Protecting Information Assets
- Week 9 -

Network Security

MIS5206 Week 9

- Team Presentation
- Network Security
- Test Taking Tip
- Quiz

In the News

- Discuss items “in the news”

Reading

- Vacca Chapter 4 -13
- Read and be prepared to discuss:
  Case 2 -SECURITY BREACH AT TJX

Network Security

The purpose of network security, quite simply, is to protect the network and its component parts from unauthorized access and misuse.

What do we mean by “Network?”

Private Network

The company’s Intranet is a private network. But, more often than not, companies depend on 3rd party service providers to carry their private network traffic in an encrypted form over their networks. So, the definition of Private Network refers to a logical network used for secure company only traffic. The growing popularity of Cloud computing has led to the development of “private clouds” that extend the company’s private network into other 3rd party domains.

Public Network

The Internet refers to the public portions of the network. Many companies depend on public network connections with their clients in order to do business. The popularity of the public Cloud continues to complicate the extent to which the public network may be a vehicle for company specific communications.

Network Components

Networks are complex electronic communications systems with a very large number of possible components. This makes this systems potentially open to many vulnerabilities. The list below, while largely comprehensive is not complete.

Gateways
Routers
Network bridges
Switches
Hubs
Repeaters

Multilayer switches
Protocol converters
Bridge routers
Proxy servers
Firewalls
NAT - network address translators

Multiplexers
Network interface controllers
Wireless network interface controllers
Modems
ISDN terminal adapters
Wireless access points

Network Security Risks

- **Breaches of Confidentiality:** Each business will identify with the need to keep certain critical information private from competitor eyes.
- **Data Destruction:** Data is a very valuable commodity for individuals and enterprises alike. It is a testament to its importance when the proliferation of backup technology available today is considered. Destruction of data can severely cripple the victim concerned.
- **Data Manipulation:** A system break-in may be easily detectable, as some hackers tend to leave tokens of their accomplishment. However, data manipulation is a more insidious threat than that. Data values can be changed and, while that may not seem to be a serious concern, the significance becomes immediately apparent when financial information is in question.
- **Interruption of Business Operations:** A severe enough attack can disrupt business operations for an extended period

Types of Network Attacks

Eavesdropping

The majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

Data Modification

After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

Identity Spoofing

(IP Address Spoofing)

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.

Password-Based Attacks

Most operating systems and network security use password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password. Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user. When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

Types of Network Attacks

Denial-of-Service Attack

The the denial-of-service attack prevents normal use of your computer or network by valid users. After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

Man-in-the-Middle Attack

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data. Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying as you to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

Compromised-Key Attack

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

Types of Network Attacks

Sniffer Attack

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted
- Read your communications

Application-Layer Attack

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
- Abnormally terminate your data applications or operating systems.
- Disable other security controls to enable future attacks.

Common security attacks and their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social Engineering
  - Education

Firewalls

Problem addressed: many network applications and protocols have security problems that are fixed over time

- Difficult for users to keep up with changes and keep host secure
- Solution
  - Administrators limit access to end hosts by using a firewall
  - Firewall is kept up-to-date by administrators

