- Coverage: Lecture 19 to Lecture 22

- Network security (about 60%)

- Firewall and IDS (about 40%)

- Web security (20%)

# Network Security

## Network Vulnerabilities

### \*\*What makes network vulnerable?\*\*

- `Unkow attacks`

- Attacks may be launched from thousands of miles away.

- Hack a machine from another hacked machine.

- Many points of attack: from any machine to any machine

- Sharing

- System/Network complexity

- Unknown perimeter (host on multiple networks)

- Unknown paths (packets may travel over many different paths to a destination)

- What are the consequences of network attacks?

### \*\*Hazy network perimeter\*\*

- HAPPENED when it’s difficult to def the boundaries of a network due to factors such as cloud-based services and mobile access.

- PROBLEM: can create vulnerabilities and make it harder to control and monitor activity.

- SOLVE: use tools and strategies suck as network segmentation, access controls, and monitoring to improve network security.

## Network Attacks

### Threat Precursors

- Are techniques or activities that can be used by potential attackers to gather information about a network, system, or organization.

- COMMON THREAT: Port scan, war dialers, social engineering, dumpster diving, network mapping, vulnerability scanners, vendor documentation.

### Eavesdropping, Wiretapping

- \*\*Eavesdropping\*\*: the unauthorized interception of information by a third party.

- \*\*Wiretapping\*\*: the interception of telephone communications by a third party.

- TECHNIQUE can be done by using:

- Packet sniffers: wireshark, ettercap, tcpdump

- Cable-based: wiretaps, inductance(tap wire, read signals without physical contact)

- Insecure wireless networks: also possibility of theft of service

### \*\*Packet Sniffing\*\*

- `Packet sniffing` is the process of capturing and analyzing network traffic. DONE using a packet sniffer tool. Promiscuous mode can be used to read all packet on the network.

- \*Ethernal Frame Structure

## Controls

– Design: separation, single point of failure, redundancy, recovery, encryption (link vs. end-to-end)

– Protocols: SSL/TLS

■ Provides additional security services

■ From TLS 1.2 to TLS1.3

– Protocols: IPsec

■ Transport Mode vs. Tunnel Mode

■ AH vs. ESP

6Network Security

■ Controls

– Design: separation, single point of failure, redundancy, recovery, encryption (link vs. end-to-end)

– Protocols: SSL/TLS

■ Provides additional security services

■ From TLS 1.2 to TLS1.3

– Protocols: IPsec

■ Transport Mode vs. Tunnel Mode

■ AH vs. ESP

6

Firewall and IDS

■ Firewall

– Types of firewalls: strengths and limitations

– What can be protected, and what cannot?

■ IDS

– Fundamental assumption: intruder behavior differs from legitimate users

– Host-based IDS vs. Network IDS

– Signature-based IDS vs. anomaly detection IDS

– Detection quality, Bayesian detection rate, and the base rate fallacy

7

## Injection

- Cross-Site Scripting(XSS)

- SQL injection

- Problem: lack of input sanitization

- Classic mistakes in the use of PHP

- PHP is a server scripting language with C-like syntax

- It can intermingle static HTML and code, embed variables in double-quote strings

```php

<input user=<?php echo $username;?>>

$username="world";

```

- Why we use PHP? Because we want to interact between the user and the server

## XSS

- `Cross-Site Scripting` is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users.

- How XSS work?

- User visit a website

- The attacker injects a script into the website

- User click the link that contains the script

- The website will echo user input

- User will be redirected to the attacker's website and send the cookie to the attacker