CE407 GÃ¼venli Programlama Hafta-9

Sertifikalar ve Åžifreleme YÃ¶ntemleri

Yazar: Dr. Ã–Ÿr. Ãœyesi UÄŸur CORUH

İçindekiler

Şekil Listesi

Tablo Listesi

1 CE407 GÃ¼venli Programlama

1.1 Hafta-9

1.1.0.1 Sertifikalar ve Åžifreleme YÃ¶ntemleri

Ä°ndir PDF[1], DOCX[2], SLIDE[3], PPTX[4]

1.1.1 Outline

- Sertifikalar ve Åžifreleme YÃ¶ntemleri
- Simetrik ve Asimetrik Åžifreleme
- Dijital Ä°mzalar ve Sertifika YÃ¶netimi

1.1.2 Hafta-9: Sertifikalar ve Åžifreleme YÃ¶ntemleri

Bu hafta, yazÄ±lÄ±m gÃ¼venliÄŸi ve iletiÅŸimde kullanÄ±lan ÅŸifreleme yÃ¶ntemleri ile sertifikalarÄ±n temel ilkelerini inceleyeceÄŸiz. Hem asimetrik hem de simetrik ÅŸifreleme algoritmalarÄ±nÄ±, dijital sertifikalarÄ±n nasÄ±l Ã§alÄ±ÅŸtÄ±ÄŸÄ±nÄ± ve uygulama gÃ¼venliÄŸine nasÄ±l katkÄ± saÄŸladÄ±klarÄ±nÄ± keÅŸfedeceÄŸiz.

1.1.2.1 1. Åžifreleme YÃ¶ntemlerinin Temelleri

Teorik AÃ§Ä±klama: Åžifreleme, verilerin gizliliÄŸini korumak ve yetkisiz eriÅŸimlere karÅŸÄ± koruma saÄŸlamak amacÄ±yla kullanÄ±lan bir tekniktir. Åžifreleme yÃ¶ntemleri iki ana kategoriye ayrÄ±lÄ±r: simetrik ve asimetrik.

- **Simetrik Åžifreleme:** AynÄ± anahtar hem ÅŸifreleme hem de ÅŸifre Ã§Ã¶zme iÅŸlemlerinde kullanÄ±lÄ±r. Ã–rnek algoritmalar: AES, DES.
- **Asimetrik Åžifreleme:** Ä°ki farklÄ± anahtar kullanÄ±lÄ±r. Bir anahtar ÅŸifreleme iÃ§in, diÄŸeri ise ÅŸifre Ã§Ã¶zme iÃ§in kullanÄ±lÄ±r. Ã–rnek algoritmalar: RSA, ECC.

[1] ce407-week-9.tr_doc.pdf
[2] ce407-week-9.tr_word.docx
[3] ce407-week-9.tr_slide.pdf
[4] ce407-week-9.tr_slide.pptx

1.1.2.2 2. Simetrik Åžifreleme YÃ¶ntemleri Teorik AÃ§Ä±klama: Simetrik ÅŸifreleme, hÄ±z ve verimlilik aÃ§Ä±sÄ±ndan asimetrik ÅŸifrelemeden daha avantajlÄ±dÄ±r, ancak anahtar paylaÅŸÄ±mÄ± sorunu vardÄ±r.

- **AES (Advanced Encryption Standard):** YaygÄ±n kullanÄ±lan ve oldukÃ§a gÃ¼venli bir blok ÅŸifreleme algoritmasÄ±dÄ±r. 128, 192 veya 256 bit anahtar uzunluklarÄ±yla Ã§alÄ±ÅŸÄ±r.
- **DES (Data Encryption Standard):** Daha eski bir algoritma olup, gÃ¼nÃ¼mÃ¼zde gÃ¼venlik aÃ§Ä±klarÄ± nedeniyle artÄ±k Ã¶nerilmemektedir.
- **Blok Åžifreleme ve Modlar:** Blok ÅŸifreleme, veriyi sabit uzunluklardaki bloklar halinde ÅŸifreler. Ã–rneÄŸin, ECB (Electronic Codebook), CBC (Cipher Block Chaining) gibi ÅŸifreleme modlarÄ± vardÄ±r.

Uygulama Ã–rnekleri:

1. **AES** kullanarak bir metni ÅŸifreleyip Ã§Ã¶zme iÅŸlemi.
2. CBC modunu kullanarak bir dosyanÄ±n ÅŸifrelenmesi ve ÅŸifre Ã§Ã¶zme iÅŸlemi.

1.1.2.3 3. Asimetrik Åžifreleme YÃ¶ntemleri Teorik AÃ§Ä±klama: Asimetrik ÅŸifrelemede iki anahtar bulunur: bir kamuya aÃ§Ä±k anahtar (public key) ve bir Ã¶zel anahtar (private key). Veri, kamuya aÃ§Ä±k anahtar ile ÅŸifrelenir ve sadece Ã¶zel anahtar ile Ã§Ã¶zÃ¼lebilir.