Firewalls

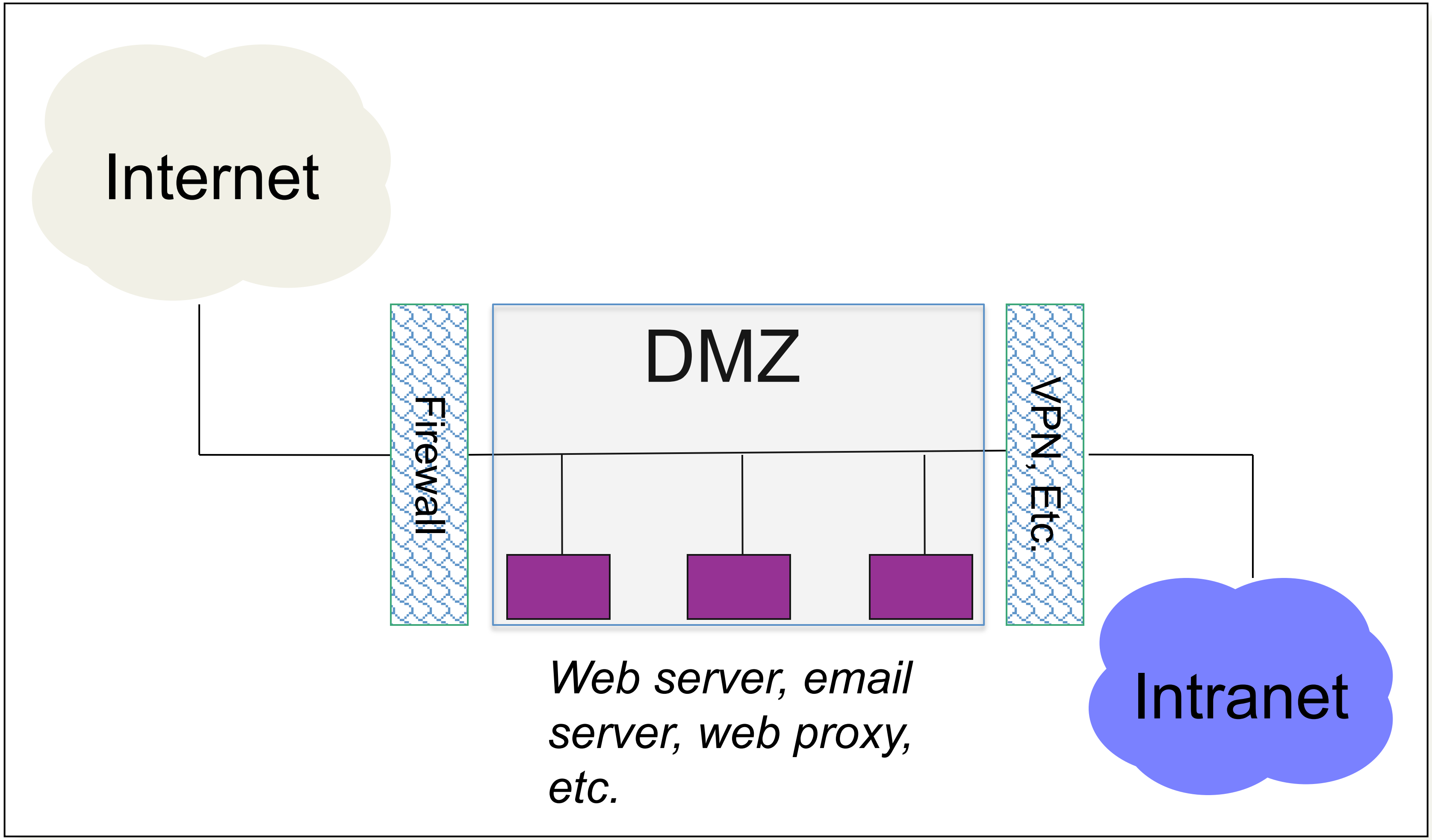
A firewall limits access from outside a network

- Only one point of access into the network
- This can be good or bad

Can be hardware or software

- Ex. Some routers come with firewall functionality
- Unix systems, Windows XP and Mac OS X have built in firewall functions
- Third party (like Norton) firewalls also available

Firewalls



Web server, email server, web proxy, etc.

Firewalls

Used to filter packets based on a combination of features

- These are called packet filtering firewalls
- Can use any combination of IP/UDP/TCP header information
- Ex. Drop packets with destination port of 23 (Telnet)

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Network Port Designations

Service	Port	Function Name
FTP	20, 21	File Transfer Protocol
SSH	22	Secure Shell
Telnet	23	Telnet
SMTP	25	Simple Mail Transfer Protocol
DNS	53	Domain Name Services
DHCP	67, 68	Dynamic Host Configuration Protocol
TFTP	69	Trivial File Transfer Protocol
HTTP	80	Hyper-Text Transfer Protocol
POP3	110	Post Office Protocol 3
NNTP	119	Network News Transport Protocol
NTP	123	Network Time Protocol
IMAP4	143	Internet Message Access Protocol
LDAP	389	Lightweight Access Directory Protocol
HTTPS	443	Secure Hyper-Text Transfer Protocol
IMAPS	993	Secure Internet Message Access Protocol
RADIUS	1812	Remote Authentication Dial In User Service
AIM	5190	AOL Instant Messenger

Intrusion Detection

Used to monitor for "suspicious activity" on a network

- Can protect against known software exploits, like buffer overflows

Uses "intrusion signatures"

