Objectives

- Understand basic network architectures
- Understand network protocols involved in security issues
- Understand routing and address translation
- Understand security zones
Reading

• Chapter 9, Conklin & White
• SpamHaus Attack = https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/

Some of the material in the chapter has been covered in ISE218

Network Architectures

• Wide area network (WAN)
  • Two or more systems in geographically separated areas connected by any of a variety of methods
• Local area network (LAN)
  • Typically smaller in terms of size and geographic coverage (e.g., home office)
  • Consists of two or more connected devices
• Intranet
  • Private network
  • Uses Internet protocols

LAN/WAN distinction is becoming irrelevant
Network Topology

• How the network is physically or logically arranged
• Examples
  • Star
  • Ring
  • Bus
  • Mixed

These definitions are becoming blurred

Topology examples usually refer to physical connections (not internal switch technology)

Network Protocol

• An agreed-upon format for exchanging or transmitting data between systems
• Defines a number of agreed upon parameters, such as
  • Handshaking
  • Data conversion
  • Data compression
  • Error checking

Protocols differ concerning the OSI level at which they operate
The OSI Model

- The OSI model, is a standard for worldwide communications that defines a framework for implementing protocols and networking components in seven distinct layers
- Each layer only needs to know about the layers above and below

Has become more of an architectural approach than a standard

Internet Protocol Stacks

When you design a system, you think that there is a connection here
Packets

- Large chunks of data (segments) are broken up into smaller, more manageable chunks (packets)
- Packet specifications depend on the protocol used
- Advantages
  - You can effectively share bandwidth with other systems
  - You don’t have to retransmit the entire segment if there is a problem in transmission

Some attacks are based on the way the protocol breaks a message into packets
Alternate is circuit switching (e.g., telephone network)

Number System Review

- Computer system terminology uses the following number systems
  - Base 10 (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, …)
  - Base 2 (0, 1, 10, 11, 100, 101, …)
  - Base 16 (1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, 10, 11, …)
- Notation
  - $1A_{16} = 26_{10} = 11100_2$

Think of base 16 (hexadecimal) as a shorthand notation for binary
$11100_2 = 0001 1100_{16}$
$= 1A_{16}$
IP Addressing

- Hosts and other devices have network interfaces identified by an IP address
- IP (IPv4) addresses are 32-bit numbers represented as four groups of 8 bits (byte)
- Written in dotted-decimal notation
- Network ID - portion of the IP address that defines the network to which the device is connected
- Host ID – portion of the IP address that defines the host

Theoretical maximum of $2^{32}$ possible IP addresses (not enough)

Dotted Decimal Notation

An IPv4 address (dotted-decimal notation)

```
172.16.254.1
```

One byte = Eight bits

Thirty-two bits (4 x 8), or 4 bytes
IP Packet

- Header
- Data section (payload)

Can be used to distinguish differing levels of service

Usually TCP or UDP

IPv4 or IPv6

TCP and UDP

- Protocols that run on top of the IP network protocol
- Major difference - the concept of “guaranteed” reliability and delivery
- UDP suitable for streaming audio and name lookup

UDP packets are usually referred to as datagrams
TCP

- Connection-oriented protocol
- Designed to provide a reliable connection between two hosts exchanging data.
- Each packet has a sequence number to show where that packet fits into the overall stream
- Useful for HTTP, FTP, and Telnet

ICMP

- Internet Control Message Protocol
- Control and information protocol used to manage networks
- ICMP packets are sent using the same header structure as IP packets
- Examples
  - Remote network’s availability
  - Length of time to reach a remote network
  - Best route for packets to take
Denial-of-Service (DoS) Attacks

- ICMP protocol has been used by attackers to execute denial-of-service (DoS) attacks
  Possibly more on DoS attacks in a later session
- Because ICMP packets are very small and connectionless, thousands of ICMP packets can be generated in a very short period of time.
- Botnets generate thousands of ICMP packets with a common destination—the attacker’s target

Local Packet Delivery

- Uses a unique hardware address
- **MAC** (Media Access Control) address
  - Assigned by manufacturer
  - Stored in HW
- Format: 6 pairs of hex digits
- To determine the MAC address from IP address IPv4 uses Address Resolution Protocol (**ARP**)

  In ARP, the sending system sends a request (e.g., Who is 10.1.1.140?). The system with that IP address replies with the MAC address
ARP Attacks

• Man in the middle attack – create false entries in a machine's ARP cache so traffic gets routed to a different device
• IPsec can be used to encrypt traffic so that man in the middle attacks become more difficult
• Additional security with IPv6

Number of IP Addresses

• Packet routing uses Internet Protocol (IP) addresses
• IPv4 (32 bit addresses) are insufficient
• IPv6 – 8 groups of 4 hex digits – 128 bit addressing
• Migration to IPv6 is proceeding slowly
Domain Name Service

- Used to map host names (contained within a URL) into network addresses (32 bit IP address)
- Name space (partial)

```
(root)
  mil.gov.net.com.edu.org
  us.them
  another
```

How DNS Works

- Browser passes host name to DNS client.
- DNS client looks up IP address from the distributed database located on the DNS name servers
  - Local
  - Root
  - Authoritative

There are 13 root server identities (A, B, C, ..., M), but many of them are aliased

DNS (Concepts to Remember)

