CNT4406/5412 Network Security

Introduction

Zhi Wang

Florida State University

Fall 2014

What is Security?

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability

Integrity

- Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity
  - ➠ e.g., data integrity, code integrity

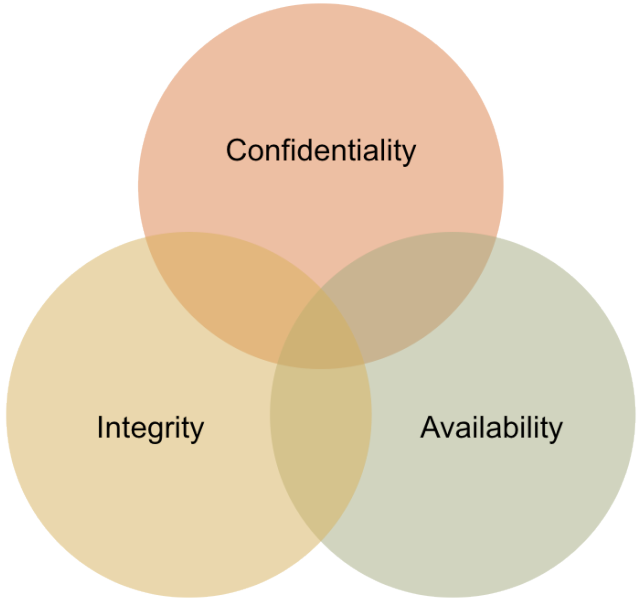
Confidentiality

- Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information
  - ➠ e.g., secrecy, privacy

Availability

- Ensuring timely and reliable access to and use of information

Security and CIA



The HBGary Hacking Saga

VS.

HBGary

DETECT. DIAGNOSE. RESPOND.

Who is Anonymous

- Anonymous is a loosely associated hacktivist group
  - originated on the imageboard 4chan in 2003
  - associated with collaborative hacktivism since 2008
  - responsible for many high-profile attacks:
    DDOS attacks against IFPI, MPAA for file sharing site closure,
    VISA, MasterCard and PayPal to support WikiLeaks
  - named by Time as one of the most influential people in 2012

Who is HBGary

- HBGary is a security company
  - founded by Greg Hoglund (rootkit.com) in 2003
  - it had two firms, HBGary and HBGary Federal
  - HBF was led by Aaron Barr focusing on the U.S federal government

Who is HBGary

- HBGary is a security company
  - founded by Greg Hoglund (rootkit.com) in 2003
  - it had two firms, HBGary and HBGary Federal
  - HBF was led by Aaron Barr focusing on the U.S federal government
- HBGary was sold to ManTech after being hacked

What Happened

- Anonymous poses serious security threats

What Happened

- Anonymous poses serious security threats
- Aaron claimed to have unmasked Anonymous "members" by correlating social media in early 2011
  - ➠ proposed a talk titled "who needs NSA when we have social media?" at the B-Sides conference to sell his idea
  - ➠ intended to sell his list to FBI

What Happened

- Anonymous poses serious security threats
- Aaron claimed to have unmasked Anonymous "members" by correlating social media in early 2011
  - ➠ proposed a talk titled "who needs NSA when we have social media?" at the B-Sides conference to sell his idea
  - ➠ intended to sell his list to FBI
- Anonymous compromised the HBGary in Feb 2011
  - ➠ compromised the websites
  - ➠ posted lots of documents and emails online
  - ➠ usurped Aaron's Twitter

Steps of an Attack

Steps of an Attack

- Reconnoiter to identify vulnerabilities

Steps of an Attack

- Reconnoiter to identify vulnerabilities
  - ➠ software configuration, network topologic, servers...

Steps of an Attack

- Reconnoiter to identify vulnerabilities
  - ➠ software configuration, network topologic, servers...
- Exploit vulnerabilities to take over (own) systems

Steps of an Attack

- Reconnoiter to identify vulnerabilities
  - ➠ software configuration, network topologic, servers...
- Exploit vulnerabilities to take over (own) systems
  - ➠ SQL injection, buffer overflow, format string vulnerability...

