Computer Networks: Basics & Security Issues

Burak Ekici

ekcburak@hotmail.com

Department of Computer Engineering,
Yaşar University,
Turkey.

April 22, 2012

Agenda

1. General Information About Networks
   - The Notion: Computer Network
   - The ISO/OSI Model
     - The ISO/OSI Layers
2. Network Security
   - Definition & The Goals: Network Security
   - Network Security: Approaches
   - Vulnerabilities: Layer by Layer
3. Summary

The Notion: Computer Network

Definition: Computer Network

*A **computer network** is simply two or more computers connected together so they can exchange information. A small network can be as simple as two computers linked together with the aim of information sharing and/or common usage of H/W devices.*

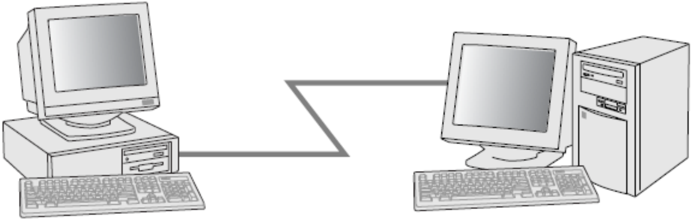


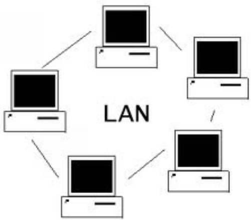
Figure: Two Networked Computers

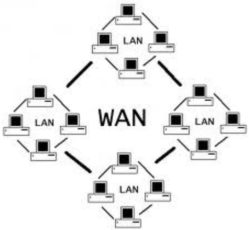
Image Source: Building a Simple Network (by Intel)

Types of Networks

Networking Types

1. *Local Area Networks (LAN): A LAN connects computers together at one location.*
2. *Metropolitan Area Networks (MAN): A MAN connects two or more LANs together but does not span outside the boundaries of a city, town, or metropolitan area.*
3. *Wide Area Networks (WAN): A WAN connects larger geographic areas. Often, smaller LANs are interconnected to form a large WAN.*





The ISO/OSI Model

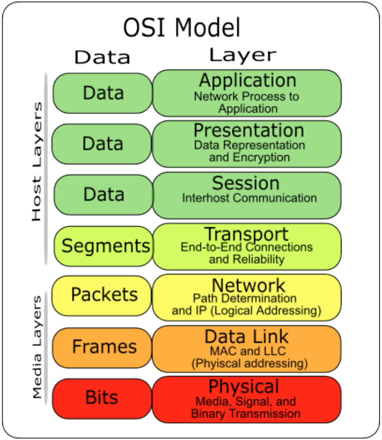

OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Figure: The OSI Layer

Definition: The ISO/OSI Model

The International Standards Organization (ISO) Open Systems Interconnect (OSI) Reference Model presents seven layers of communications types, and the interfaces between them.

The aim is connecting two computers in different platforms together.

The ISO/OSI Layers

Each layer provides service to the its above and below layers.

The ISO/OSI Layers

The Pysical Layer

- *Physical Layer defines the physical environment in/on which information, in the form of bits, is transferred.*
  - *Wired Communication Environment*
  - *Wireless Communication Environment*
- *In order for both sender and receiver machines to put the same meaning on the transferred data; the same protocols should be used.*
- *Protocols that are used in this layer: ISDN, RS-232, EIA-422, RS-449, EIA-485, 10BASE-T, 100BASE-TX, SONET, DSL, ...*

Physical Transmission of the Data!!!

The ISO/OSI Layers

The Pysical Layer

- *Physical Layer defines the physical environment in/on which information, in the form of bits, is transferred.*
  - *Wired Communication Environment*
  - *Wireless Communication Environment*
- *In order for both sender and receiver machines to put the same meaning on the transferred data; the same protocols should be used.*
- *Protocols that are used in this layer: ISDN, RS-232, EIA-422, RS-449, EIA-485, 10BASE-T, 100BASE-TX, SONET, DSL, ...*

Physical Transmission of the Data!!!

The ISO/OSI Layers

The Pysical Layer

- *Physical Layer defines the physical environment in/on which information, in the form of bits, is transferred.*
  - *Wired Communication Environment*
  - *Wireless Communication Environment*
- *In order for both sender and receiver machines to put the same meaning on the transferred data; the same protocols should be used.*
- *Protocols that are used in this layer: ISDN, RS-232, EIA-422, RS-449, EIA-485, 10BASE-T, 100BASE-TX, SONET, DSL, ...*

Physical Transmission of the Data!!!

The ISO/OSI Layers

The Pysical Layer

- *Physical Layer defines the physical environment in/on which information, in the form of bits, is transferred.*
  - *Wired Communication Environment*
  - *Wireless Communication Environment*
- *In order for both sender and receiver machines to put the same meaning on the transferred data; the same protocols should be used.*
- *Protocols that are used in this layer: ISDN, RS-232, EIA-422, RS-449, EIA-485, 10BASE-T, 100BASE-TX, SONET, DSL, ...*

Physical Transmission of the Data!!!

The ISO/OSI Layers

The Data Link Layer

- *Data Link Layer defines the access rights to the Physical Layer.*
- *Responsible for the integrity of the data.*
- *Adds MAC address to the transferred data.*
- *The unit of transmitted information is called a frame which consists of a link-layer header followed by bits.*
- *Protocols that are used in this layer: Ethernet, HDLC, Wi-Fi, Token ring, FDDI, PPP, ...*

Hardware address evaluation!!!

The ISO/OSI Layers

The Data Link Layer

- *Data Link Layer defines the access rights to the Physical Layer.*
- *Responsible for the integrity of the data.*
- *Adds MAC address to the transferred data.*
- *The unit of transmitted information is called a frame which consists of a link-layer header followed by bits.*
- *Protocols that are used in this layer: Ethernet, HDLC, Wi-Fi, Token ring, FDDI, PPP, ...*

Hardware address evaluation!!!

The ISO/OSI Layers

The Data Link Layer

- *Data Link Layer defines the access rights to the Physical Layer.*
- *Responsible for the integrity of the data.*
- *Adds MAC address to the transferred data.*
- *The unit of transmitted information is called a frame which consists of a link-layer header followed by bits.*
- *Protocols that are used in this layer: Ethernet, HDLC, Wi-Fi, Token ring, FDDI, PPP, ...*

Hardware address evaluation!!!

The ISO/OSI Layers

The Data Link Layer

- *Data Link Layer defines the access rights to the Physical Layer.*
- *Responsible for the integrity of the data.*
- *Adds MAC address to the transferred data.*
- *The unit of transmitted information is called a frame which consists of a link-layer header followed by bits.*
- *Protocols that are used in this layer: Ethernet, HDLC, Wi-Fi, Token ring, FDDI, PPP, ...*

Hardware address evaluation!!!

The ISO/OSI Layers

The Data Link Layer

- *Data Link Layer defines the access rights to the Physical Layer.*
- *Responsible for the integrity of the data.*
- *Adds MAC address to the transferred data.*
- *The unit of transmitted information is called a frame which consists of a link-layer header followed by bits.*
- *Protocols that are used in this layer: Ethernet, HDLC, Wi-Fi, Token ring, FDDI, PPP, ...*

Hardware address evaluation!!!

