Network Security

Session 9A

Cryptography - 1

Sheba Pari

Session 9A: Focus

- Cryptography Introduction
- Attacks
- Passive Vs Active attacks
- Cryptographic Techniques
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
- Quiz 1 to 4

Course page where the course materials will be posted as the course progresses:

Introduction to Cryptography

Cryptography: An Introduction

- The word “cryptography” derives from the Greek word for “secret writing”.
- The Concise Oxford English Dictionary defines cryptography as “the art of writing or solving codes.”
- But cryptography nowadays encompasses much more than this, it deals with mechanisms for
  - Ensuring integrity, techniques for exchanging secret keys
  - Protocols for authenticating users
  - Electronic auctions and elections
  - Digital cash, and more.

Cryptography

Cryptanalysis:

- The art or process of deciphering coded messages without being told the key.
- Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

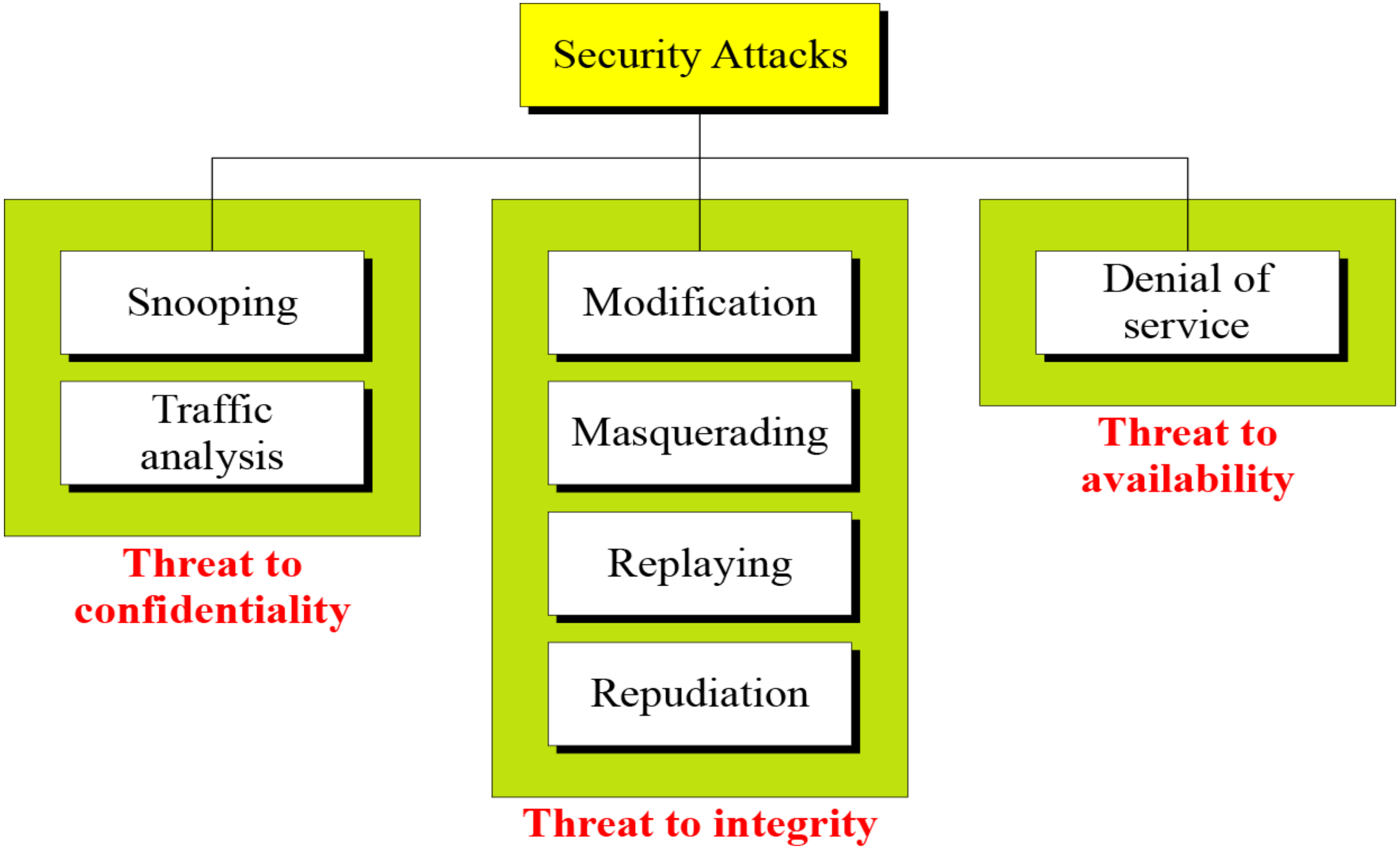
Cryptology:

