Computer Security

Class-9

Networks (Review)

- A collection of nodes or devices in a topology format

- A set of components
    - Computers
    - Printers
    - Storage devices.

Network Transmission Media (Review)

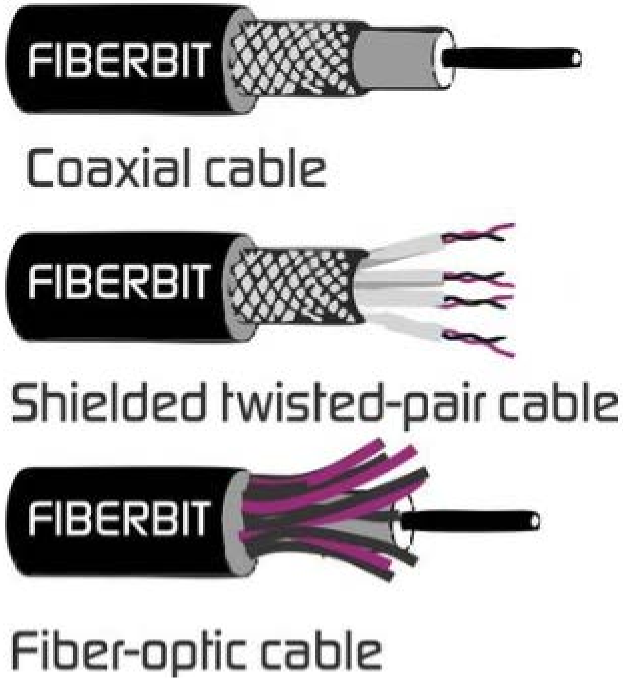
- Signal interception is a serious potential network vulnerability.

- Cable
  - Ethernet
  - Lan
  - MAC (Media access control)

- Packet Sniffing
  - A program or device which sniffs all packets in the LAN.

Network Transmission Media (Cont.) (Review)

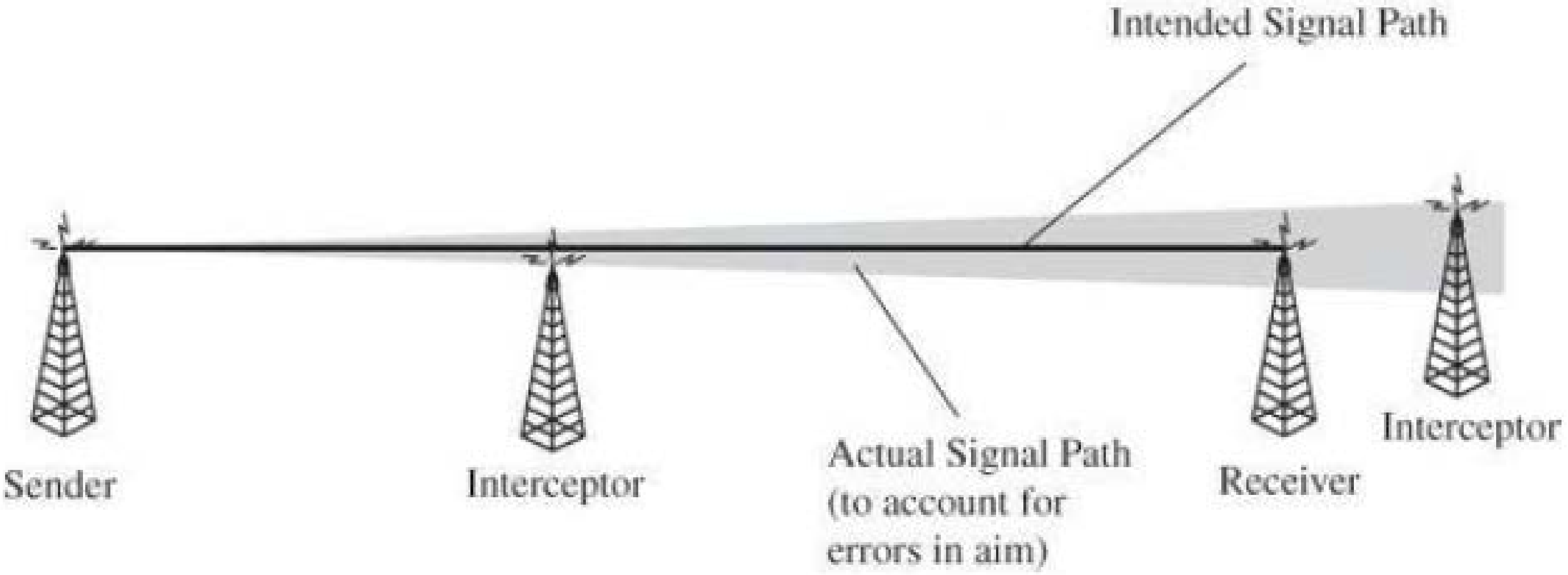
- Cable Splicing
  - If no inductance available, then direct cut
  - Inner conductor
  - Outer conductor



- Optical Fiber
  - Two security advantages over others
    - Entire optical network is tuned before a new connection
    - Carries light energy not electricity

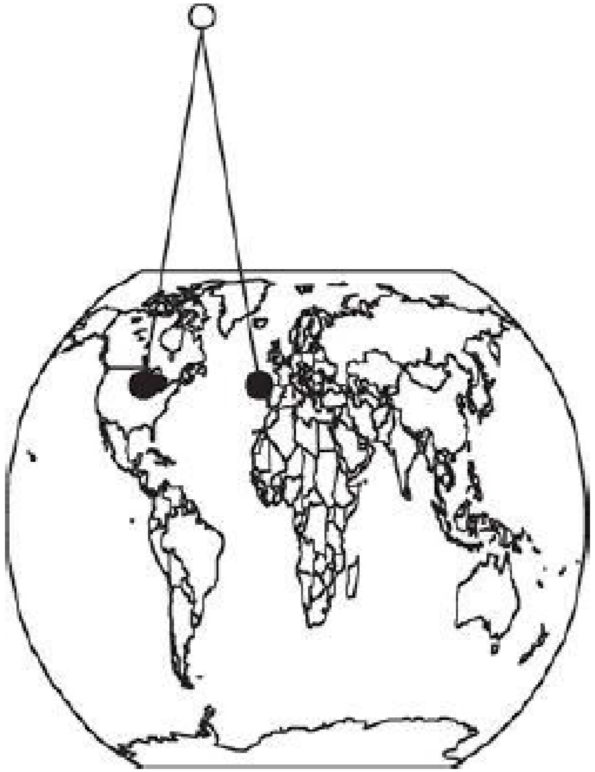
Network Transmission Media (Cont.) (Review)

