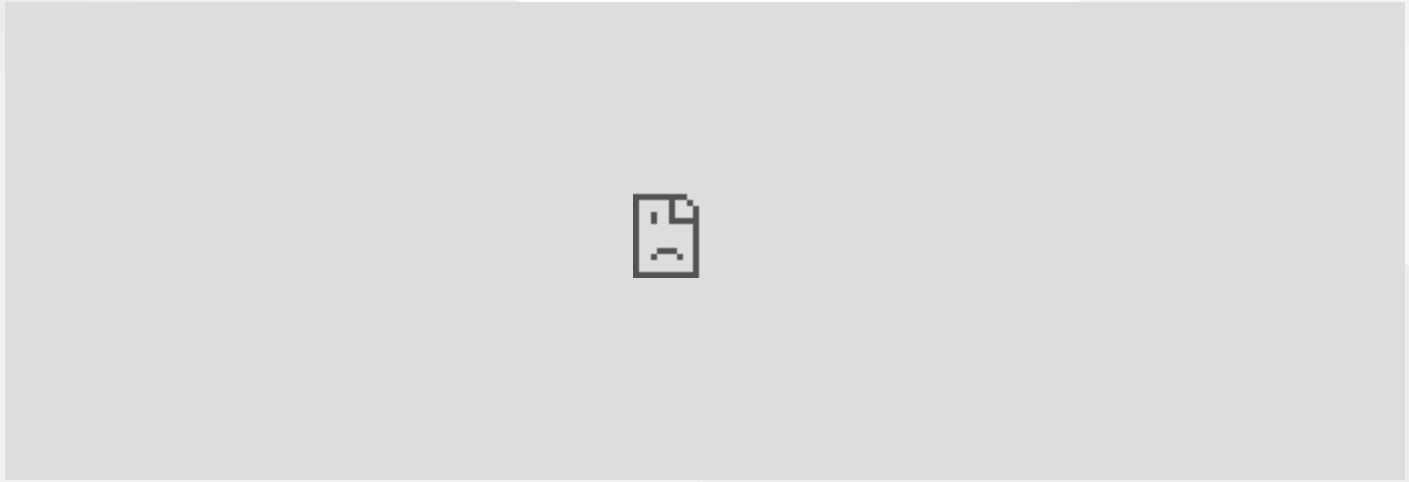
CE407 Güvenli Programlama

Hafta-9

Sertifikalar ve Şifreleme Yöntemleri

İndir PDF, DOCX, SLIDE, PPTX



Outline

- Sertifikalar ve Şifreleme Yöntemleri
- Simetrik ve Asimetrik Şifreleme
- Dijital İmzalar ve Sertifika Yönetimi

Hafta-9: Sertifikalar ve Şifreleme Yöntemleri

Bu hafta, yazılım güvenliği ve iletişimde kullanılan şifreleme yöntemleri ile sertifikaların temel ilkelerini inceleyeceğiz. Hem asimetrik hem de simetrik şifreleme algoritmalarını, dijital sertifikaların nasıl çalıştığını ve uygulama güvenliğine nasıl katkı sağladıklarını keşfedeceğiz.

1. Şifreleme Yöntemlerinin Temelleri

Teorik Açıklama: Şifreleme, verilerin gizliliğini korumak ve yetkisiz erişimlere karşı koruma sağlamak amacıyla kullanılan bir tekniktir. Şifreleme yöntemleri iki ana kategoriye ayrılır: simetrik ve asimetrik.

- **Simetrik Şifreleme:** Aynı anahtar hem şifreleme hem de şifre çözme işlemlerinde kullanılır. Örnek algoritmalar: AES, DES.
- **Asimetrik Şifreleme:** İki farklı anahtar kullanılır. Bir anahtar şifreleme için, diğeri ise şifre çözme için kullanılır. Örnek algoritmalar: RSA, ECC.