- The scientific study of cryptography and cryptanalysis.

Attacks

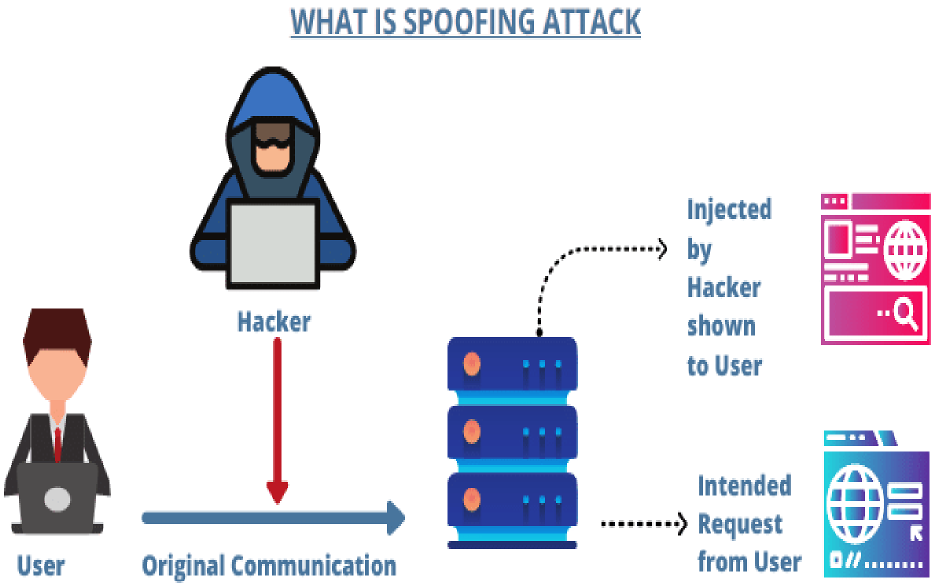
Security Attacks

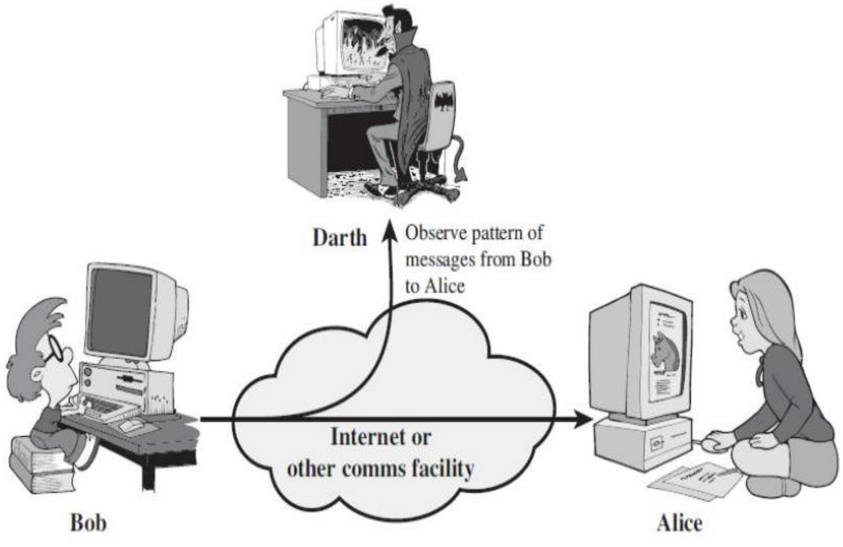
Taxonomy of Attacks with relation to security goals