- Microware
  - Wireless signals (Air)
  - Line-of-sight technology
  - Not shielded



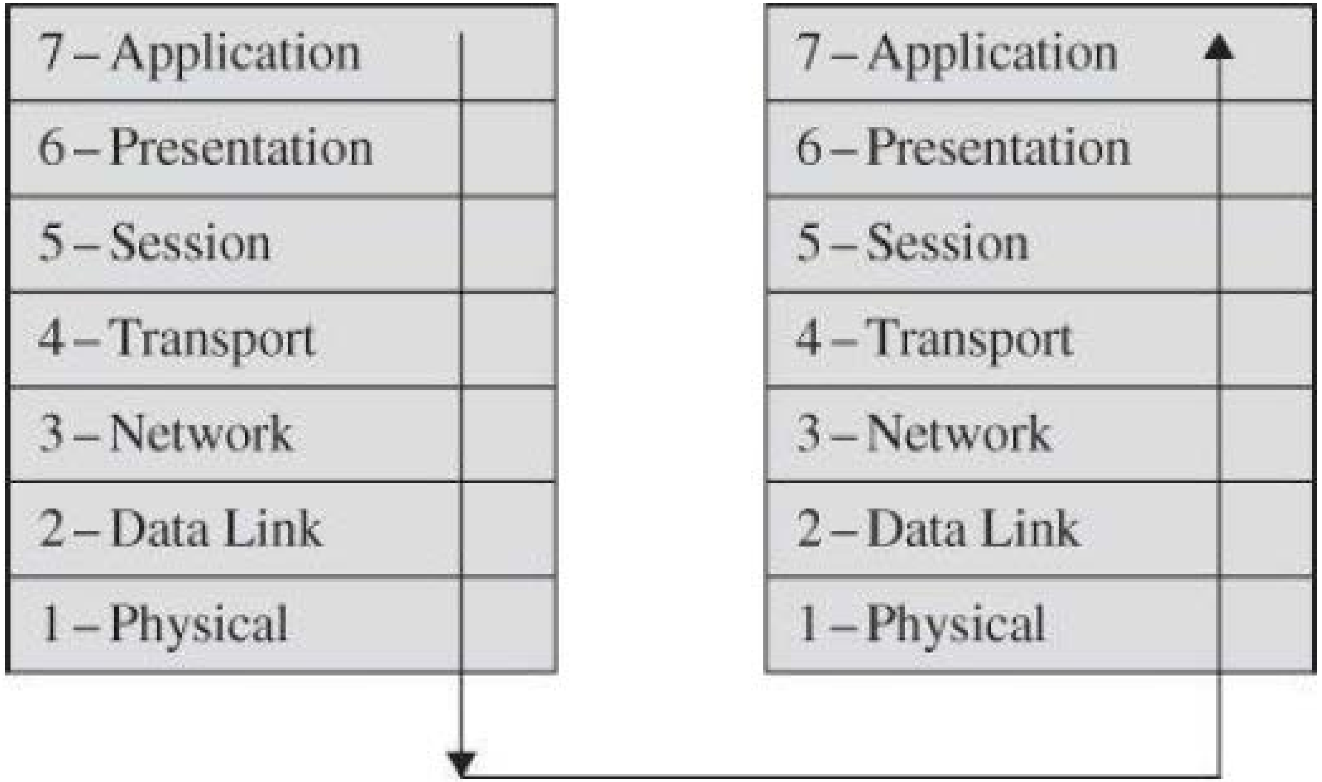
Network Transmission Media (Cont.) (Review)

- Satellite Communication
  - Signals can be bounced off a satellite: from earth to the satellite and back to earth again
  - The sender and receiver are fixed points; the sender beams a signal over a wide area in which the satellite is located, and the satellite rebroadcasts that signal to a certain radius around the receiver.



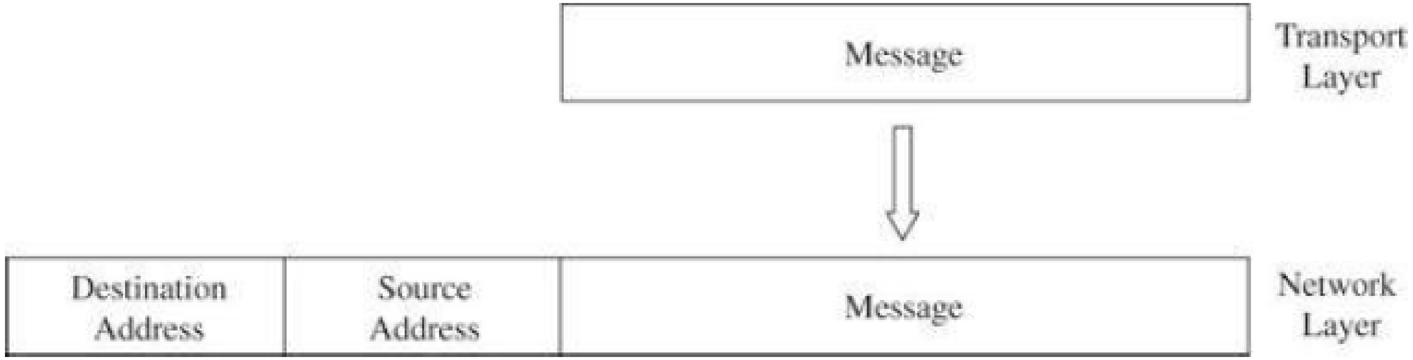
Protocol Layers (Review)

- The OSI model, most useful conceptually, describes similar processes of both the sender and receiver.