The ISO/OSI Layers

The Data Link Layer

- *Data Link Layer defines the access rights to the Physical Layer.*
- *Responsible for the integrity of the data.*
- *Adds MAC address to the transferred data.*
- *The unit of transmitted information is called a frame which consists of a link-layer header followed by bits.*
- *Protocols that are used in this layer: Ethernet, HDLC, Wi-Fi, Token ring, FDDI, PPP, ...*

Hardware address evaluation!!!

The ISO/OSI Layers

The Network Layer

- *Network Layer manages the network traffic to avoid the possible collision.*
- *The unit of transmitted information is called a packet which consists of a network layer header followed by a frame.*
- *Adds IP address to the transferred data.*
- *Protocols that are used in this layer: IP, IPv4, IPv6, ICMP, ARP, IGMP, . . .*

Network address evaluation!!!

The ISO/OSI Layers

The Network Layer

- *Network Layer manages the network traffic to avoid the possible collision.*
- *The unit of transmitted information is called a packet which consists of a network layer header followed by a frame.*
- *Adds IP address to the transferred data.*
- *Protocols that are used in this layer: IP, IPv4, IPv6, ICMP, ARP, IGMP, . . .*

Network address evaluation!!!

The ISO/OSI Layers

The Network Layer

- *Network Layer manages the network traffic to avoid the possible collision.*
- *The unit of transmitted information is called a packet which consists of a network layer header followed by a frame.*
- *Adds IP address to the transferred data.*
- *Protocols that are used in this layer: IP, IPv4, IPv6, ICMP, ARP, IGMP, . . .*

Network address evaluation!!!

The ISO/OSI Layers

The Network Layer

- *Network Layer manages the network traffic to avoid the possible collision.*
- *The unit of transmitted information is called a packet which consists of a network layer header followed by a frame.*
- *Adds IP address to the transferred data.*
- *Protocols that are used in this layer: IP, IPv4, IPv6, ICMP, ARP, IGMP, . . .*

Network address evaluation!!!

The ISO/OSI Layers

The Network Layer

- *Network Layer manages the network traffic to avoid the possible collision.*
- *The unit of transmitted information is called a packet which consists of a network layer header followed by a frame.*
- *Adds IP address to the transferred data.*
- *Protocols that are used in this layer: IP, IPv4, IPv6, ICMP, ARP, IGMP, . . .*

Network address evaluation!!!

The ISO/OSI Layers

The Transport Layer

- *Transport Layer is the first purely logical layer*
- *It also ensures error-freeness of the transmission.*
- *Data-transmission rates, congestion control are also the responsibilities of the layer.*
- *The unit of transmitted information is called a segment which consists of a transport layer header followed by a packet.*
- *Protocols that are used in this layer: TCP, UDP, SCTP, DCCP, ...*

Connection Type Evaluation

The ISO/OSI Layers

The Transport Layer

- *Transport Layer is the first purely logical layer*
- *It also ensures error-freeness of the transmission.*
- *Data-transmission rates, congestion control are also the responsibilities of the layer.*
- *The unit of transmitted information is called a segment which consists of a transport layer header followed by a packet.*
- *Protocols that are used in this layer: TCP, UDP, SCTP, DCCP, ...*

Connection Type Evaluation

The ISO/OSI Layers

The Transport Layer

- *Transport Layer is the first purely logical layer*
- *It also ensures error-freeness of the transmission.*
- *Data-transmission rates, congestion control are also the responsibilities of the layer.*
- *The unit of transmitted information is called a segment which consists of a transport layer header followed by a packet.*
- *Protocols that are used in this layer: TCP, UDP, SCTP, DCCP, ...*

Connection Type Evaluation

The ISO/OSI Layers

The Transport Layer

- *Transport Layer is the first purely logical layer*
- *It also ensures error-freeness of the transmission.*
- *Data-transmission rates, congestion control are also the responsibilities of the layer.*
- *The unit of transmitted information is called a segment which consists of a transport layer header followed by a packet.*
- *Protocols that are used in this layer: TCP, UDP, SCTP, DCCP, ...*

Connection Type Evaluation

The ISO/OSI Layers

The Transport Layer

- *Transport Layer is the first purely logical layer*
- *It also ensures error-freeness of the transmission.*
- *Data-transmission rates, congestion control are also the responsibilities of the layer.*
- *The unit of transmitted information is called a segment which consists of a transport layer header followed by a packet.*
- *Protocols that are used in this layer: TCP, UDP, SCTP, DCCP, ...*

Connection Type Evaluation

The ISO/OSI Layers

The Transport Layer

- *Transport Layer is the first purely logical layer*
- *It also ensures error-freeness of the transmission.*
- *Data-transmission rates, congestion control are also the responsibilities of the layer.*
- *The unit of transmitted information is called a segment which consists of a transport layer header followed by a packet.*
- *Protocols that are used in this layer: TCP, UDP, SCTP, DCCP, ...*

Connection Type Evaluation

The ISO/OSI Layers

The Session Layer

- *Session Layer provides the mechanism for opening, closing and managing a session between end-user application processes.*
- *Protocols that are used in this layer: Named Pipes, Socket, NetBIOS, SAP, Half Duplex, Full Duplex, Simplex, SDP, RPC, SMPP, SSH*

Opening and Closing Connections!!!

The ISO/OSI Layers

The Session Layer

- *Session Layer provides the mechanism for opening, closing and managing a session between end-user application processes.*
- *Protocols that are used in this layer: Named Pipes, Socket, NetBIOS, SAP, Half Duplex, Full Duplex, Simplex, SDP, RPC, SMPP, SSH*

Opening and Closing Connections!!!

The ISO/OSI Layers

The Session Layer

- *Session Layer provides the mechanism for opening, closing and managing a session between end-user application processes.*
- *Protocols that are used in this layer: Named Pipes, Socket, NetBIOS, SAP, Half Duplex, Full Duplex, Simplex, SDP, RPC, SMPP, SSH*

Opening and Closing Connections!!!

The ISO/OSI Layers

The Presentation Layer

- *Presentation Layer puts meaning on the transmitted information for its receiver to understand it.*
- *Different programs could use each other's data format.*
- *Protocols that are used in this layer: TDI, ASCII, MPEG, ISO 8822, ISO 8823, ISO 8824, ITU-T T.73, ITU-T X.409, ...*

Data Sequence Management!!!

The ISO/OSI Layers

The Presentation Layer

- *Presentation Layer puts meaning on the transmitted information for its receiver to understand it.*
- *Different programs could use each other's data format.*
- *Protocols that are used in this layer: TDI, ASCII, MPEG, ISO 8822, ISO 8823, ISO 8824, ITU-T T.73, ITU-T X.409, ...*

Data Sequence Management!!!

The ISO/OSI Layers

The Presentation Layer

- *Presentation Layer puts meaning on the transmitted information for its receiver to understand it.*
- *Different programs could use each other's data format.*
- *Protocols that are used in this layer: TDI, ASCII, MPEG, ISO 8822, ISO 8823, ISO 8824, ITU-T T.73, ITU-T X.409, ...*

Data Sequence Management!!!

