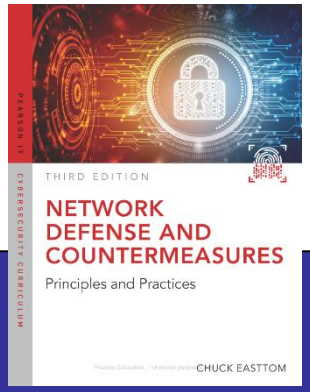
Introduction to Network Security

Based on slides accompanying the book
Network Defense and Countermeasures
by Chuck Easttom (2018)



Objectives

- Identify the most common dangers to networks
- Understand basic networking
- Employ basic security terminology
- Find the best approach to network security for an organization
- Evaluate the legal issues that will affect your work as a network administrator
- Use resources available for network security

Introduction

- The growth of the Internet has brought many ways in which networks can be compromised and data stolen.

- Legislators are working to create laws to prevent identity theft and ways to reduce the effects of viruses and worms such as MyDoom, MSBlaster, and others.

The Basics of a Network

- You need to understand the following:
  - Basic network structure
  - Data packets
  - IP addresses
  - Uniform Resource Locators (or URL)
  - MAC addresses
  - Protocols
  - Basic network utilities
  - The ISO/OSI Model

Basic Network Structure

- The fundamental purpose of networks is for communication
- Part of the network structure includes:
  - NICs, hubs, switches, routers, and firewalls
- Network architecture comprises the format in which these devices are connected

Data Packets

- This is the package that holds the data and transmission information

  A network packet = header + payload

- Ultimately formatted in binary

- Information included in packets:
  - Source and destination (IP Address) information
  - Packet size (in bytes) and type (e.g. Ethernet)
  - Data and other header information

IP Addresses

= network prefix + host identifier

- IPv4 is a series of four three-digit numbers separated by periods: 107.22.98.129 (the *dot-decimal* notation)
  - Each three-digit is between 0 and 255 (a byte/octet)

- Classful network addressing
  - The first byte indicates the network class.
  - classes A through E (See the table in https://en.wikipedia.org/wiki/Classful_network)

Bitwise representation of Classful IP addressing

source: https://en.wikipedia.org/wiki/Classful_network

class D for multicasting
class E reserved (for experimental use)

- *n* indicates a bit used for the network ID.
- *H* indicates a bit used for the host ID.
- *X* indicates a bit without a specified purpose.

```
Class A
  0.  0.  0.  0 = 00000000.00000000.00000000.00000000
127.255.255.255 = 01111111.11111111.11111111.11111111
                  0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B
128.  0.  0.  0 = 10000000.00000000.00000000.00000000
191.255.255.255 = 10111111.11111111.11111111.11111111
                  10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH

Class C
192.  0.  0.  0 = 11000000.00000000.00000000.00000000
223.255.255.255 = 11011111.11111111.11111111.11111111
                  110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH

Class D
224.  0.  0.  0 = 11100000.00000000.00000000.00000000
239.255.255.255 = 11101111.11111111.11111111.11111111
                  1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Class E
240.  0.  0.  0 = 11110000.00000000.00000000.00000000
255.255.255.255 = 11111111.11111111.11111111.11111111
                  1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX
```

IP Addresses

= network prefix + host identifier

- Classless Inter-Domain Routing (CIDR)
  - The suffix indicate the number of bits of the network prefix
  - e.g., 192.0.1.2/24

Q1: What is the network prefix?

Q2: What is the range of host addresses?

