

An Overview of COMP4631

**Cunsheng Ding
HKUST, Hong Kong, CHINA**

Cryptography

Private-key ciphers, public key ciphers, PKI and digital signature, hash and keyed hash functions, authentication protocols, secret sharing.



Unix Security
[Authentication &
access control]

Operating
Systems
Security

"Firewalls"
Kerberos
IPSec

Network
Security

SSL, TLS,
PGP, S/MIME,
VPN, SSH

Web and
Application
Security

Classification of attacks by capability

- Passive attacks
- Active attacks

Security services covered?

- You are given 5 minutes for writing down all the security services covered in this course.

Security services covered

- Data confidentiality
- Sender (data origin) authentication
- Mutual authentication
- Sender nonrepudiation
- Data integrity (data authentication)
- Anti-reply
- Traffic flow confidentiality
- User identification and authentication
- Access control
- Network boundary safeguarding

How to provide data confidentiality?

Data confidentiality: ciphers

- Ciphers are classified into two types
 - One-key ciphers
 - Two-key ciphers
- Can every two-key cipher be used as public-key cipher?
- What are the main applications of public-key ciphers?

Data confidentiality: ciphers

- Can every two-key cipher be used as a public-key cipher?
- What are the main applications of public-key ciphers?
 - Digital signature (nonrepudiation, sender authentication, data integrity)
 - Session key distribution
 - Mutual authentication

Data confidentiality: ciphers



Original



*Encrypted using ECB
mode*



Encrypted using other modes

Electronic codebook (ECB), **Cipher block chaining (CBC)**,
Cipher feedback (CFB), Output feedback (OFB), Counter

How to provide mutual authentication?

The two most important mutual authentication protocols

- What are the two most important mutual authentication protocols introduced in this course?

The two most important mutual authentication protocols

- What are the two most important mutual authentication protocols introduced in this course?
 - Kerberos (Type-1: Windows 2000, Windows NT5)
 - Challenge-response protocol using a public key (IPSec, SSL, TLS)

**How to provide sender
authentication + data
integrity simultaneously?**

The major techniques for data integrity + sender authentication

- What are the major techniques for sender authentication plus data integrity?

Two major techniques for data integrity and sender authentication

- What are the major techniques for data integrity plus sender authentication?
 - Digital signature (public-key cipher) [PGP, S/MIME]
 - Message authentication codes
 - keyed hash function
 - secret key + hash function with HMAC (IPSec, SSL/TLS, SSH)

Key management

How to establish a secret number by two parties

- What are the two mostly used methods for two parties to establish a secret number?

How to establish a secret number by two parties

- What are the two mostly used methods for two parties to establish a secret number?
 - DH [DH groups] (IPSec, SSL/TLS)
 - Using a public key cipher (IPSec, SSL/TLS)

X.509 digital certificate

X.509 Digital Certificate

- Three versions (v.1, v.2, v3)
 - We introduced only Version 1. That is why you see different ones.
- It is used in:
 - S/MIME
 - IP Security
 - SSL/TLS
 - SET

How to provide sender nonrepudiation?

Digital Signature

- Two methods:
 - RSA+ Hash
 - DSS + Hash (not covered)
- There are similarities and differences between handwritten and digital signature
- Important (nonrepudiation, sender authentication, data integrity)
- Used in PGP and S/MIME

How to provide anti-replay?

How to provide anti-replay

- To encrypt a time-stamp with a shared key
- To add a sequence number for every packet and maintain the sequence numbers of all received packets for a windows of time.

How to provide traffic flow confidentiality?

How to provide traffic flow confidentiality

- What is traffic flow confidentiality?
- How do you provide this service?
- Which security systems covered in this course can provide this service?

How to do identify and authenticate users?

How to identify and authenticate users

- Identifying users
 - User registration
 - Biometrics storage
- Authenticating users
 - Password
 - Biometrics
 - A combination of them
- What are the advantages and disadvantages of one over the other?

How to do access control?

How to do access control

- What is access control?
- What is the basic access control model?
- What are the two approaches to access control?
- What are the advantages and disadvantages of one over the other?
- How to make access control efficient?

How to safeguard boundaries between networks?

How to safeguard boundaries between networks

- By traffic filtering
- What are the major filtering techniques?
 - Packet filtering
 - Session filtering

Q & A