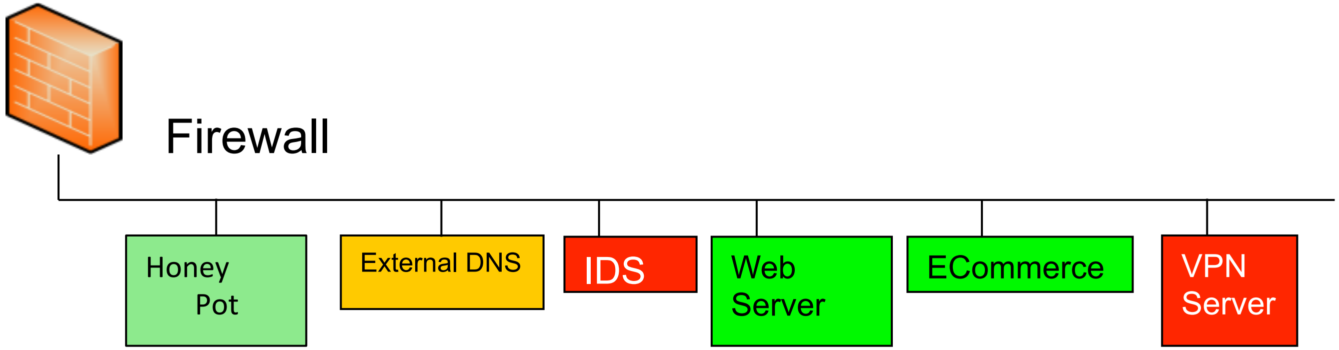
- Well known patterns of behavior
  - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.

Honeypots & Honeynets

Honeypot: A system with a special software application which appears easy to break into

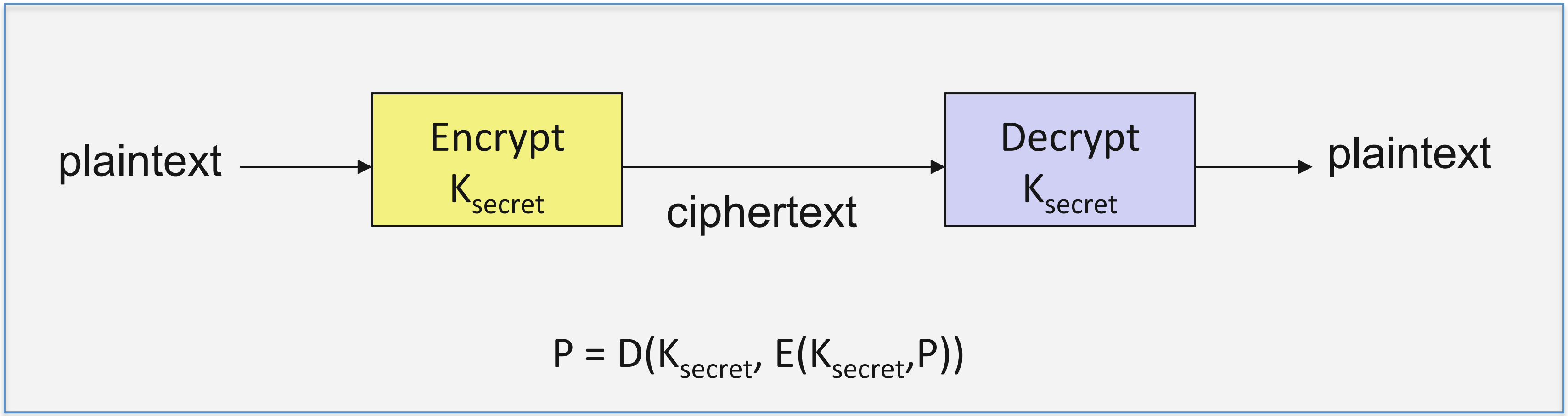
Honeynet: A network which appears easy to break into

- Purpose: Catch attackers
- All traffic going to honeypot/net is suspicious
- If successfully penetrated, can launch further attacks
- Must be carefully monitored



Encryption

Encryption is more and more becoming the standard for data transmission *and* storage in large companies



$$P = D(K_{secret}, E(K_{secret},P))$$

Test Taking Tip

If you see the response that you anticipated, chose it. Then, check to be sure that none of the other responses is better.

- This approach speeds-up your pace. On an exam where there is no penalty for wrong answers, your goal is to have more opportunities to answer questions that you know.
- Your first answer is probably the correct one.
- Reading the other answers gives you an opportunity to make sure that your interpretation of the question is correct.

Quiz