IP Addresses

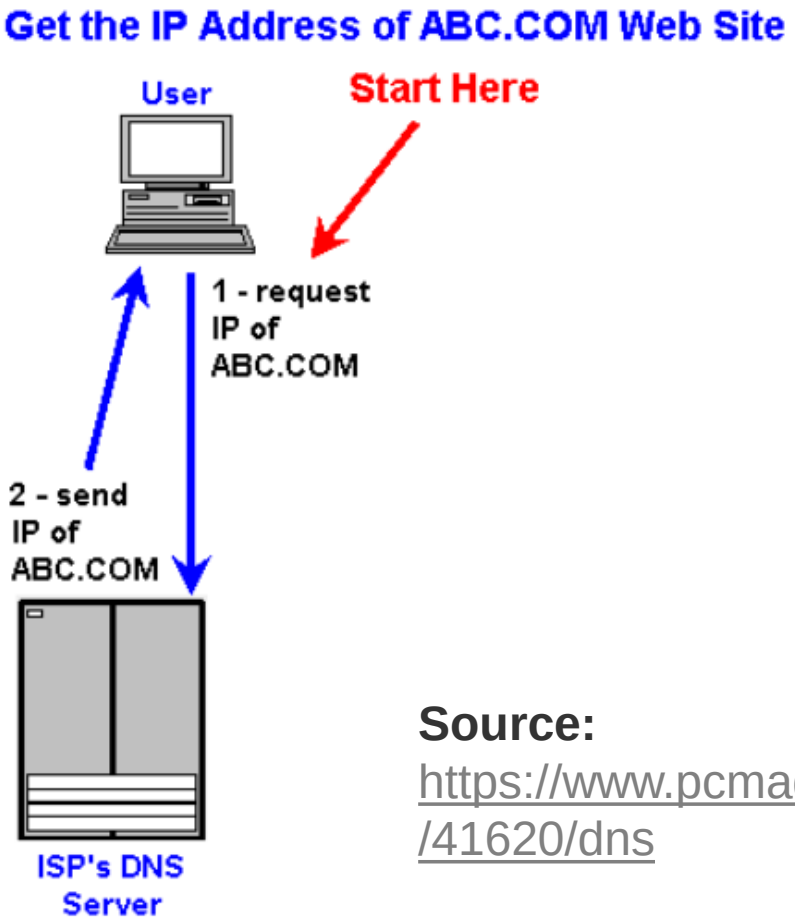
- Certain ranges are private, for use within a private network
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

IP Addresses

- IPv6 uses a 128-bit address and hex numbering.
  - IPv6 addresses are represented as eight groups of four hexadecimal digits (with the groups being separated by colons)
    - Example: 2001:0db8:0000:0042:0000:8a2e:0370:7334
    - An IPv6 address may have more than one representation.

Initial address: 2001:0db8:0000:0000:0000:ff00:0042:8329
After removing all leading zeroes in each group:
2001:db8:0:0:0:ff00:42:8329
After using :: to replace consecutive sections of zeroes:
2001:db8::ff00:42:8329

Uniform Resource Locators



- URLs are text-based web addresses, such as www.chuckeasttom.com, that translate into Internet IP addresses
- Translation is performed by Domain Name System/Service (DNS) servers

Source:
https://www.pcmag.com/encyclopedia/term/41620/dns

MAC Addresses

- MAC addresses are unique hardware addresses
- Every NIC in the world has a unique MAC address
- Six-byte hexadecimal numbers
- Address Resolution Protocol (ARP) converts IP addresses to MAC addresses

