CS 640 Introduction to Computer Networks

Lecture28

Today's lecture

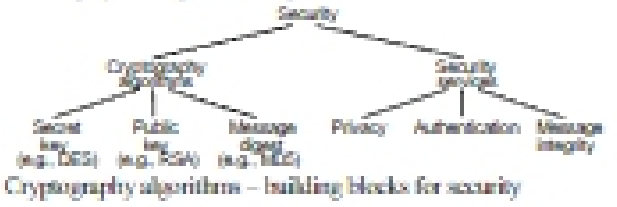
- Network security
  - Encryption Algorithms
  - Authentication Protocols
  - Message Integrity Protocols
  - Key distribution
  - Example: SSH

Why do we care about Security?

- "Toto… I have a feeling we're not in Kansas anymore." Dorothy, *The Wizard of Oz*
- "The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable." ***The Art of War***, Sun Tzu
- There are bad guys out there who can easily take advantage of you.
- Reference: *Cryptography and Network Security, Principles and Practice*, William Stallings, Prentice Hall

Overview

- Security services in networks
  - Privacy: preventing unauthorized release of information
  - Authentication: verifying identity of the remote participant
  - Integrity: making sure message has not been altered



- Cryptography algorithms – building blocks for security
  - Privacy/Authentication
    - Secret key (e.g., Data Encryption Standard (DES))
    - Public key (e.g., Rivest, Shamir and Adleman (RSA))
  - Integrity
    - Message digest/hash (e.g., Message Digest version 5 (MD5))

Issues in Security

- Threat models
  - How are bad guys trying to do bad things to you?
- Key distribution
  - How do folks get their keys?
- Implementation and verification
  - How can we be sure systems are secure?
- Non goal: details of crypto algorithms
  - We are not going to focus on proving anything about crypto algorithms
    - See CS642

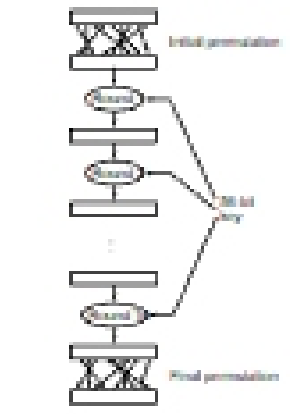
Crypto 101

- Cryptographic algorithms determine how to generate encoded text (ciphertext) from plaintext using keys (string of bits)
  - Can only be decrypted by key holders
- Algorithms:
  - Published and stable
  - Keys must be kept secret
  - Keys cannot be deduced
  - Large keys make breaking code VERY hard
  - Computational efficiency

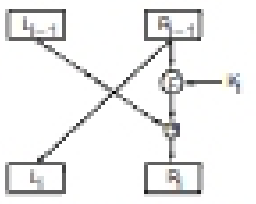
Secret Key (DES)

- Approach: Make algorithm so complicated that none of the original structure of plaintext exists in ciphertext

- Encrypt 64 bit blocks of plaintext with 64 bit key (56 bits + 8 bit parity)
- 16 rounds



- Each Round



- L, R – 32 bit halves of 64 bit block
- K – 48 bits of 64 bit key
- F – combiner function
- + – XOR

- Encryption steps are the same as decryption
- Repeat for larger messages (cipher block chaining)
  - IV = initialization vector = random number generated by sender