- **RSA (Rivest-Shamir-Adleman):** YaygÄ±n kullanÄ±lan asimetrik ÅŸifreleme algoritmasÄ±dÄ±r. BÃ¼yÃ¼k asal sayÄ±lara dayalÄ±dÄ±r ve hem ÅŸifreleme hem de dijital imza iÅŸlemlerinde kullanÄ±lÄ±r.
- **ECC (Elliptic Curve Cryptography):** Daha kÃ¼Ã§Ã¼k anahtar boyutlarÄ± ile RSAâ€™ya kÄ±yasla daha gÃ¼Ã§lÃ¼ gÃ¼venlik saÄŸlayan asimetrik bir ÅŸifreleme algoritmasÄ±dÄ±r.

Uygulama Ã–rnekleri:

1. **RSA** kullanarak bir metni ÅŸifreleme ve Ã§Ã¶zme iÅŸlemi.
2. **ECC** kullanarak dijital imza oluÅŸturma ve doÄŸrulama.

1.1.2.4 4. Hibrit Åžifreleme Teorik AÃ§Ä±klama: Hibrit ÅŸifreleme, hem simetrik hem de asimetrik ÅŸifrelemeyi bir arada kullanÄ±r. Simetrik anahtarlar, asimetrik ÅŸifreleme ile gÃ¼venli bir ÅŸekilde paylaÅŸÄ±lÄ±r, ardÄ±ndan veriler simetrik anahtarla ÅŸifrelenir.

- **Uygulama:** E-posta ve HTTPS gibi birÃ§ok gÃ¼venli iletiÅŸim protokolÃ¼nde kullanÄ±lÄ±r.

Uygulama Ã–rnekleri:

1. Simetrik anahtarÄ±n asimetrik olarak ÅŸifrelenmesi ve ardÄ±ndan verilerin simetrik ÅŸifre ile korunmasÄ±.
2. Hibrit ÅŸifreleme kullanarak iki cihaz arasÄ±nda gÃ¼venli veri alÄ±ÅŸveriÅŸi.

1.1.2.5 5. Dijital Sertifikalar ve Sertifika Yetkilileri (CAs) Teorik AÃ§Ä±klama: Dijital sertifikalar, bir kiÅŸinin veya kuruluÅŸun kimliÄŸini doÄŸrulayan elektronik belgeler olarak tanÄ±mlanabilir. Bu sertifikalar genellikle bir sertifika yetkilisi (Certificate Authority - CA) tarafÄ±ndan imzalanÄ±r ve kullanÄ±cÄ±lara gÃ¼venli bir ÅŸekilde iletilir.

- **X.509 SertifikasÄ±:** En yaygÄ±n kullanÄ±lan sertifika tÃ¼rÃ¼dÃ¼r.
- **Sertifika Yetkilisi (CA):** SertifikalarÄ± dijital olarak imzalayan gÃ¼venilir otoriteler.
- **Sertifika Zinciri:** SertifikalarÄ±n doÄŸrulanabilir bir hiyerarÅŸi ile baÄŸlandÄ±ÄŸÄ± yapÄ±. Her sertifika, bir Ã¼st otorite tarafÄ±ndan imzalanÄ±r.

Uygulama Ã–rnekleri:

1. Bir web sunucusu iÃ§in **SSL/TLS** sertifikasÄ± oluÅŸturma ve yÃ¼kleme.
2. **X.509** sertifikalarÄ±nÄ±n doÄŸrulanmasÄ± ve gÃ¼venlik zincirinin incelenmesi.

1.1.2.6 6. Dijital Ä°mzalar Teorik AÃ§Ä±klama: Dijital imzalar, verilerin kimliÄŸini doÄŸrulamak ve deÄŸiÅŸikliÄŸe uÄŸrayÄ±p uÄŸramadÄ±ÄŸÄ±nÄ± kontrol etmek iÃ§in kullanÄ±lÄ±r. Ä°mza,

bir mesajÄ±n karmasÄ±nÄ± (hash) hesaplayarak ve bu karmayÄ± Ã¶zel bir anahtarla ÅŸifreleyerek oluÅŸturulur.

- **Ä°mzanÄ±n DoÄŸrulanmasÄ±:** Ä°mza, kamuya aÃ§Ä±k anahtar kullanÄ±larak doÄŸrulanabilir.
- **Uygulama AlanlarÄ±:** E-posta, yazÄ±lÄ±m daÄŸÄ±tÄ±mÄ±, dijital sÃ¶zleÅŸmeler.

