ECE453 – Introduction to Computer Networks

Lecture 19 – Network Security (II)

Network Security

- Application Layer Security
- Transport Layer Security
- Network Layer Security
- Link Layer Security
- Physical Layer Security

Cryptography

- Secrecy
  - Substitution cipher
  - Transposition cipher
  - One-time pad
  - Symmetric-key cryptography
  - Public-key cryptography
- Authentication
- Nonrepudiation
- Integrity

Kerckhoff’s principle: All algorithms must be public; only the keys are secret
Refreshness and Redundancy in the message
IPsec

- Where to put security?
- A framework for multiple services, algorithms, and granularities
  - Services: secrecy, integrity, prevent replay attack
- Connection-oriented
  - SA (Security Association)

The IPsec authentication header in transport mode for IPv4

(a) ESP in transport mode.
(b) ESP in tunnel mode.

Firewalls

A firewall consisting of two packet filters and an application gateway

Virtual Private Networks

(a) A leased-line private network. (b) A virtual private network
Authentication Based on a Shared Secret Key

1. Challenge-response protocol

2. A shortened protocol

3. The reflection attack

4. Using HMAC to counter reflection attack

Establishing a Shared Key: The Diffie-Hellman Key Exchange

1. Alice picks x

2. Bob computes g^x mod p

3. Alice computes g^y mod p

4. n = g^{xy} mod p

5. Each party holds xi

Authentication Using a Key Distribution Center

1. Alice

2. HDC

3. K_A (K_B)

Authentication Using Public-Key Cryptography

1. Alice

2. E_K_B (A, R_A)

3. E_K_B (R_A, R_B, K_B)

4. K_B (R_B)