2. Simetrik Şifreleme Yöntemleri

Teorik Açıklama: Simetrik şifreleme, hız ve verimlilik açısından asimetrik şifrelemeden daha avantajlıdır, ancak anahtar paylaşımı sorunu vardır.

- **AES (Advanced Encryption Standard):** Yaygın kullanılan ve oldukça güvenli bir blok şifreleme algoritmasıdır. 128, 192 veya 256 bit anahtar uzunluklarıyla çalışır.
- **DES (Data Encryption Standard):** Daha eski bir algoritma olup, günümüzde güvenlik açıkları nedeniyle artık önerilmemektedir.
- **Blok Şifreleme ve Modlar:** Blok şifreleme, veriyi sabit uzunluklardaki bloklar halinde şifreler. Örneğin, ECB (Electronic Codebook), CBC (Cipher Block Chaining) gibi şifreleme modları vardır.

Uygulama Örnekleri:

1. **AES** kullanarak bir metni şifreleyip çözme işlemi.
2. CBC modunu kullanarak bir dosyanın şifrelenmesi ve şifre çözme işlemi.

3. Asimetrik Şifreleme Yöntemleri

Teorik Açıklama: Asimetrik şifrelemede iki anahtar bulunur: bir kamuya açık anahtar (public key) ve bir özel anahtar (private key). Veri, kamuya açık anahtar ile şifrelenir ve sadece özel anahtar ile çözülebilir.

- **RSA (Rivest-Shamir-Adleman):** Yaygın kullanılan asimetrik şifreleme algoritmasıdır. Büyük asal sayılara dayalıdır ve hem şifreleme hem de dijital imza işlemlerinde kullanılır.
- **ECC (Elliptic Curve Cryptography):** Daha küçük anahtar boyutları ile RSA'ya kıyasla daha güçlü güvenlik sağlayan asimetrik bir şifreleme algoritmasıdır.

Uygulama Örnekleri:

1. **RSA** kullanarak bir metni şifreleme ve çözme işlemi.
2. **ECC** kullanarak dijital imza oluşturma ve doğrulama.

4. Hibrit Şifreleme

Teorik Açıklama: Hibrit şifreleme, hem simetrik hem de asimetrik şifrelemeyi bir arada kullanır. Simetrik anahtarlar, asimetrik şifreleme ile güvenli bir şekilde paylaşılır, ardından veriler simetrik anahtarla şifrelenir.

- **Uygulama:** E-posta ve HTTPS gibi birçok güvenli iletişim protokolünde kullanılır.

Uygulama Örnekleri:

1. Simetrik anahtarın asimetrik olarak şifrelenmesi ve ardından verilerin simetrik şifre ile korunması.
2. Hibrit şifreleme kullanarak iki cihaz arasında güvenli veri alışverişi.

5. Dijital Sertifikalar ve Sertifika Yetkilileri (CAs)

Teorik Açıklama: Dijital sertifikalar, bir kişinin veya kuruluşun kimliğini doğrulayan elektronik belgeler olarak tanımlanabilir. Bu sertifikalar genellikle bir sertifika yetkilisi (Certificate Authority - CA) tarafından imzalanır ve kullanıcılara güvenli bir şekilde iletilir.

- **X.509 Sertifikası:** En yaygın kullanılan sertifika türüdür.
- **Sertifika Yetkilisi (CA):** Sertifikaları dijital olarak imzalayan güvenilir otoriteler.
- **Sertifika Zinciri:** Sertifikaların doğrulanabilir bir hiyerarşi ile bağlandığı yapı. Her sertifika, bir üst otorite tarafından imzalanır.

Uygulama Örnekleri:

1. Bir web sunucusu için **SSL/TLS** sertifikası oluşturma ve yükleme.
2. **X.509** sertifikalarının doğrulanması ve güvenlik zincirinin incelenmesi.