Uygulama Ã–rnekleri:

1. Bir dosya iÃ§in **dijital imza** oluÅŸturma ve doÄŸrulama.
2. **PGP/GPG** kullanarak bir mesajÄ±n imzalanmasÄ± ve doÄŸrulanmasÄ±.

1.1.2.7 7. Sertifika TabanlÄ± Kimlik DoÄŸrulama Teorik AÃ§Ä±klama: Sertifikalar, Ã¶zellikle sunucular arasÄ± gÃ¼venli iletiÅŸimde kimlik doÄŸrulama iÃ§in kullanÄ±lÄ±r. Ä°stemci ve sunucu birbirlerinin sertifikalarÄ±nÄ± doÄŸrulayarak gÃ¼venli bir iletiÅŸim kanalÄ± oluÅŸturur.

- **SSL/TLS:** Web tarayÄ±cÄ±larÄ± ve sunucular arasÄ±ndaki gÃ¼venli iletiÅŸimde kullanÄ±lan bir protokoldÃ¼r.
- **Mutual Authentication:** Hem sunucu hem de istemci birbirlerini sertifikalar aracÄ±lÄ±ÄŸÄ±yla doÄŸrular.

Uygulama Ã–rnekleri:

1. **SSL/TLS** kullanarak gÃ¼venli bir baÄŸlantÄ± kurulmasÄ±.
2. Sertifika tabanlÄ± Ã§ift taraflÄ± kimlik doÄŸrulama senaryosu uygulama.

1.1.2.8 8. PKI (Public Key Infrastructure - AÃ§Ä±k Anahtar AltyapÄ±sÄ±) Teorik AÃ§Ä±klama: PKI, dijital sertifikalarÄ±n oluÅŸturulmasÄ±, daÄŸÄ±tÄ±lmasÄ±, yÃ¶netilmesi ve doÄŸrulanmasÄ± sÃ¼reÃ§lerini iÃ§eren bir yapÄ±dÄ±r. PKI, gÃ¼venli iletiÅŸim saÄŸlamak iÃ§in gerekli anahtar Ã§iftlerinin ve sertifikalarÄ±n yÃ¶netimini saÄŸlar.

- **BileÅŸenler:** CA (Certificate Authority), RA (Registration Authority), CRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol).
- **Uygulama AlanlarÄ±:** SSL/TLS, VPN, e-posta gÃ¼venliÄŸi, kod imzalama.

Uygulama Ã–rnekleri:

1. **PKI** kullanarak bir sertifika yÃ¶netim altyapÄ±sÄ± kurma.
2. **OCSP** ve **CRL** ile sertifika iptallerinin kontrol edilmesi.

1.1.2.9 9. Beyaz Kutu Kriptografisi (Whitebox Cryptography) Teorik AÃ§Ä±klama: Beyaz kutu kriptografisi, Ã¶zellikle ÅŸifreleme algoritmalarÄ±nÄ±n aÃ§Ä±k bir sistemde gÃ¼venli bir ÅŸekilde uygulanmasÄ±nÄ± saÄŸlar. Bu teknikle, ÅŸifreleme iÅŸlemleri sÄ±rasÄ±nda anahtarlar ve diÄŸer hassas bilgiler koruma altÄ±nda tutulur.

- **Whitebox AES/DES:** AES ve DES gibi simetrik ÅŸifreleme algoritmalarÄ±nÄ±n beyaz kutu ortamlarÄ±nda uygulanmasÄ±.
- **Uygulama AlanÄ±:** Dijital hak yÃ¶netimi (DRM), mobil uygulama gÃ¼venliÄŸi.

Uygulama Ã–rnekleri:

1. **Whitebox AES** kullanarak bir dosya ÅŸifreleme iÅŸlemi gerÃ§ekleÅŸtirmek.
2. Whitebox kriptografi ile hassas verileri koruma altÄ±na almak.

1.1.2.10 10. Sertifika ve Anahtar YÃ¶netimi Teorik AÃ§Ä±klama: SertifikalarÄ±n ve kriptografik anahtarlarÄ±n etkin bir ÅŸekilde yÃ¶netilmesi, gÃ¼venli sistemlerin temel yapÄ± taÅŸlarÄ±ndan biridir. SertifikalarÄ±n zamanÄ±nda yenilenmesi, iptal edilmesi ve saklanmasÄ±, gÃ¼venli bir iletiÅŸim ortamÄ± iÃ§in kritik Ã¶neme sahiptir.

Uygulama Ã–rnekleri:

1. SertifikalarÄ±n otomatik olarak yenilenmesi ve eski sertifikalarÄ±n iptal edilmesi (CRL veya OCSP kullanÄ±mÄ±).

2. **Anahtar yÃ¶netim sistemleri** (Key Management Systems) ile anahtarlarÄ±n gÃ¼venli bir ÅŸekilde yÃ¶netilmesi.

$9. Hafta - Sonu$