

CEN429 GÄ¼venli Programlama Hafta-9

Sertifikalar ve Äzifreleme YÄ¶ntemleri

Yazar: Dr. Ä-ÄŸr. Äoeyesi UÄŸur CORUH

İçindekiler

1 CEN429 GÄ¼venli Programlama	1
1.1 Hafta-9	1
1.1.1 Outline	1
1.1.2 Hafta-9: Sertifikalar ve Äzifreleme YÄ¶ntemleri	1

Şekil Listesi

Tablo Listesi

1 CEN429 GÄ¼venli Programlama

1.1 Hafta-9

1.1.0.1 Sertifikalar ve Äzifreleme YÄ¶ntemleri Ändir

- PDF¹
- DOC²
- SLIDE³
- PPTX⁴

1.1.1 Outline

- Sertifikalar ve Äzifreleme YÄ¶ntemleri
- Simetrik ve Asimetrik Äzifreleme
- Dijital Ämzalar ve Sertifika YÄ¶netimi

1.1.2 Hafta-9: Sertifikalar ve Äzifreleme YÄ¶ntemleri

Bu hafta, yazÄ±lan gÄ¼venliÄyi ve iletiŸimde kullanÄlan Äyifreleme yÄ¶ntemleri ile sertifikalarÄn temel ilkelerini inceleyeceÄyiz. Hem asimetrik hem de simetrik Äyifreleme algoritmalarÄnÄ, dijital sertifikalarÄn nasÄl ÄŸalÄŸtÄŸÄnÄ ve uygulama gÄ¼venliÄyine nasÄl katkı saÄladÄklarÄnÄ keÄfedeceÄyiz.

1.1.2.1 1. Äzifreleme YÄ¶ntemlerinin Temelleri Teorik AÄŸÄklama: Äzifreleme, verilerin gizliliÄyini korumak ve yetkisiz eriŸimlere karŸÄ koruma saÄlamak amacıyla kullanÄlan bir tekniktir. Äzifreleme yÄ¶ntemleri iki ana kategoriye ayrÄlÄr: simetrik ve asimetrik.

- **Simetrik Äzifreleme:** AynÄ anahtar hem Äyifreleme hem de Äyifre ÄŸÄzme iÄlemlerinde kullanÄlÄr. ÄrneÄ algoritmalar: AES, DES.

¹pandoc_cen429-week-9.pdf

²pandoc_cen429-week-9.docx

³cen429-week-9.pdf

⁴cen429-week-9.pptx

- **Asimetrik Ğzifreleme:** Ğ°ki farklı anahtar kullanılır. Bir anahtar Ğifreleme için, diğeri ise Ğifreleme için kullanılır. Ğrnekteki algoritmalar: RSA, ECC.

1.1.2.2 2. Simetrik Ğzifreleme Yöntemleri Teorik Açıklama: Simetrik Ğifreleme, hız ve verimlilik açısından asimetrik Ğifrelemeye göre avantajlıdır, ancak anahtar paylaşım sorunu vardır.

- **AES (Advanced Encryption Standard):** Yaygın kullanılan ve oldukça güvenli bir blok Ğifreleme algoritmasıdır. 128, 192 veya 256 bit anahtar uzunluklarıyla çalışır.
- **DES (Data Encryption Standard):** Daha eski bir algoritma olup, günümüzde güvenli değil olarak kabul edilir.
- **Blok Ğzifreleme ve Modlar:** Blok Ğifreleme, veriyi sabit uzunluklardaki bloklar halinde Ğifreler. Ğrneğin, ECB (Electronic Codebook), CBC (Cipher Block Chaining) gibi Ğifreleme modları vardır.

Uygulama Örnekleri:

1. AES kullanarak bir metni Ğifreleyip Ğzime iğleyelim.
2. CBC modunu kullanarak bir dosyanın Ğifrenmesi ve Ğifreleme için iğleyelim.

1.1.2.3 3. Asimetrik Ğzifreleme Yöntemleri Teorik Açıklama: Asimetrik Ğifrelemede iki anahtar bulunur: bir kamuya açık anahtar (public key) ve bir özel anahtar (private key). Veri, kamuya açık anahtar ile Ğifrenilir ve sadece özel anahtar ile Ğzilebilir.

- **RSA (Rivest-Shamir-Adleman):** Yaygın kullanılan asimetrik Ğifreleme algoritmasıdır. Büyük asal sayılara dayalıdır ve hem Ğifreleme hem de dijital imza işlemlerinde kullanılır.
- **ECC (Elliptic Curve Cryptography):** Daha küçük anahtar boyutlarıyla RSA'ya kıyasla daha güvenli sağılayan asimetrik bir Ğifreleme algoritmasıdır.

Uygulama Örnekleri:

1. RSA kullanarak bir metni Ğifreleme ve Ğzime iğleyelim.
2. ECC kullanarak dijital imza oluşturma ve doğrulama.

1.1.2.4 4. Hibrit Ğzifreleme Teorik Açıklama: Hibrit Ğifreleme, hem simetrik hem de asimetrik Ğifrelemeyi bir arada kullanır. Simetrik anahtarlar, asimetrik Ğifreleme ile güvenli bir şekilde paylaşılır, ardından veriler simetrik anahtarla Ğifrenilir.