The ISO/OSI Layers

The Presentation Layer

- *Presentation Layer puts meaning on the transmitted information for its receiver to understand it.*
- *Different programs could use each other's data format.*
- *Protocols that are used in this layer: TDI, ASCII, MPEG, ISO 8822, ISO 8823, ISO 8824, ITU-T T.73, ITU-T X.409, ...*

Data Sequence Management!!!

The ISO/OSI Layers

The Application Layer

- *Application layer provides services for software applications.*
- *also supplies the ability for user applications to interact with the network.*
- *Protocols that are used in this layer: HTTP, HTTPS, SMTP, POP, FTP, TFTP, UUCP, NNTP, SSL, SSH, IRC, SNMP, SIP, RTP, Telnet, ...*

Applications for network interactions!!!

The ISO/OSI Layers

The Application Layer

- *Application layer provides services for software applications.*
- *also supplies the ability for user applications to interact with the network.*
- *Protocols that are used in this layer: HTTP, HTTPS, SMTP, POP, FTP, TFTP, UUCP, NNTP, SSL, SSH, IRC, SNMP, SIP, RTP, Telnet, ...*

Applications for network interactions!!!

The ISO/OSI Layers

The Application Layer

- *Application layer provides services for software applications.*
- *also supplies the ability for user applications to interact with the network.*
- *Protocols that are used in this layer: HTTP, HTTPS, SMTP, POP, FTP, TFTP, UUCP, NNTP, SSL, SSH, IRC, SNMP, SIP, RTP, Telnet, ...*

Applications for network interactions!!!

The ISO/OSI Layers

The Application Layer

- *Application layer provides services for software applications.*
- *also supplies the ability for user applications to interact with the network.*
- *Protocols that are used in this layer: HTTP, HTTPS, SMTP, POP, FTP, TFTP, UUCP, NNTP, SSL, SSH, IRC, SNMP, SIP, RTP, Telnet, ...*

Applications for network interactions!!!

Network Security Basics

What is Network Security

Network Security is a specialized field in computer networking standing for keeping networks away from:

- *Distortion and destruction of the data transmitted,*
- *Penetration and cracking,*
- *Interruption of the communication.*

together with the goals of:

- *Confidentiality: avoidance of unauthorized access to the data*
- *Integrity: keeping data unchanged*
- *Availability: authorized user could use the network when/every time they need.*
- *Authentication: the receiver should be sure about the origin or sender of the data (authentica data)*
- *Non-repudiation: the sender should not deny the data he/she sent.*

Network Security Basics

What is Network Security

Network Security is a specialized field in computer networking standing for keeping networks away from:

- *Distortion and destruction of the data transmitted,*
- *Penetration and cracking,*
- *Interruption of the communication.*

together with the goals of:

- *Confidentiality: avoidance of unauthorized access to the data*
- *Integrity: keeping data unchanged*
- *Availability: authorized user could use the network when/every time they need.*
- *Authentication: the receiver should be sure about the origin or sender of the data (authentica data)*
- *Non-repudiation: the sender should not deny the data he/she sent.*

Network Security Basics

In order to achieve these goals:

1. *Identifying a security policy*:
   - *Well-defined access rights.*
   - *Well-defined cases in the usages of network assets.*
2. *Being aware about system features*:
   - *define the weakest and strongest parts,*
   - *the most important assets,*
   - *the available and visible assets and links (all the time).*
3. *Forcing the limits to understand system vulnerabilities*:
   - *define possible attack strategies against your system,*
   - *possible attackers,*
   - *the reasons for these attacks.*
4. *Defining a security mechanism (ways to secure the vulnerable parts)*:
   - *Usages of secure hard and softwares.*
   - *Cryptography: Encrypted transmission of the data.*
   - *Security Expertise.*

Network Security Basics

In order to achieve these goals:

1. *Identifying a security policy*:
   - *Well-defined access rights.*
   - *Well-defined cases in the usages of network assets.*
2. *Being aware about system features*:
   - *define the weakest and strongest parts,*
   - *the most important assets,*
   - *the available and visible assets and links (all the time).*
3. *Forcing the limits to understand system vulnerabilities:*
   - *define possible attack strategies against your system,*
   - *possible attackers,*
   - *the reasons for these attacks.*
4. *Defining a security mechanism (ways to secure the vulnerable parts):*
   - *Usages of secure hard and softwares.*
   - *Cryptography: Encrypted transmission of the data.*
   - *Security Expertise.*

Network Security Basics

In order to achieve these goals:

1. *Identifying a security policy:*
   - *Well-defined access rights.*
   - *Well-defined cases in the usages of network assets.*
2. *Being aware about system features:*
   - *define the weakest and strongest parts,*
   - *the most important assets,*
   - *the available and visible assets and links (all the time).*
3. *Forcing the limits to understand system vulnerabilities:*
   - *define possible attack strategies against your system,*
   - *possible attackers,*
   - *the reasons for these attacks.*
4. *Defining a security mechanism (ways to secure the vulnerable parts):*
   - *Usages of secure hard and softwares.*
   - *Cryptography: Encrypted transmission of the data.*
   - *Security Expertise.*

Network Security Basics

In order to achieve these goals:

1. *Identifying a security policy*:
   - *Well-defined access rights.*
   - *Well-defined cases in the usages of network assets.*
2. *Being aware about system features*:
   - *define the weakest and strongest parts,*
   - *the most important assets,*
   - *the available and visible assets and links (all the time).*
3. *Forcing the limits to understand system vulnerabilities*:
   - *define possible attack strategies against your system,*
   - *possible attackers,*
   - *the reasons for these attacks.*
4. *Defining a security mechanism (ways to secure the vulnerable parts)*:
   - *Usages of secure hard and softwares.*
   - *Cryptography: Encrypted transmission of the data.*
   - *Security Expertise.*

Network Security Basics

Security Mechanisms

1. *Prevention Mechanisms: efforts for avoiding attacks*
2. *Detection Mechanism: efforts for detecting attacks*
3. *Recovery Mechanism: efforts for reconstructing a subverted system*
4. *User Awareness: informing users about the risks in the ways that they use resources*
5. *Physical Protection of H/W Devices*
6. *Usages of Access Control Softwares: through Need-to-Know Principal*
7. *Usages of Cryptographic Schemes*
8. *Monitoring the System Activity: auditing*

Network Security Basics

Security Mechanisms

1. *Prevention Mechanisms: efforts for avoiding attacks*
2. *Detection Mechanism: efforts for detecting attacks*
3. *Recovery Mechanism: efforts for reconstructing a subverted system*
4. *User Awareness: informing users about the risks in the ways that they use resources*
5. *Physical Protection of H/W Devices*
6. *Usages of Access Control Softwares: through Need-to-Know Principal*
7. *Usages of Cryptographic Schemes*
8. *Monitoring the System Activity: auditing*