- Provides name to IP address mapping
- Implemented through local address caching
- Distributed database service
  - Very reliable
  - Not always fast
  - Not always up to date
- Vulnerable to attack, for example
  - Responses not encrypted
  - Root servers can be attacked
  - Cache poisoning – cache values can be changed to map to an attacker’s site

SPAMHAUS ATTACK
Spam

- Use of electronic messaging systems to send unsolicited bulk messages
- Very low operating costs
- Huge percentage of e-mail is spam

Attack Parties

- Spamhaus
  - A spam-prevention service based in Europe
  - Victim of one of the largest known cyber attacks
- CyberBunker
  - Web hosting service know to host spammers
  - Affiliated with hacking groups
  - Suspected of organizing the attack
**Attack Summary**

- IN 2013, attackers tried to overwhelm Spamhaus's servers using a distributed denial of service attack
- Used **DNS Reflection**
- Attackers used relatively few computers
- Attackers located in countries with no related laws or limited enforcement
- Generated as much as 300 Gbs of traffic, compared with European Internet Exchange
  - 1 terrabit/sec average traffic
  - 1.5 terrabit/sec peak
- Disrupted Internet service for millions of users in Europe

**DNS Amplification Attack**

- 25 million open DNS servers (100,000 involved in attack)
- Attacker spoofs send address to be the recipient of the attack
- DNS servers respond with 50-100 times the size of the request string
- DNS servers perform the role of a virtual botnet
Outcome

• Attack abated
• Consulting firm redirected attacks to alternate servers
• Slow resolution of DNS server vulnerability

DNS Security Approach

• DNSSEC (DNS Security Extensions)
• Extension of DNS specification – adds new records to the DNS protocol
• Makes DNS more trustworthy
• Uses digital signatures – protects DNS client resolvers from accepting forged DNS data
• Can add significant load to DNS servers
• Slow adoption – 15% in 2016
Port

• To communicate with a computer, you need to specify
  • the address of the host computer
  • the identity of the receiving process on the host computer

Routing

• The process of selecting paths in a network along which to send network traffic
• Router - device that forwards data packets between computer networks
• When a packet reaches a router, the router looks at the destination address to determine where to send the packet.
• Routers use forwarding tables
Subnet

- Logically visible subdivision of an IP network
- Divides the 32 bit IP address into
  - Network ID – network routing
  - Host ID
- Number of bits used for network ID and host ID can vary
- Efficient way of allocating IP addresses
- Host ID can be further divided into subnet number and host ID

Network ID Specification

- Specification of the size of network prefix (and subnet prefixes) is done with
  - CIDR notation – IPv4 and IPv6 (arbitrary network/host boundary)
  - Submask notation – IPv4 (network/host boundary in increments of 8 bits)
- IPv4 notation inefficiently allocates IP addresses

Textbook primarily considers IPv4 notation
CIDR Notation

- First address of a network, followed by a slash character (/), and ending with the bit-length of the prefix.
- Compact specification of
  - IP address
  - Associated routing prefix
- Constructed using IP address and network prefix size
- Host identifier - least-significant bits following the prefix
- For example: 192.168.100.0/24 denotes a 24-bit network ID for Internet routing

CIDR is pronounced “cider”

Called a slash 24 network

Subnet Mask Notation

- Only for IPv4
- A bit mask is shown in dotted decimal notation
- Bitmask is logically “anded” with the IP address to form the network ID
- A subnet mask of 255.255.255.0 specifies the first 24 bits as the network ID
  - \(255_{10} = 11111111_2\)
- A subnet mask of 255.255.255.224 specifies the first 27 bits as the network ID

1 “and” 1 is 1
1 “and” 0 is 0
0 “and” 0 is 0
Subnet Mask Example

- IP address 10.10.10.101 with a subnet mask of 255.255.255.0.

```
00001010.00001010.00001010.01100101
11111111.11111111.11111111.00000000
00001010.00001010.00001010.00000000
```

Network ID

Network Classes

- Class A - subnet mask of 255.0.0.0 (slash 8 network)
- Class B - subnet mask of 255.255.0.0 (slash 16 network)
- Class C - subnet mask of 255.255.255.0 (slash 24 network)

Each network supports $2^{N-2}$ interfaces (N is the slash number)
Example – Conficker Worm

• Identified by SRI (2008)
• SRI identified new malware with honeypot
  • Powerful computer
  • Class B subnet
  • Virtual machine for each distinct IP address
  • Software to monitor malware incidents on each virtual machine
• Issues
  • MS patches (design flaws, # unprotected OSs, patch Tuesday)
  • Separation of attack code from attack
  • Internet connection back to attacker (encrypted)

VLANs

• Logical implementation of a LAN that allows computers connected to different physical networks to act and communicate as if they were on the same physical network
• Has many of the same characteristic attributes of a LAN
• Behaves much like a physical LAN
• Implemented using switches and software

honeypot - trap set to detect, deflect, or counteract attacks

Restricts routers to enhance security
VPN

- Virtual Private Network
- Allows two networks to connect securely across an insecure stretch of network

![VPN Diagram]

Tunneling

- Packets are encapsulated within packets
- Enables dissimilar protocols to coexist in a single communication stream
- Packaging can involve encryption
- Can be used to sneak past a firewall (by encapsulating firewall prohibited protocols within an accepted protocol)
Have You Satisfied the Objectives?

• Understand basic network architectures
• Understand network protocols involved in security issues
• Understand routing and address translation
• Understand security zones