CS 456 Hao Pan
Salahuddin, Mohammad
Spring 2018

Chapter 1.6 - Networks Under Attack: Security

15/05/2018 [T]

Network Security

The internet was not originally designed with much security in mind.

- The internet was originally envisoned to be ”a group of mutually trusting users attached to a transparent network”.
- Obviously, the internet did not turn out that way. Bad people may try to *attack* computer networks.
- Thus, internet protocol designers are playing ”catch-up” in order to *defend* networks against attacks.
- **Malware** is placed into hosts via the internet. They can get in from:
  - **Virus**, which are self-replicating infections from receiving or executing an object (**ex.** *e-mail attachment*).
  - **Worm**, self-replicating infections from receiving an object that is executed on its own.
- **Spyware** can record keystrokes or websites visited. Collected info is uploaded to a collection site.
- Infected hosts may be enrolled in a **botnet**, which is used for *DDoS attacks*.
- **DoS** (*Denial of Service*) attacks make resources (such as server or bandwidth) unavailable by *legitimate traffic*. It does this by flooding the resources with *bogus traffic*. It uses the following steps:
  - Hosts around the network are broken into and enrolled in the botnet.
  - Compromised hosts send packets to the target.
- **Packet sniffing** is also sometimes used to obtain data. A network places itself between a source and destination network and reads all packets passed between them.
- **IP spoofing**: when packets are sent with a *fake IP address* in order to mask the identity of the sender or to impersonate another system.