Steps of an Attack

- Reconnoiter to identify vulnerabilities
  - ➠ software configuration, network topologic, servers...
- Exploit vulnerabilities to take over (own) systems
  - ➠ SQL injection, buffer overflow, format string vulnerability...
- Harvest information, install malware/backdoors
  - ➠ document, design, email...

Steps of an Attack

- Reconnoiter to identify vulnerabilities
  - ➠ software configuration, network topologic, servers...
- Exploit vulnerabilities to take over (own) systems
  - ➠ SQL injection, buffer overflow, format string vulnerability...
- Harvest information, install malware/backdoors
  - ➠ document, design, email...
- Cover it up: files, logs...

The HBGary Hacking: Reconnaissance

- Hbgaryfederal.com was powered by a third-party CMS with SQL injection vulnerabilities
  - ➠ an example of the SQL inject vulnerability:

    statement = "SELECT * FROM users WHERE name = '" + userName + "';"

    userName = "' or '1'='1' - - '"

    → SELECT * FROM users WHERE name = '' OR '1'='1' - - ';

The HBGary Hacking: Reconnaissance

- Hbgaryfederal.com was powered by a third-party CMS with SQL injection vulnerabilities
  - ➠ an example of the SQL inject vulnerability:

    statement = "SELECT * FROM users WHERE name = '" + userName + "';"

    userName = "' or '1'='1' - - '"

    → SELECT * FROM users WHERE name = '' OR '1'='1' - - ';
  - ➠ The vulnerable URL is:

http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27

The HBGary Hacking: Reconnaissance

- Hbgaryfederal.com was powered by a third-party CMS with SQL injection vulnerabilities
  - ➠ an example of the SQL inject vulnerability:

    statement = "SELECT * FROM users WHERE name = '" + userName + "';"

    userName = "' or '1'='1' - - '"

    → SELECT * FROM users WHERE name = '' OR '1'='1' - - ';
  - ➠ The vulnerable URL is:

    http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27
- User database was retrieved from CMS:
  - ➠ CMS admins' usernames, email addresses, and password hashes

The HBGary Hacking: Password Cracking

- Three properties of an ideal cryptographic hash function:
  - one-way property:
    given h, it's infeasible to find m with $h = H(m)$

The HBGary Hacking: Password Cracking

- Three properties of an ideal cryptographic hash function:
  - one-way property:
    given h, it's infeasible to find m with $h = H(m)$
  - weak collision resistance:
    given m_1, it's infeasible to find m_2 with $H(m_1) = H(m_2)$

The HBGary Hacking: Password Cracking

- Three properties of an ideal cryptographic hash function:
  - one-way property:
    given h, it's infeasible to find m with $h = H(m)$
  - weak collision resistance:
    given m_1, it's infeasible to find m_2 with $H(m_1) = H(m_2)$
  - strong collision resistance:
    it's infeasible to find m_1 and m_2 with $H(m_1) = H(m_2)$

The HBGary Hacking: Password Cracking

- Three properties of an ideal cryptographic hash function:
  - one-way property:
    given h, it's infeasible to find m with $h = H(m)$
  - weak collision resistance:
    given m_1, it's infeasible to find m_2 with $H(m_1) = H(m_2)$
  - strong collision resistance:
    it's infeasible to find m_1 and m_2 with $H(m_1) = H(m_2)$
- Brutal force is the main method to guess passwords

The HBGary Hacking: Password Cracking

- Brute-forcing passwords has never been easier
  - more than 100 million real-world passwords are leaked
  - real-world passwords instead of words in a dictionary
  - patterns in password construction
  - Rainbow tables, pre-computed hashes, are widely available
  - super computing power is cheap and available: cloud, GPGPU

The HBGary Hacking: Password Insecurity

- Weak passwords
  - ➠ CEO and COO of HBF uses weak passwords in a rainbow table

The HBGary Hacking: Password Insecurity

- Weak passwords
  - CEO and COO of HBF uses weak passwords in a rainbow table
- Password reuse
  - average web user has 25 accounts, but uses just 6.5 passwords
  - both CEO and COO reuse the passwords across their accounts
  - Aaron (CEO) is the Google Apps (email) administrator
    $\rightarrow$ access to anyone's email, including Greg Hoglund

