken şifre çözme anahtarı herkese açık değildir.
 - Şifreleme anahtarından şifre çözme anahtarının hesaplanması zor olmalıdır !!

Kriptografik Temeller(devamı)

- Tek yönlü işlevler – hesaplanması kolay ancak tersine çevrilmesi zor işlevler
 - x verildiğinde $f(x)$ 'i hesaplamak kolaydır
 - $f(x)$ verildiğinde x 'i hesaplamak zordur

Bu kulağa kolay geliyor ama bu tür işlevlerin var olduğuna dair hiçbir **kanıtımız yok!** Var olduklarını varsayacağız.

- Trapdoor tek yönlü işlevler – tek yönlü işlevler şöyle ki
 - $f(x)$ ve bir miktar y verildiğinde x 'i hesaplamak kolaydır



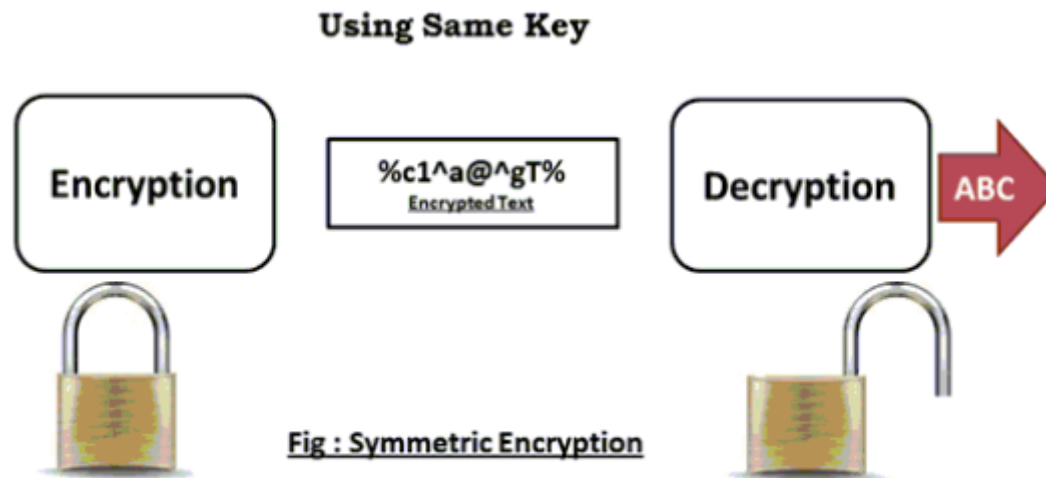
Kriptografik Temeller(devamı)

- **Gösterim:** 1 yönlü hash fonksiyonları – Aynı zamanda 1 yönlü bir fonksiyon olan bir hash fonksiyonu.
- İyi bir 1 yönlü hash işlevi aynı zamanda **çarpışmadan da arındırılmıştır**
- 1-yönlü bir hash fonksiyonunun güvenliği onun 1-yönlü olmasıdır.

