
DENNIS GUNAWAN



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

IF470 COMPUTER SECURITY

09 SECURITY IN EXTERNAL NETWORK COMMUNICATION



REVIEW: INTERNAL NETWORK SECURITY

- Threat
 - Port Scan
- Harm
 - Knowledge and Exposure
- Vulnerability
 - Revealing Too Much
 - Allowing Internet Access
- Countermeasure
 - System Architecture
 - Firewall
 - Network Address Translation (NAT)
 - Security Perimeter

COURSE SUB LEARNING OUTCOMES (SUB-CLO)

- Sub-CLO 9
 - Students are able to relate security in external network communication to real case in their daily life (C3)

OUTLINE

- Wireless or WiFi Network Communications
- Interception
- Peer-to-Peer Networks

INTRODUCTION



- Some degree of external connectivity is almost inevitable for most computer users
- As soon as you decide to connect to points outside your security perimeter, that connection leaves your zone of protection
 - You are at risk others will read, modify, and even obliterate your communication
- How to do that with reasonable security

WIFI (WIRELESS FIDELITY)

- The means by which many of us connect wirelessly to other networks
- The perimeter of protection is not immediately obvious



WIFI (WIRELESS FIDELITY)



**FREE
WI-FI
UNLIMITED**

- Many people have a false sense of security (or an ignorance of great insecurity) concerning WiFi access
- Coffee shops, bookstores, airports, and hotels use free wireless access to attract and keep customers

When you connect to a free access point, what security do you have?

WIFI BACKGROUND

- Wireless traffic uses a section of the radio spectrum
 - All communications are on predefined radio frequencies
 - The signals are available to anyone with an effective antenna within range
- Wireless computing is so exposed
 - You can expect an eavesdropping attacker to try to intercept and impersonate
 - It requires measures to protect communications between a computer (the client) and a wireless base station / access point

WIRELESS COMMUNICATION

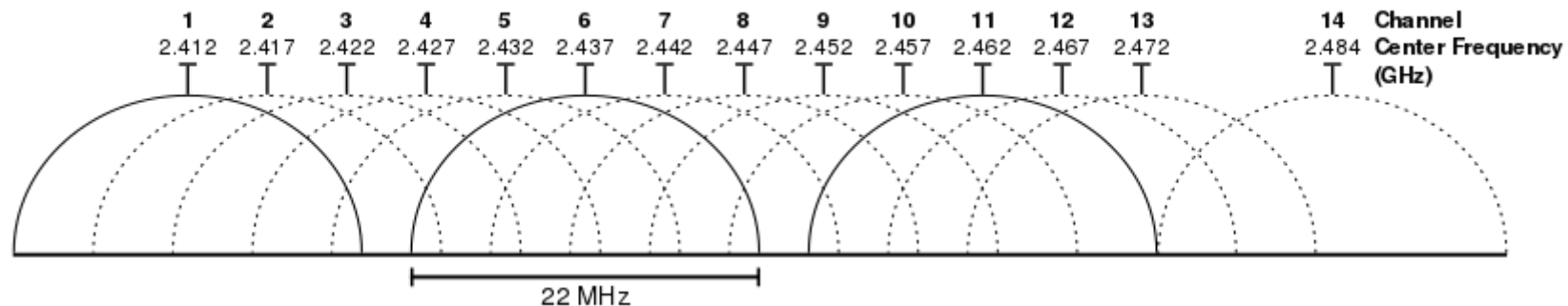
- Wireless (and also wired) data communications are implemented through an orderly set of exchanges called a **protocol**
- These protocols are an internationally agreed-on standard, called the **802.11** suite of protocols
 - You can use your computer, made in one country with software written in another, to connect to wireless access points all around the world

A familiar protocol involves making and receiving a telephone call

1. You press buttons to activate your phone
2. You press buttons to select and transmit the friend's number (dialing the phone)
3. Your friend hears a tone and presses a button to accept your call
4. Your friend says "hello", or some other greeting
5. You say hello
6. You begin your conversation

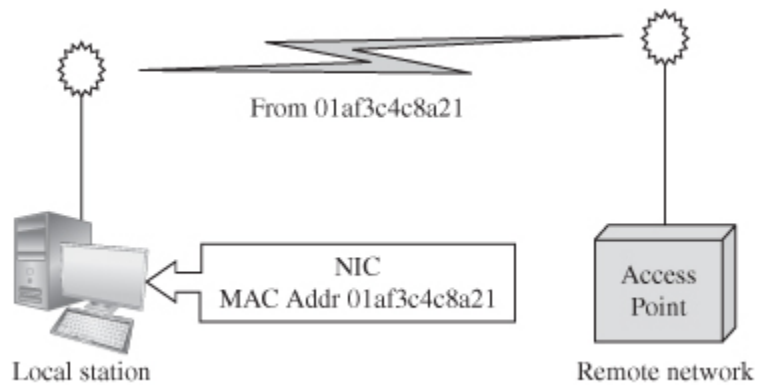
802.11 PROTOCOL SUITE

The 802.11 protocols all describe how devices communicate in the 2.4 GHz radio signal band (essentially 2.4 GHz – 2.5 GHz) allotted to WiFi



- The band is divided into 14 channels or subranges within the band
 - These channels overlap
- To avoid interference with nearby devices, WiFi devices are designed to use only a few of these, often channels 1, 6, and 11

802.11 PROTOCOL SUITE



Access Point

The hub of the wireless subnetwork

- Each device must have a **network interface card (NIC)** that communicates radio signals with the access point
- The NIC is identified by a unique 48– or 64–bit hardware address called a **medium access code (MAC)**
- MAC addresses are supposed to be fixed and unique, but MAC addresses can be changed

WIFI ACCESS RANGE

Protocol	Ordinary Signal Range
802.11a	100 ft / 35 m
802.11b	300 ft / 100 m
802.11g	300 ft / 100 m
802.11n	1000 ft / 350 m

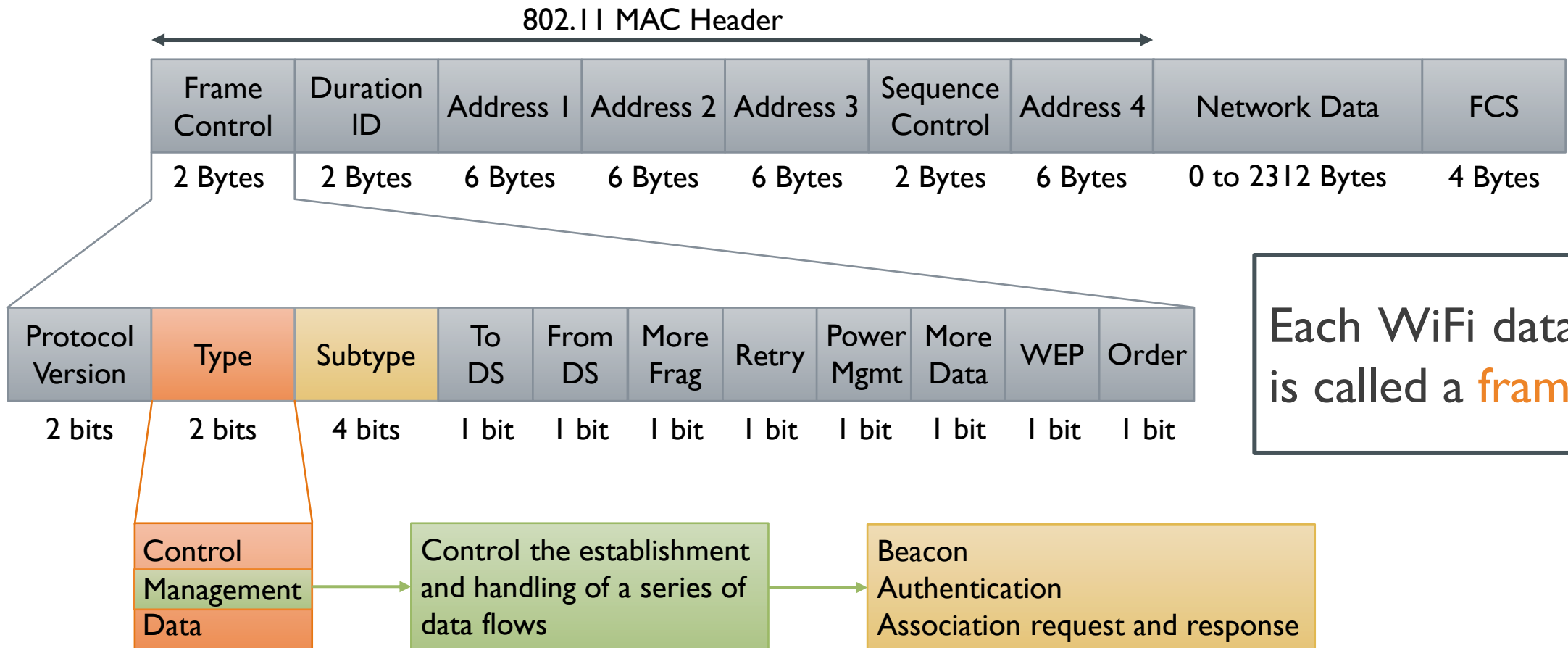
Experimental results with 802.11n have demonstrated reception at distances of approximately 5000 ft / 1600 m in ideal conditions