Protocols

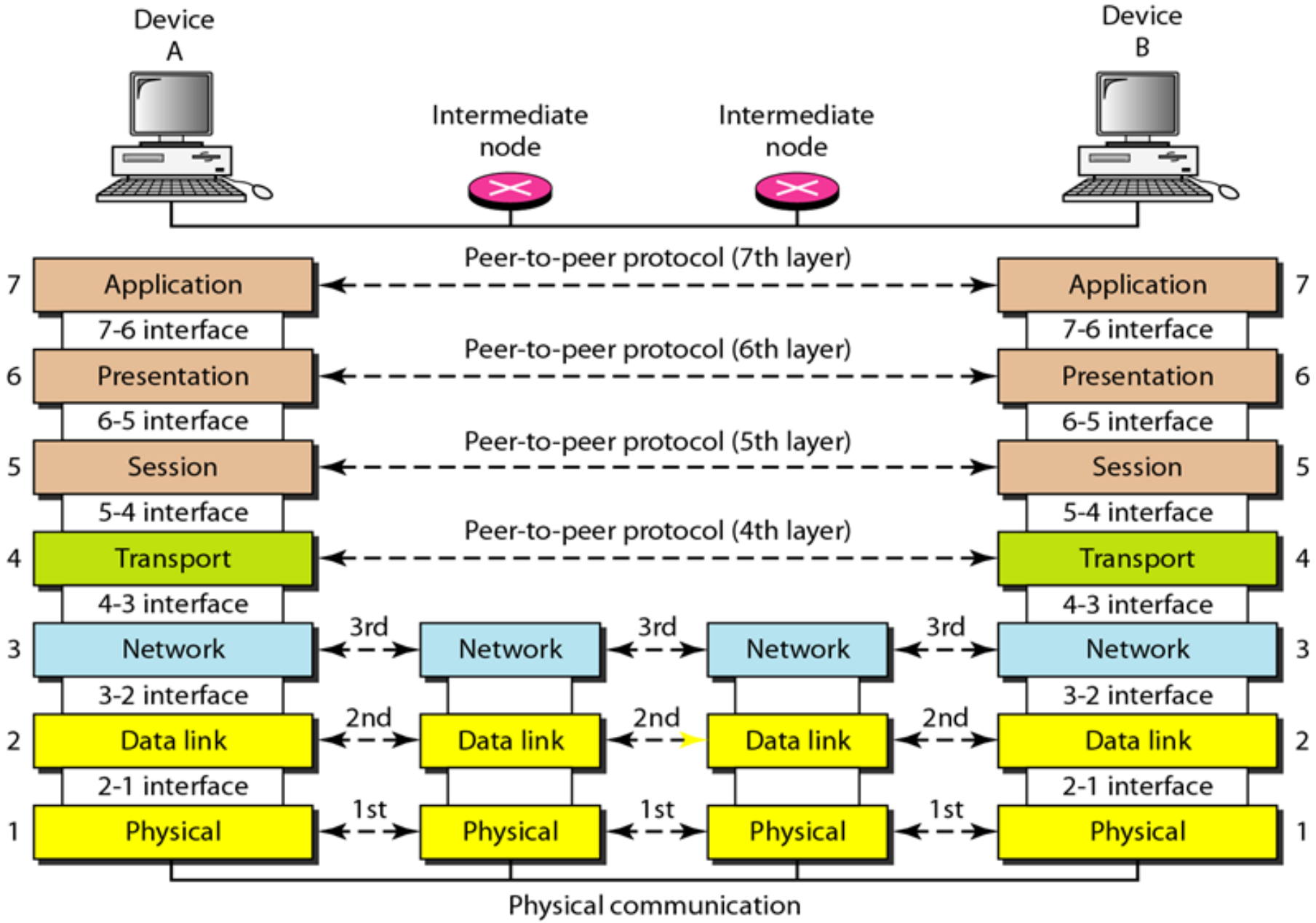
- Types/standards of network communication are called protocols
- Examples include
  - FTP, SSH, Telnet, SMTP
  - WhoIS, DNS, tFTP
  - HTTP, POP3, NNTP
  - NetBIOS, IRC, HTTPS
  - SMB, ICMP

Basic Network Utilities

- Ipconfig
  - gives you information about the computer's network connection, addresses, …
- Ping
  - Used to send a test packet to a target machine to find out whether that machine is reachable and how long it takes …
- Tracert
  - Trace route (= ping + intermediate hops)
- Netstat
  - Net Status

The Open Systems Interconnect (OSI) Model

Layer	Description	Protocols
Application	This layer interfaces directly to applications and performs common application services for the application processes.	POP, SMTP, DNS, FTP, Telnet
Presentation	The presentation layer relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems.	Telnet, Network Data Representation (NDR), Lightweight Presentation Protocol (LPP)
Session	The session layer provides the mechanism for managing the dialogue between end-user application processes.	NetBIOS
Transport	This layer provides end-to-end communication control.	TCP, UDP
Network	This layer routes the information in the network.	IP, ARP, ICMP
Data link	This layer describes the logical organization of data bits transmitted on a particular medium. The data link layer is divided into two sublayers: the Media Access Control layer (MAC) and the Logical Link Control layer (LLC).	SLIP, PPP
Physical	This layer describes the physical properties of the various communications media, as well as the electrical properties and interpretation of the exchanged signals. In other words, the physical layer is the actual NIC, Ethernet cable, and so forth.	IEEE 1394, DSL, ISDN



Source: http://www.ques10.com/p/18473/what-is-osi-model-give-functions-and-services-of-e/

What Does This Mean for Security?