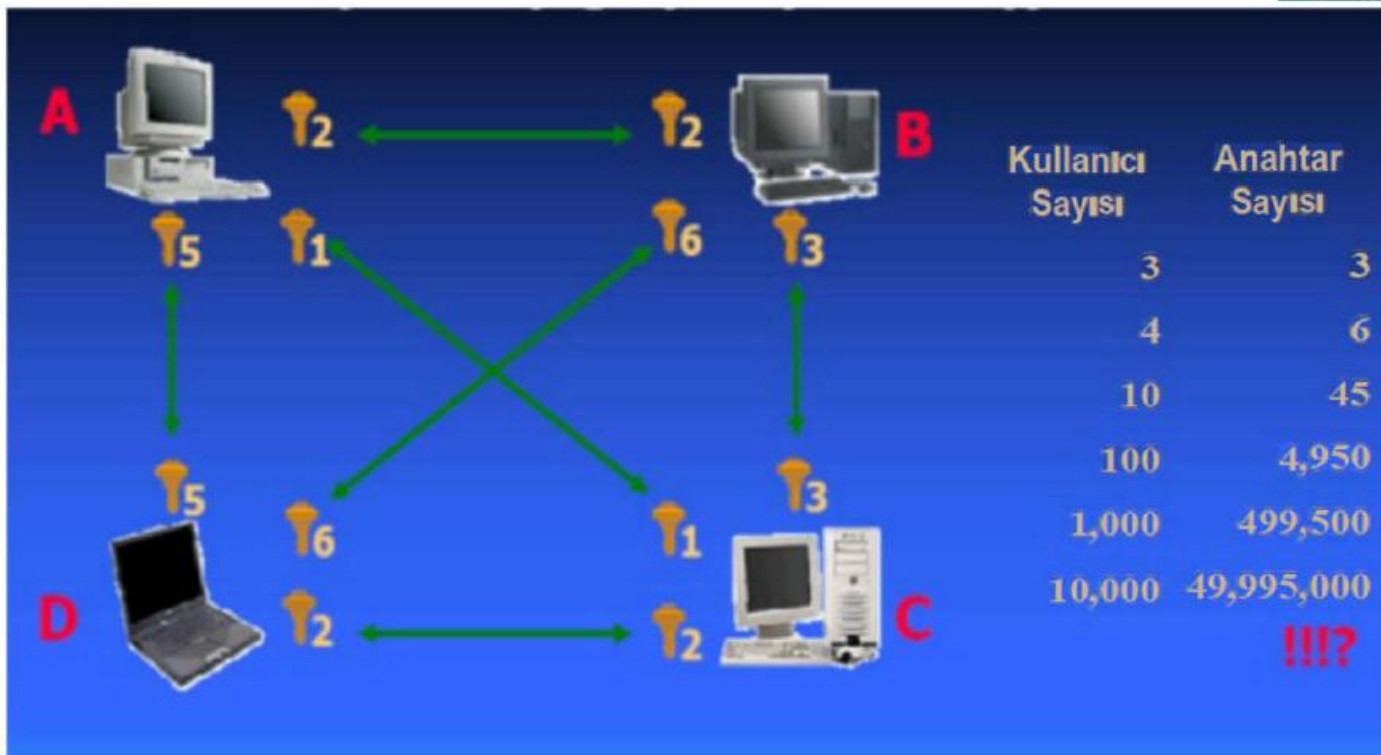
Simetrik/Gizli Anahtarlı Şifreleme

- Simetrik şifreleme algoritmaları, şifreleme ve açma işlemleri için aynı anahtarı kullanır.
- Gizli veri alışverişi yapacak kişi veya uygulamalar simetrik anahtarı kendi aralarında, emniyetli bir şekilde, değiştirmelidir.
- Simetrik şifreleme algoritmasıyla şifrelenmiş bir verinin güvenliği, şifreleme işleminde kullanılmış olan anahtarın gizliliği ile doğrudan ilişkilidir

Simetrik/Gizli Anahtarlı Şifreleme



Simetrik Şifreleme





Simetrik Şifreleme

- + Şifreleme ve şifre çözme işlemleri hızlıdır. Donanım ile gerçekleştirilebilir.
- + İletişim gizliliği sağlanır
- + Algoritmaları basit olduğundan değiştirilerek daha güçlü ve kırılması zor şifreler oluşturulabilir, diğer şifreleme türlerine zemin hazırlayabilir.



Simetrik Şifreleme

- Güvenilir anahtar dağıtımı zordur.
- Anahtar saklamak zordur.
- Anahtar çoğunlukla birden fazla kez değiştirilir.
- Kimlik doğrulama (authenticity) sağlanmaz.
- Veri herhangi bir kişi tarafından değiştirilmiş olabilir.



