Computer and Network Security: Cryptographic Protocols Overview

Kameswari Chebrolu

Recap

- Understood basic building blocks
  - Confidentiality, Integrity and Authentication
  - Private key and public key crypto
- How to secure communication between two parties using above blocks?
  - Need Cryptographic Protocols
    - Protect messages, protect parties involved, ensure communication etc

Example: Human Protocol

Protocol

- Defines format and rules for exchange of messages for a specific goal
  - E.g. TCP, IP, CSMA/CD (Ethernet)
  - What to send: Format
  - When to send & How to act : Rules
- Cryptographic Protocols: How to “establish, maintain and use” secure communication channels ?
  - Achieve some security related goal
  - E.g. Confidentiality, integrity, authenticity, non-repudiation; combinations thereof

Challenges

- Assumptions: Attacker can
  - Access all messages
  - Modify/Inject/drop messages
- Few Example Attacks:
  - Replay attack: record messages and replays them later
  - Man-in-the-middle: Interposes between two communicating parties and pretends to be the other
- Distributed nature → only local view

Simple Example

- A → B : Send $E_k(M)|MAC(E_k(M))$ or $E_{B,pu}(M|S)$
  - M: Transfer 1 Lakh rupees; S: signature
- Replay attack: Attacker snoops and sends same message again
  - B thinks it is valid and acts on it
  - Need to preserve **originality**
- Delay attack: Attacker delays the message (e.g buying stock)
  - Originality preserved (B gets only one copy) but **timeliness** lost

Crypto Protocols

- Crypto Protocol design notoriously hard
- Focus: Authentication protocols
  - How to establish the channel?
    - Identity of end parties needs to be confirmed
  - Once channel established (identity confirmed), maintain and use are easier to handle within protocol
  - Authentication is also about preserving timeliness and originality

Factors

- Human vs Computer
  - Remembering Passwords, biometrics, public or private machine
- Password vs Cryptographic
  - Ease vs complexity
- One-way vs Two-way vs Mediated authentication

Basic Idea

- Long term key:
  - Could be shared/secret key or public key
  - Exists before authentication protocol begins
  - Does not change from session to session
- Short term / Session key:
  - Often shared key because public key operations are expensive
  - Authentication protocols help agree on this key
  - Valid only for that session of the protocol

Gist

- Use Long-term key to authenticate
- In the process establish a short-term session key
- Use session key for confidentiality and integrity

Why like this?

- Shared key operations are faster than public key; pre-distribution of shared keys difficult
  - Use public key for authentication and session key establishment; then use session key for confidentiality
- Changing session key
  - Yields less ciphertext for cryptoanalysis
  - Less information exposed if key compromised
  - Deters replay attacks

Outline

- Long-term Key Management
  - Shared and Public key systems
- Authentication Protocol
  - Short-term/session key establishment
  - One way, two-way and mediated authentication
  - Confidentiality/Integrity of data