Addressing and Routing (Review)

- Protocol
  - allow a user to view the network at a high, abstract level of communication (viewing it in terms of user and data); the details of how the communication is accomplished are hidden within software and hardware at both ends.
- Addressing
  - Sender/receiver (routers)
  - Skku.edu
  - Packet
  - MAC Address



Addressing and Routing (Review)

- Routing
  - Routers direct traffic on a path that leads to a destination.
- Ports
  - Daemons (services)
  - Number associated with an application program that serves or monitors for a network service

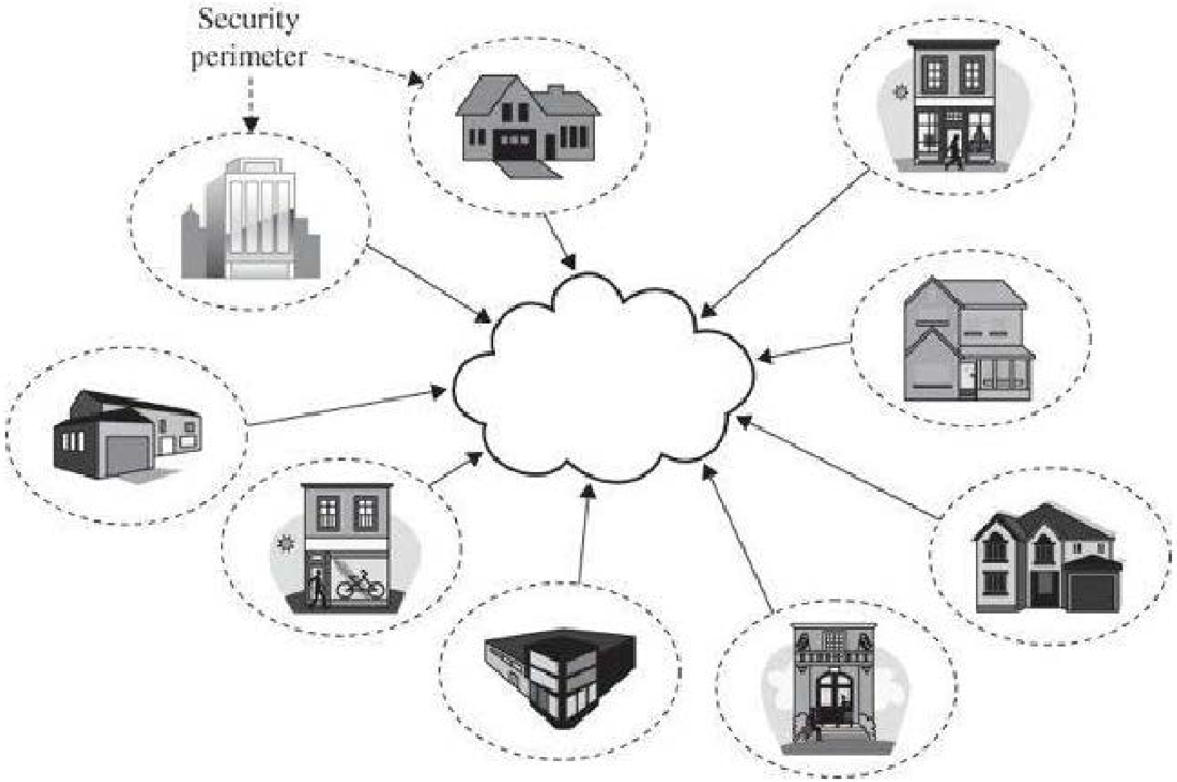
War on Networks: Network Security Attacks (Review)

- Threats to Network Communications
  - interception, or unauthorized viewing
  - modification, or unauthorized change
  - fabrication, or unauthorized creation
  - interruption, or preventing authorized access