Network Security Basics

Security Mechanisms

1. *Prevention Mechanisms: efforts for avoiding attacks*
2. *Detection Mechanism: efforts for detecting attacks*
3. *Recovery Mechanism: efforts for reconstructing a subverted system*
4. *User Awareness: informing users about the risks in the ways that they use resources*
5. *Physical Protection of H/W Devices*
6. *Usages of Access Control Softwares: through Need-to-Know Principal*
7. *Usages of Cryptographic Schemes*
8. *Monitoring the System Activity: auditing*

Network Security Basics

Security Mechanisms

1. *Prevention Mechanisms: efforts for avoiding attacks*
2. *Detection Mechanism: efforts for detecting attacks*
3. *Recovery Mechanism: efforts for reconstructing a subverted system*
4. *User Awareness: informing users about the risks in the ways that they use resources*
5. *Physical Protection of H/W Devices*
6. *Usages of Access Control Softwares: through Need-to-Know Principal*
7. *Usages of Cryptographic Schemes*
8. *Monitoring the System Activity: auditing*

Network Security Basics

Security Mechanisms

1. *Prevention Mechanisms: efforts for avoiding attacks*
2. *Detection Mechanism: efforts for detecting attacks*
3. *Recovery Mechanism: efforts for reconstructing a subverted system*
4. *User Awareness: informing users about the risks in the ways that they use resources*
5. *Physical Protection of H/W Devices*
6. *Usages of Access Control Softwares: through Need-to-Know Principal*
7. *Usages of Cryptographic Schemes*
8. *Monitoring the System Activity: auditing*

Network Security Basics

Security Mechanisms

1. *Prevention Mechanisms: efforts for avoiding attacks*
2. *Detection Mechanism: efforts for detecting attacks*
3. *Recovery Mechanism: efforts for reconstructing a subverted system*
4. *User Awareness: informing users about the risks in the ways that they use resources*
5. *Physical Protection of H/W Devices*
6. *Usages of Access Control Softwares: through Need-to-Know Principal*
7. *Usages of Cryptographic Schemes*
8. *Monitoring the System Activity: auditing*

Network Security Basics

Security Mechanisms

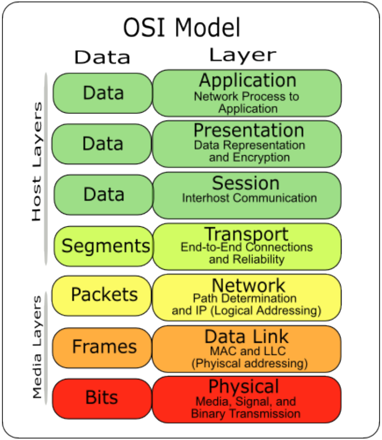
1. *Prevention Mechanisms: efforts for avoiding attacks*
2. *Detection Mechanism: efforts for detecting attacks*
3. *Recovery Mechanism: efforts for reconstructing a subverted system*
4. *User Awareness: informing users about the risks in the ways that they use resources*
5. *Physical Protection of H/W Devices*
6. *Usages of Access Control Softwares: through Need-to-Know Principal*
7. *Usages of Cryptographic Schemes*
8. *Monitoring the System Activity: auditing*

Network Security Basics

Security Mechanisms

1. *Prevention Mechanisms: efforts for avoiding attacks*
2. *Detection Mechanism: efforts for detecting attacks*
3. *Recovery Mechanism: efforts for reconstructing a subverted system*
4. *User Awareness: informing users about the risks in the ways that they use resources*
5. *Physical Protection of H/W Devices*
6. *Usages of Access Control Softwares: through Need-to-Know Principal*
7. *Usages of Cryptographic Schemes*
8. *Monitoring the System Activity: auditing*

Network Security: Approaches



OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Figure: The OSI Layer

The General Approach

1. *Detection of the vulnerabilities of each OSI/ISO layer:*
   - *from which part of a layer; an attack could be performed*
2. *Securing each layer:*
   - *using current state of art in order to close the security gaps.*

Network Security: Approaches

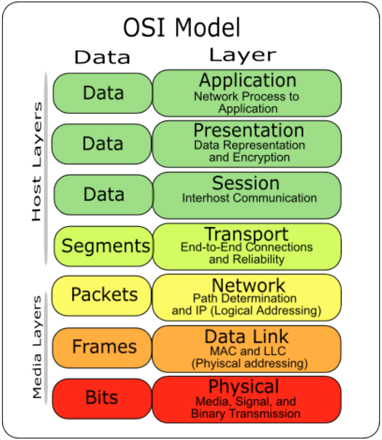

OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Figure: The OSI Layer

The General Approach

1. *Detection of the vulnerabilities of each OSI/ISO layer:*
   - *from which part of a layer; an attack could be performed*
2. *Securing each layer:*
   - *using current state of art in order to close the security gaps.*

Vulnerabilities of Physical Layer: Transmission Media Security

Physical Layer: In The Sense of Security

- *Vulnerability: due to communications are being established and hardly performed at this layer; it is possible to eavesdrop on the communication by sniffing the actual medium (tapping).*
- *Attack Types: depends on the used media in communication.*
    - *wired communication environments*
    - *wireless communication environments*

Vulnerabilities of Physical Layer: Transmission Media Security

Physical Layer: In The Sense of Security

- *Vulnerability: due to communications are being established and hardly performed at this layer; it is possible to eavesdrop on the communication by sniffing the actual medium (tapping).*
- *Attack Types: depends on the used media in communication.*
  - *wired communication environments*
  - *wireless communication environments*

Transmission Media Security: Wired Communication Environments

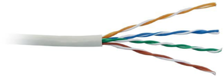


Figure: A Twisted Pair

Figure: A Coaxial Cable

Tapping into the media: Twisted Pair/Coaxial Cable

- *the most vulnerable cable types*
- *relatively easy to hack (minimal equipments and knowledge)*
- *problematic case: they can be tapped into at any point along the cable without being detected*
- *twisted pairs emit electromagnetic energy that can be picked up with sensitive equipment even without physically tapping into the media*

Transmission Media Security: Wired Communication Environments

Figure: A Fiber Optic Cable

Tapping into the media: Fiber Optic Cable

- *the least vulnerable cable: no electromagnetic waves are generated; data is transmitted as beams of light*
- *relatively hard to hack (tap) but still holds the risk*
- *positive situation (user's case): hiding the tap is too hard; if tapping case happens with breaking the strand, then connection immediately shuts down.*

Transmission Media Security: Wireless Communication Environments

Tapping into the media: Wireless Communication

- *Easy to eavesdrop with special equipments,*
- *More detailedly: Next Session on Wireless Network Basics and Security!*

Method(s) of Prevention: Physical Layer

1. **Proper Monitoring!!!**
2. **Encrypted Data!!!**

Transmission Media Security: Wireless Communication Environments

Tapping into the media: Wireless Communication

- *Easy to eavesdrop with special equipments,*
- *More detailedly: Next Session on Wireless Network Basics and Security!*

Method(s) of Prevention: Physical Layer

1. **Proper Monitoring!!!**
2. **Encrypted Data!!!**

Transmission Media Security: Wireless Communication Environments

Tapping into the media: Wireless Communication

- *Easy to eavesdrop with special equipments,*
- *More detailedly: Next Session on Wireless Network Basics and Security!*