The HBGary Hacking: Password Insecurity

- Weak passwords
  - ➠ CEO and COO of HBF uses weak passwords in a rainbow table
- Password reuse
  - ➠ average web user has 25 accounts, but uses just 6.5 passwords
  - ➠ both CEO and COO reuse the passwords across their accounts
  - ➠ Aaron (CEO) is the Google Apps (email) administrator
    $\rightarrow$ access to anyone's email, including Greg Hoglund
- Public key authentication is not used for SSH by Aaron

The HBGary Hacking: Host Insecurity

- Privilege-escalation vulnerabilities
  - ➠ the attacker owned an unprivileged account by a reused password
  - ➠ he then owned the system by exploiting such a vulnerability: GNU dynamic linker expands $ORIGIN in library search path for setuid applications

The HBGary Hacking: Social Engineering

- Authentic information was used to bypass authentication
  - Grey Hoglund is the creator of rootkit.com
  - Grey's email is compromised, which allows to impersonate him
  - His compromised email leaked two pieces of information:
    the hashes of the root password in rootkit.com
    Jussi at Nokia has root access to rootkit.com

The HBGary Hacking: Social Engineering

- Authentic information was used to bypass authentication
  - ➠ Grey Hoglund is the creator of rootkit.com
  - ➠ Grey's email is compromised, which allows to impersonate him
  - ➠ His compromised email leaked two pieces of information:
    the hashes of the root password in rootkit.com
    Jussi at Nokia has root access to rootkit.com
- Jussi was convinced and handed over Grey's account
  - ➠ he authenticated "Grey" by shared secret

The HBGary Hacking: Social Engineering

- Authentic information was used to bypass authentication
  - Grey Hoglund is the creator of rootkit.com
  - Grey's email is compromised, which allows to impersonate him
  - His compromised email leaked two pieces of information:
    the hashes of the root password in rootkit.com
    Jussi at Nokia has root access to rootkit.com
- Jussi was convinced and handed over Grey's account
  - he authenticated "Grey" by shared secret
  - the attack was claimed to be executed by a teenage girl

More Security Incidents

Stuxnet

LinkedIn

YAHOO!

Surveillance State

In This Course

- Explore fundamental issues that cause this insecurity from both network and systems POV

In This Course

- Explore fundamental issues that cause this insecurity from both network and systems POV
- Explain defense mechanisms that mitigate these issues

In This Course

- Explore fundamental issues that cause this insecurity from both network and systems POV
- Explain defense mechanisms that mitigate these issues
- Cover the topics of: cryptography, hashes and message digests, public key cryptography, important standards such as PKI, SSL, SSH, and IPSec, operating system security

You Should Know

- TCP/IP networking
- Operating systems architecture and design
  - e.g., virtual memory, file systems, networking,...
- Discrete mathematics

Course Materials

- Course website: http://www.cs.fsu.edu/~zwang/cnt5412.html
  - ➠ course schedules, assignments, slides,
- Course textbook
  - ➠ Kaufman, C., Perlman, R., and Speciner, M., Network Security: Private Communication in a Public World, 2nd Edition, Prentice Hall 2002
- Office hour: Monday 2:30-4:30pm, or by appointment
  - ➠ come to the office hour for help!

Grading

item	percentage
homework	30%
project	30%
midterm	30%
quizzes	10%

Course Policy

- Academic honor policy: zero-tolerance for cheating
  http://academichonor.fsu.edu
- Ethics: act responsibly in security practices
- Disabilities: contact the instructor for accommodation

