Network Security
A Layered Perspective

7 OSI Layer
- Application
  - TFTP, DNS, HTTP, SSH, Telnet, SMTP, SNMP, POP3, etc.
- Presentation
  - AFP, NCP, XDR, NDR
- Session
  - ASP, H.245, PAP, PPTP, RPC, SMPP, SCP, ZIP

7 OSI Layer
- Transport
  - TCP, UDP, RSVP, SCTP, RUDP
- Network
  - IPv4, IPv6, ICMP, ARP, RARP, IGMP
- Data Link
  - Ethernet, Wi-Fi, ATM, FDDI, Token Ring, Bluetooth
7 OSI Layer

- Physical
  - Modems, Ethernet cards, UTP, fiber optics, RS232, USB, SONET, GSM, Bluetooth.
  - Additional layers?
    - People
    - Robotic Machines

Components of IT Security

- Physical Security
  - Locks
  - Guards
- Communications Security
  - Cryptography
  - Spread Spectrum (FHSS, DSSS)
- Computer Security
  - Security Models (Bell-LaPadula, Biba, Clark-Wilson, Chinese Wall)
  - Trusted Computing Base (TCB)

Network Security

- Intrusion Prevention/Detection Systems
- Packet Filtering
- Application Security
  - Secure coding
  - Static Analysis
- User Security
  - Awareness Training
  - Social Engineering

Fundamental Objectives

- Confidentiality
- Integrity
- Availability
Physical Layer Security

Types of Attack
- Illegal data transfer
  - Portable drives (USB, floppy CD-ROM, iPods)
  - Trojan-loaded freebies
    - Easy to enable any drive with autorun feature

Physical Layer

Attacks
- Illegal data transfer
- Steganography
- Lock picking
- Wire tapping
- Rogue access points
- Key stroke loggers

Types of Attack
- Steganography
  - The art of concealing messages through hidden data that is embedded in a carrier medium

Physical Layer
Types of Attack

- **Lock Picking**
  - The manipulation of lock mechanism without the key

- **Wiretapping**
  - Unauthorized tapping of communication line to listen in
  - How safe is optical cable from tapping?

- **Rogue Access Points**
  - The installation of unauthorized wireless access point to tap into network resources.

- **Keystroke Loggers**
  - The surveillance of activity carried out through a software (Trojan virus) or hardware.

---

Signs of a Compromised System

- Suspicious user accounts
- Unusual activities on open ports
- Unauthorized changes in Windows registry entries
- Unusual scheduled tasks
- Presence of rootkits

---

Investigating an Attack

- Check log files for suspicious events/failed logons
- Look at file shares (net share)
- Check for open sessions (net session)
- Look at NETBIOS over TCP/IP activity (netstat -S)
- Check listening ports (netstat -na)
Investigating an Attack
- Look at unusual scheduled tasks
- Verify administrator accounts
- Check unexpected processes
- Look at unusual services
- Check sudden changes in disk space

Data Link Layer
- Two Sublayers: MAC and LLC
- MAC Address
  - First 3 octets (identifies the manufacturer) (what for ????)
- ARP
- Identify the frame type
  - Look at the EtherType(13th and 14th octet) of the Ethernet frame: 0x0800 (IP); 0x0806 (ARP)

Data Link Layer Security
- Application
- TCP
- UDP
- IP
- Data Link
- Physical

Data Link Layer Attacks
- Packet Sniffing
- MAC Address Spoofing
- ARP Poisoning and Flooding
- Wireless MITM
- WEP Cracking
- Wireless DOS and Frequency Jamming
Packet Sniffing

- Protocol Analyzers
  - **Ethernet** (available for Linux and Windows and now called Wireshark)
  - Packet capture libraries: libpcap, winpcap, jpcap.
  - Place NIC in promiscuous mode to be able to capture all packets.
  - TCPDump/WinDump – console mode packet capturing tool
  - NetStumbler and Kismet – wireless sniffers

