Lecture 25

CS625: Advanced Computer Networks
Fall 2003

Wednesday, 15 October 2003

Bhaskaran Raman
CSE, IIT-Kanpur

http://www.cse.iitk.ac.in/users/braman/courses/cs625-fall2003/outline.html

Topic for Today

- Basics in Cryptography and Security
- *Scribe for today?*

Cryptography Fundamentals

- Privacy versus Authentication:
  - Privacy: preventing third party from snooping
  - Authentication: preventing impostering
- Two kinds of authentication:
  - Guarantee that no third party has modified data
  - Receiver can prove that only the sender originated the data
    - Digital Signature
    - E.g., for electronic transactions

Cryptographic Privacy and Authentication

- Encrypt before sending, decrypt on receiving
  - Terms: plain text and cipher text
- Two components: key, and the algorithm
  - Should algorithm be secret?
    - Yes, for military systems
    - No, for commercial systems
- Key distribution must be secure
- Can also be used for authentication

Cryptanalysis

- Cryptanalysis: attacker tries to break the system
  - E.g., by guessing the plain text for a given cipher text
  - Or, by guessing the cipher text for some plain text
- Possible attacks:
  - Cipher-text only attack
  - Known plain-text attack
  - Chosen plain-text attack
  - Chosen text attack

Security Guarantees

- Two possibilities:
  - Unconditional
  - Computational security
- Unconditional security: an example
  - One-time tape
- Most systems have computational security
  - How much security to have?
  - Depends on cost-benefit analysis for attacker

Public-Key Systems

- Shared-key ==> difficulties in key distribution
  - C(n,2) = O(n^2) keys
- Public key system
  - Public component and a private component
  - Two kinds:
    - Public key distribution: establish shared key first
    - Public key cryptography: use public/private keys in encryption/decryption
  - Public key cryptography can also be used for digital signatures

Some Example Systems

- Permuted alphabet (common puzzle)
  - Can be attacked using frequency analysis, patterns, digrams, trigrams
  - Attack becomes difficult if alphabet size is large
- Transposition
- Poly-alphabetic: periodic or running key
- Codes versus ciphering
  - Codes are stronger, and also achieve data compression

Some Popular Systems

- DES, 3DES
- Public key systems:
  - RSA: based on difficulty of factoring
  - Galois-Field (GF) system: based on difficulty of finding logarithm
  - Based on knapsack problem

Taxonomy of Ciphers

- Block ciphers: divide plain text into blocks and encrypt each independently
- Properties required:
  - No bit of plain text should appear directly in cipher text
  - Changing even one bit in plain text should result in huge (50%) change in cipher text
  - Exact opposite of properties required for systematic error correction codes
- Stream cipher: encryption depends on current state

Key Management

- Keys need to be generated periodically
  - New users
  - Some keys may be compromised
- Addressing the O(n^2) problem with key distribution
  - Link encryption
  - Key Distribution Centre (KDC): all eggs in one basket
  - Multiple KDCs: better security

Some Non-Crypto Attacks

- Man-in-the-middle attack: play a trick by being in the middle
- Traffic analysis
  - Can learn information by just looking at presence/absence of traffic, or its volume
  - Can be countered using data padding
- Playback or replay attacks
  - To counter: need to verify *timeliness* of message from sender while authenticating
  - Beware of issues of time synchronization

Error Control and Cryptography

- Internal error control: error control is internal to encryption (before encryption)
  - Can provide automatic authentication
- External error control: error control is external to encryption (after encryption)
  - Required for error correction

Next week...

- Denial of Service Attacks
  - Assigned Reading