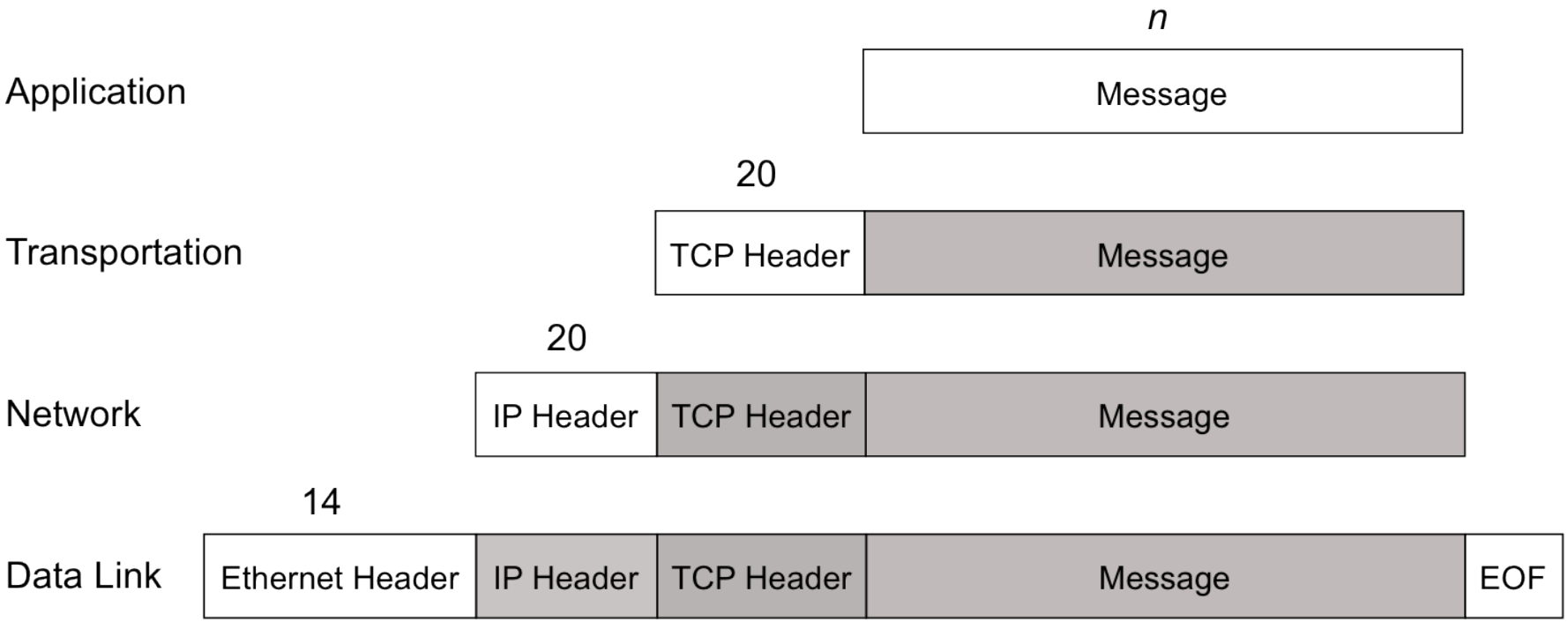
OSI Reference Model

Layer	Name	Who	Example	PDU
7	application	E-E	HTTP	message
6	presentation	E-E	UTF8	
5	session	E-E	Web Conference	
4	transport	E-E	TCP/UDP	segment/datagram
3	network	router	IP	packet
2	data link	bridge, switch	Ethernet	frame
1	physical	repeater	Ethernet	bit stream

