IT322
Security Protocols

(3-0-0: 3)

Objective of this course

Protocols describe how entities communicate among themselves over a communication medium.

It has been observed that a protocol may fail in three ways: the protocol design may be flawed; the cryptographic primitives used in the protocol may be weak; or the implementation contains bugs.

This course aims to cover:

- Security protocol goals, assumptions, trust model.
- Some well-known protocols including Kerberos, SSL, IPSec, WPA.
- Attacks and Fix on security protocols.
- Design and analysis of security protocols.

Topics

- **Security goals** - authentication, privacy, integrity, anonymity,…
- **Key management** - public key infrastructures
- **Fundamental Security Protocols** - Needham-Schroeder, Diffie-Hellman, Kerberos, SSL/TLS, IPSec
- **Threats, Attacks, and Defenses** - replay, man-in-the-middle, session freshness, forward secrecy, denial-of-service
- **Key agreement** - secret key based, public key based
- **Protocol analysis** – Logic-based approach
- **Anonymity** – e-cash, micro-payment
- **Multiparty computation** - Oblivious transfer, bit commitment

Reading material

- Network Security -- Kaufman, Perlman, Speciner, [Prentice Hall], 2002.
- Cryptography and Network Security: Principles and Practice -- William Stallings, [Prentice Hall], 2003.

And, a number of research papers related to topics. The research papers are listed on course homepage.

Grading policy (tentative)

- First In-semester exam : 20 %
- Quizzes/Class participation: 20 %
- Second In-semester exam
  OR research paper study and presentation : 20 %
- End-sem exam: 40 %

What is Security?

- In an objective sense, security measures the **absence of threats** to acquire values.

- In a subjective sense, security measures the **absence of fear** that such values will be attacked.

- **Security is a system property**. Security is much more than a set of functions and mechanisms (crypto). It is the process of ensuring confidentiality, integrity, and availability of systems/computers, their programs, hardware devices, and data.

What is Security?

- Making sure that bad things do not happen
- Reducing the chances that bad things will happen
- Lowering the impact of bad things
- Providing means to recover from bad things

…

- Allowing good things to happen
- Managing the cost of the system

Example: Security Protocols' goal

- Protocols describe how communication between entities takes place.
  - A set of rules that governs the interaction between entities.

- Security protocol is an exchange of messages between two or more entities, with security-relevant goals such as:
  - establishing a session key
  - Ensuring secure data transmission
  - achieving authentication
  - Ensuring anonymity
  - …

Example: Security Protocols' assumption

- The protocol may require to work in hostile environments, where the network is under the control of an adversary who can:
  - overhear messages
  - intercept messages
  - modify messages
  - replay messages

- Security protocols use underlying assumptions and cryptographic primitives to achieve their security goal(s).