Method(s) of Prevention: Physical Layer

1. **Proper Monitoring!!!**
2. **Encrypted Data!!!**

Transmission Media Security: Wireless Communication Environments

Tapping into the media: Wireless Communication

- *Easy to eavesdrop with special equipments,*
- *More detailedly: Next Session on Wireless Network Basics and Security!*

Method(s) of Prevention: Physical Layer

1. **Proper Monitoring!!!**
2. **Encrypted Data!!!**

Transmission Media Security: Wireless Communication Environments

Tapping into the media: Wireless Communication

- *Easy to eavesdrop with special equipments,*
- *More detailedly: Next Session on Wireless Network Basics and Security!*

Method(s) of Prevention: Physical Layer

1. **Proper Monitoring!!!**
2. **Encrypted Data!!!**

Vulnerabilities of Data Link Layer

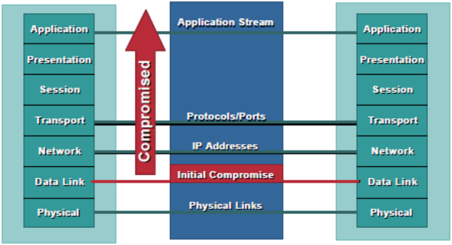


Figure: The OSI Layer: Domino Effect

Data Link Layer: In The Sense of Security

- *OSI was built to allow different layers to work without knowledge of each other. That means that if a layer two is compromised; the other layers will not be aware which is called "Domino effect".*
- *Attack Types:*
  - *ARP Based Attacks*
  - *MAC Address Based Attacks*

Vulnerabilities of Data Link Layer

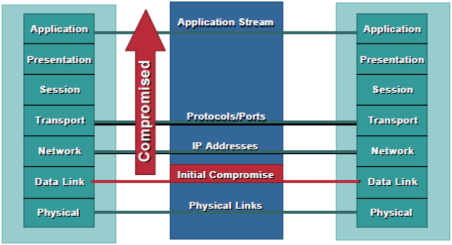
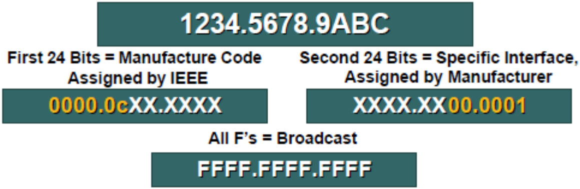


Figure: The OSI Layer: Domino Effect

Data Link Layer: In The Sense of Security

- *OSI was built to allow different layers to work without knowledge of each other. That means that if a layer two is compromised; the other layers will not be aware which is called "Domino effect".*
- *Attack Types:*
  - *ARP Based Attacks*
  - *MAC Address Based Attacks*

Vulnerabilities of Data Link Layer: MAC Attacks



1234.5678.9ABC

First 24 Bits = Manufacture Code Assigned by IEEE

0000.0cXX.XXXX

Second 24 Bits = Specific Interface, Assigned by Manufacturer

XXXX.XX00.0001

All F's = Broadcast

FFFF.FFFF.FFFF

Figure: MAC Address

Definition: MAC Address

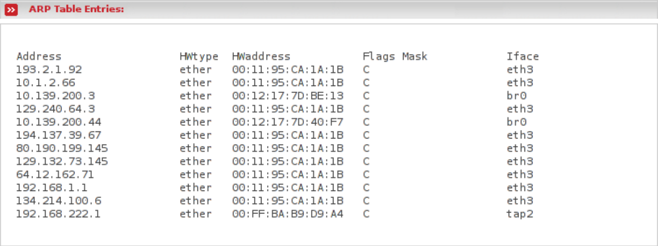
A *Media Access Control address (MAC)* *is a* **48-bit unique identifier** *assigned to network interfaces for communications on the physical network segment.*

Vulnerabilities of Data Link Layer: ARP Attacks

Definition: ARP

The Address Resolution Protocol (ARP) is a widely used protocol for resolving network layer addresses into link layer addresses by using ARP tables.

Conversion of IP addresses to MAC (physical) addresses or vice versa.



ARP Table Entries:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
193.2.1.92               ether   00:11:95:CA:1A:1B   C                     eth3
10.1.2.66                ether   00:11:95:CA:1A:1B   C                     eth3
10.139.200.3             ether   00:12:17:7D:BE:13   C                     br0
129.240.64.3             ether   00:11:95:CA:1A:1B   C                     eth3
10.139.200.44            ether   00:12:17:7D:40:F7   C                     br0
194.137.39.67            ether   00:11:95:CA:1A:1B   C                     eth3
80.190.199.145           ether   00:11:95:CA:1A:1B   C                     eth3
129.132.73.145           ether   00:11:95:CA:1A:1B   C                     eth3
64.12.162.71             ether   00:11:95:CA:1A:1B   C                     eth3
192.168.1.1              ether   00:11:95:CA:1A:1B   C                     eth3
134.214.100.6            ether   00:11:95:CA:1A:1B   C                     eth3
192.168.222.1            ether   00:FF:BA:B9:D9:A4   C                     tap2
```

Figure: An ARP Table

Vulnerabilities of Data Link Layer: ARP Attacks

How ARP Works?

1. *An ARP Request: Computer A asks the network, "Who has this IP address?"*
2. *An ARP Reply: Computer B tells Computer A, "I have that IP. My MAC address is [whatever it is]."*
3. *A Reverse ARP Request (RARP): Same concept as ARP Request, but Computer A asks, "Who has this MAC address?"*
4. *A RARP Reply: Computer B tells Computer A, "I have that MAC. My IP address is [whatever it is]"*