- The quality of the signal diminishes with distance
- Wireless signals degrade because of interference from intervening objects, such as walls, machinery, and trees
 - Outdoor signals, with fewer objects to interfere, generally travel longer distances than indoor signals
- A receiver will not establish, or may drop, a connection with a poor signal
 - One that is weak or has lost a lot of data

WIFI ACCESS RANGE

- Devices called **repeaters** can extend the range of existing wireless transmitters
- Antennas can be tuned to the frequency of wireless communication
 - Focusing directly on the source of the signal can also improve reception at great distance

WIFI FRAMES



MANAGEMENT FRAMES: BEACON

- Each access point periodically sends a **beacon frame** to announce its presence and relay information
 - Timestamp, identifier, and other parameters regarding the access point
- Any NICs that are within range receive this beacon

When you connect to a WiFi service at a coffee shop, your computer receives the beacon signal from the shop to be able to initiate communication.

MANAGEMENT FRAMES: AUTHENTICATION

- A NIC initiates a request to interact with an access point by sending its identity in an **authentication frame**
- The access point may request additional authentication data and finally either accepts or rejects the request
- Either party sends a **deauthentication frame** to terminate an established interaction

Your computer responds to the coffee shop's beacon signal by returning its identity (MAC address) in an authentication frame.

MANAGEMENT FRAMES: ASSOCIATION REQUEST AND RESPONSE

- Following authentication, a NIC requests an access point to establish a session
- The NIC and access point exchange information about their capabilities and agree upon parameters of their interaction
- A **deassociation request** is a request to terminate a session

An important part of establishing the association is agreeing upon encryption

- An access point may be able to handle 3 different encryption algorithms, call them A, B, and C
- The requesting NIC can handle only 2 algorithms, call them B and D
- In the association these two would determine that they share algorithm B and thus agree to use that form of encryption to communicate

SERVICE SET IDENTIFIER (SSID)

Service Set Identifier (SSID)

Identification of an access point

A string of up to 32 characters
chosen by the access point's administrator

- One other important data value in WiFi communication is the designation of an access point
 - A wireless device can distinguish among access points if it receives more than one signal
- The SSID is the identifier the access point broadcasts in its beacon
 - It is the ongoing link that ties an associated NIC's communications to the given access point

HARM: CONFIDENTIALITY

- If data signals are transmitted in the open, unintended recipients may be able to get the data
- A's communicating with access point B or the duration or volume of communication may also be sensitive
- The nature of the traffic, whether web page access, peer-to-peer networking, email, or network management, can also be confidential
- The mode in which 2 units communicate – encrypted or not and if encrypted, by what algorithm – is potentially sensitive

HARM: INTEGRITY

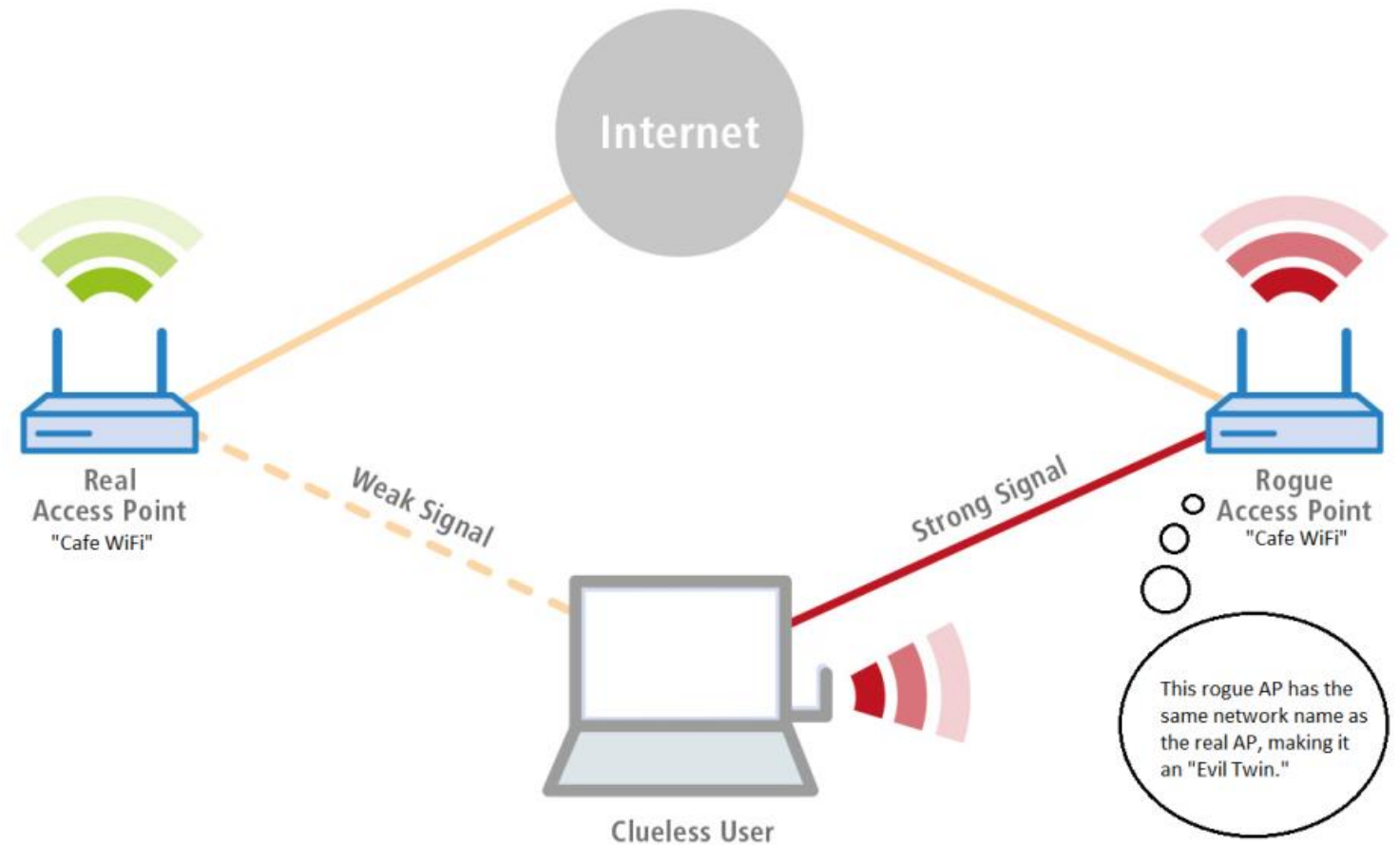
- Nonmalicious sources of harm
 - Interference from other devices
 - Loss or corruption of signal due to distance or intervening objects
 - Reception problems caused by weather
 - Sporadic communication failures within the hardware and software that implement protocol communication
- Direct, malicious attacks to change the content of a communication

HARM:AVAILABILITY

- 3 potential problems
 - When a component of a wireless communication stops working
 - Hardware fails, power is lost, or some other catastrophe strikes
 - Loss of some but not all access, typically manifested as slow or degraded service
 - Interference
 - The demand for service exceeds the capacity of the receiving end
 - The possibility of rogue network connection
 - Although service is available, the security of that service may be limited