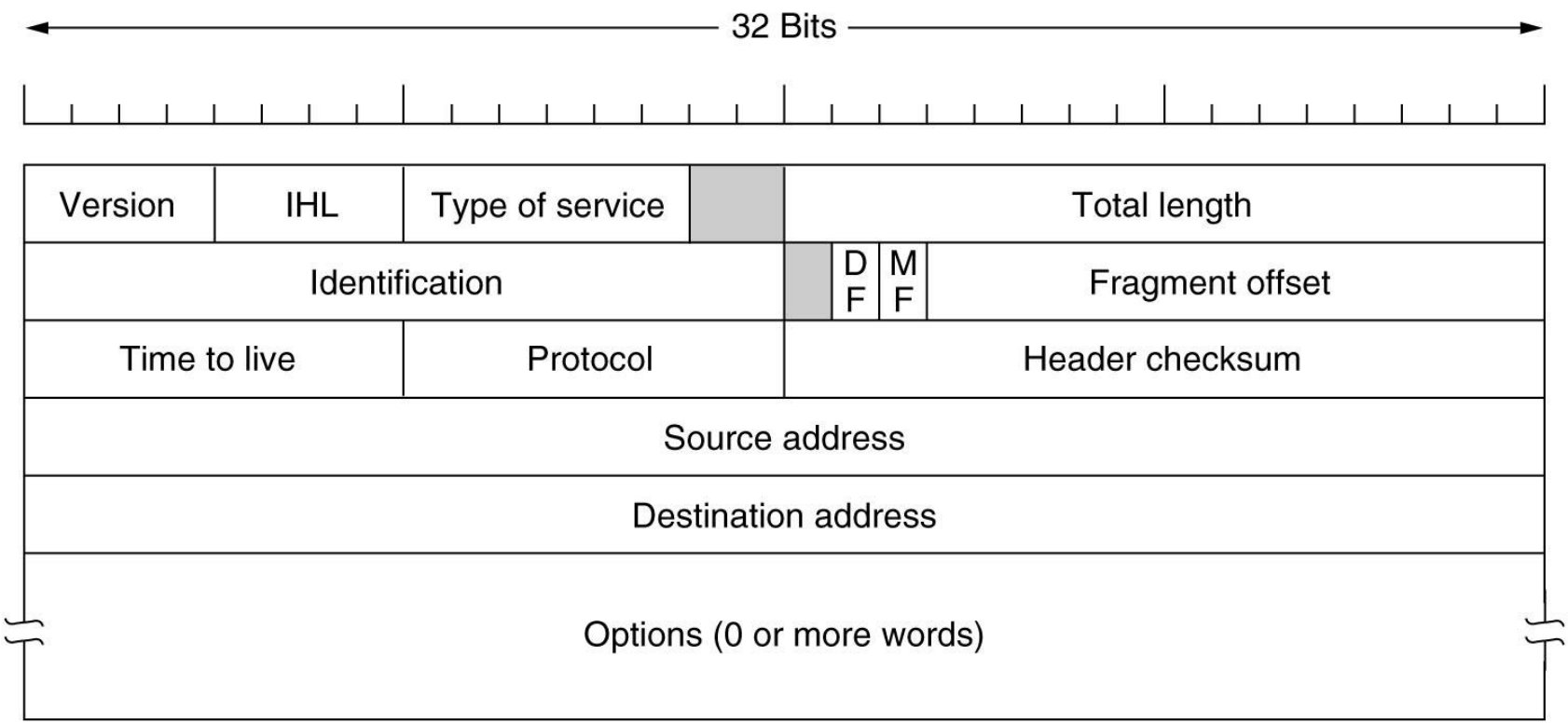
Network Security Layers

Layer	Security
Physical	Blacklisting
Data link	Wireless Ethernet, PPP Authentication
Network	IPSec
Transport	SSL (TLS)
Application	PGP (email)