```
arp -a
```

```
sudo arpspoof -i wlan0 -t 192.168.2.1 192.168.40.1
```

Vulnerabilities of Data Link Layer: ARP Attacks

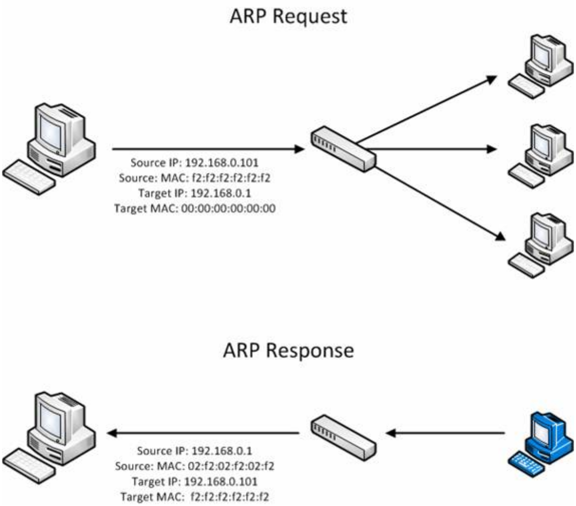

ARP Request
Source IP: 192.168.0.101
Source: MAC: f2:f2:f2:f2:f2:f2
Target IP: 192.168.0.1
Target MAC: 00:00:00:00:00:00
ARP Response
Source IP: 192.168.0.1
Source: MAC: 02:f2:02:f2:02:f2
Target IP: 192.168.0.101
Target MAC: f2:f2:f2:f2:f2:f2

Figure: ARP Request & Response

Vulnerabilities of Data Link Layer: ARP Attacks

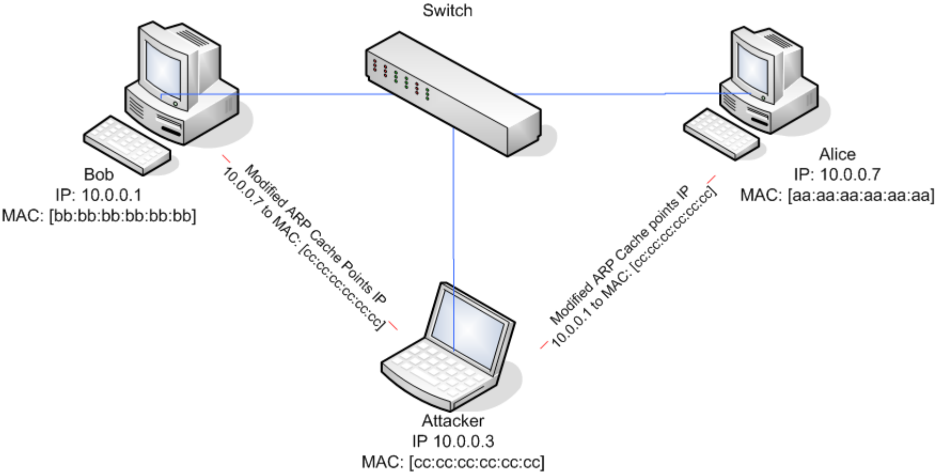


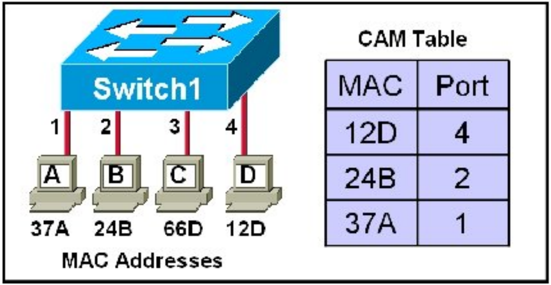
Figure: ARP Poisoning

Vulnerabilities of Data Link Layer: Risk Mitigation in ARP Attacks

Method(s) of Prevention: ARP Attacks

- *Use static ARP Caches*
- *Detect ARP Changes (ARPWATCH)*

Vulnerabilities of Data Link Layer: MAC Attacks



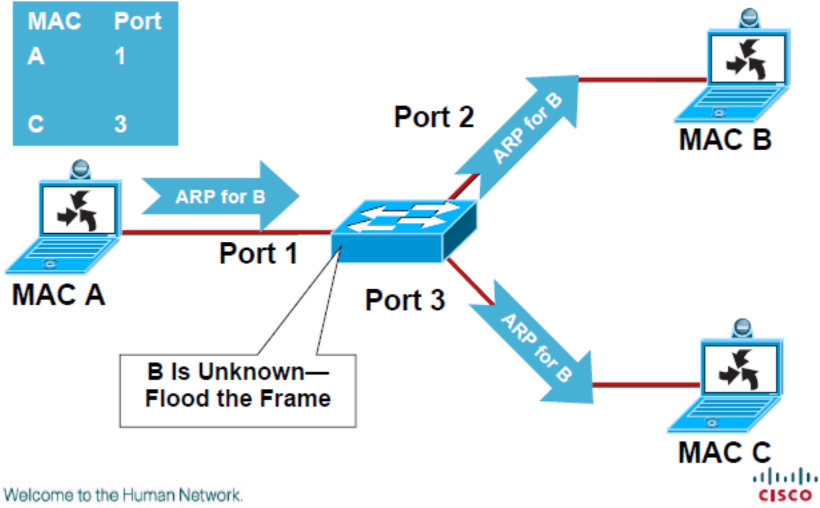
MAC	Port
12D	4
24B	2
37A	1

Figure: A CAM Table

Definition: CAM Table

A CAM (content-addressable memory) is a table in an Ethernet switch which involves Media Access Control (MAC) addresses of stations and the ports on which they connect to that switch.

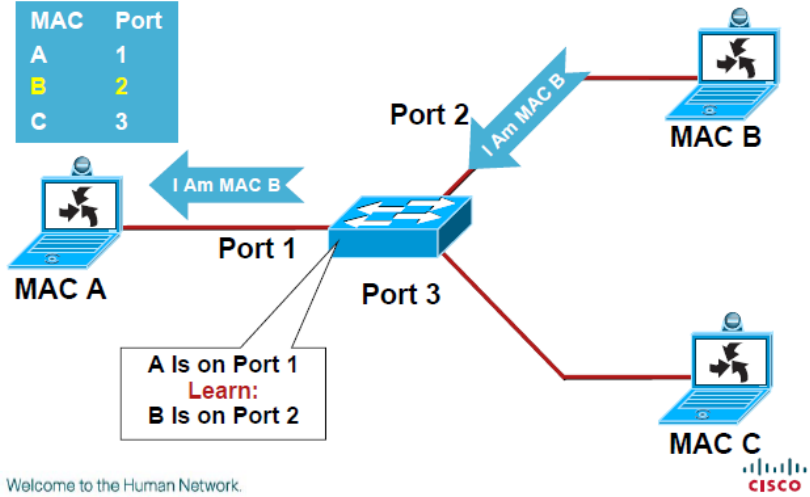
Vulnerabilities of Data Link Layer: MAC Attacks



MAC	Port
A	1
C	3

Figure: CAM Behavior

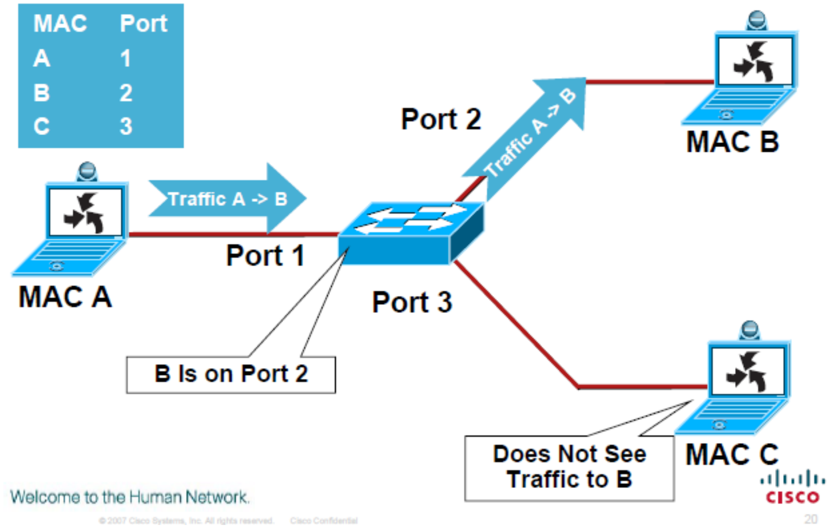
Vulnerabilities of Data Link Layer: MAC Attacks



MAC	Port
A	1
B	2
C	3

Figure: CAM Behavior

Vulnerabilities of Data Link Layer: MAC Attacks

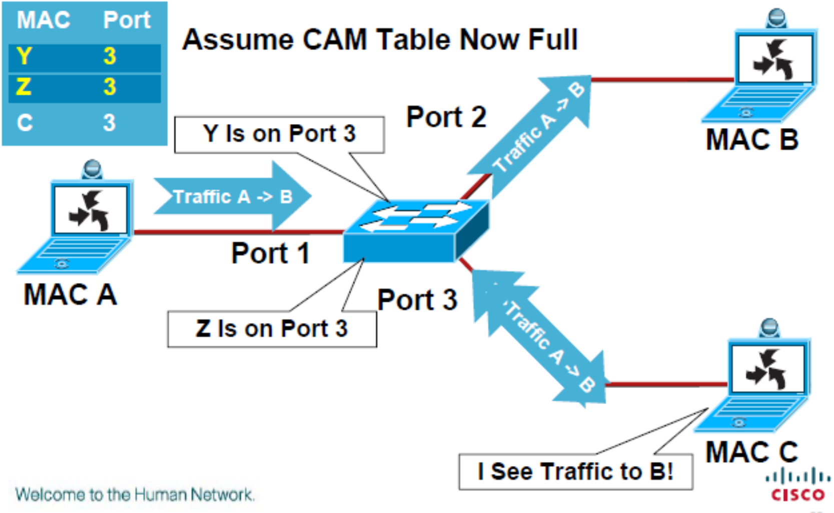


MAC	Port
A	1
B	2
C	3

Traffic A -> B
Port 1
MAC A
Port 2
Traffic A -> B
MAC B
Port 3
B Is on Port 2
Does Not See Traffic to B
MAC C
Welcome to the Human Network.
© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential
cisco
20

Figure: CAM Behavior

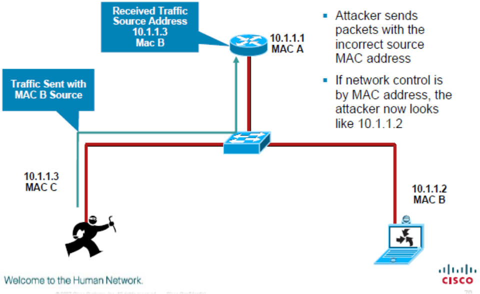
Vulnerabilities of Data Link Layer: MAC Attacks



MAC	Port
Y	3
Z	3
C	3

Figure: CAM Overflow

Vulnerabilities of Data Link Layer: MAC Attacks


Received Traffic Source Address 10.1.1.3 Mac B
10.1.1.1 MAC A
Traffic Sent with MAC B Source
10.1.1.3 MAC C
10.1.1.2 MAC B
Welcome to the Human Network.
cisco

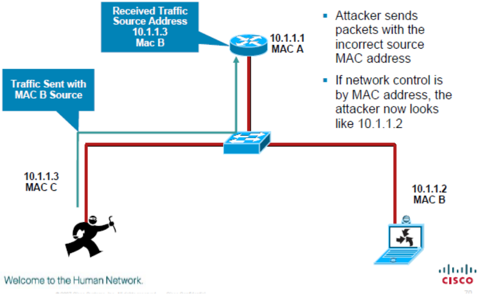
- Attacker sends packets with the incorrect source MAC address
- If network control is by MAC address, the attacker now looks like 10.1.1.2

MAC Attacks: MAC Address Spoofing

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network device to bypass access control lists on servers or routers for gaining unauthorized access.

Configuring Port Security Settings: Only 1 MAC address allowed on each Port!!!

Vulnerabilities of Data Link Layer: MAC Attacks



- Attacker sends packets with the incorrect source MAC address
- If network control is by MAC address, the attacker now looks like 10.1.1.2

Welcome to the Human Network.

MAC Attacks: MAC Address Spoofing

