Securing TCP/IP

Chapter 6

Lecturer: Pei-yih Ting

Overview

- TCP/IP
- Open Systems Interconnection Model
- Anatomy of a Packet
- Internet Protocol Security (IPSec)
- Web Security (HTTP over TLS, Secure-HTTP)

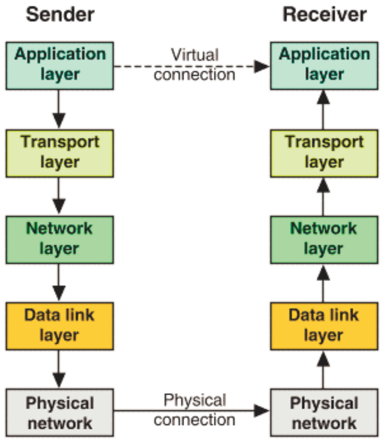
Introduction to TCP/IP

- Transmission Control Protocol / Internet Protocol
- TCP/IP comprises a suite of four protocols
- These protocols completely describe how devices communicate on TCP/IP networks – the Internet

- The TCP/IP design is consistent with the Open Systems Interconnection (OSI) reference model

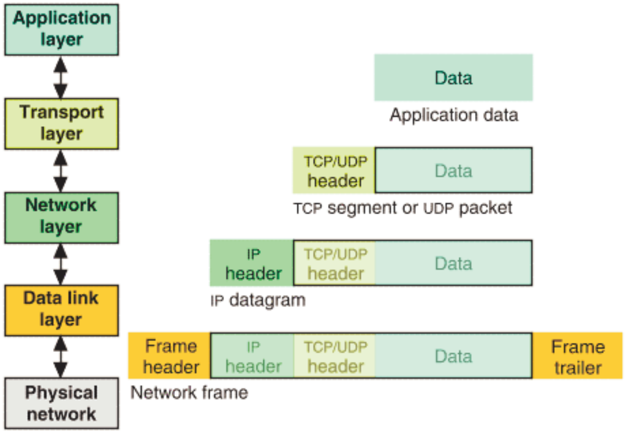
Introduction to TCP/IP (cont'd)

- Layered protocol stack: hierarchical cooperation



Introduction to TCP/IP (cont'd)

- Data encapsulation


Application layer
Transport layer
Network layer
Data link layer
Physical network

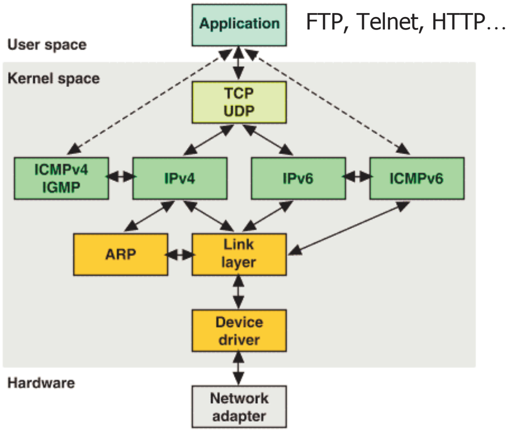
Data
Application data

TCP/UDP header | Data
TCP segment or UDP packet

IP header | TCP/UDP header | Data
IP datagram

Frame header | IP header | TCP/UDP header | Data | Frame trailer
Network frame

TCP/IP Suite


Application
FTP, Telnet, HTTP…
User space
Kernel space
TCP UDP
ICMPv4 IGMP
IPv4
IPv6
ICMPv6
ARP
Link layer
Device driver
Hardware
Network adapter

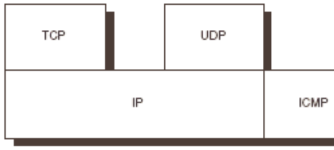


Figure 6.4 Relationships among protocols in the TCP/IP suite

Internet Protocol (IP)

- The Internet Protocol provides routing functions for datagrams traversing the network
- Each datagram has source and destination addresses (IP address, logical)
- IP determines if the datagram has reached its destination or if it must be forwarded
  - If it must be forwarded, IP determines the next hop
- IP does NOT provide a reliability guarantee
  - No assurance that a packet will reach its specified destination
  - Best effort attempt

Internet Protocol (cont'd)

- IP is also responsible for fragmentation of datagrams
- A datagram cannot exceed the maximum size for the network it is traveling on
  - This is not known at creation time by the sender
- Datagrams that are too large must be broken into fragments
- Each fragment must contain the information required to reassemble the original datagram
  - Labeled with a length and an offset
  - Together with the identification field in the header

