

General Concepts

- **Players:**

Alice, Bob and Trudy.

- **How to communicate *securely* over an *insecure* medium?**

Alice should be able to send a message to *Bob* that *Trudy* can't **understand** or **modify** and *Bob* is assured that *Alice* is the **sender**.

- **Passive Attacks:**

The attacker *eavesdrops* and *read/record* messages in transit.

- **Active Attacks:**

The attacker may *transmit* new messages, *replay* old messages, *modify/delete* messages on transit.

- **Layers and Cryptography:**

- Application (e.g., **PEM**),
- Transport (e.g., **SSL**),
- Network (e.g., **IPsec**).

- **Authentication:**

Who are you?

- **Authorization:**

Should you be doing that?
ACL (access control list) & Groups.

- **Trojan horse/virus/worm:**

Malicious code written by bad guys.

- Modern mail systems & Internet connectivity (Cable Modems/DSL) contribute to its spread.
- Virus Checkers: looks for instruction sequences for known viruses and uses message digests for files.

- **Security Levels:**

unclassified < confidential < secret < top secret

- **Mandatory Access Control Rules:**

No **read-up** (read higher rating object).

No **write-down** (write an object with lower rating).

- **Covert Channels :**

Very low bandwidth (e.g., 1 bit every 10 seconds),
but can be used to steal cryptographic keys.

E.g., a Trojan horse may use **timing channel** or **storage channel**

Loops 1 minute if a bit is 1 and **waits** 1 minute if a bit is 0.

Creates a file for 1 minute if a bit is 1 and **deletes** the file for 2 minute if a bit is 0.

- **Steganography:**

Hide secret messages in other messages.

E.g., hide messages in images by replacing the least significant bit of each byte of the image with the bits of the message.

DEMO: /home/cs772/public_html/demos/steganography

- **The Orange Book:**

Rates computer systems (*D, C1, C2, B1, B2, B3 and A1*). E.g.,

- C1 classical time-sharing system like Unix (use login/password and access control (owner/group/world) to protect files.
- C2 is C1 + access control per user granularity, clearing allocated memory file space, and audit trails.
- B1 is C2 + use security labels for users/processes/files and prevent read-up and write-down., printers attach label to each printed page.

- **Patents & Export Control:**

Luckily most patents have expired (e.g. RSA Sept 20, 2000),
and recently most export control has been lifted.

The US considered encryption as dangerous as the weapons of mass destruction, like nuclear and biological technology.