**CS 458/658 - Computer Security and Privacy** **Fall 2018**

Lecture 10: October 11, 2018

*Lecturer: Ian Goldberg* *Notes By: Harsh Mistry*

# 10.1 Network Security

## 10.1.1 Network Concepts

- Internet is a network of network where all components communicate via TCP/IP

### 10.1.1.1 TCP/IP protocol suite

- Transport and network layer designed in the 1970's to connect local networks at different universities and research labs
- Participants knew and trusted each other
- Design addressed non-malicious errors, but no delicious errors.

### 10.1.1.2 Threats in networks

- Intelligence
- Attacks on confidentiality
- Impersonation and spoofing
- Attacks on integrity
- Protocols failures
- Web site vulnerabilities
- Denial of Service
- Botnets
- Threats in active/mobile code
- Script Kiddies

### 10.1.1.3 Port Scan

- To distinguish between multiple applications running on the server, each application runs on a port
- Attacker sends queries to ports on target machine and tries to identify whether and what kind of application is running on a port

- Identification based on loose-lipped applications or how exactly implements a protocol
- Loose-lopped systems reveal information that could facilitate an attack
- Nmap tool can identify many applications
- Goal of attacker is to find application with remotely exploitable flaw

#### 10.1.1.4 Intelligence

- Social Engineering (Attacker gathers sensitive information from a person)
- Dumpster diving
- Eavesdropping on oral communication
  - Owner of node can always monitor communication flowing through node
  - Can also eavesdrop while communication is flowing across a link
  - Eavesdropping can also occur if secure communications are mistakenly sent to the wrong recipient.
- Social media and cloud data can be used to collect alot of senstive information as we share more details online

#### 10.1.1.5 Impersonation

- Impersonate a person by stealing his/her password
  - Guessing attack
  - Exploit default passwords that have not been changed
  - Sniff password while it is being transmitted two nodes
- Exploit trust relationship between machines/accounts
  - Rhosts/rlogin allows user A on machine X to specify that user B on machine Y can act as A on X without having to enter password
  - Rlogin is trust based on encrypted or reliant on passwords

#### 10.1.1.6 Spoofing

- Object masquerades as another object
- URL spoofing
- Web page spoofing and URL spoofing are used in Phishing attacks
- **Evil Twin** attack for Wifi access points
- Spoofing is also used in session hijacking and man-in-the-middle attacks

#### 10.1.1.7 Session Hijacking

- TCP protocol sets up state at sender and receiver end nodes and uses the state while exchanging packets
- Web servers sometimes have client keep a little piece of data ”cookies” to re-identify client for future visits
  - Attacker can sniff or steal cookie and masquerade as client
- Man in the middle attacks can be executed to capture sensitive data

#### 10.1.1.8 Integrity Attacks

- Attacker can modify packets while they are being transmitted
  - Change payload of packets
  - Change address of sender of receiver end node
  - Replay previously seen packets
  - Delete or create packets
- Line noise, network congestion, or software errors, could also cause these problems.
- DNS cache poisoning is an excellent example of an integrity attack
  - DNS will keep a cache of mappings between domain names and destination addresses.
  - An attacker can modify these mappings or create new wrong ones to point the user to a different end location.

#### 10.1.1.9 Protocol Failures

- TCP/IP assumes that all nodes implement protocols faithfully
- E.g TCP includes a mechanism that ass a sender node to slow down if the network is congested.
- Some implementations do no check whether a packet is well formatted
- Protocols can be very complicated, behaviour in rare cases may not be uniquely defined
- Some protocols include broken security