- There are three points of attack:
  - The data itself
    - Data at rest vs data in transit/motion
  - The network connection points
  - The people

Assessing Likely Threats to the Network

- Extreme, ill-informed attitudes about security threats can lead to poor decisions.

- These are the two ends of the spectrum
  - There is no real threat, nothing to worry about
  - Extreme alarm: all hackers are experts and out to break into my network

Assessing Likely Threats to the Network

- No real threat:
  - Fosters a laissez-faire attitude toward security
  - Promotes a reactive approach to security
  - Security measures are not put in place until after a breach has occurred.
  - This approach must be avoided at all costs.

Assessing Likely Threats to the Network

- Is the world full of hackers out to get me?
  - Yes, they exist, but not to the extent publicized
  - Lesser skilled hackers are more pervasive
    - They target smaller companies
  - Usually experts seek high profile networks
  - Financial and ideological gain are the targets

Assessing Likely Threats to the Network

- The only practical approach is the realistic one.
- This approach is a moderate solution to the two extremes.
- Assessment is a complex task.
- Many factors need to be addressed.

Classifying Threats by Function

- Intrusion
  - Cracking
  - Social engineering
  - War-dialing
  - War-driving
- Blocking
  - Denial of Service (DoS)
  - Distributed Denial of Service (DDoS)
- Malware
  - Viruses
  - Worms
  - Trojan horses
  - Bots
  - Ransomware
  - Spyware
    - Cookies
    - Key loggers

Likely Attacks

- Administrators should ask:
  - What are the realistic dangers?
  - What are the most likely attacks for our network?
  - What are some common vulnerabilities?
  - What is the likelihood of an attack?

→ Risk Management

Threat Assessment Factors

- Attractiveness of the system (discussed earlier)
- The nature of the information on the system
- Traffic to the system (security devices in place)

Threat Assessment

- Vulnerability score

- A numerical scale can be assigned to each factor
  - Attractiveness (A): 1–10
  - Information content (I): 1–10
  - Security devices present (S): 1–10
- The equation is: V = (A + I) – S
  - Where V equals Vulnerability score
  - Lower score indicates lower risk (-18 .. 19)

Understanding Security Terminology

Hacking terminology

- White hat hackers
- Black hat hackers
- Gray hat hackers
- Script kiddy
- Cracker
- Ethical hacker (or pen tester)
- Phreaking