ROGUE ACCESS POINT – EVIL TWIN

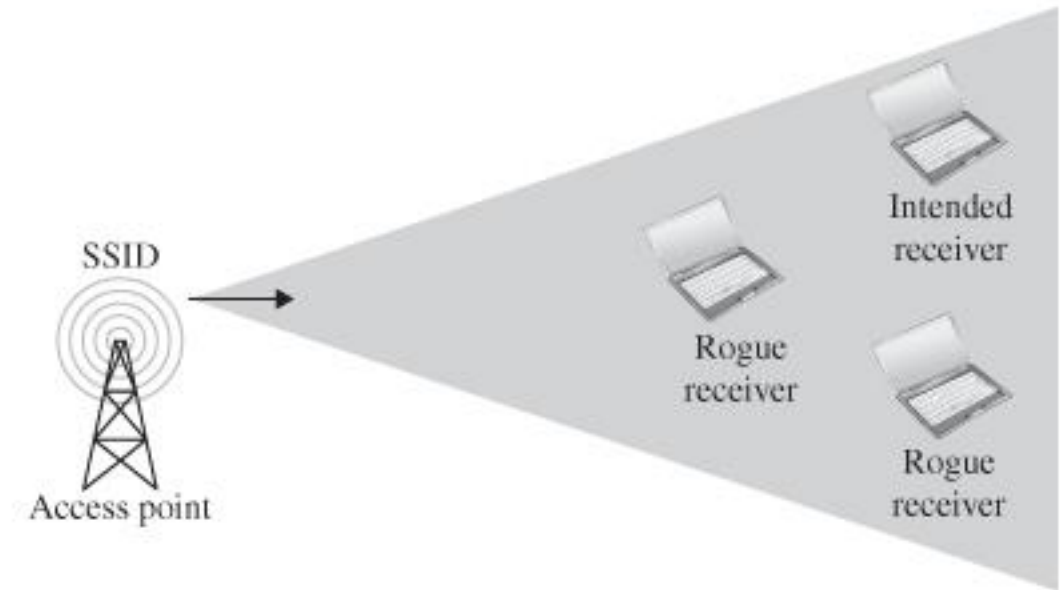
- The attacker can try to take over a communication stream by force
- WiFi radio receivers that receive 2 signals prefer the stronger one
- If a rogue access point intercepts a signal from a client and sends out a strong signal, appearing to come from the server's access point, the rogue may be able to commandeer the communication stream



PROTOCOL WEAKNESSES: PICKING UP THE BEACON

Open Mode

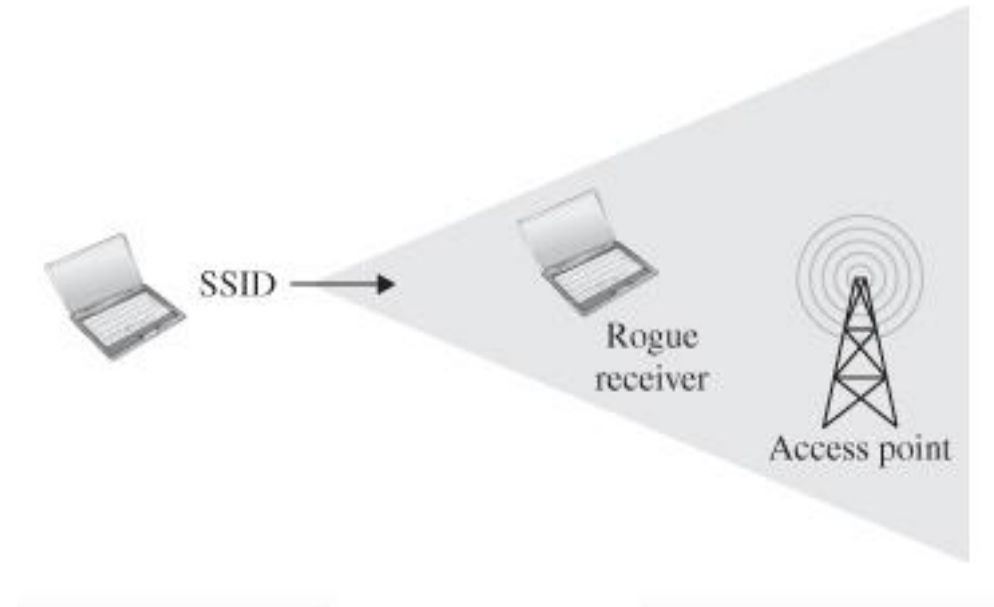
- An access point continually broadcasts its appeal in its beacon, indicating that it is open for the next step in establishing a connection
- The client is quiet, monitoring beacons, until it finds one to which it wants to connect
 - The client is not constantly visible



PROTOCOL WEAKNESSES: PICKING UP THE BEACON

Closed Mode / Stealth Mode / SSID Cloaking

- The client must send a signal seeking an access point with a particular SSID before the access point responds to that one query with an invitation to connect
- The client effectively becomes a beacon, sending a continuing series of messages saying, in essence, “I am MAC address mmm, looking for SSID sss.Are you sss?”
 - A rogue host can learn the expected values needed to impersonate an access point to which the client hopes to connect



PROTOCOL WEAKNESSES: SSID IN ALL FRAMES

In both closed and open modes,
even after the initial handshake,
all subsequent management and data frames
contain the SSID

—
Sniffing any one of these frames
reveals the SSID

- Anyone who sniffs the SSID can save the SSID (which is seldom changed in practice) to use later
- It is also a good guess that the client will attempt to connect to this same access point again in the future
- The rogue has the information needed to imitate either the client or the access point in the future

PROTOCOL WEAKNESSES: CHANGEABLE MAC ADDRESS

- Changing the NIC's MAC address undermines MAC-based authentication on an access point

MAC spoofing


One device impersonates another,
thereby assuming another device's communication session

PROTOCOL WEAKNESSES: PREFERRED ASSOCIATIONS

- To simplify connecting, the wireless interface software builds a list of favorite connection points (home, school, office) to which it will try to connect automatically
- There is usually no confusion, because these networks will have distinct names (actually SSIDs)

Wi-Fi

Manage known networks

 Add a new network


Search this list


Sort by: Preference ▾

Filter by: All ▾

 3dlink

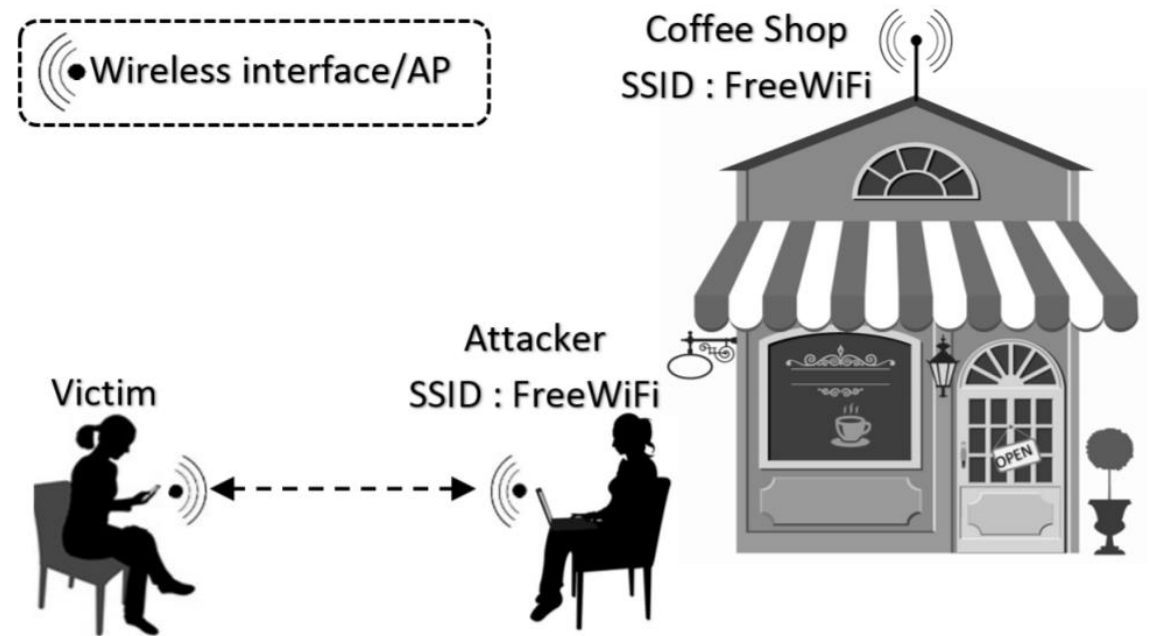
 UPC1801307

 CNC Network

 CNC5

PROTOCOL WEAKNESSES: PREFERRED ASSOCIATIONS

- Unfortunately, the name of an SSID is not bound to any physical characteristic
- Your computer does not distinguish between FreeWiFi as an access point at your coffee shop or a rogue point intended to lure unsuspecting visitors
- Your computer will continue to search for an access point with SSID FreeWiFi and connect to any such point it finds