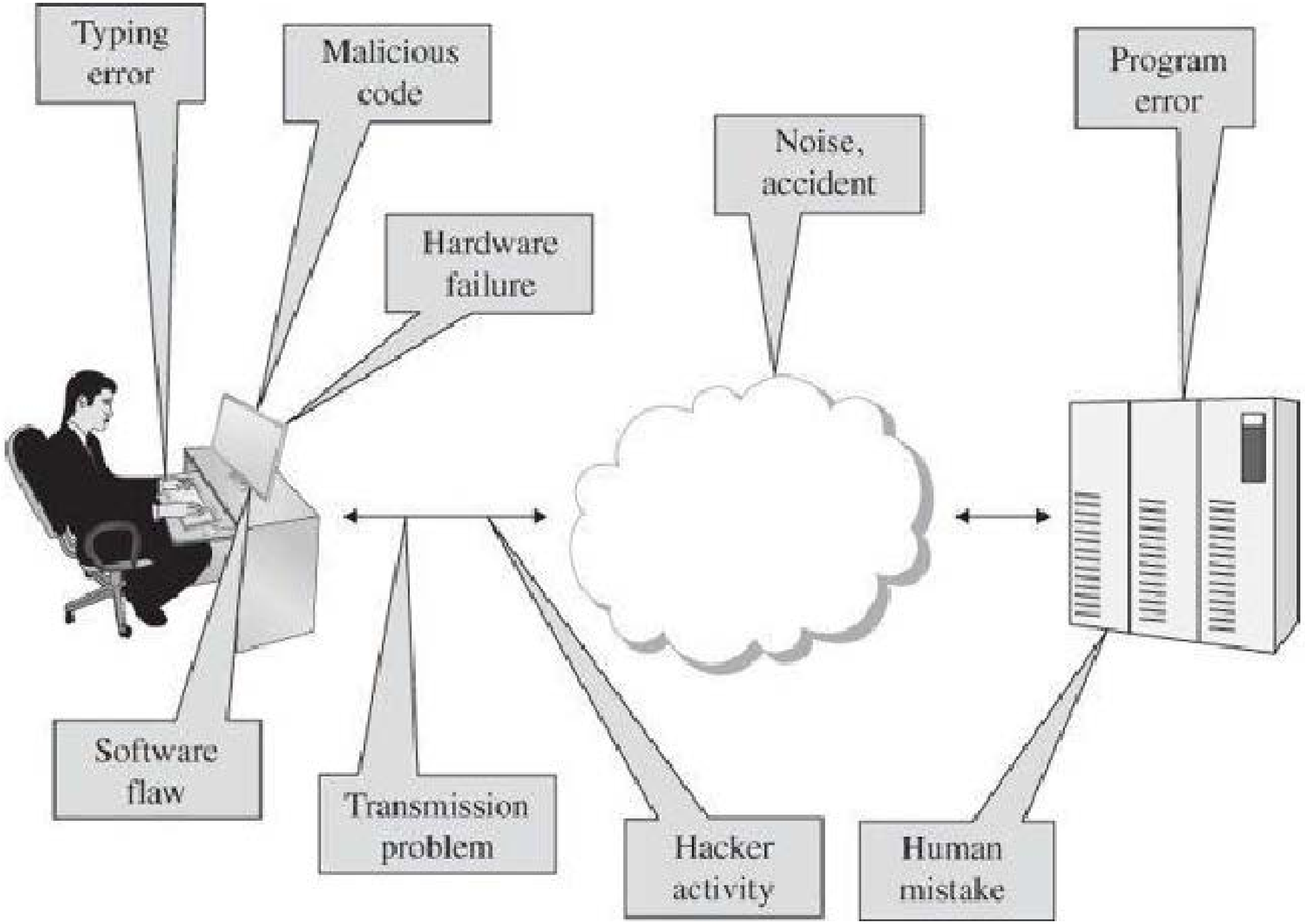
Interception: Eavesdropping and Wiretapping (Review)

- Eavesdropping
  - Secretly listening to a conversation

- Wiretapping
  - Data interception



Modification, Fabrication: Data Corruption (Review)

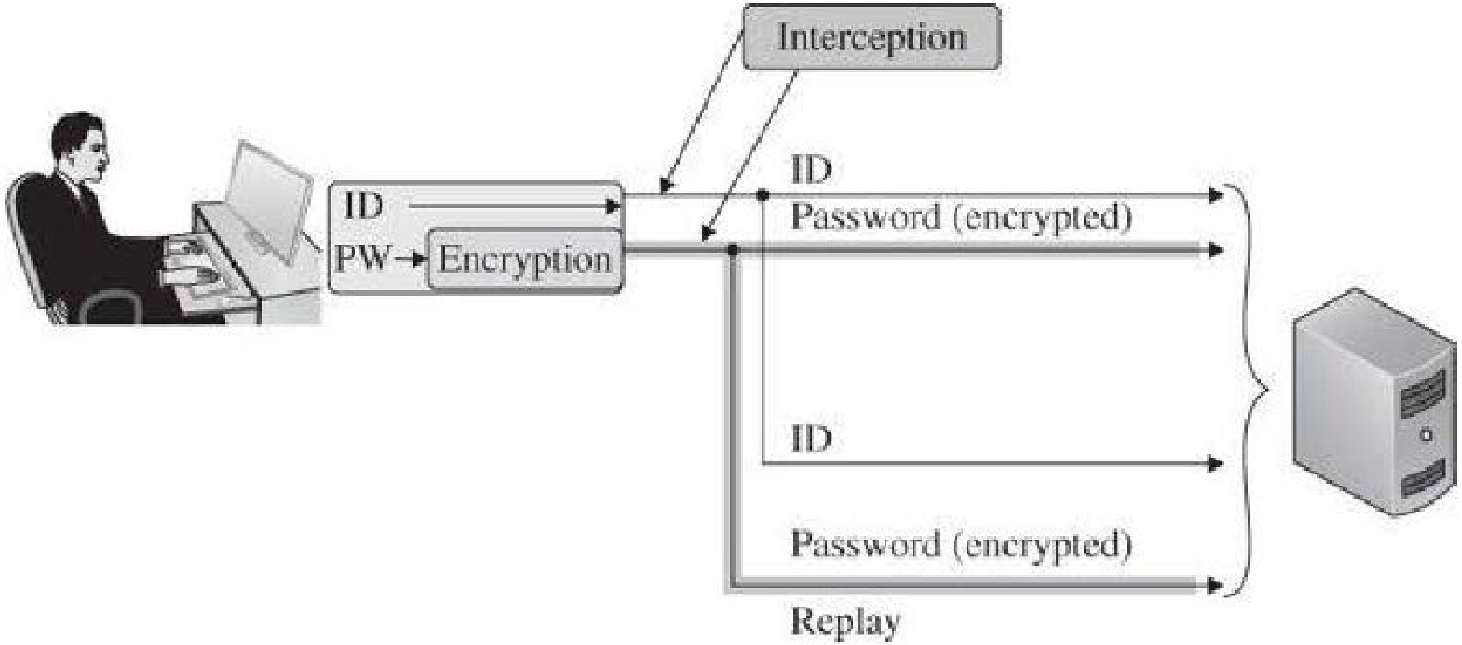


Modification, Fabrication: Data Corruption (Review)

- Network data corruption occurs naturally because of minor failures of transmission media. Corruption can also be induced for malicious purposes. Both must be controlled.
- Sequencing
  - A sequencing attack or problem involves permuting the order of data.
  - A sequencing error occurs when a later fragment of a data stream arrives before a previous one: Packet 2 arrives before packet 1.
- Substitution
  - A substitution attack is the replacement of one piece of a data stream with another.