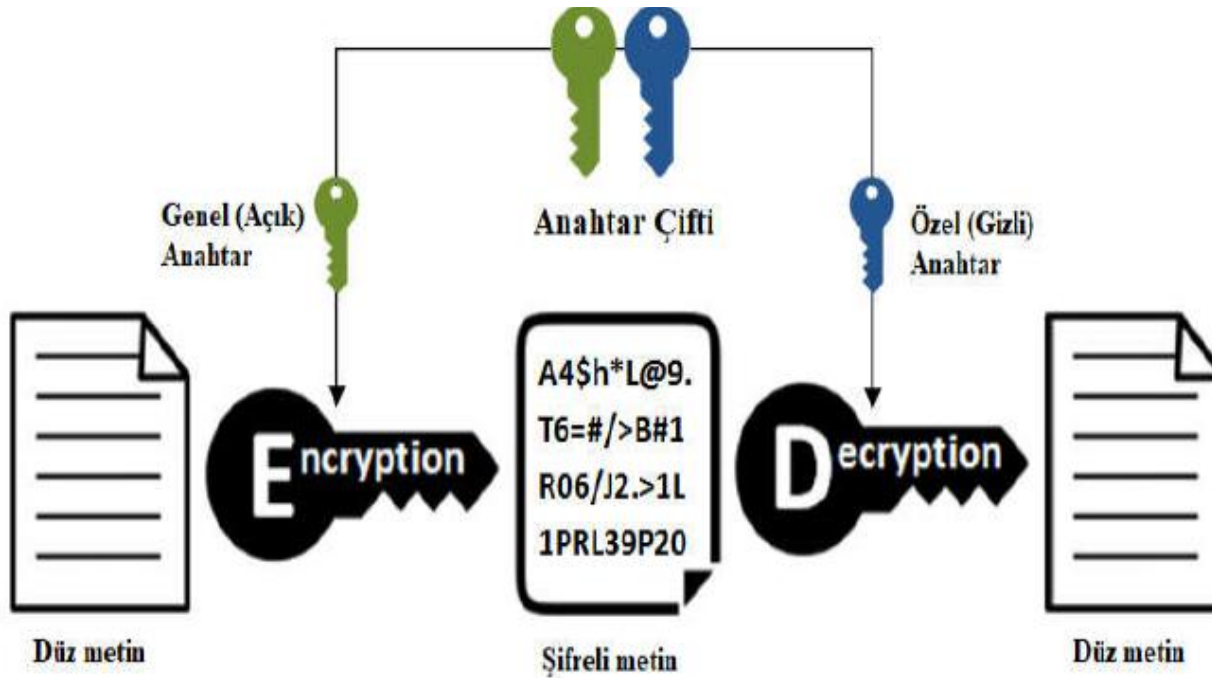
Simetrik Şifreleme

- Shift Cipher - Caesar Cipher
- Affine Cipher
- Vigenere Cipher
- Hill Cipher
- DES
- IDEA
- Blowfish
- RC5
- RC2
- 3DES
- AES

Asimetrik Açık Anahtarlı Şifreleme

- Asimetrik şifrelemede, özel(private) ve açık(public) olmak üzere bir anahtar çifti vardır. Kişi kendi özel anahtarını gizli tutarken, açık anahtarını şifreli iletişim kuracağı kişilere iletir.
- Bu anahtarlar birbirine matematiksel bir ilişkiyle bağlanmıştır fakat; anahtarlardan birini kullanarak diğerini elde etmek çok zor hatta imkansızdır. (En azından şimdilik, yada asal sayıların formülü bulunana kadar)
- Anahtarlardan açık olanıyla şifrelenen bir veri ancak bu açık anahtara karşılık gelen özel anahtarla açılabilir.
- İlk olarak 1976 da Martin Hellman and Whitfield Diffie tarafından makale olarak sunuldu.