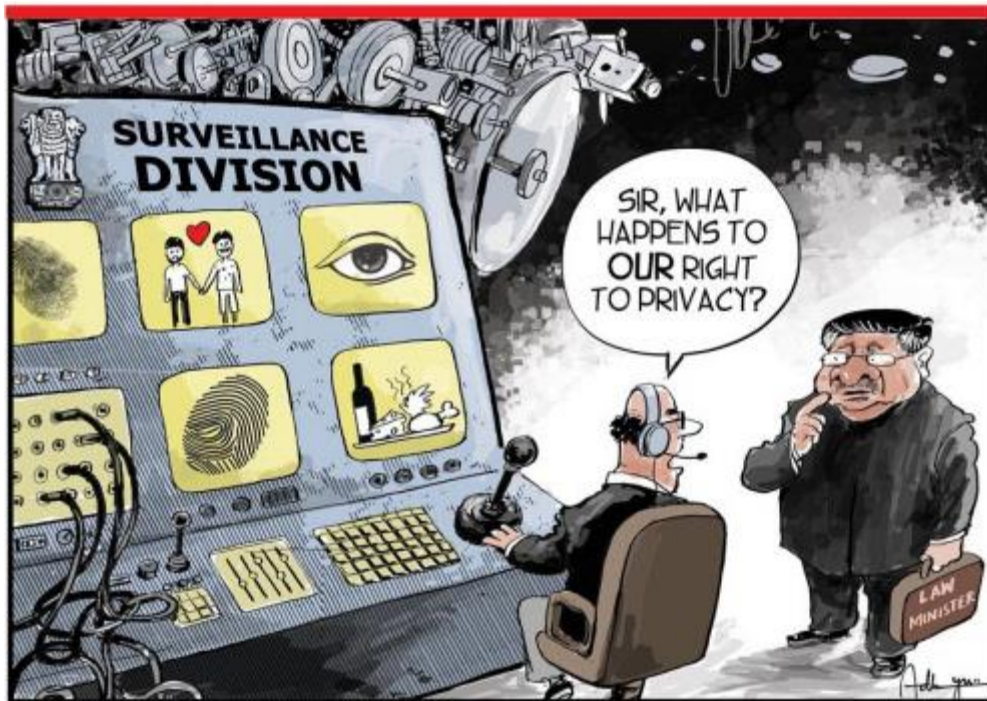
STRENGTH OF WPA & WPA2 (STRONGER BUT NOT PERFECT) OVER WEP (FAILED)

WEP	WPA & WPA2
Static Key WEP uses an encryption key that is unchanged until the user enters a new key at the client and access point	Nonstatic Encryption Key WPA has a key change approach, called Temporal Key Integrity Program (TKIP), by which the encryption key is changed automatically on each packet
No Authentication WEP uses the encryption key as an authenticator, albeit insecurely	Authentication WPA employs the Extensible Authentication Protocol (EAP) by which authentication can be done by password, token, certificate, or other mechanism
Weak Encryption <ul style="list-style-type: none">▪ The encryption algorithm for WEP had been RC4, which has cryptographic flaws both in key length and design▪ The initialization vector for RC4 is only 24 bits, a size so small that collisions commonly occur▪ There is no check against initialization vector reuse	Strong Encryption <ul style="list-style-type: none">▪ WPA2 adds AES as a possible encryption algorithm▪ It uses a longer encryption key

STRENGTH OF WPA & WPA2 (STRONGER BUT NOT PERFECT) OVER WEP (FAILED)

WEP	WPA & WPA2
Faulty Integrity Check <ul style="list-style-type: none">▪ WEP includes a 32-bit integrity check separate from the data portion▪ An attacker could modify content and the corresponding check without having to know the associated encryption key	Integrity Protection <p>WPA includes a 64-bit integrity check that is encrypted</p>
	Session Initiation <ul style="list-style-type: none">▪ The setup protocol for WPA and WPA2 is much more robust than that for WEP▪ Setup for WPA involves 3 protocol steps<ul style="list-style-type: none">▪ Authentication▪ A four-way handshake<ul style="list-style-type: none">▪ To ensure that the client can generate cryptographic keys▪ To generate and install keys for both encryption and integrity on both ends▪ An optional group key handshake (for multicast communication)

INTERCEPTION



- Even wired communications can be intercepted, as landline telephone taps indicate, but wireless communications are inherently more exposed
- Although a networking communications requirement might be worded as “communications are to be transmitted from their originator and delivered to their recipient”, for security we must add the phrase “and nobody else” or “and nothing more” to that requirement

INTERCEPTION: CABLE

Packet Sniffing

- A device called a **packet sniffer** retrieves all packets on its LAN

Radiation

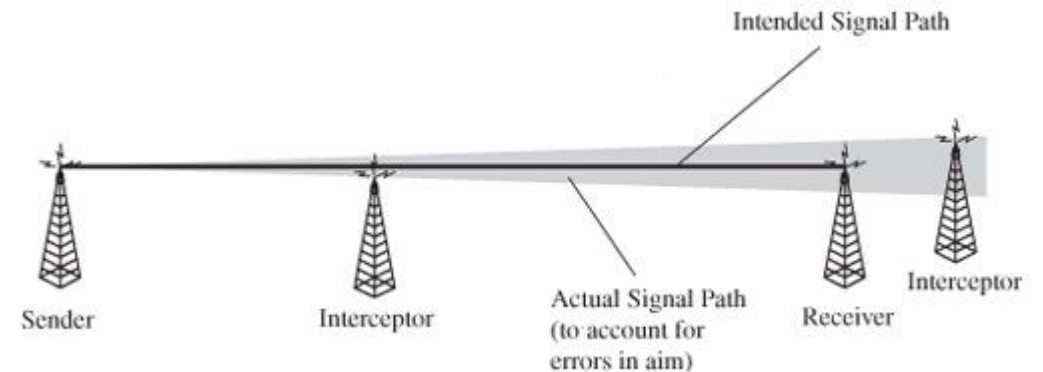
- By a process called **inductance** an intruder can tap a wire and read radiated signals without making physical contact with the cable

Cable Splicing

- The easiest form of intercepting a cable is by **direct cut**
- An attacker can easily splice in a secondary cable that then receives a copy of all signals along the primary cable

INTERCEPTION: MICROWAVE

- The signal path is fairly wide, to be sure of hitting the receiver
- Someone can intercept a microwave transmission by interfering with the line of sight between sender and receiver
- Someone can also pick up an entire transmission from an antenna located close to but slightly off the direct focus point



INTERCEPTION: SATELLITE COMMUNICATION

- Transmission to the satellite can cover a wide area around the satellite, because nothing else is nearby to pick up the signal
- On return to Earth, however, the wide dissemination radius, called the broadcast's footprint, allows any antenna within range to obtain the signal without detection



INTERCEPTION: OPTICAL FIBER

- 2 significant security advantages over other transmission media
 - The entire optical network must be tuned carefully each time a new connection is made
 - No one can tap an optical system without detection
 - Clipping just one fiber in a bundle will destroy the balance in the network
- Optical fiber carries light energy, not electricity
 - Light does not create a magnetic field as electricity does
 - An inductive tap is impossible on an optical fiber cable

INTERCEPTION: OPTICAL FIBER

- Just using fiber does not guarantee security
- The repeaters, splices, and taps along a cable are places at which data may be available more easily than in the fiber cable itself
- The connections from computing equipment to the fiber may also be points for penetration

WIRETAPPING

Wiretapping

Data interception,
often covert and unauthorized

- A wide area network can be far riskier than a well-controlled local network

WIRETAPPING

Telephone System

A call from New York to Sydney might travel west by satellite, transfer to an undersea cable, and reach the ultimate destination on conventional wire. Along the way, the signal could pass through different countries, as well as international regions of the oceans and sky.