Modification, Fabrication: Data Corruption

- Insertion
  - Data values are inserted into a stream. (Encryption)
- Replay
  - Legitimate data are intercepted and reused, generally without modification.



Modification, Fabrication: Data Corruption

- Physical Replay
  - Security camera monitoring

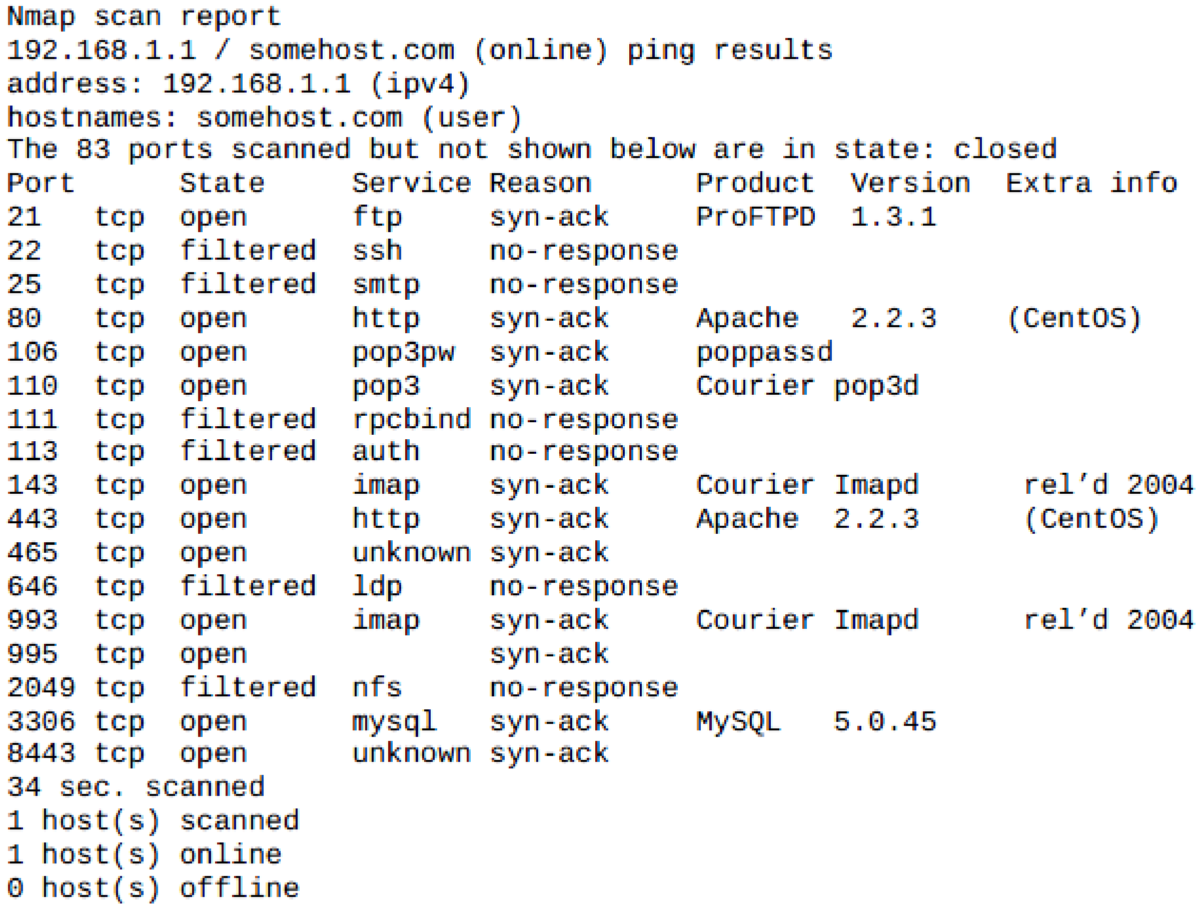
- Modification Attacks in General
  - precise
  - accurate
  - unmodified
  - modified only in acceptable ways
  - modified only by authorized people
  - modified only by authorized processes
  - consistent
  - internally consistent
  - meaningful and usable

Interruption: Loss of Service

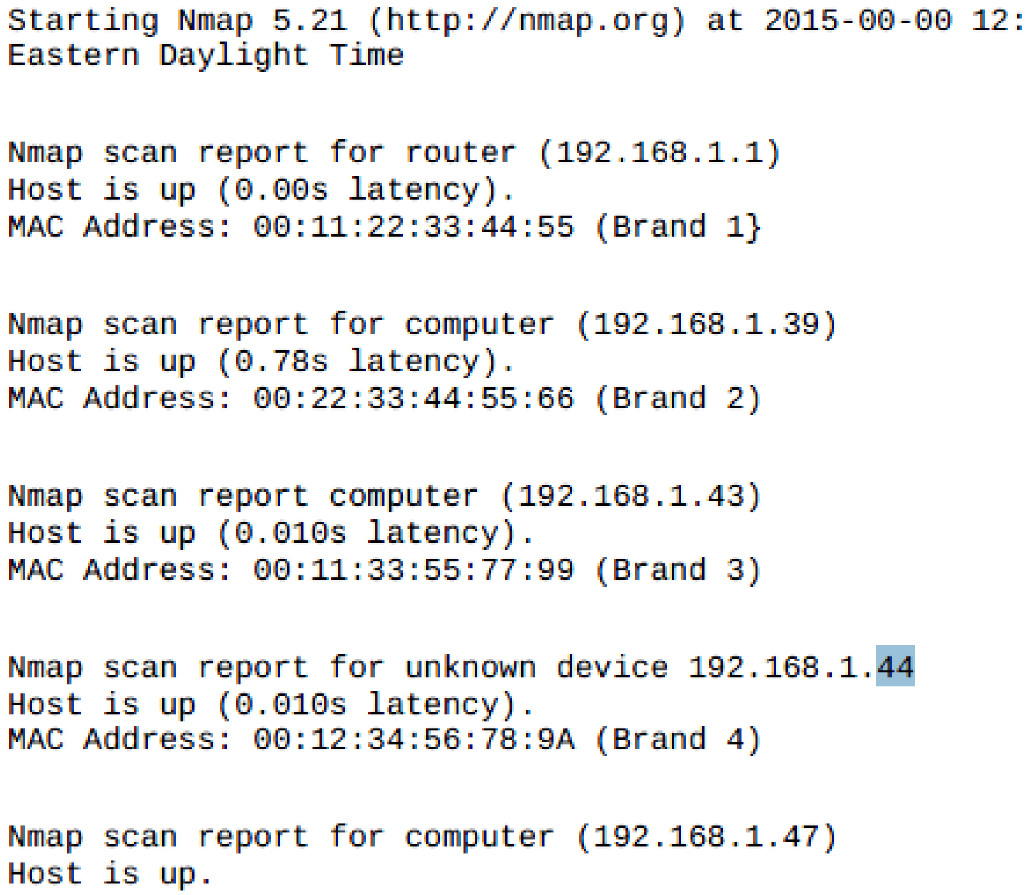
- Network design incorporates redundancy to counter hardware failures.
- Routing
  - Routing supports efficient resource use and quality of service. Misused, it can cause denial of service.
- Excessive Demand
  - Denial-of-service attacks usually try to flood a victim with excessive demand.
- Component Failure
- Port Scanning
  - A port scan maps the topology and hardware and software components of a network segment.

