Introduction to Cryptography CS 355

Lecture 35

Additional Slides on Key Establishment Protocols

Notions of Authentication

- Entity authentication: identity of a party, and aliveness at a given instant
- Data origin authentication: identity of the source of the data
- Implicit key authentication: one party is assured that no other party aside from a specifically identified second party may gain access to a particular secret key.
- Key confirmation: one party is assured that a second party actually has possession of a particular secret key.
- Explicit key authentication: both (implicit) key authentication and key confirmation hold.

Objectives

- Authentication protocol
  - e.g., challenge/response, ZK proof
- Key establishment protocol
  - e.g., Diffie-Hellman
- Authenticated key establishment: key establishment protocol which provides key authentication
- Authenticated key establishment with entity authentication

Assumptions and Adversaries

- Assumption: Protocol messages are transmitted over open networks
- An adversary may
  - deduce a session key using eavesdropping.
  - altering messages to be able to deduce the key
  - deceive a legitimate party regarding the identity of the party with which is shares a key
  - initiate one or more protocol execution (possibly simultaneously) and combine messages from one with another)

Effects of Key Compromise

- Perfect forward secrecy: compromise of long-term key does not compromise past session keys.
- Known-key attack: compromise of past session keys allows either a passive adversary to compromise future session keys, or impersonation by an active adversary in the future.

Other Issues in Key Establishment

- Type of the authentication: unilateral vs. mutual
- Key freshness: whether the established key could be one used in previous sessions
- Key control: key distribution vs. key agreement
- Efficiency: communication (number of message and communication rounds) and computation (exponentiations and digital signatures) costs
- Use of trusted third party (TTP):
  - on-line/off-line/no third party
  - degree of trust required in a third party

Key Establishment by Means of Symmetric Encryption

- Every pair shares one long-term key
- Use TTP
  - Each entity maintains long-term keys with TTP
  - Easy to add and remove entities
  - Each entity needs to store only one long-term secret key
  - Trust in TTP, it can read all messages.
  - Compromise of TTP leads to compromise of all communication channels.

Coming Attractions …

- Information Theory