- Users generally have little control over the routing of a signal
 - The signal may travel through hostile regions and areas full of competitors
- Along the way may be people with method, opportunity, and motive to obtain your data

WHAT MAKES A NETWORK VULNERABLE TO INTERCEPTION?

Anonymity

- The potential attacker is safe behind an electronic shield
- The attack can be passed through many other hosts in an effort to disguise the attack's origin

An attacker can mount an attack from thousands of miles away and never come into direct contact with the system, its administrators, or users

WHAT MAKES A NETWORK VULNERABLE TO INTERCEPTION?

When a file is stored in a network host remote from the user, the data or the file itself may pass through many hosts to get to the user

Many points of attack

- An attack can come from any host to any host, so a large network offers many points of vulnerability

WHAT MAKES A NETWORK VULNERABLE TO INTERCEPTION?

Sharing

- Because networks enable resource and workload sharing, more users have the potential to access networked systems than on single computers

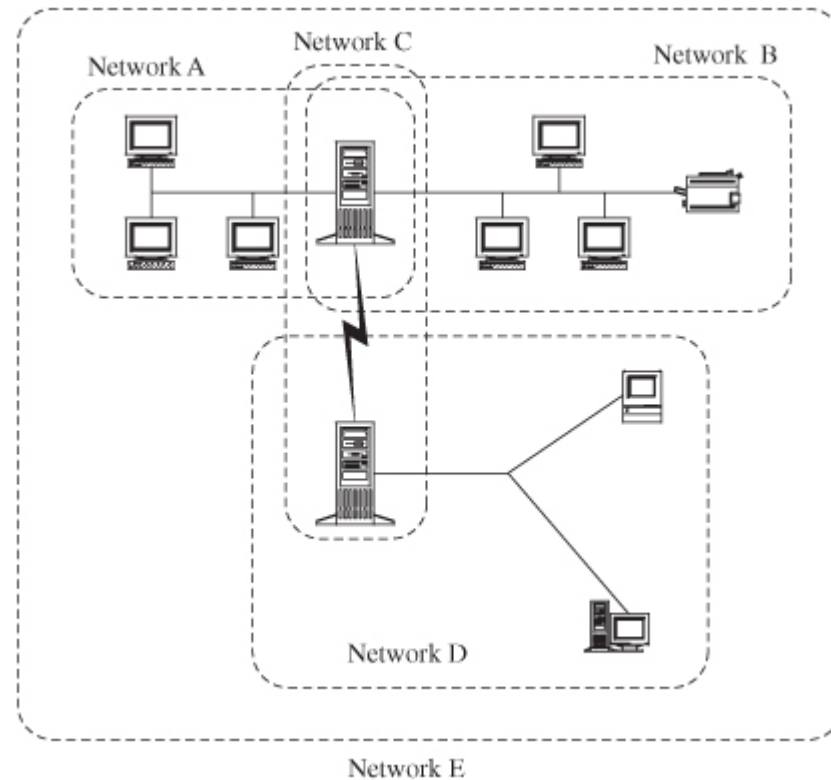
Complexity of system

- An operating system is a complicated piece of software
- Reliable security is difficult, if not impossible, on a large operating system
- A network combines 2 or more possibly dissimilar operating systems
- A network operating / control system is likely to be more complex than an operating system for a single computing system

WHAT MAKES A NETWORK VULNERABLE TO INTERCEPTION?

Unknown perimeter

- A network's expandability also implies uncertainty about the network boundary
- One host may be a node on 2 different networks, so resources on one network are accessible to the users of the other network as well

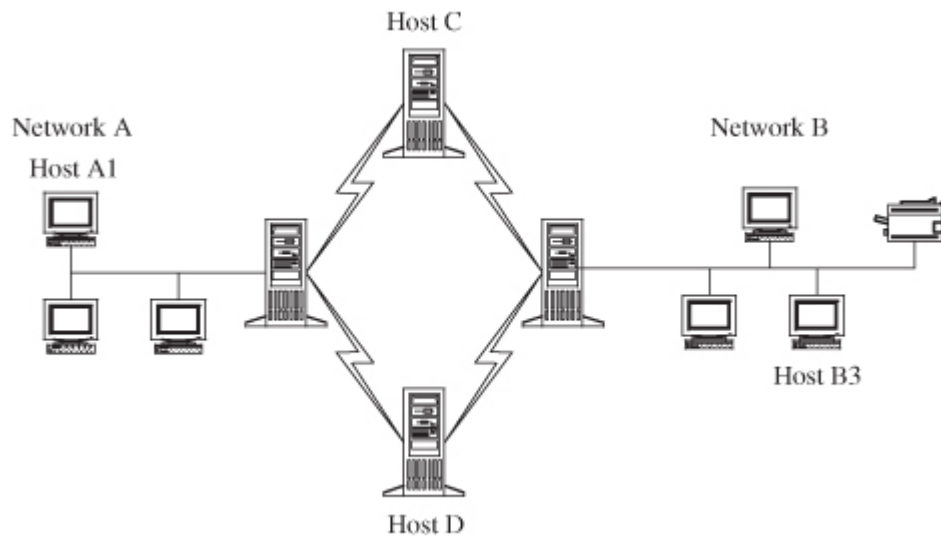


- A user on a host in network D may be unaware of the potential connections from users of networks A and B
- The host in the middle of networks A and B in fact belongs to A, B, C, and E
- If there are different security rules for these networks, to what rules is that host subject?

WHAT MAKES A NETWORK VULNERABLE TO INTERCEPTION?

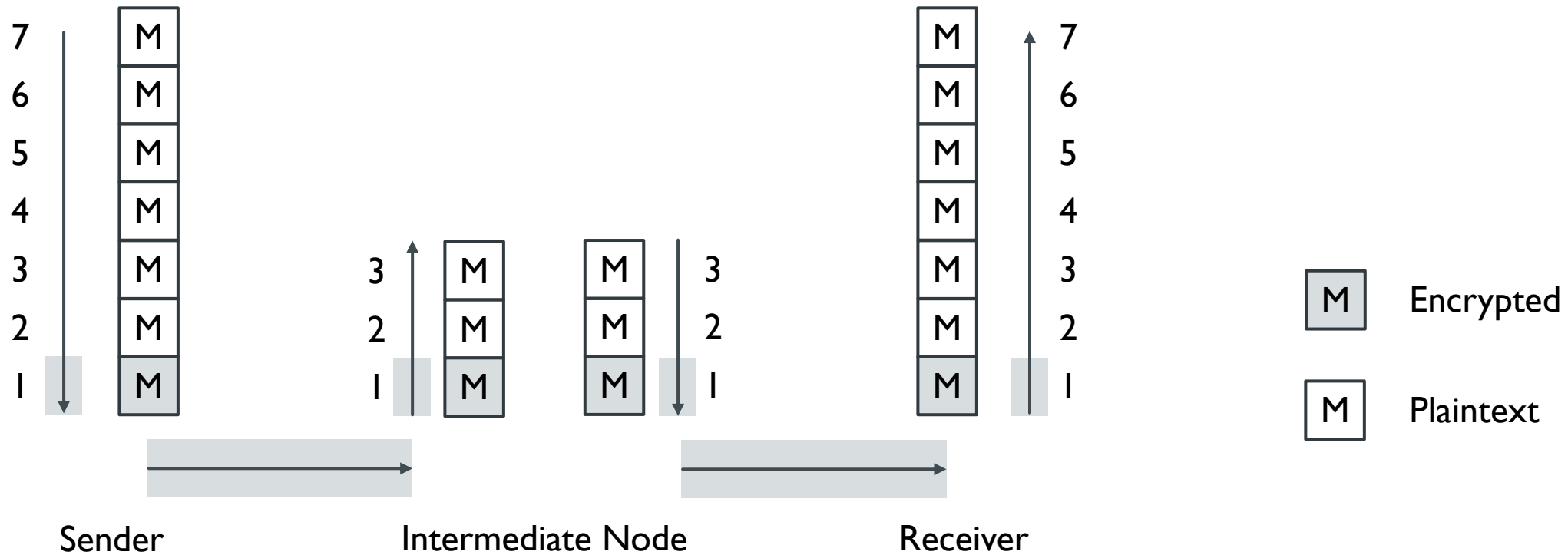
Unknown path

- There may be many paths from one host to another
- Network users seldom have control over the routing of their messages