Interruption: Loss of Service

- Port Scanning tool (nmap)



```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port      State     Service Reason      Product  Version  Extra info
21   tcp  open      ftp     syn-ack     ProFTPD  1.3.1
22   tcp  filtered  ssh     no-response
25   tcp  filtered  smtp    no-response
80   tcp  open      http    syn-ack     Apache   2.2.3    (CentOS)
106  tcp  open      pop3pw  syn-ack     poppassd
110  tcp  open      pop3    syn-ack     Courier pop3d
111  tcp  filtered  rpcbind no-response
113  tcp  filtered  auth    no-response
143  tcp  open      imap    syn-ack     Courier Imapd      rel'd 2004
443  tcp  open      http    syn-ack     Apache  2.2.3      (CentOS)
465  tcp  open      unknown syn-ack
646  tcp  filtered  ldp     no-response
993  tcp  open      imap    syn-ack     Courier Imapd      rel'd 2004
995  tcp  open              syn-ack
2049 tcp  filtered  nfs     no-response
3306 tcp  open      mysql   syn-ack     MySQL   5.0.45
8443 tcp  open      unknown syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```



```
Starting Nmap 5.21 (http://nmap.org) at 2015-00-00 12:
Eastern Daylight Time

Nmap scan report for router (192.168.1.1)
Host is up (0.00s latency).
MAC Address: 00:11:22:33:44:55 (Brand 1}

Nmap scan report for computer (192.168.1.39)
Host is up (0.78s latency).
MAC Address: 00:22:33:44:55:66 (Brand 2)

Nmap scan report computer (192.168.1.43)
Host is up (0.010s latency).
MAC Address: 00:11:33:55:77:99 (Brand 3)

Nmap scan report for unknown device 192.168.1.44
Host is up (0.010s latency).
MAC Address: 00:12:34:56:78:9A (Brand 4)