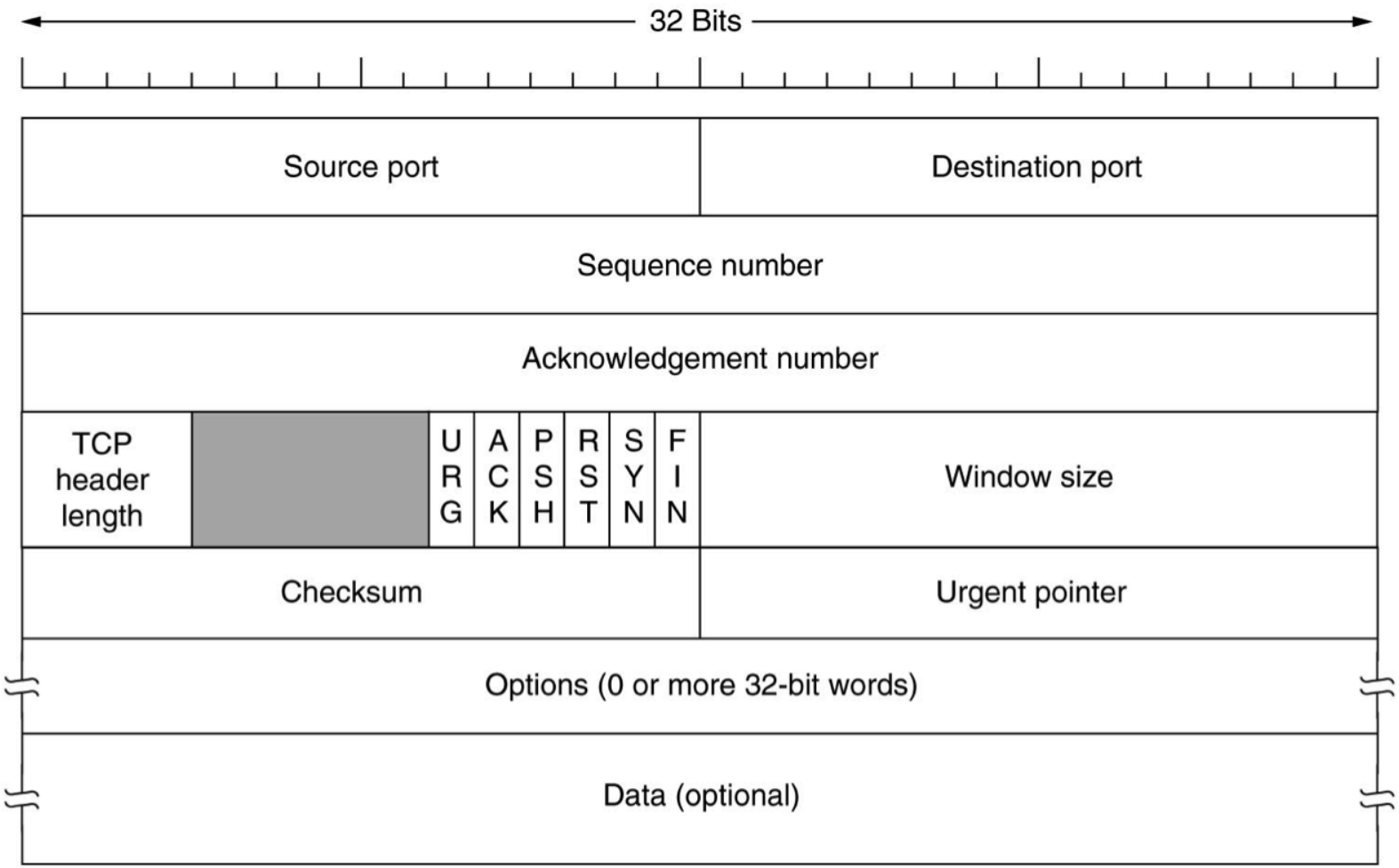
Data Encapsulation/Fragmentation



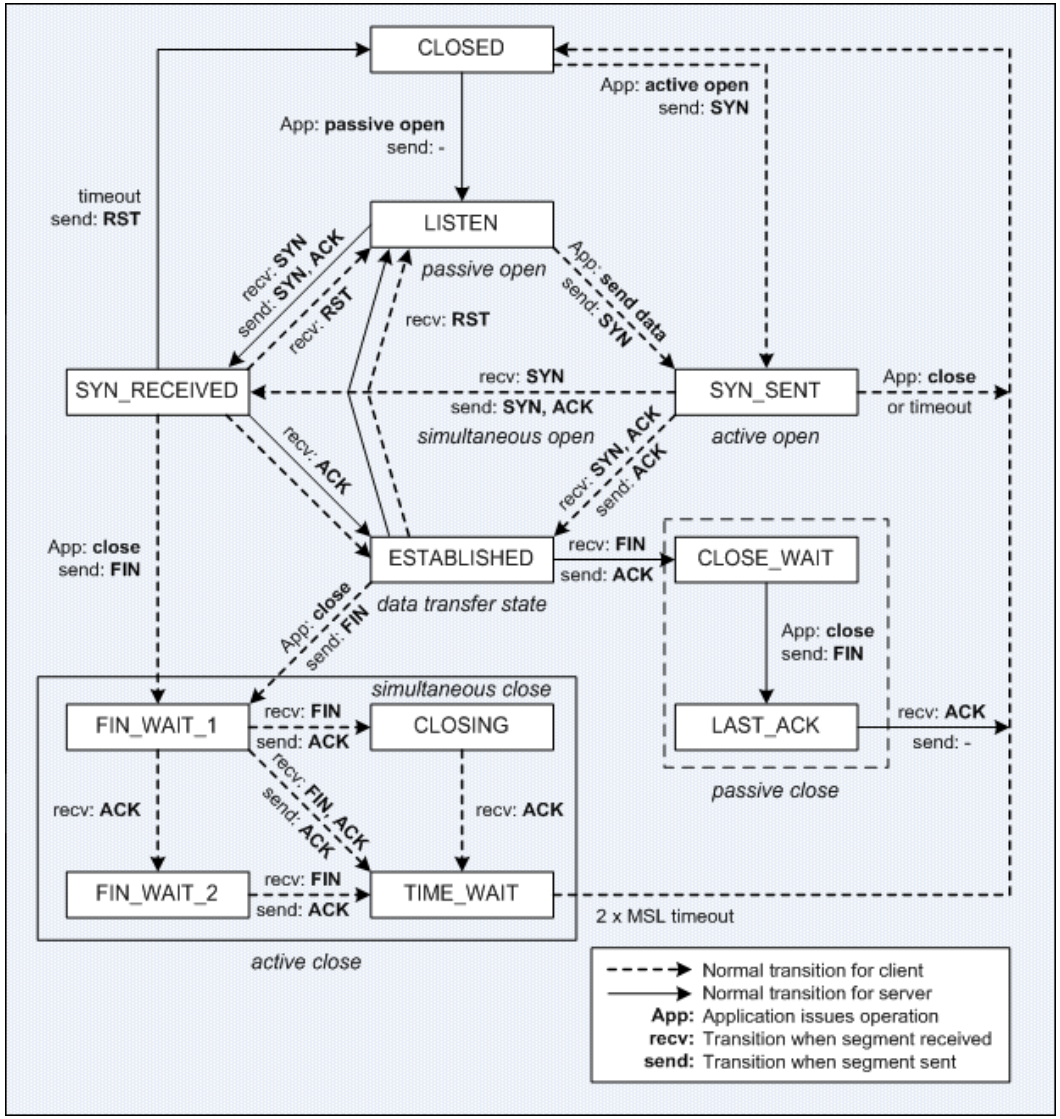
IP Header


32 Bits
Version
IHL
Type of service
Total length
Identification
D F
M F
Fragment offset
Time to live
Protocol
Header checksum
Source address
Destination address
Options (0 or more words)

TCP Header


32 Bits
Source port
Destination port
Sequence number
Acknowledgement number
TCP header length
URG
ACK
PSH
RST
SYN
FIN
Window size
Checksum
Urgent pointer
Options (0 or more 32-bit words)
Data (optional)

TCP State Machine



Active and Passive Attack

- Passive attack: intruder eavesdrops, but does not modify the message
  - ➠ unencrypted messages, side channel attacks (tax, health)

Active and Passive Attack

- Passive attack: intruder eavesdrops, but does not modify the message
  - ➠ unencrypted messages, side channel attacks (tax, health)
- Active attack: intruder may transmit, replay, modify, delete messages
  - ➠ man-in-the-middle, Denial-of-service

Denial-of-Service (DOS) Attack

- Exploit legitimate behavior or vulnerabilities with crafted packets
  - E-Mail bomb: sending auto-generated emails to victim
  - smurf: sending ICMP echo (ping) traffic to IP broadcast address with a spoofed source address of a victim
  - tear drop: overlapping (fragmented) packets
  - SYN flood: sending lots of TCP SYN packets

Denial-of-Service (DOS) Attack

- Exploit legitimate behavior or vulnerabilities with crafted packets
  - E-Mail bomb: sending auto-generated emails to victim
  - smurf: sending ICMP echo (ping) traffic to IP broadcast address with a spoofed source address of a victim
  - tear drop: overlapping (fragmented) packets
  - SYN flood: sending lots of TCP SYN packets
- Launch Distributed DOS (DDOS) with botnets

Personae

Alice:	first participant
Bob, Carol, Dave:	second, third, fourth participant
Eve:	eavesdropper
Trudy:	malicious active attacker

Secure Communication

- Secrecy: Alice can send a message to Bob only he can read
- Authentication: Bob knows for sure that Alice sent it
- Nonrepudiation : Alice can't deny she sent the message

Summary

- What is security
- Real-world attacks
- Course mechanisms
- A primer of networking

- Next lecture: Introduction to cryptography