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network device to bypass access control lists on servers or routers for gaining unauthorized access.

Configuring Port Security Settings: Only 1 MAC address allowed on each Port!!!

Vulnerabilities of Network Layer

Network Layer: In The Sense of Security

Vulnerabilities:

- *False source addressing on malicious packets!!!*

Attack Types:

- *IP Address Spoofing: False source addressing on malicious packets!!!*

Vulnerabilities of Network Layer: IP Based Attacks

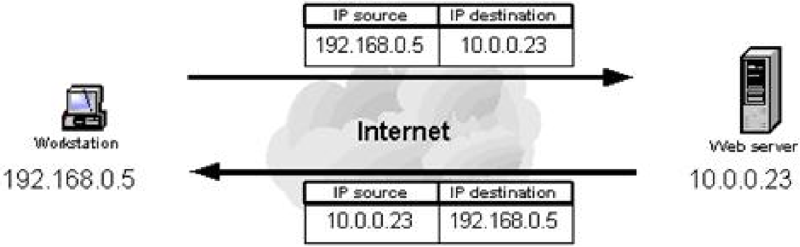


Figure: Valid Connection

Vulnerabilities of Network Layer: IP Based Attacks

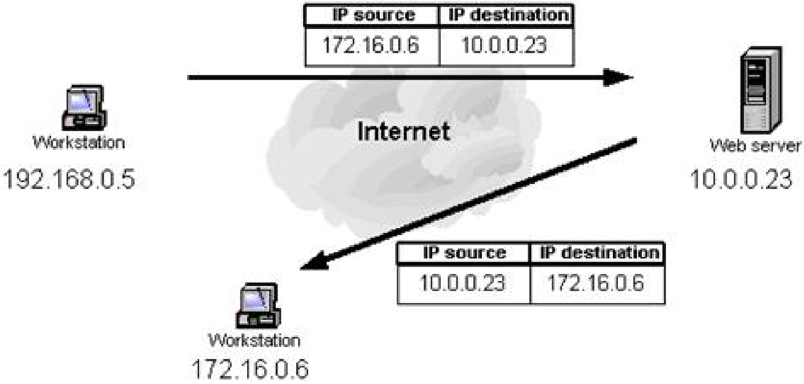


Figure: IP Spoofed Connection

Vulnerabilities of Network Layer: Risk Mitigation

Method(s) of Prevention: Network Layer

- *Route policy controls - Use strict anti-spoofing and route filters at network edges*
- *Firewalls with strong filter & anti-spoof policy*

Vulnerabilities of Transport Layer

Transport Layer: In The Sense of Security

Vulnerabilities:

- *End-to-end communication could be interrupted.*

Attack Types:

- *DoS Attacks: SYN Flood Attacks*
- *Port Scan Attacks*

Vulnerabilities of Transport Layer

Transport Layer: In The Sense of Security

Vulnerabilities:

- *End-to-end communication could be interrupted.*

Attack Types:

- *DoS Attacks: SYN Flood Attacks*
- *Port Scan Attacks*

Vulnerabilities of Transport Layer: Scan Attacks

Port Scan Attacks

A port scan is an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.

nmap

Vulnerabilities of Transport Layer: Scan Attacks

Port Scan Attacks

A port scan is an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.

nmap

Vulnerabilities of Transport Layer: DoS Attacks

Dos Attacks: SYN Flooding

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

hping3

Vulnerabilities of Transport Layer: DoS Attacks

Dos Attacks: SYN Flooding

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

hping3

Vulnerabilities of Transport Layer: Risk Mitigation

Method(s) of Prevention: Transport Layer

- *use syn cookies against syn flooding attack.*
- *Strict firewall rules limiting access to specific transmission protocols and sub-protocol information such as TCP/UDP port number or ICMP type*

Vulnerabilities of Session & Presentation Layers

Session & Presentation Layers: In The Sense of Security

Vulnerabilities:

- *It is virtually impossible to attack these layers.*
- *These layers just handle things like token management, synchronization and encoding translations.*

Vulnerabilities of Application Layer

Application Layer: In The Sense of Security

Vulnerabilities:

- *Back-doors and application design flaws bypass standard security controls malicious Codes: Viruses, Trojans, Worms...*
- *DNS Based Attacks*

What is DNS?

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