Datagram Fragmentation

Figure 6.1
Original datagram

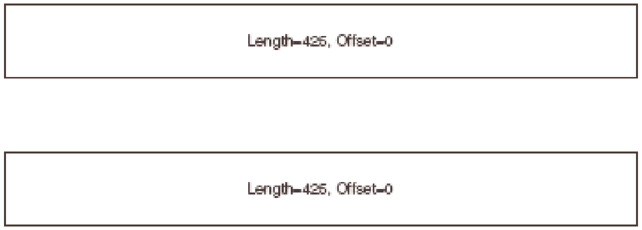
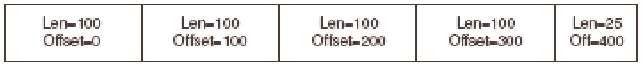


Figure 6.2
Fragmented datagram



Transmission Control Protocol (TCP)

- Has 3 important features
  - TCP is a reliable protocol (guarantees delivery of packets from source to destination by acknowledgement and retransmission)
  - TCP provides error-checking (using a checksum)
  - TCP is connection-oriented (provides session establishment and teardown handshaking protocols to create dedicated process-to-process communication, has sequence controls)
- After a TCP packet is constructed, it is transformed into an IP datagram by adding information to the headers (*encapsulation*)

TCP Handshaking Protocol

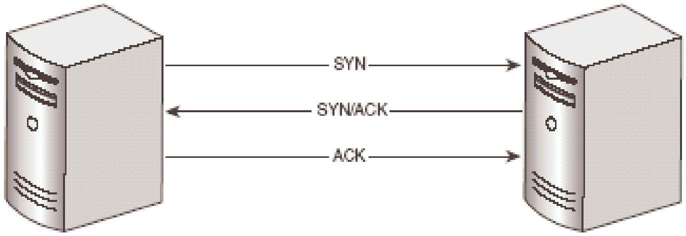


Figure 6.3 Three-way TCP handshake session establishment

User Datagram Protocol (UDP)

- Like TCP, UDP is a transport layer protocol
- Unlike TCP, UDP is connectionless and does not provide a reliability guarantee
- Used to deliver a packet from one process to another with very low overhead (efficiency)
  - Does not use handshaking to establish connections
  - Does not keep track of sequencing and acknowledge information
- Often used for application like streaming media that do not depend on guaranteed delivery of every packet

Internet Control Message Protocol (ICMP)

- Responsible for transmitting control messages between networked hosts
- Types of control messages include
  - Network/host/port unreachable
  - Packet time to live expired
  - Source quench (overloaded gateway, pause traffic)
  - Redirect messages (used to reroute traffic)
  - Echo request and echo reply messages (ping)
- Include basic portions of IP header to use the same routing infrastructure as IP

Open Systems Interconnection Reference Model (OSI)

- Developed in the late 1970s to describe basic functionality of networked data communications

- Uses encapsulation to sequentially process data through the layers until it is ready for transmission
  - Each layer performs some transformation of data such as adding a header or converting data into another form
  - At the sender, data is transformed from application to physical layer
  - At the recipient, data is transformed from physical to application layer

OSI Model (cont'd)

- Has seven layers

	層次名稱	主要功能
7	應用層 (Application Layer)	應用系統間的溝通
6	表示層 (Presentation Layer)	資料的表示、編碼與格式化
5	會議層 (Session Layer)	會議溝通的建立與管理
4	傳輸層 (Transport Layer)	可靠的端對端的訊息傳送
3	網路層 (Network Layer)	網路相連與訊息流通的控制
2	鏈結層 (Data Link Layer)	網路流量控制與資料偵錯
1	實體層 (Physical Layer)	訊號傳送的實體媒介

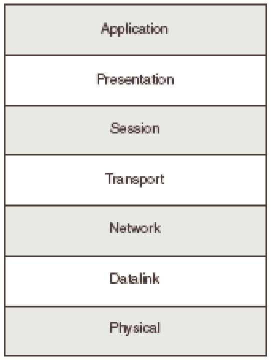
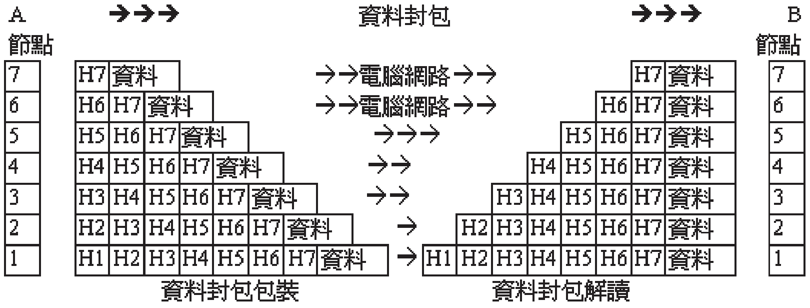


Figure 6.5
OSI model

OSI Model (cont'd)