MAC Address Spoofing

- **In Linux/Unix**
  - Set the MAC address using `ifconfig eth0 hw ether`

- **In Windows**
  - Start > Control Panel > Network Connections > Properties > Configure > Advanced > Locally Administered Address
  - Change registry setting
  - Use the SMAC tool

The SMAC Tool

- **ARP Poisoning and Flooding**
  - **ARP Poisoning**
    - Associating a valid IP address to a false MAC address
  - **ARP Flooding**
    - ARP poisoning aimed at network switches.
**Wireless MITM Attack**

- A situation where an adversary, E, inserts itself in all communications between hosts A and C, and neither A nor C is aware of the presence of E. Now, all messages between A and C are transmitted via E.
- Can be automated using a **Monkey_Jack** (part of a tool suite called **Air_Jack**)

**WEP Cracking**

- **WEP** is based on the **RC4** cipher
- It uses a 40 bit key concatenated to 24-bit **Initialization Vector** (IV) to form the **RC4** traffic key
- The **IV** gets to be reused after so many iterations
- Large number of frames are collected
- The key is revealed after a sufficient amount of mathematically weak frames
- **Aircrack Tool Suite** is a complete tool chest for **WEP** cracking.

**Defending the Data Link Layer**

- Use encryption (**IPSec** and **VPN**)  
- Use secure shell (**ssh**) instead of **telnet**, **rsh**, and **rcp**. 
- Monitor your network. Watch for
  - Network response/latency variations
  - Network cards in promiscuous modes
- Use static arp table entries (**arp -s**)
- Enforce 128-bit **WEP** encryption
- hmmm... not secure enough?... use WPA or **WPA2**
**Network Layer Security**

- **Application**
- **TCP**
- **UDP**
- **IP**
- **Data Link**
- **Physical**

---

**Internet Protocol Header**

- TTL (Time to Live)
- Source Address
- Destination Address
- Protocol
- Port Numbers
- Length
- Header Checksum
- Options
- Data

---

**TOS (Type of Service)**

First 3 bits are the precedence value:

- 000 (Normal)
- 001 (Priority)
- 010 (Immediate)
- 011 (Flash)
- 100 (Flash Override)
- 101 (Critical)
- ...

The next 3 bits determine the QOS:

- normal, least delay, greatest throughput, best reliability, or least cost.

---

**Protocol Values**

- 0x01 ICMP
- 0x06 TCP
- 0x08 EGRP (Exterior Gateway Routing)
- 0x11 UDP
- 0x09 IGRP (Interior Gateway Routing)

---

**TTL Default Values**

- Windows 2003/XP (128)
- Solaris (255)
- Linux 2.4 (64)
ICMP Packet

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 or 8</td>
<td>0</td>
<td>Echo Request/Reply</td>
</tr>
<tr>
<td>3</td>
<td>0 to 15</td>
<td>Destination Unreachable</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>Source Quench</td>
</tr>
<tr>
<td>5</td>
<td>0 to 3</td>
<td>Redirect</td>
</tr>
<tr>
<td>11</td>
<td>0 or 1</td>
<td>Time Exceeded</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>Parameter Fault</td>
</tr>
<tr>
<td>13 or 14</td>
<td>0</td>
<td>Timestamp Request/Reply</td>
</tr>
<tr>
<td>17 or 18</td>
<td>0</td>
<td>Subnet Request/Reply</td>
</tr>
</tbody>
</table>

Common ICMP Functions
- Ping
- Destination Unreachable
- Traceroute
- Path Discovery
- Traffic Redirection

Ping Options
- `-t` ping specified host infinitely
- `-a` resolve address to hostname
- `-c` count number of echo request to send
- `-d` set DF flag
- `-i` TTL set TTL value
- `-v` TOS set Type of Service
- `-r` count record route for count hops
- `-j` host-list loose source route along host-list
- `-k` host-list strict source route along host-list
- `-w` timeout timeout in msec to wait for each reply