searchnetworking.techtarget.com/definition/domain-name-system

Vulnerabilities of Application Layer

Application Layer: In The Sense of Security

Vulnerabilities:

- *Back-doors and application design flaws bypass standard security controls malicious Codes: Viruses, Trojans, Worms...*
- *DNS Based Attacks*

What is DNS?

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

searchnetworking.techtarget.com/definition/domain-name-system

Vulnerabilities of Application Layer: DNS Spoofing

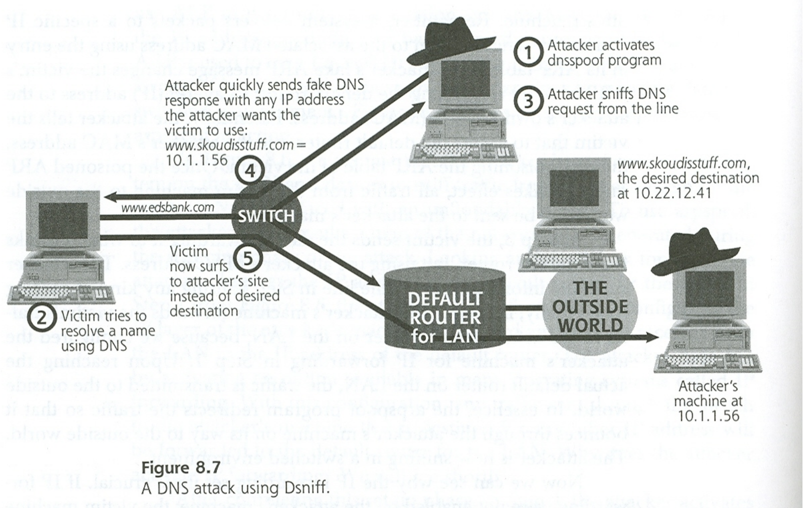
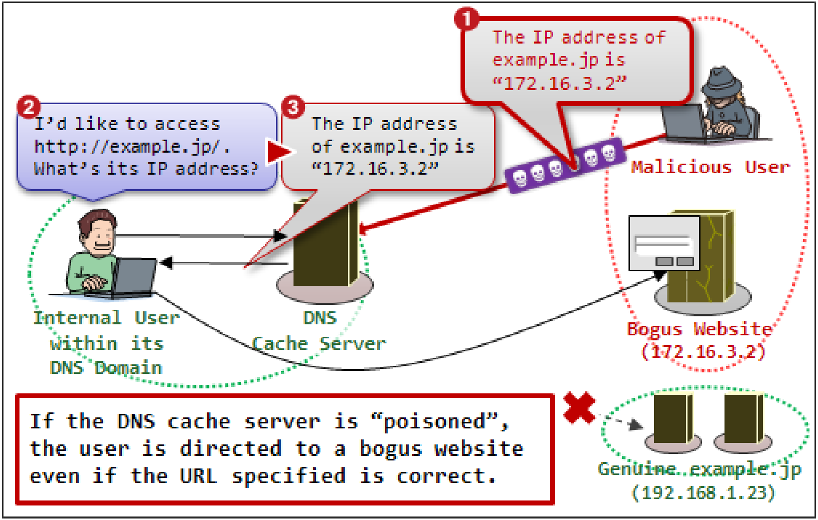

1 Attacker activates dnsspoof program
3 Attacker sniffs DNS request from the line
Attacker quickly sends fake DNS response with any IP address the attacker wants the victim to use: www.skoudisstuff.com = 10.1.1.56
4
www.skoudisstuff.com, the desired destination at 10.22.12.41
www.edsbank.com
SWITCH
Victim now surfs to attacker's site instead of desired destination
5
2 Victim tries to resolve a name using DNS
DEFAULT ROUTER for LAN
THE OUTSIDE WORLD
Attacker's machine at 10.1.1.56

Figure 8.7
A DNS attack using Dsniff.

Figure: DNS Spoofing

Vulnerabilities of Application Layer: DNS Poisoning


1
The IP address of example.jp is "172.16.3.2"
2
I'd like to access http://example.jp/. What's its IP address?
3
The IP address of example.jp is "172.16.3.2"
Malicious User
Internal User within its DNS Domain
DNS Cache Server
Bogus Website (172.16.3.2)
Genuine example.jp (192.168.1.23)

If the DNS cache server is "poisoned", the user is directed to a bogus website even if the URL specified is correct.

Figure: DNS Cache Poisoning

Vulnerabilities of Application Layer: Risk Mitigation

Method(s) of Prevention: Application Layer

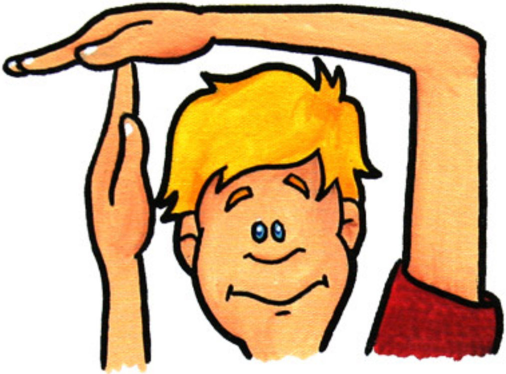
- *Application Level Access Control*
- *Standards, testing, review of application code and functionality*
- *Intrusion Detection Systems to monitor application inquiries and activity*
- *Host based firewalls*
- *Anti-virus software*
- *For DNS Spoofing and Poisoning Specific:*
  - *hard to detect: since they are passive attacks.*
  - *type IP addresses directly.*

Summary

Summarization

1. *Basics of Computer Networking*
2. *Introduction of ISO/OSI Model: Layer by Layer*
3. *Network Security: Basics and Goals involved*
4. *Defining a Security Mechanism*
5. *Vulnerabilities of each layer in ISO/OSI Model*
6. *Possible Attack Scenarios*

Let's Have a Break!!!



Bibliography

[UZUNAY2005]
Yusuf UZUNAY, Middle East Technical University, Turkey.
Layer-to-Layer Network Security.

[Reed2003]
Damon Reed - SANS Institute InfoSec Reading Room.
Applying the OSI Seven Layer Network Model To Information Security.

[Esparza2004]
Charles R. Esparza - SANS Institute InfoSec Reading Room.
Transmission Media Security.

[Khan1999]
Ameel Zia Khan.
Computer Network Security Basics - LUMS-ACM Chapter Topic Presentation.