Network Security: Introduction

Intro

We'll mostly be looking at how you design protocols with security in mind.

Key Requirements for Security

Confidentiality: only the sender and the intended recipients should be able to read/understand the message contents. Note that the contents could include the headers (as opposed to just the payload).

Authentication: sender and receiver need to confirm each other's identities.

Message Integrity: the sender and receiver want to ensure that the message hasn't been altered without detection.

Access and Availability: prevent activity that makes services inaccessible or unavailable to users.

Note you may not want all of these all the time – you may just want message integrity in a given instance, for example.

Friends and Enemies

Bob and Alice want to communicate securely over an unsafe channel. Trudy (an intruder) may intercept, delete, and/or add messages to the channel.

Network Security Threats

Depending on the context, not all threats matter. Here are some potentially relevant ones:

- eavesdropping – someone is intercepting messages

  - this can be very hard to detect if the messages aren't being modified
- actively inserting messages
- impersonation – pretend to be somebody else
  - can construct arbitrary packets/frames with false addresses
- hijacking – take over ongoing connection by removing sender or receiver and replacing them with yourself
- denial of service – prevent the service from being used by others

Cryptography

Cryptography refers to techniques for secure communication in the presence of third-parties.

It involves encryption, where a message is converted to an encoded message which is useless to an adversary.

It should be easy for a recipient to decode a message but very hard to a third-party.