Nmap scan report for computer (192.168.1.47)
Host is up.
```

Interruption: Loss of Service

- Port Scanning tool (nmap)
  - how many hosts there are
  - what their IP addresses are
  - what their physical (MAC) addresses are
  - what brand each is
  - what operating system each runs, and what version
  - what ports respond to service requests
  - what service applications respond, and what program and version they are running
  - how long responses took (which reveals speed of various network connections and thus may indicate the design of the network)

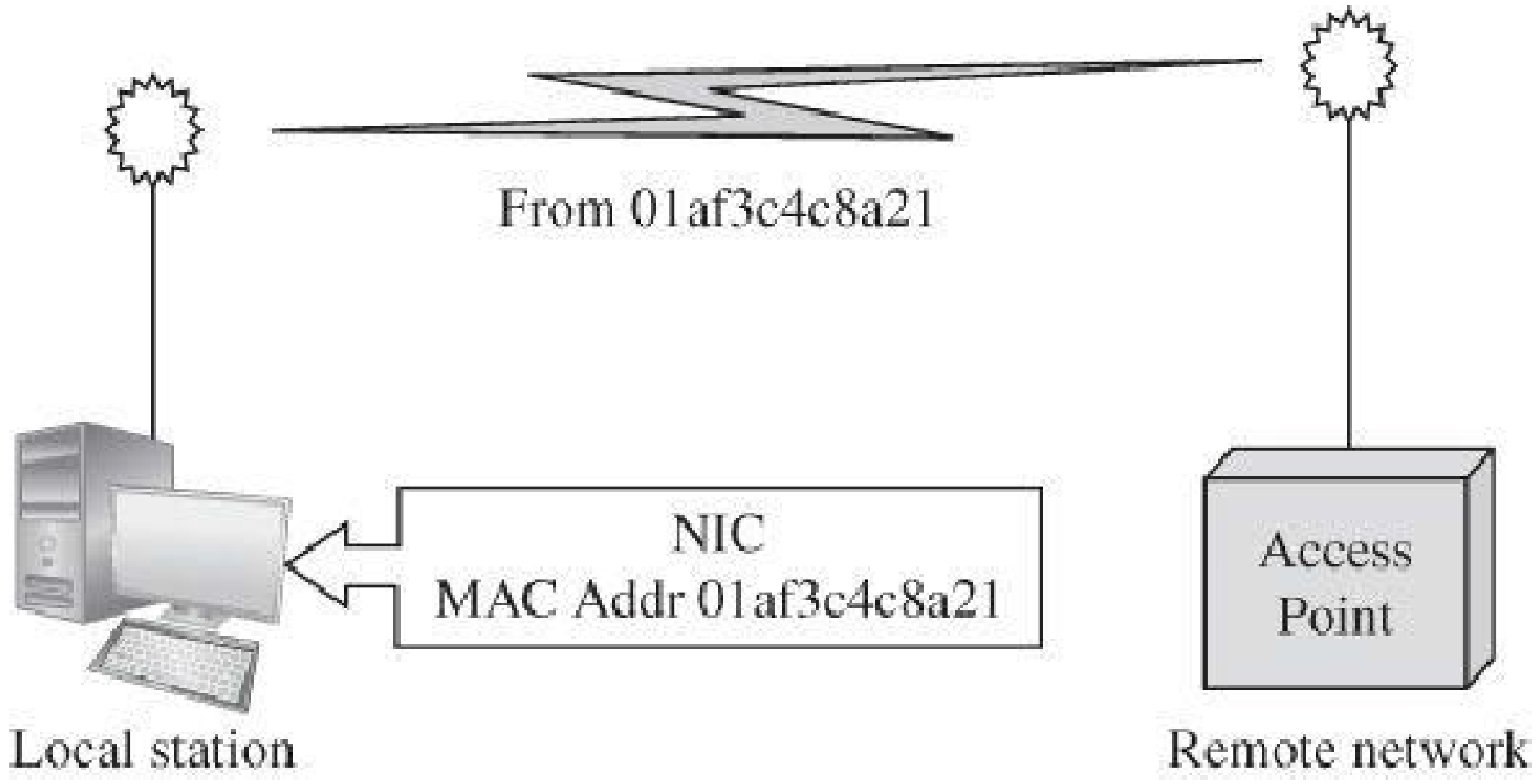
Wireless Network Security

- Wireless communication will never be as secure as wired, because the exposed signal is more vulnerable.
- Wireless Communication
  - You press buttons to activate your phone.
  - You press buttons to select and transmit the friend’s number (a process that used to be called dialing the phone).
  - Your friend hears a tone and presses a button to accept your call.
  - Your friend says “hello,” or some other greeting.
  - You say hello.
  - You begin your conversation.

The 802.11 Protocol Suite

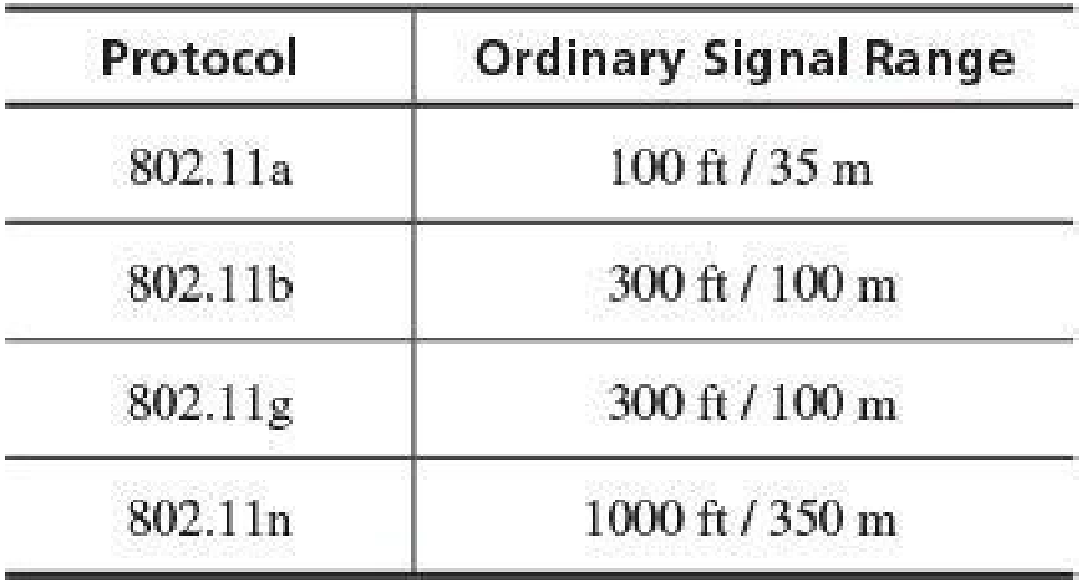
- How devices communicate in the 2.4 GHz radio signal band (essentially 2.4 GHz–2.5 GHz) allotted to WiFi
- The band is divided into 14 channels or subranges within the band
- Wireless signals can travel up to 100 meters (300 feet), although the quality of the signal diminishes with distance, and intervening objects such as walls and trees also interfere with communication.
- A NIC identifies itself (and hence its connected computer) by a supposedly unique MAC address.

The 802.11 Protocol Suite



The 802.11 Protocol Suite

- WiFi Access Range

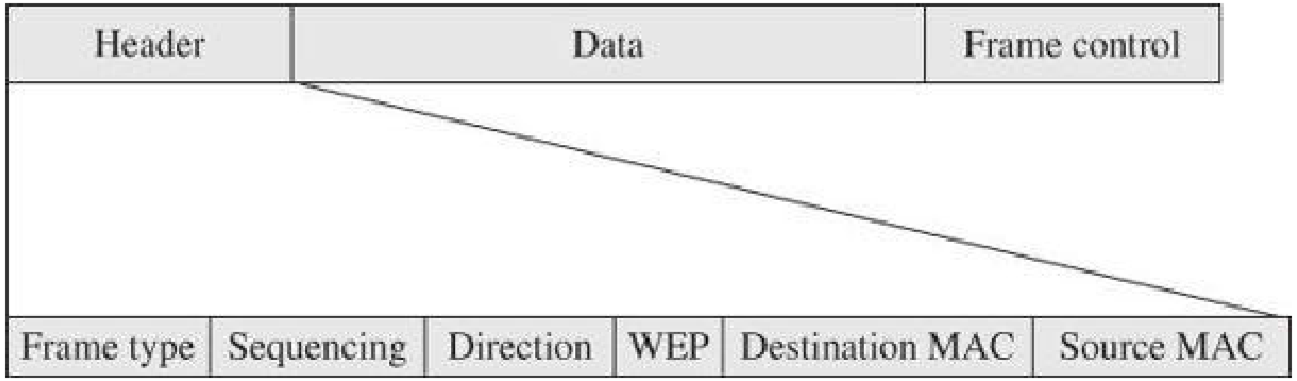


Protocol	Ordinary Signal Range
802.11a	100 ft / 35 m
802.11b	300 ft / 100 m
802.11g	300 ft / 100 m
802.11n	1000 ft / 350 m

- WiFi Frames
  - Each WiFi data unit is called a frame.

The 802.11 Protocol Suite

- WiFi Frames
  - frame type: control, management, or data
  - ToDS, FromDS: direction of this frame: to or from the access point
  - fragmentation and order control bits
  - WEP (wired equivalent privacy) or encryption bit: encryption, described shortly
  - up to four MAC addresses (physical device identifiers): sender and receiver’s addresses, plus two optional addresses for traffic filtering points



Header	Data	Frame control