- Encapsulation



A →→→ 資料封包 →→→ B

節點 節點

7 | H7 | 資料 →→電腦網路→→ H7 | 資料 | 7

6 | H6 | H7 | 資料 →→電腦網路→→ H6 | H7 | 資料 | 6

5 | H5 | H6 | H7 | 資料 →→→ H5 | H6 | H7 | 資料 | 5

4 | H4 | H5 | H6 | H7 | 資料 →→ H4 | H5 | H6 | H7 | 資料 | 4

3 | H3 | H4 | H5 | H6 | H7 | 資料 →→ H3 | H4 | H5 | H6 | H7 | 資料 | 3

2 | H2 | H3 | H4 | H5 | H6 | H7 | 資料 → H2 | H3 | H4 | H5 | H6 | H7 | 資料 | 2

1 | H1 | H2 | H3 | H4 | H5 | H6 | H7 | 資料 → H1 | H2 | H3 | H4 | H5 | H6 | H7 | 資料 | 1

資料封包包裝 資料封包解讀

OSI Layers

- Application layer is the highest layer of OSI model
  - Contains software that interacts directly with computer users
    - Web browsers, e-mail, office productivity suites, etc.
  - Majority of security vulnerabilities occur at this layer
    - Malicious code objects such as viruses, worms, and Trojan horses
- Presentation layer
  - Responsible for converting data into formats for exchange between higher and lower layers
  - Responsible for allowing data in Application layer to be shared among applications
  - Responsible for encryption and decryption of data

OSI Layers (cont'd)

- Session layer
  - Responsible for network connections between processes
  - A security vulnerability at this layer is session hijacking
    - Hijacker takes over a session after authentication has taken place
- Transport layer
  - Responsible for data flow between two systems
    - Error recovery functionality, flow control mechanism
  - Common transport protocols are TCP and UDP
  - Many security vulnerabilities at this level
    - SYN Flood attack
      - Attacks TCP's three-way handshaking process
    - Buffer overflow attacks

OSI Layers (cont'd)

- Network Layer
  - Ex. Internet Protocol
  - Responsible for ensuring that datagrams are routed across the network
  - Responsible for addressing and fragmentation of datagrams
  - Fragmentation attacks were common at this layer, modern operating systems are less vulnerable
    - Two fragments overlap
    - Two adjacent fragments do not meet

Network Layer Fragment Attacks

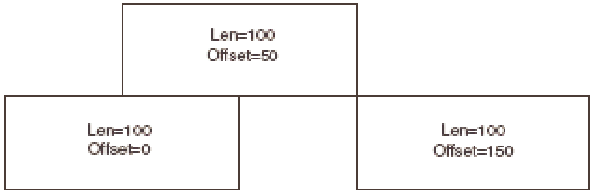


Figure 6.7

Overlapping fragment attack

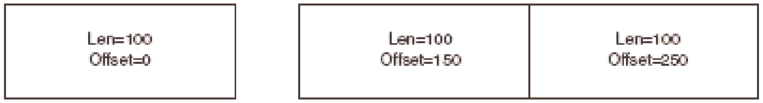


Figure 6.8

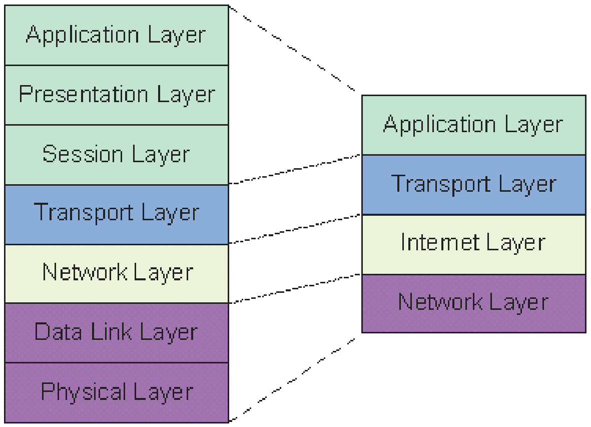
Nonadjacent fragment attack

OSI Layers (cont'd)

- Data Link Layer
  - Conversion between datagrams and binary
  - Two sublayers
  - Logical Link Control (LLC) sublayer
    - Error correction, flow control, frame synchronization
  - MAC sublayer
    - 48-bit physical addressing scheme for network devices
- Physical layer

  Ex. 00:00:0C:45:12:A6
  - Converts binary data to network impulses
    - Type of impulse depends on media, electrical, or optic
  - Physical threats include the use of packet sniffers to monitor traffic