Destination Unreachable

ICMP Type 3 Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Network Unreachable Error</td>
</tr>
<tr>
<td>1</td>
<td>Host Unreachable Error</td>
</tr>
<tr>
<td>2</td>
<td>Protocol Unreachable</td>
</tr>
<tr>
<td>3</td>
<td>Port Unreachable Error</td>
</tr>
<tr>
<td>4</td>
<td>Fragmentation Blocked Error</td>
</tr>
<tr>
<td>5</td>
<td>Source Route Failed</td>
</tr>
<tr>
<td>6</td>
<td>Targets network not found in routing table</td>
</tr>
<tr>
<td>7</td>
<td>Target host not found in routing table</td>
</tr>
<tr>
<td>8</td>
<td>...</td>
</tr>
<tr>
<td>13</td>
<td>Router packet filtering prevents access</td>
</tr>
</tbody>
</table>
**Traceroute**

- Sends packet at an ever-increasing TTL values
- Starts with TTL value=1
- Each time the TTL is decremented to zero, an ICMP type-11 code 0 message is sent
- Sender increments TTL by 1 and resends ICMP packet
- Continues until an unreachable message is generated

**Path MTU Discovery**

- Sender tries to determine the minimum MTU along the path
- Sender sends an ICMP packet with DF=1
- Router or gateway that cannot accommodate discards packet and sends an ICMP type 3 code 4 message

**Redirects**

- Router generates an ICMP message that informs the source of a shorter route
- ICMP Redirect Codes
  - Code  Purpose
  - 0    To target network
  - 1    To target host
  - 2    To service and network
  - 3    To service and host

**Additional Tools**

- Hostname
- Ipconfig
- Nbtstat
- Netsh
- Netstat
- Nslookup
- Pathping
- Event Viewer
- Performance Logs and Alerts
- Network Monitor
- Netdiag
Network Layer Attacks

- **Spoofing**
  - masquerading as the trusted host by using its credentials

- **Non-blind Spoofing**
  - attacker on the same subnet
  - attacker corrupts the datastream of an established connection and re-establishes it based on correct sequence and acknowledgement numbers

- **Blind Spoofing**
  - attacker not on the same subnet
  - attacker sends several packets to the target machine in order to sample sequence numbers
  - works in old systems but newer systems implement random sequence number generation, making it difficult to predict them accurately

Network Layer Attacks

- **Fragmentation**
  - Attacker evades the IDS by sending a fragment that has a shorter timeout than an identical fragment sent to the target
  - Teardrop attack (aka DOS) is made by crafting overlapping fragments. Receivers that are not designed to handle these would lockup/stall

- **Passive Fingerprinting**
  - A system reconnaissance activity to determine the operating system and other characteristics of the remote host

- **Fingerprinting Tools**
  - nmap
  - p0f
  - snort
Network Layer Attacks
- Typical Signatures Used for Fingerprinting
  - TTL value
  - DF flag
  - TOS values
  - Window Size
- Values are matched with entries in a signature database to determine the system.

Network Layer Defense
- Port Knocking
  - Requires a number of predetermined ports in a certain sequence before a service accepts a connection
  - How secure is it?

Network Layer Defense
- Secure IP
  - Use encryption and authentication
  - IPSec Modes
    - Tunnel mode – authenticated header and encapsulated (encrypted) payload
    - Transport mode – only encapsulated (encrypted) payload

Network Layer Defense
- Secure ICMP
  - Disable ICMP
    - in Linux, edit /etc/sysctl.conf and add:
      ```
      net.ipv4.icmp_echo_ignore_broadcasts = 1
      net.ipv4.icmp_echo_ignore_all = 1
      ```
    - then run:
      ```
      sysctl -p
      ```
    - in Windows, enable the ICMP filter controls on the Advanced option of the Windows Firewall
Network Layer Defense

- Secure Routers and Routing Protocols
  - Use built-in packet filtering
  - Configuration is made through the Access Control List (ACL)
  - Disable unused services and interfaces
    - Cisco Discovery Protocol (CDP)
    - DNS
    - Finger
    - HTTP

Questions???