Asimetrik Açık Anahtarlı Şifreleme



Asimetrik Açık Anahtarlı Şifreleme

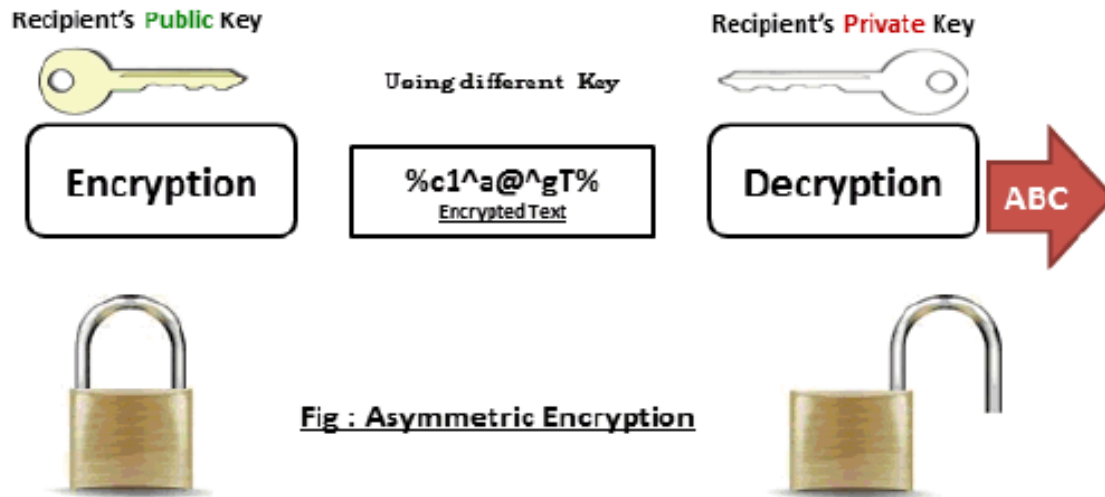


Fig : Asymmetric Encryption

Asimetrik Açık Anahtarlı Şifreleme

- + Bütünlük, Kimlik Doğrulama ve İnkâr Edememezlik güvenlik hizmetleri sağlanabilir.
- + Gizli/Açık anahtar çifti uzun periyot kullanılabilir.
- + Verilerin gizliliğini sağlar.
- + Büyük ağlarda anahtar sayısı simetrik anahtarlara göre oldukça azdır.
- + Private key gizli tutulmalıdır. Public key ortak bir sunucuda saklanabilir.
- + Kripto-analize karşı dirençli (Kırılması zor).

Asimetrik Açık Anahtarlı Şifreleme



- Anahtar uzunluğu simetriklere göre daha uzundur.
- Algoritmalar karmaşık olduğundan simetrik şifrelemelere göre daha yavaştır.
- Donanımsal olarak gerçekleştirilmesi ve paralelleştirilmesi simetrik şifrelere göre daha zordur.



Asimetrik Açık Anahtarlı Şifreleme

- RSA
- DSA
- DH
- Rabin
- El-Gamal
- McEliece
- Knapsack
- Eliptik Eğri (EEC)



Protokol Telaffuz et (...) n.

1.

- a. Diplomatlar ve devlet başkanları tarafından uygulanan tören ve görgü kuralları.
- b. Doğru davranış kuralları: güvenlik protokolleri; akademik protokol.

2. Bir anlaşmanın veya benzeri bir belgenin onaylanmadan önceki ilk kopyası.

3. Bir işlemin ön taslağı veya kaydı.

4. Bir tıbbi tedavi süreci veya bilimsel bir deney için plan.

5. Bilgisayar Bilimi. Bilgisayarlar arasında veri aktarımını düzenlemek için standart bir prosedür.



Protokoller

- Protokol – bir görevi gerçekleştirmek için iki veya daha fazla tarafın dahil olduğu bir dizi adım.
 - Açıkça belirtilmelidir.
 - Bir bakıma tamamlanmış olmalıdır (birçok olası durum için belirlenmiş eylem).
 - Her adım ya bir hesaplama ya da bir mesajdır.
 - Taraflar birbirlerine güvenmeyebilir.



Protokol Türleri

- Protokollerimiz kriptografiktir; gizlice dinlemeyi, hile yapmayı vb. önlemek için kriptografiyi kullanırız.
- Protokolün amacı gizliliğin ötesindedir.
 - **Örnek:** Aynı anda sözleşme imzalamak, birbirlerini kimlikleri konusunda ikna etmek, vb.
- Protokoller birçok şekilde sınıflandırılabilir
 - Şuna göre: İlgili taraflara, amaca, çevreye vb.



Taraflara Göre Sınıflandırma

- **Tahkime** dayalı protokoller
- Karara bağlanan protokoller
- **Kendi kendini uygulayan** protokoller



Tahkimli Protokoller

- Tahkimli protokoller – bir hakeme, bir protokolü tamamlaması için güvenilen tarafsız bir üçüncü tarafa sahiptir.
 - Taraflar yüz yüze ise daha kolaydır.
 - Bilgisayar ağları üzerinde bu, gecikmeye ve genel masraflara neden olur.
 - Hakem darboğaz haline gelir.
 - Ölçeklendirme sorunları vardır.
 - Hakem savunmasızdır.



Kararlařtırılmıř Protokoller

- Karara baėlanan protokoller – řunları ięeren iki ařamalı bir protokol:
 - Tahkime dayalı olmayan bir alt protokol
 - Yalnızca istisnai durumlarda (bir anlaşmazlık) yürütölen, tahkime dayalı bir alt protokol.
- Bu tür hakemlere **yargıę** denir.
 - Yargıę sadece protokolün adil bir řekilde uygulanmasını deėerlendirmek için çağrılır. Hileyi önlemek yerine tespit eder.
 - **İyi kararlařtırılmıř protokol**– yargıę hile yapanın kimliėini belirleyebilmelidir.