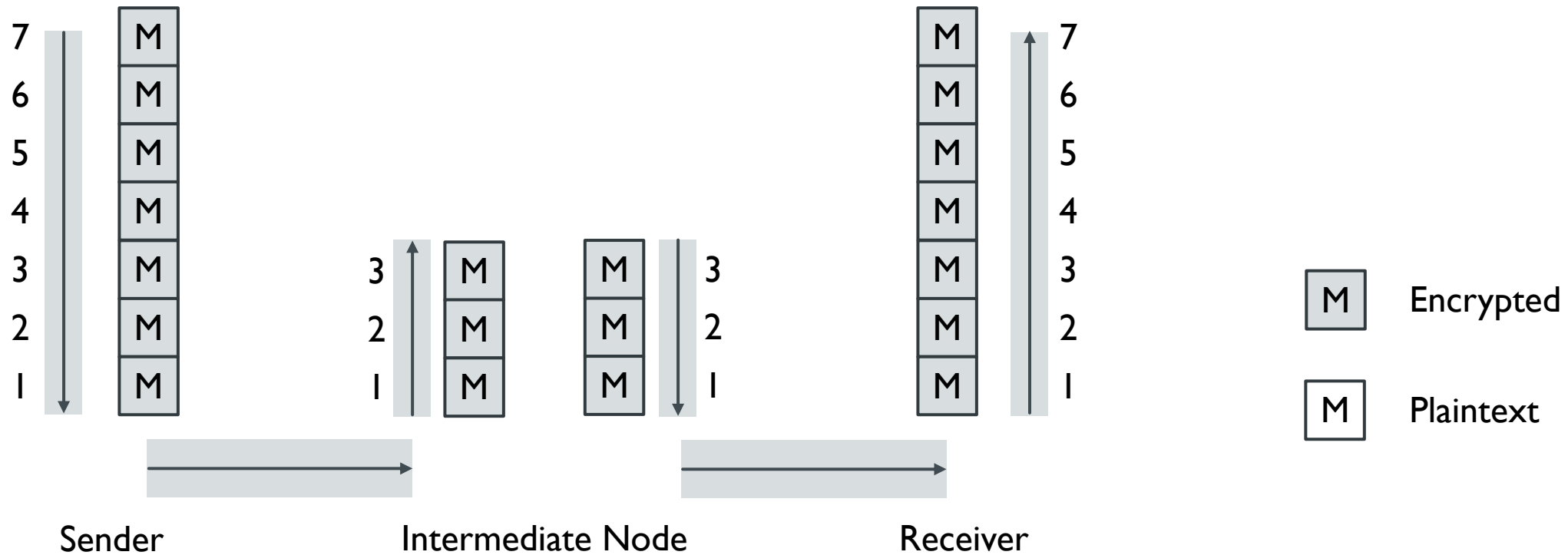


- A user on host A1 wants to send a message to a user on host B3
- That message might be routed through hosts C or D before arriving at host B3
- Host C may provide acceptable security, but not D

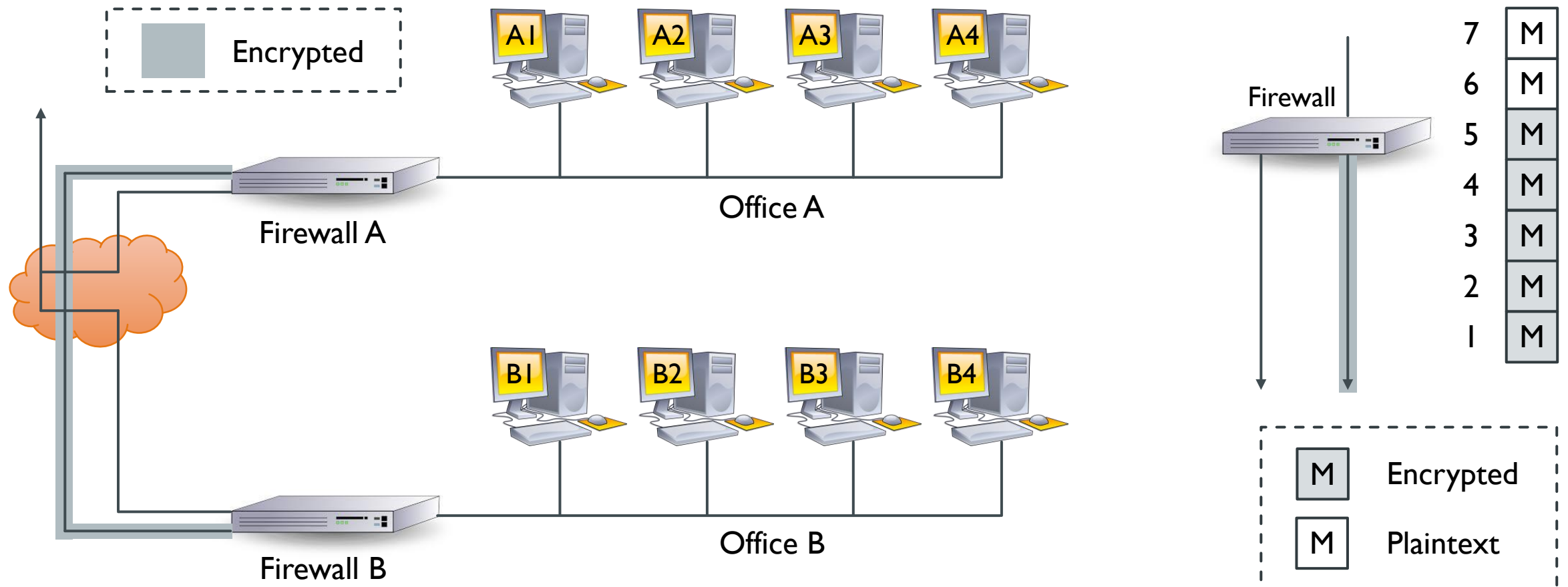
NETWORK ENCRYPTION: LINK ENCRYPTION



NETWORK ENCRYPTION: END-TO-END ENCRYPTION



VIRTUAL PRIVATE NETWORKS



ASYMMETRIC CRYPTOGRAPHY

Motivation



Symmetric cryptography has an equation of $n * (n - 1) / 2$ for the number of keys needed

In a situation with 1000 users, that would mean 499,500 keys



Asymmetric cryptography, using key pairs for each of its users, has n as the number of key pairs needed