Frame type	Sequencing	Direction	WEP	Destination MAC	Source MAC

The 802.11 Protocol Suite

- Management Frames
  - Control the establishment and handling of a series of data flow.
- Beacon
  - A beacon signal advertises a network accepting connections.
- Authentication
  - A NIC requests a connection by sending an authentication frame.
- Association request and response.
- SSID
  - Service set identifier
  - An SSID is a string to identify a wireless access point.

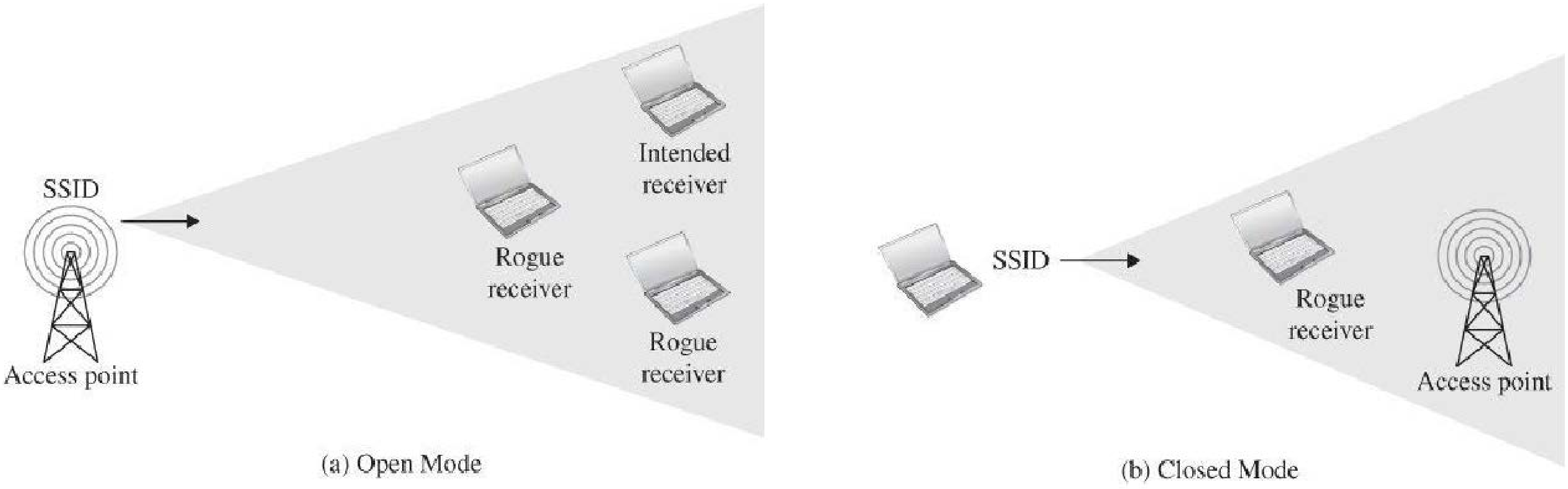
Vulnerabilities in Wireless Networks

- Confidentiality
- Integrity
- Availability
- Unauthorized WiFi Access
- WiFi Protocol Weaknesses
- Picking Up the Beacon

Sungkyunkwan University (SKKU)

Vulnerabilities in Wireless Networks

- Picking Up the Beacon



(a) Open Mode

(b) Closed Mode

Sungkyunkwan University (SKKU)

Vulnerabilities in Wireless Networks

- SSID in All Frames
- Authentication in Wireless Networks (Access point)
- Changeable MAC Addresses
- Stealing the Association
- Preferred Associations

Failed Countermeasure: WEP (Wired Equivalent Privacy)

- WEP Security Weaknesses
  - Wired equivalent privacy
- Weak Encryption Key
  - 64- or 128-bit encryption key
- Static Key
- Weak Encryption Process
  - 40-104 (brute force)
- Weak Encryption Algorithm
  - Small sequence
- Faulty Integrity Check

Stronger Protocol Suite: WPA (WiFi Protected Access)

- WiFi Protected Access or WPA
- Strengths of WPA over WEP
- Non-Static Encryption Key
- Authentication
- Strong Encryption
- Integrity Protection
- Session Initiation

Attacks on WPA

- Man-in-the-Middle

- Incomplete Authentication

- Exhaustive Key Search

Denial of Service

- Massive Estonian Web Failure
- Among the sites under attack were those of
  - the president
  - parliament
  - many government departments
  - political parties
  - major news organizations
  - major banks
  - telecommunications firms

Denial of Service

- The source of a denial-of-service attack is typically difficult or impossible to determine with certainty.
- How Service Is Denied
  - DOS can occur from excessive volume, a failed application, a severed link, or hardware or software failure.
- Flooding
  - A flooding attack occurs from demand in excess of capacity, from malicious or natural causes.
- Blocked Access
- Access Failure
  - If a network works, administrators are tempted to expand it incrementally instead of redesigning it to address increased usage