Kendi Kendine Uygulanan Protokol

- **Kendi kendine uygulanan protokoller** – protokolün kendisi adaleti garanti eder.
 - Hakem veya yargıç yok – bir taraf hile yaparsa, diğerleri hileyi tespit eder.
 - En iyi protokol türü.
 - Her durum için mevcut değildir.
- **Alıştırma:** Kendi kendine uygulanan protokollerin bulunmadığı bir durum bulun.

Amaca Göre Protokol Sınıflandırması

- Anahtar deęişim protokolleri
- Kimlik doęrulama protokolleri
- Kimlik doęrulama ve Anahtar deęişim protokolleri
- Elektronik Ticaret protokolleri
- ...



Anahtar Değişim Protokolleri

- Amaç, güvenli oturumlar, kanallar, iletişim vb. için anahtarları dağıtmaktır.
- Klasik anahtar değişim protokolleri
 - TMN
 - Symmetric Needham-Schroeder
 - Denning-Sacco
- Dağıtılan Protokoller
 - Kerberos IV
 - SSL/TLS



The TMN Protocolü (1990)

(Tatebayashi-Matsuzaki-Newman)

- Ağlar ve mobil bilgi işlem için uygundur.
- Simetrik. Güvenilir Sunucu S.
- Tarafların uzun vadeli anahtarları yoktur.
- Rastgele seçilen anahtarlar K_A , K_B , vb.
- Standart şifreleme işlevi $E(.)$, sadece sunucu tarafından tersine çevrilebilir.
- Vernam şifreleme işlevi $V(., .)$
 - $V(M, V(M, N)) = N$



The TMN Protocol

1. $A \rightarrow S : A, S, B, E(K_A)$
 2. $S \rightarrow B : S, B, A$
 3. $B \rightarrow S : B, S, A, E(K_B)$
 4. $S \rightarrow A : S, A, B, V(K_A, K_B)$
- A 4'üncü mesajdan K_B çıkarır.
 - Taraflar B tarafından seçilen oturum anahtarı üzerinde anlaşmalıdır.



TMN'nin Uygulaması

- $n = p \cdot q$, p , q asal sayılardır
- $E(x) = x^3 \text{ mod } n$
- S , n 'nin 2 asal çarpanını bilir
- $V(x, y) = x$ **münhasır-veya** y

Protokol güzel görünüyor ama büyük kusurları var!



Kimlik Doğrulama Protokolleri

- Kimlik doğrulama protokolleri– tarafların kimlik doğrulaması için (*asli failer*)
- Kimlik doğrulama – kiminle konuştuğunuzun güvencesi
- **Özel amaçlara örnekler:**
 - Oturum anahtarını alanların söyledikleri kişi olduğundan emin olmak için
 - Anahtarın olduğunu düşündüğünüz yöneticiye ait olduğundan emin olun



Kimlik Doğrulama Protokolleri

- Genellikle sistem yöneticileri tarafından kullanılan parolalar veya paylaşılan anahtarlar
- Kimlik doğrulama, anahtar değişim protokolünün bir yan ürünü olabilir
- Bazı kimlik doğrulama protokolleri
 - Feige-Fiat-Shamir (1987)
 - Guillou-Quisquater (1988)
 - Schnorr (1989)



Guillou-Quisquater Protokolü

- Akıllı kartlar ve diğer uygulamalar
- Nejdet, J bit dizisi olan kimliğini Fatih'e kanıtlamak istiyor
- Genel bilgi: v üssü, ve n sayısı
 - ($n = p \cdot q$, p and q **asal sayılar**)
- Özel anahtar: B ile $JB^v = 1 \pmod{n}$



Guillou-Quisquater Protokolü

- $A \longrightarrow V : J$

P, bu J'nin kendisine ait olduğunu kanıtlamak istiyor.

1. $A \longrightarrow V: T = r^v \text{ mod } n$ ($1 < r < n - 1$, r rastgele)
2. $V \longrightarrow A: d$ ($0 < d < v - 1$, d rastgele)
3. $A \longrightarrow V: D = rB^d \text{ mod } n$
4. $V, T' = D^v J^d \text{ mod } n$ formülünü hesaplar. Eğer $T = T' \text{ (mod } n)$ ise kimlik doğrulama başarılıdır



3 Önemli Kavram

- Güvenlik
- Gizlilik
- Güvenilirlik



Güvenlik

- Güvenlik – bilginin **kontrolü**.
 - Bunu sağlar:
 - Yetkili tarafların kimlik doğrulaması uygun şekilde yapılır
 - Mesajları değiştirilmeden ağ üzerinden gönderilir.
 - Güvenli bir sistemde mesajın **kaynağı**, **içeriği** ve **hedef alıcıları** güvence altına alınabilir.
 - Güvenlik, gizlilik **değildir**.