In a situation with 1000 users, that would mean 1000 key pairs

Characteristics

Each user has 2 keys: a **public key** and a **private key**

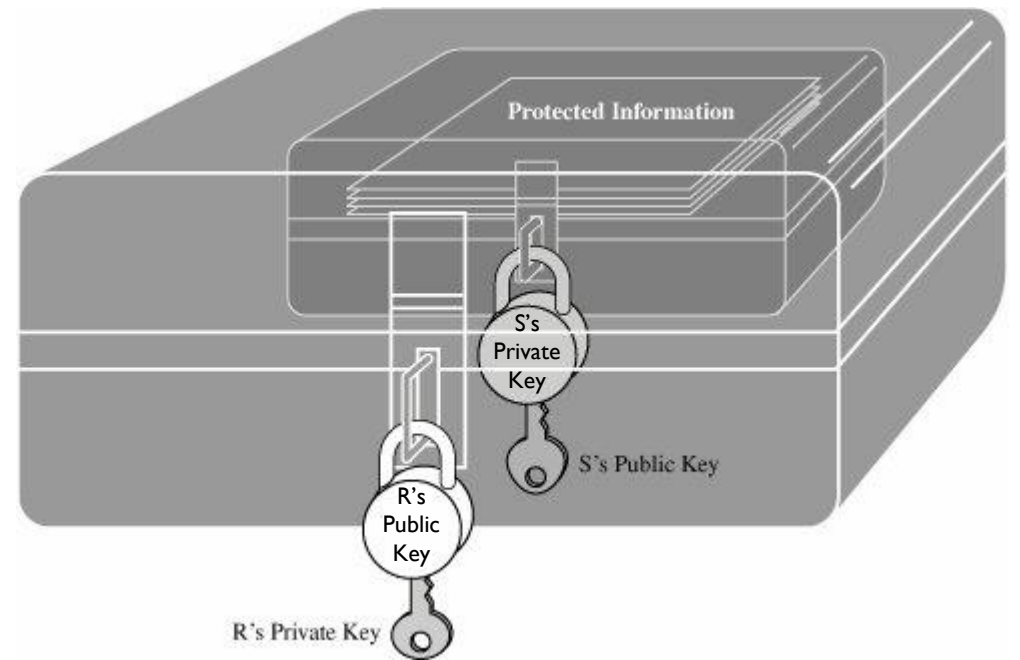
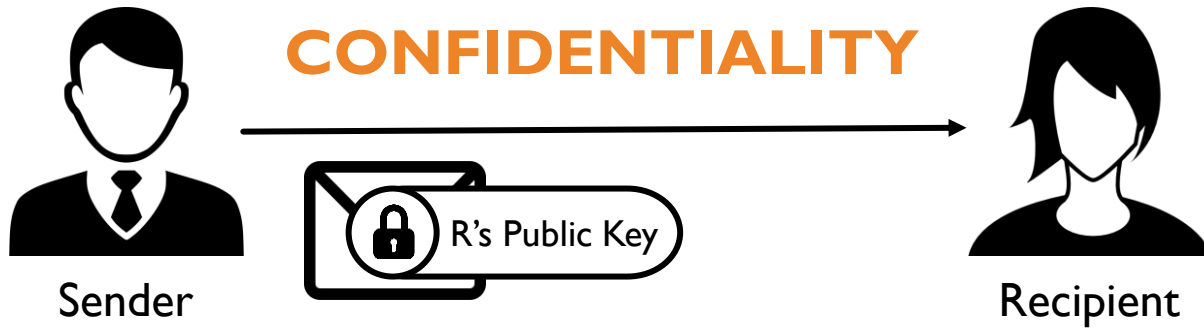
$$P = D(k_{\text{PRIV}}, E(k_{\text{PUB}}, A))$$

A user can decode with a private key what someone else has encrypted with the corresponding public key

$$P = E(k_{\text{PRIV}}, A)$$

A user can encrypt a message with a private key, and the message can be revealed only with the corresponding public key

ASYMMETRIC CRYPTOGRAPHY: KEY EXCHANGE WITH PUBLIC KEY ENCRYPTION



ASYMMETRIC CRYPTOGRAPHY: RIVEST–SHAMIR–ADLEMAN (RSA) CRYPTOSYSTEM

Key Generation

Output: public key: $k_{pub} = (n, e)$ and private key: $k_{pr} = (d)$

1. Generate two large distinct random primes p and q
2. Compute $n = pq$
3. Compute $\phi = (p - 1)(q - 1)$
4. Select a random integer e , $1 < e < \phi$, such that $\gcd(e, \phi) = 1$
5. Use the extended Euclidean algorithm to compute the unique integer d , $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$

Key Generation

1. $p = 17$ and $q = 11$
2. $n = pq = 17 \times 11 = 187$
3. $\phi = (p - 1)(q - 1) = 16 \times 10 = 160$
4. $e = 7$
5. $d = 23$

$$ed \equiv 1 \pmod{\phi}$$

$$7d \equiv 1 \pmod{160}$$

$$d \equiv 7^{-1} \pmod{160}$$

$$160 = 7 \times 22 + 6 \quad \rightarrow \quad 6 = 160 - 7 \times 22$$

$$7 = 6 \times 1 + 1 \quad \rightarrow \quad 1 = 7 - 6$$

$$1 = 7 - 6$$

$$1 = 7 - (160 - 7 \times 22)$$

$$1 = 7 - 160 + 7 \times 22$$

$$1 = -160 + 23 \times 7$$

ASYMMETRIC CRYPTOGRAPHY: RIVEST–SHAMIR–ADLEMAN (RSA) CRYPTOSYSTEM

Encryption

Plaintext: $M < n$
Ciphertext: $C = M^e \bmod n$

Decryption

Ciphertext: C
Plaintext: $M = C^d \bmod n$

Key Generation

1. $p = 17$ and $q = 11$
2. $n = 187$
3. $\phi = 160$
4. $e = 7$
5. $d = 23$

Encryption

Plaintext: $M = 88$

Ciphertext: $C = 88^7 \bmod 187 = 11$

Decryption

Ciphertext: $C = 11$

Plaintext: $M = 11^{23} \bmod 187 = 88$

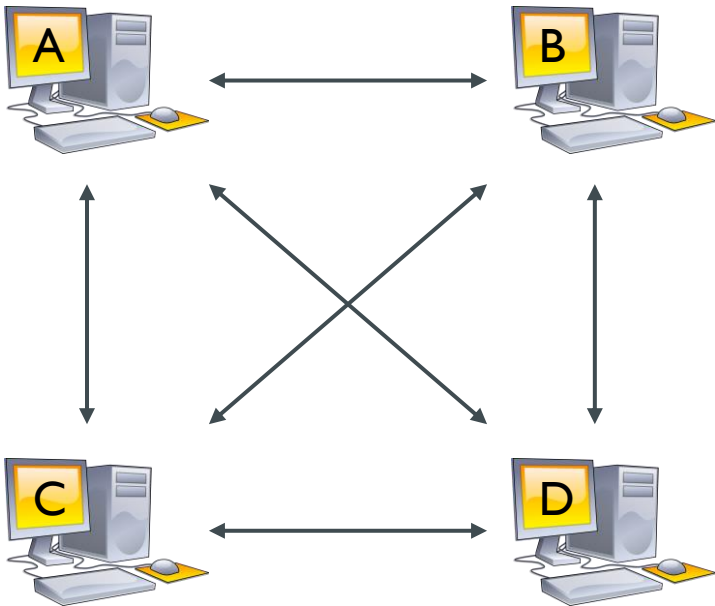
$$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$

$$11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187$$

PEER-TO-PEER SHARING

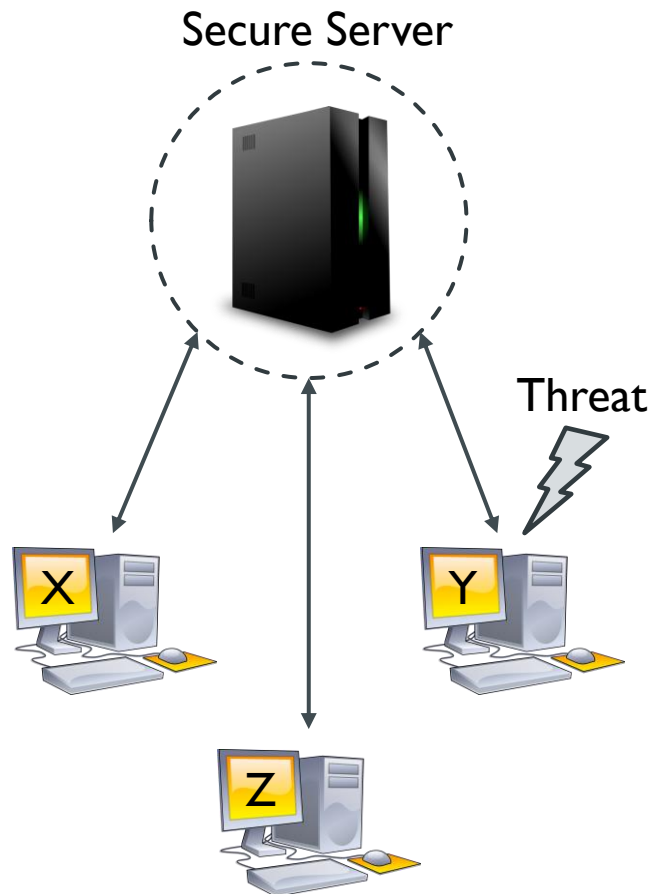
- Peer-to-peer sharing (P2P), and sharing in general, lets people expand the usefulness of computers
 - Users contribute to a common goal and by pooling data and effort, at least in theory, they do the work more easily than had they worked individually
- Peer-to-peer sharing networks were originally developed largely to circumvent copyright restrictions on music and other media
 - Users gladly offered their music files in order to get more music from other users

P2P MODEL



- The P2P model is like a mesh with all users as equals sharing with each other
- All users decide what they are willing to share and place sharable objects in positions from which all other peer users can inspect and access them
- Access control is thus simplified but also runs the risk of lacking accountability