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

Uygulama Örnekleri:

1. Simetrik anahtarın asimetrik olarak Ğifrenmesi ve ardından verilerin simetrik Ğifre ile korunması.
2. Hibrit Ğifreleme kullanarak iki cihaz arasında güvenli veri alışverişini.

1.1.2.5 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 kullanıcılarına güvenli bir şekilde iletilir.

- **X.509 Sertifikası:** En yaygın kullanılan sertifika türüdür.
- **Sertifika Yetkilisi (CA):** Sertifikalar dijital olarak imzalayan güvenilir otoriteler.
- **Sertifika Zinciri:** Sertifikalar doğrudan bir hiyerarşiyi ile bağlanabilir yapıdır. Her sertifika, bir üst otorite tarafından imzalanır.

Uygulama Örnekleri:

1. Bir web sunucusu için SSL/TLS sertifikası oluşturma ve yapılandırma.
2. X.509 sertifikalarının doğrulanması ve güvenli zincirinin incelenmesi.

1.1.2.6 6. Dijital Ėmzalar Teorik AĖŖĖklama: Dijital imzalar, verilerin kimliĖini doĖrulamak ve deĖiĖikliĖe uĖrayıp uĖramadĖn kontrol etmek iĖin kullanĖlĖr. Ėmza, bir mesajn karmasĖn (hash) hesaplayarak ve bu karmayĖn Ėzel bir anahtarla Ėifreleyerek oluĖturulur.

- **ĖmzanĖn DoĖrulanmasĖ:** Ėmza, kamuya aĖĖk anahtar kullanĖlarak doĖrulanabilir.
- **Uygulama AlanlarĖ:** E-posta, yazĖlĖm daĖĖtĖmĖ, dijital sĖzlemeler.

Uygulama Ėrneklere:

1. Bir dosya iĖin **dijital imza** oluĖturma ve doĖrulama.
2. **PGP/GPG** kullanarak bir mesajn imzalanmasĖ ve doĖrulanmasĖ.

1.1.2.7 7. Sertifika TabanĖ Kimlik DoĖrulama Teorik AĖŖĖklama: Sertifikalar, Ėzellikle sunucular arasĖ gĖvenli iletiĖimde kimlik doĖrulama iĖin kullanĖlĖr. Ėstemci ve sunucu birbirlerinin sertifikalarĖnĖ doĖrularak gĖvenli bir iletiĖim kanalĖ oluĖturur.

- **SSL/TLS:** Web tarayĖcĖlarĖ ve sunucular arasĖndaki gĖvenli iletiĖimde kullanĖlan bir protokoldĖr.
- **Mutual Authentication:** Hem sunucu hem de istemci birbirlerini sertifikalar aracĖlĖyle doĖrular.

Uygulama Ėrneklere:

1. **SSL/TLS** kullanarak gĖvenli bir baĖlantĖ kurulmasĖ.
2. Sertifika tabanĖ Ėift taraflĖ kimlik doĖrulama senaryosu uygulama.

1.1.2.8 8. PKI (Public Key Infrastructure - AĖŖĖk Anahtar AltyapĖsĖ) Teorik AĖŖĖklama: PKI, dijital sertifikalarĖn oluĖturulmasĖ, daĖĖtĖlmesĖ, yĖnetilmesi ve doĖrulanmasĖ sĖreĖlerini iĖeren bir yapĖdĖr. PKI, gĖvenli iletiĖim saĖlamak iĖin gerekli anahtar Ėiftlerinin ve sertifikalarĖn yĖnetimini saĖlar.

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

Uygulama Ėrneklere:

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

1.1.2.9 9. Beyaz Kutu Kriptografisi (Whitebox Cryptography) Teorik AĖŖĖklama: Beyaz kutu kriptografisi, Ėzellikle Ėifreleme algoritmalarĖnĖ aĖĖk bir sistemde gĖvenli bir Ėekilde uygulanmasĖnĖ saĖlar. Bu teknikte, Ėifreleme iĖlemleri sĖrasĖnda anahtarlar ve diĖer hassas bilgiler koruma altĖnda tutulur.

- **Whitebox AES/DES:** AES ve DES gibi simetrik Ėifreleme algoritmalarĖnĖ beyaz kutu ortamlarĖnda uygulanmasĖ.
- **Uygulama AlanlarĖ:** Dijital hak yĖnetimi (DRM), mobil uygulama gĖvenliĖi.

Uygulama Ėrneklere:

1. **Whitebox AES** kullanarak bir dosya Ėifreleme iĖlemi gerĖekleĖtirmek.
2. Whitebox kriptografi ile hassas verileri koruma altĖna almak.

1.1.2.10 10. Sertifika ve Anahtar YĖnetimi Teorik AĖŖĖklama: SertifikalarĖn ve kriptografik anahtarlarĖn etkin bir Ėekilde yĖnetilmesi, gĖvenli sistemlerin temel yapĖ taĖlarĖndan biridir. SertifikalarĖn zamanĖnda yenilenmesi, iptal edilmesi ve saklanması, gĖvenli bir iletiĖim ortamĖ iĖin kritik Ėneme sahiptir.

Uygulama Ėrneklere:

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

9.Hafta – Sonu