Gizlilik

- Privacy – bilginin sahibi bilgiyi kontrol edebilir.
 - Gizlilik, güvenliği gerektirir; ancak güvenlik tek başına yeterli **değildir**.
 - Güvenlik gizliliği engelleyebilir! (Bilgiye konu olan **kişilerin** söz konusu bilgilerin kullanımı konusunda ne kontrolü ne de bilgisi olduğunu garanti ederek)



Güvenilirlik

- Güvenilirlik – Ağ arızaları, bellek kayıpları ve saldırıların varlığında kesinlik sağlar.
 - Güvenilirlik ve güvenlik **birbirine bağlıdır.**
 - Güvenilirlik **güvenlik değildir.** Güvenli olmayan sunuculardaki güvenilir protokoller, gerçek kullanıcılara olduğu kadar saldırınlara da güvenilir hizmetler sağlar.
- Güvenilir elektronik ticaret, hatasız işlemler gerektirir.



Güvenlik Özellikleri

- **Kimlik doğrulama** – Bir mesajın alıcısı, onun kaynağını belirleyebilmelidir.
 - Davetsiz misafir başka biri gibi davranmamalı.
 - Paylaşılan bilgiler kullanılarak veya benzersiz bilgileri kanıtlama yeteneği kullanılarak uygulanır (PIN'ler ve Şifreler).
- Gizlilik – gizlilik. Eğer bir mesaj gizli ise sadece hedeflenen alıcılar tarafından okunabilir.
 - Gizlice dinlemek zor veya işe yaramaz



Güvenlik Özellikleri (devamı)

- Bütünlük – Bir mesajın alıcısı, mesajın iletim sırasında değiştirilmediğini doğrulayabilir.
 - Bütünlük tek başına güvenlik anlamına gelmez.
- Erişilebilirlik – bir sistem erişilebilir olmalıdır.
 - Kötü niyetli bilgisayar korsanları, ağ arızaları veya ticari casusluk nedeniyle erişilebilirlik tehlikeye girebilir.
- Reddedilemezlik – bir taraf makul bir şekilde bir eylemde bulunmadığını iddia edemez.
 - Örnek: gönderici, mesajı gönderdiğini yalanlayarak reddeder.



Güvenilirlik Özellikleri

- Atomiklik – bölünemezlik. Atomik bir işlem ya tamamen başarısız olur ya da tamamen başarılı olur.
- Tutarlılık – ilgili tüm taraflar değişimin kritik gerçekleri üzerinde hemfikirdir.
- İzolelik – Birbiriyle örtüşen bir dizi işlemin sonucu izole edilmelidir.
- Dayanıklılık: Bir işlem son tutarlı durumuna geri dönebilmelidir.



Diğer Özellikler

Başka özelliklere de ihtiyaç duyulabilir.

Örneğin, e-Ticarette;

- Sertifikalı teslimat
- Ürünlerin atomikliği
- Vb.

Ayrıca gereklidir.



En Yaygın Kimlik Doğrulama Protokolleri

1. Kerberos – Merkezi kimlik doğrulama sistemi
2. OAuth 2.0 – Üçüncü taraf kimlik doğrulama protokolü
3. SAML (Security Assertion Markup Language) – Web tabanlı tek oturum açma (SSO)
4. TOTP (Time-Based One-Time Password) – Zaman bazlı tek kullanımlık şifre
5. EAP (Extensible Authentication Protocol) – Kablosuz ağ kimlik doğrulaması

OAuth 2.0 – Üçüncü taraf kimlik doğrulama protokolü



Kullanıcı, istemciye izin veriyor, istemci erişim jetonu alıyor ve kaynak sunucusuna erişiyor.

TOTP (Time-Based One-Time Password) – Zaman bazlı tek kullanımlık şifre



Kullanıcı, doğrulama sunucusu ile bir şifre paylaşıyor, mobil uygulama OTP oluşturuyor ve kimlik doğrulama sağlanıyor.



Kaynaklar

- Bruce Schneier, Applied Cryptography
- Linda Jean Camp, Privacy and Reliability in Electronic Commerce, PhD dissertation, CMU



Sonu

Sorular





TEŞEKKÜRLER

Dr. Fatih KALEMKUŞ