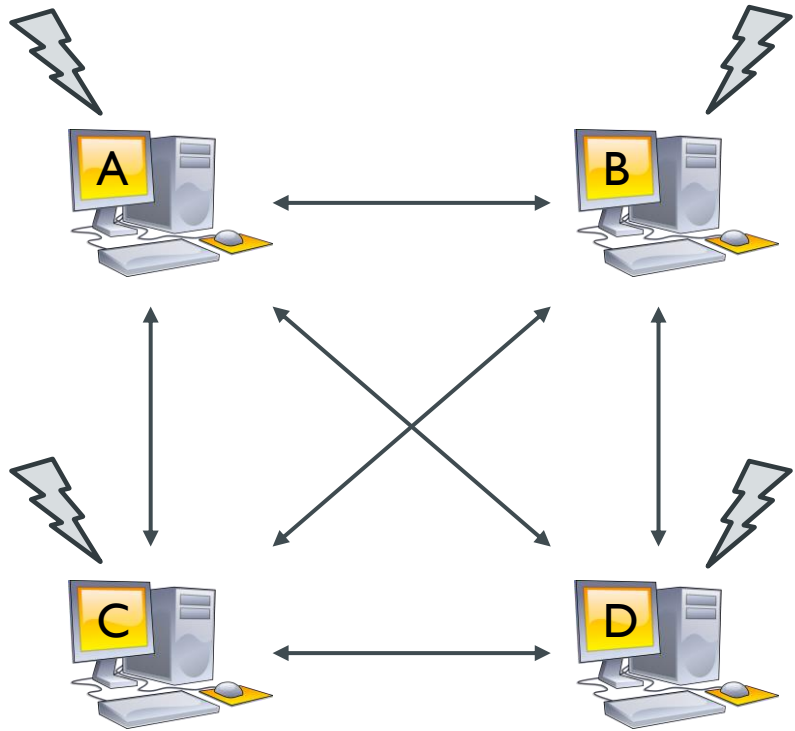
DIFFERENCES BETWEEN THREATS IN CLIENT-SERVER & P2P MODELS



- In a client-server network, the central repository of sensitive data is the server
 - The server can control access strictly
- Although any individual node may have some data and be a target of an attack, any one node will likely have only a small amount of data
- The impact of the attack will be small

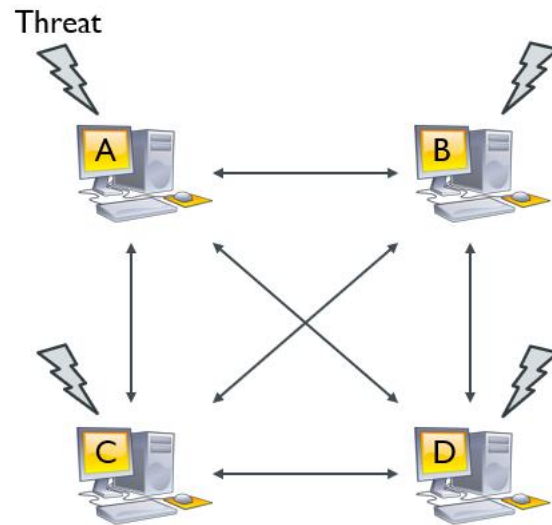
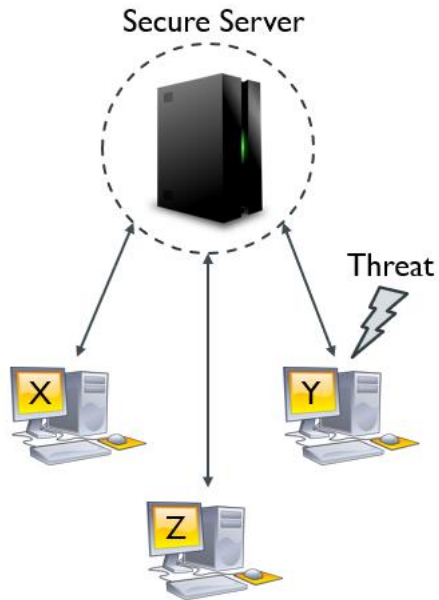
DIFFERENCES BETWEEN THREATS IN CLIENT-SERVER & P2P MODELS

Threat



- In a P2P network, all nodes are the network
- For reliability and performance, each node will have a significant proportion of sensitive data
- An attack on a single node is likely to net more sensitive data

DIFFERENCES BETWEEN THREATS IN CLIENT–SERVER & P2P MODELS



- Being centrally managed, a server is likely to be more strongly protected against security threats than is an individual node
- Attacking a P2P node is more likely to succeed
- Sensitive data is more exposed on a P2P system than in a client–server model

PEER-TO-PEER SHARING: THREAT

Inappropriate Data Disclosure

- Users' files become available to any P2P network user, causing a loss of confidentiality
- The threat is exacerbated by the gradual blending of personal, work, school, and private computing

Introduction of Malicious Software

- Downloading of files containing malicious code, which is a problem of integrity

I'll Never Love Again.mp3

.exe

Exposure to Unauthorized Access

- A port is open, allowing largely unrestricted access to a user's computer – another integrity issue

PEER-TO-PEER SHARING:VULNERABILITY

User Failure to Employ Access Controls

- The user set the parameter to share all folders
- The user ignored or forgot the sharing boundary and stored sensitive files in the sharing folder

Malicious Downloaded Software

- Users unjustifiably trust in P2P networks
- P2P networking is popular with younger people, who have less experience with the kinds of tricks malicious code authors play and are less attuned to risk
- Users engaging in file sharing know their activity can be in a legal and ethical gray area
(Such indifference increases the risk of undetected harmful impact)

PEER-TO-PEER SHARING: VULNERABILITY

Unsafe User Interface

- Unsafe default

Establishing the default sharing space as the root (c:\) unless the user resets it

- Encouraging sharing

Making their P2P networks desirable by rewarding users for offering many files to share, thus encouraging users to open much of their file space for sharing and even suggesting that the user offer all email and attachment folders for sharing

- Aggressive scanning

Searching the user's file system for any media files and including all folders containing media as sharable

- Creeping access

Adding folders to the list of sharable ones each time a user offers a piece of media from a previously unsharable folder

PEER-TO-PEER SHARING: COUNTERMEASURE

User Education

- User awareness and training is an ongoing need, in part because threats and countermeasures are continually evolving
- Devices are not the complete solution to computer security problems, because the human element is so important
- Human caution needs to be a part of security protection

Secure-by-Default Software

- Making it easy for the user to choose a secure approach
- Secure default values, prompts warning the user of potentially insecure actions, and transparency of a program's activity

Outbound Firewall or Guard

- Control traffic flow in both directions, limiting inflow of executable code and outflow of sensitive documents

PEER-TO-PEER SHARING: COUNTERMEASURE

Legal Action

■ Copyrights

- Protect the expression of ideas
- Apply to a creative work (works in the arts and literature)

■ Patents

- Protect inventions, tangible objects, or ways to make them, not works of the mind
- Apply to the results of science, technology, and engineering

■ Trade Secrets

- Information that gives one company a competitive edge over others

■ Reverse engineering

Studies a finished object to determine how it is manufactured or how it works

REFERENCES

- Pfleeger, Charles P. and Shari Lawrence Pfleeger (2012), *Analyzing Computer Security*, 1st Edition, Prentice Hall.

NEXT WEEK: MAN-IN-THE-MIDDLE ATTACKS

- Threat
 - Man in the Middle
 - “In-the-Middle” Activity
- Vulnerability
 - Unwarranted Trust
 - Failed Identification and Authentication
 - Unauthorized Access
 - Inadequate Attention to Program Details
 - Protocol Weakness
- Countermeasure
 - Trust
 - Identification and Authentication
 - Cryptography
- Replay Attacks
- Session Hijack



AS THE WORLD IS INCREASINGLY INTERCONNECTED,
EVERYONE SHARES THE RESPONSIBILITY OF
SECURING CYBERSPACE



Vision

To become an **outstanding** undergraduate Computer Science program that produces **international-minded** graduates who are **competent** in software engineering and have **entrepreneurial spirit** and **noble character**.



Mission

1. To conduct studies with the best technology and curriculum, supported by professional lecturer
2. To conduct research in Informatics to promote science and technology
3. To deliver science-and-technology-based society services to implement science and technology