7.5 hp, Spring term 2008

Network Security

Lecture 1

Basic principles and terminology

Symmetric ciphers

Kristina.Kunert@hh.se

Security attacks

Passive	***Active***
Extract information	Alter or affect system
Not affecting system	↓
↓	Masquerade
Release of message contents	Replay
Traffic analysis	Modification of messages
↓	Denial of Service
Prevention	↓
	Detection

Security services

Authentication

- Each is the entity it claims to be
- Connection is not interfered with to prevent masquerading
- Peer entity authentication, Data origin authentication

Access control

- Limit and control access to systems and applications

Data confidentiality

- Protection of transmitted data against passive attacks
- Protection of data flow against analysis

Security services

Data integrity

Connection-oriented vs. Connection-less

↓ ↓

Message stream modification | Message modification

Denial of Service

With recovery vs. Without recovery

↓ ↓

Recover from violation | Report violation

Nonrepudiation

- Prevents sender or receiver from denying a transmitted message

Availability service

- System being accessable upon demand by an authorized system
- Address security concerns raised by denial of service attacks

Symmetric ciphers

- = Symmetric encryption, Conventional encryption, Secret-key encryption, Single-key encryption
- Principles
  - plaintext, encryption algorithm, sekret key, ciphertext, dekryption algorithm
- Secure use
  - Strong encryption algorithm
  - Secrecy of the key
- Cryptographic systems classification
  - Type of operations used during encryption, Number of keys, Processing of plaintext

Cipher Structure

- Feistel Cipher Structure: Sequence of rounds, Substitutions, Permutations, Secret key value
- Parameters: Block size, Key size, Number of rounds, Subkey generation algorithm, Round function
- Design consideration: Fast software en-/decryption, Ease of analysis
- Decryption: Essentially the same as encryption

7

Algorithms

DES

- Plaintext 64 bits, Key 56 bits, 16 rounds, 16 subkeys
- No fatal weaknesses in the algorithm, Relatively short key

3DES

- 3 keys → keylength 168 bits
- 3 DES executions

$$C = E(K_3, D(K_2, E(K_1,P)))$$

AES

- No Feistel structure
- Rounds with: Byte substitution, Permutation, Arithmetic operations, XOR with a key
- Decryption: not only reverse
- Number of rounds depends on keylength

8

Stream ciphers

- Processes input elements continuously
- Produces output one element at a time
- Key = Input to a bit generator → keystream
- Keystream combined with plaintext stream by bitwise XOR: $P \oplus K = C$
- Decryption the same: $C \oplus K = P$
- Design
  - Long period of repeat in the bit generator
  - Keystream as random-like as possible
  - Long keylength

9

Stream algorithms

RC4

- Variable-size key, Byte-oriented operation, Period > 10^{100}, Very fast software

RC4 - Functionality

- Key intitializes 256-byte vector ***S***
- Generate 1 byte *k* by selection from ***S***
- Permute ***S***
- Encryption: XOR *k* with next byte from plaintext
- Decryption: XOR *k* with next byte from ciphertext

10

Location of encryption devices

Link encryption vs. End-to-end encryption

↓	↓
Many of devices	Unaltered transport
High level of security	through network
Vulnerable at switch	Traffic pattern open

↓

Combine for greatest security

11

Self study

- Cipher block modes of operation
  - Chapter 2.4
- Key distribution
  - Chapter 2.6

Will also be included in the exam.

Use also the group-wise exercise hours next week to discuss questions.

12