OSI vs TCP/IP Layers

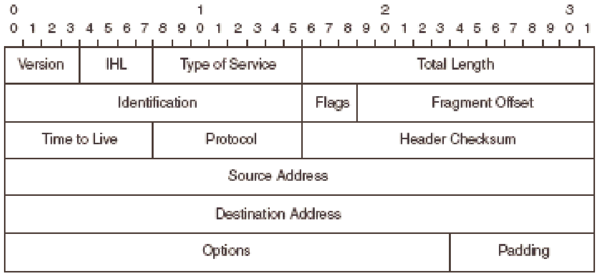


Packet Anatomy

- Packets have two main components
  - Packet header
  - Packet payload
- Packet sniffers are hardware or software that passively monitor traffic on a network
  - can be used maliciously to view unauthorized information
  - are also used by system administrators to understand and analyze traffic flow and possible attacks
- To use a packet sniffer, you must understand the components and structure of a packet

Packet Anatomy (cont'd)

- Packet headers are built sequentially with each layer potentially adding information (Encapsulation)
- IP headers include
  - Total length and offset fields for fragmentation
  - Source Address and Destination Address (IP addresses)

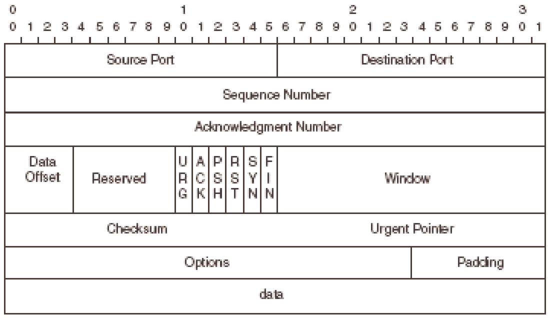


<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="6">Source Address</td></tr>
<tr><td colspan="6">Destination Address</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

Figure 6.9
IP header (source: RFC 791)

Packet Anatomy (cont'd)

- TCP headers include
  - Source Port and Destination Port
  - SYN, ACK, RST, FIN flags
  - checksum



Source Port							Destination Port	
Sequence Number								
Acknowledgment Number								
Data Offset	Reserved	U R G	A C K	P S H	R S T	S Y N	F I N	Window
Checksum							Urgent Pointer	
Options								Padding
data								

Figure 6.10
TCP header (source: RFC 793)

Packet Anatomy (cont'd)

- UDP headers are added when UDP is the transport protocol
  - Only four fields for minimal overhead
  - Fields are Source Port, Destination Port, Length, and Checksum
- Packet payload is the actual data content that is to be transported
  - Anything that can be expressed in binary (images, word documents, etc.)

Internet Protocol Security (IPSec)

- TCP/IP is inherently insecure, designed originally to operate between a small number of trusted machines
- IPSec is a security-enhanced version of IP
  - Security Associations (SAs) contain identification and key materials, ISAKMP is responsible for create and maintain SAs
  - Authentication Headers (AHs) provide integrity and authentication functionality
  - Encapsulating Security Payload (ESP) adds confidentiality guarantees
    - Transport mode used when intermediate network may not support IPSec, headers are not encrypted
    - Tunnel mode allows encryption of all data including headers, often found in gateway-to-gateway traffics

Web Security

- WWW comprises the second largest portion of traffic on the Internet (e-mail is first)
- SSL and HTTP-S are technologies used to add security to Web communications
- Secure Socket Layers (SSL) v.2, v.3
  - Usually used between Web browser clients and servers, known as HTTP over SSL (https)
  - Facilitates exchange of digital certificates
  - Replaced by Transport Layer Security (TLS) v.1
- Secure-HTTP (HTTP-S)
  - A connectionless protocol, found in only a few less common browsers

Summary

- TCP/IP is a suite of four main protocols
  - IP, TCP, UDP, ICMP
- IP provides routing functions and datagram fragmentation
- TCP provides reliability guarantees, establishes two-way communication channels between processes
- UDP is connectionless, it delivers packets between processes efficiently but without reliability guarantees
- ICMP provides for administrative control of packets traversing a network

Summary (cont'd)

- The Open Systems Interconnection (OSI) model is a reference model for networked data communications
- OSI describes 7 layers
  - Application, Presentation, Session, Transport, Network, Data Link, Physical
  - Data is processed sequentially from the user interfaces at the Application layer to the transmission of physical impulses at the Physical layer
  - Each layer has particular security vulnerabilities
  - Each layer transforms data in some way, either by adding information to packet headers or converting data into a new form - encapsulation

Summary (cont'd)

- Packets are the chunks of data that are sent across a network
  - Packet headers contain the information necessary to transmit the packet over the network
  - Packet payload is the actual data content being transmitted
- IPSec is a security-enhanced version of the Internet Protocol
- Web security technologies include
  - Secure Sockets Layer (SSL)
  - Secure-HTTP (HTTP-S)

Assignments

- Reading: Chapter 6
- Practice 6.7 Challenge Questions
- Turn in Challenge Exercise 6.2 next week
- Group Assignment (Exercise 6.1), three weeks from now