6. Dijital İmzalar

Teorik Açıklama: Dijital imzalar, verilerin kimliğini doğrulamak ve değişikliğe uğrayıp uğramadığını kontrol etmek için kullanılır. İmza, bir mesajın karmasını (hash) hesaplayarak ve bu karmayı özel bir anahtarla şifreleyerek oluşturulur.

- **İmzanın Doğrulanması:** İmza, kamuya açık anahtar kullanılarak doğrulanabilir.
- **Uygulama Alanları:** E-posta, yazılım dağıtımı, dijital sözleşmeler.

Uygulama Örnekleri:

1. Bir dosya için **dijital imza** oluşturma ve doğrulama.
2. **PGP/GPG** kullanarak bir mesajın imzalanması ve doğrulanması.

7. Sertifika Tabanlı Kimlik Doğrulama

Teorik Açıklama: Sertifikalar, özellikle sunucular arası güvenli iletişimde kimlik doğrulama için kullanılır. İstemci ve sunucu birbirlerinin sertifikalarını doğrulayarak güvenli bir iletişim kanalı oluşturur.

- **SSL/TLS:** Web tarayıcıları ve sunucular arasındaki güvenli iletişimde kullanılan bir protokoldür.
- **Mutual Authentication:** Hem sunucu hem de istemci birbirlerini sertifikalar aracılığıyla doğrular.

Uygulama Örnekleri:

1. **SSL/TLS** kullanarak güvenli bir bağlantı kurulması.
2. Sertifika tabanlı çift taraflı kimlik doğrulama senaryosu uygulama.

8. PKI (Public Key Infrastructure - Açık Anahtar Altyapısı)

Teorik Açıklama: PKI, dijital sertifikaların oluşturulması, dağıtılması, yönetilmesi ve doğrulanması süreçlerini içeren bir yapıdır. PKI, güvenli iletişim sağlamak için gerekli anahtar çiftlerinin ve sertifikaların yönetimini sağlar.

- **Bileşenler:** CA (Certificate Authority), RA (Registration Authority), CRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol).
- **Uygulama Alanları:** SSL/TLS, VPN, e-posta güvenliği, kod imzalama.

Uygulama Örnekleri:

1. **PKI** kullanarak bir sertifika yönetim altyapısı kurma.
2. **OCSP** ve **CRL** ile sertifika iptallerinin kontrol edilmesi.

9. Beyaz Kutu Kriptografisi (Whitebox Cryptography)

Teorik Açıklama: Beyaz kutu kriptografisi, özellikle şifreleme algoritmalarının açık bir sistemde güvenli bir şekilde uygulanmasını sağlar. Bu teknikle, şifreleme işlemleri sırasında anahtarlar ve diğer hassas bilgiler koruma altında tutulur.

- **Whitebox AES/DES:** AES ve DES gibi simetrik şifreleme algoritmalarının beyaz kutu ortamlarında uygulanması.
- **Uygulama Alanı:** Dijital hak yönetimi (DRM), mobil uygulama güvenliği.

Uygulama Örnekleri:

1. **Whitebox AES** kullanarak bir dosya şifreleme işlemi gerçekleştirmek.
2. Whitebox kriptografi ile hassas verileri koruma altına almak.

10. Sertifika ve Anahtar Yönetimi

Teorik Açıklama: Sertifikaların ve kriptografik anahtarların etkin bir şekilde yönetilmesi, güvenli sistemlerin temel yapı taşlarından biridir. Sertifikaların zamanında yenilenmesi, iptal edilmesi ve saklanması, güvenli bir iletişim ortamı için kritik öneme sahiptir.

Uygulama Örnekleri:

1. Sertifikaların otomatik olarak yenilenmesi ve eski sertifikaların iptal edilmesi (CRL veya OCSP kullanımı).
2. **Anahtar yönetim sistemleri** (Key Management Systems) ile anahtarların güvenli bir şekilde yönetilmesi.

$9. Hafta - Sonu$