Security terminology

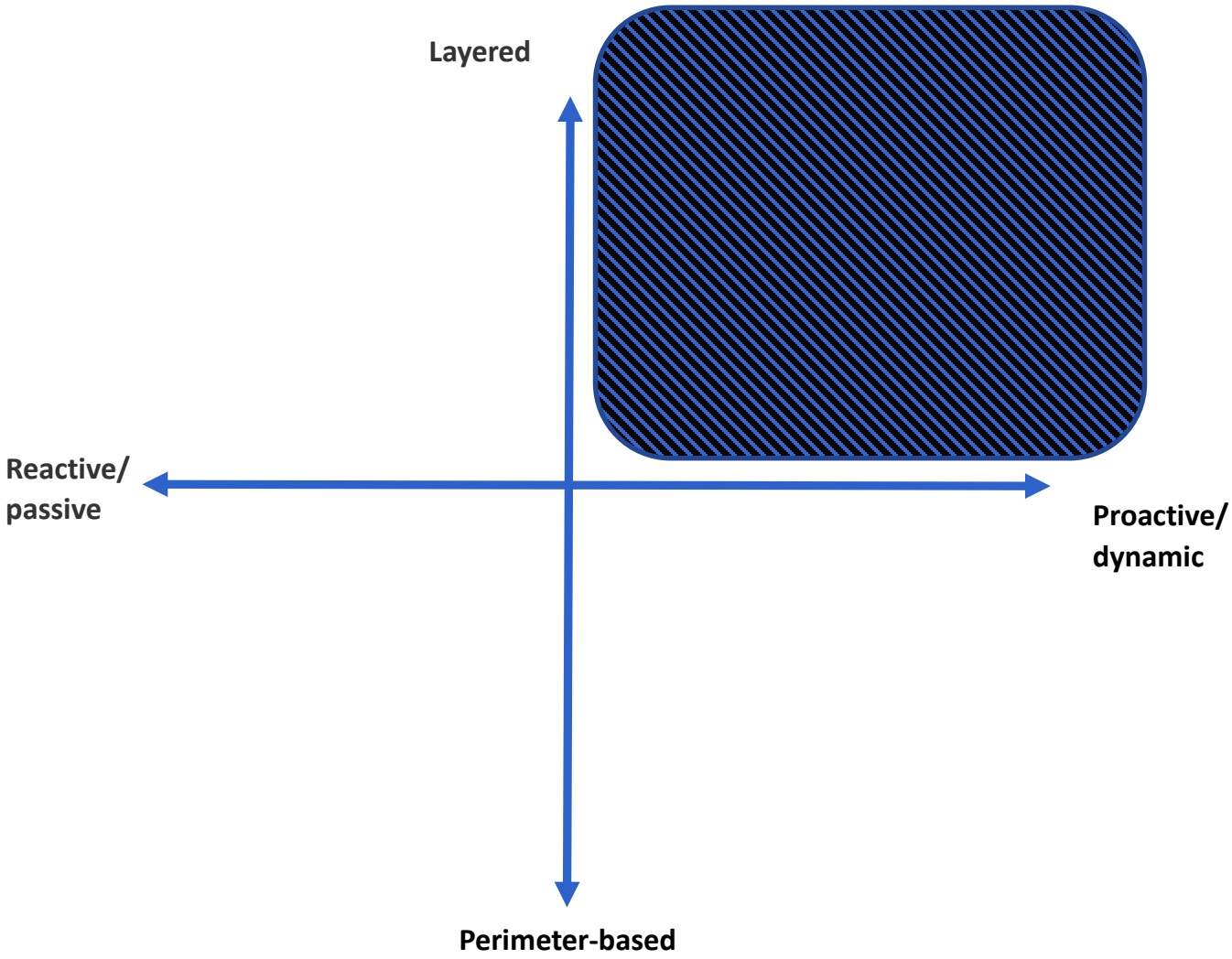
- Firewall
- Proxy server
- Intrusion-detection system
- Non-repudiation
- Confidentiality
- Authentication
- Data integrity vs origin integrity
- Auditing
- Access control
- …

Helpful Websites for Security Terminology

- www.yourwindow.to/information%2Dsecurity/
- www.ietf.org/rfc/rfc2828.txt

Approaching Network Security

- Proactive versus reactive/passive
- *Perimeter security approach*: Focus is on perimeter devices; internal devices are still vulnerable
- *Layered security approach*: Focus includes both perimeter and individual computers within the network
- *Hybrid security approach*: Combination of multiple security paradigms


Layered
Reactive/
passive
Proactive/
dynamic
Perimeter-based

Network Security and the Law

- Sarbanes-Oxley (SOX)
- Computer Security Act of 1987
- Health Insurance Portability and Accountability Act (HIPAA)

Using Security Resources

- CERT (www.cert.org/)
- Microsoft Security TechCenter (https://technet.microsoft.com/en-us/security)
- F-Secure Corporation (www.f-secure.com/)
- SANS Institute (www.sans.org/)

Summary

- Most common dangers to networks are viruses, worms, Trojan horses, and ransomware.
- Basic security terminology:
  - Hacking terms: Deal with people and activities
  - Security terms: Deal with devices and policies
- Approaches to securing your network:
  - Proactive versus reactive
  - Perimeter versus Layered
  - Hybrid

Summary

- Legal issues:
  - SOX
  - HIPAA
  - State-specific legislation regarding computer crimes
  - Business-specific legislations
- Resources available for network security:
  - CERT
  - Microsoft Security TechCenter
  - F-Secure Corporation
  - SANS institute