Computer and Network Security: Network Security Overview

Kameswari Chebrolu

What is Network Security?

*"**Network security** consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer **network** and **network**-accessible **resources**. "*

(From wikipedia.org)

Why are networks vulnerable?

- **Protocols not designed with security in mind**
- Protocols complex and heterogeneous
  - Many points of attack
- Built-in anonymity
- Lot of sharing
  - Services (printer), media (e.g. wireless), files (windows sharing) etc

Protocol Security

In the past, protocols not designed with security in mind

- Confidentiality: No one can read our data
  - Reality: No encryption by default in any protocol (data or headers)
- Integrity: No one can alter our data
  - Reality: Simple checksum, CRCs; not cryptographically secure

- No notion of authenticity (signatures)
- Availability: Network resources available to us when we want (further, not available to unauthorized users)
  - Reality: Distributed implementation gives some tolerance but still susceptible to say DOS attacks

Current Status

Things are not so bad …

- Application Layer: SSH (remote login), PGP (for emails), DNSSEC (for DNS)
- Transport Layer: SSL/TSL
  - Used by applications to add security on top of TCP

- Network Layer: IPsec, BGP-S (secure BGP routing protocol)
  - Ipsec: Needs OS changes; mostly used by VPNs (virtual private networks)
    - Two modes:
      - Transport: IP payload encrypted)
      - Tunnel: entire IP encrypted and put in another IP packet; helps with NATs
- Link Layer: WEP, WPA (wireless)
- Firewalls, DMZ (demilitarized Zone) etc

Network Battlefield

- Attacks
- Defenses

Composition of an Attack

- Scanning for vulnerable machines
- Sniffing traffic to determine current state
- Spoofing to cover up tracks
- Exploit i.e. use vulnerability to execute the attack

Scanning

- Can scan network topology, OS used by machines; ports and services open on machines
  - Scanning often employed by sysads also
- Network topology: How?
  - Ping sweeping (which machines are up)
  - Traceroute: path taken by acket

- OS: How?
  - Make TCP connection to target; Examine initial window size, distribution of sequence numbers, TCP options etc
- Ports and Services: How?
  - Establish TCP/UDP connections to different ports
    - Check port open or closed
    - Well-known ports mapped to specific services
    - Banner grabbing: guess service at a port based on message/challenge received from remote machine
- NMAP: A useful tool to check out

Sniffing

- Can sniff traffic to mine username/passwords, locate important machines (DHCP/DNS servers etc)
  - Tools: tcmpdump/wireshark; set interface in monitor/promiscuous mode
- Difficult to sniff with Ethernet star topology; Wireless is easier
  - Attacks like ARP cache poisoning, MAC flooding (to be covered later) can help sniff

Spoofing

- Take on some other IP or MAC address
  - Can cover track (longer hops, better it is)
  - Gain access to resources (e.g. MAC address based authentication)
- Note: With IP spoofing, Reply will go to original source

Vulnerability/Exploits

- Weak passwords, OS flaws, software bugs, un-validated user input
- Get a remote shell, preferably with root permissions
  - Access private data, install malicious software, delete files
- Above done with good intentions → penetration test (find exploitable vulnerabilities)
- Tools to check out: Nessus, Core Impact (commercial)

Defenses

- Hard problem; need to defend against many points of attack
  - Requires proper planning, careful execution and regular maintenance

Common techniques:

- Fix Protocol shortcomings (not always possible due to wide spread use)

- Perimeter via firewalls:
  - Keeps certain type of traffic away from computers protected by it
  - Logic: Alls eggs in one basket; watch carefully
- Intrusion Detection System (IDS)
  - Match traffic to known attack patterns (signatures) and block
  - Clever attacker can use IDS as a honey pot
    - Launch false attack to trip IDS, then carry real attack

- Host based defenses
  - Firewalls and HIPS (host based intrusion prevention system)
  - Anti-virus, anti-spyware to locate malware
  - Integrity checkers (e.g. tripwire) ensure files are not modified
    - Periodically compare file on disk with its hash

Summary

- Internet a very powerful resource but full of dangers
  - Any machine connected to it can be exploited
- Network protocols not designed with security in mind
  - Many attacks possible
- Network Security becoming increasingly important → Variety of defense mechanisms are being put in place to provide security