Attacks Threatening Confidentiality

- 2 types of attacks threaten the confidentiality of information
  - **Snooping** refers to **unauthorized access** to or **interception** of data.
  - **Traffic analysis** refers to obtaining some other type of information by **monitoring online traffic**.




Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

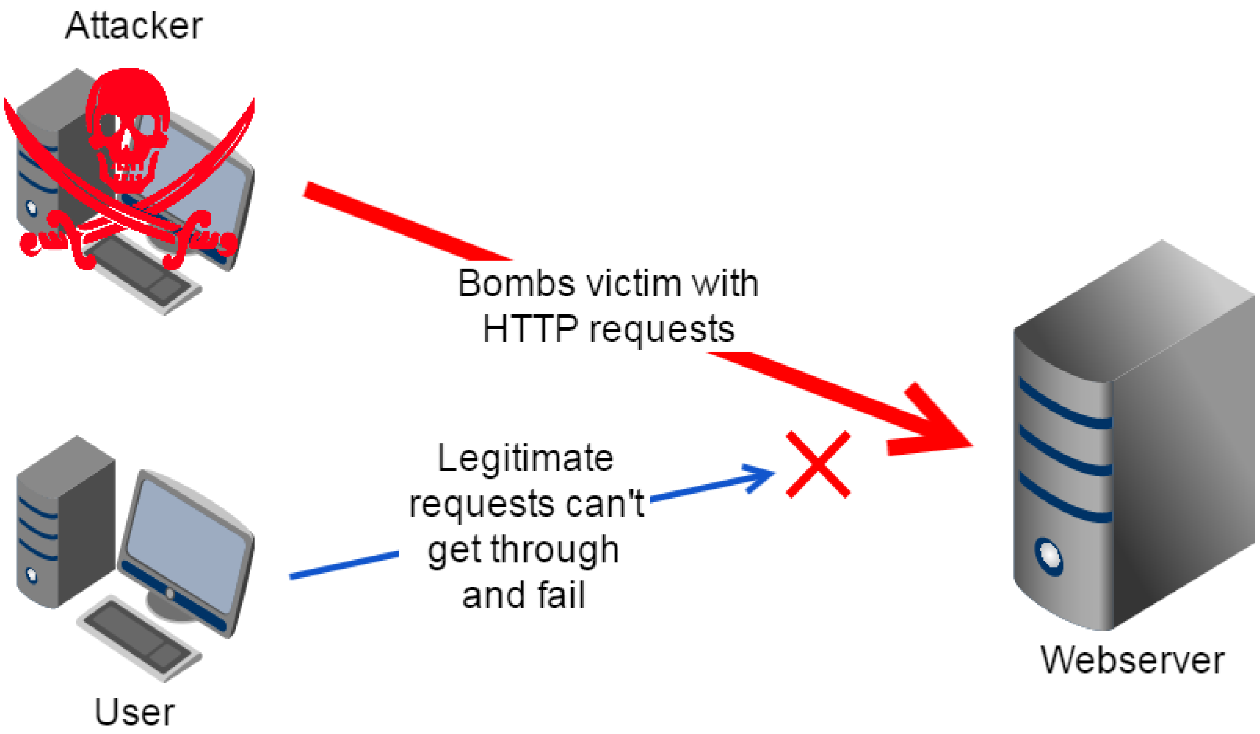
(b) Traffic analysis

Attacks Threatening Integrity

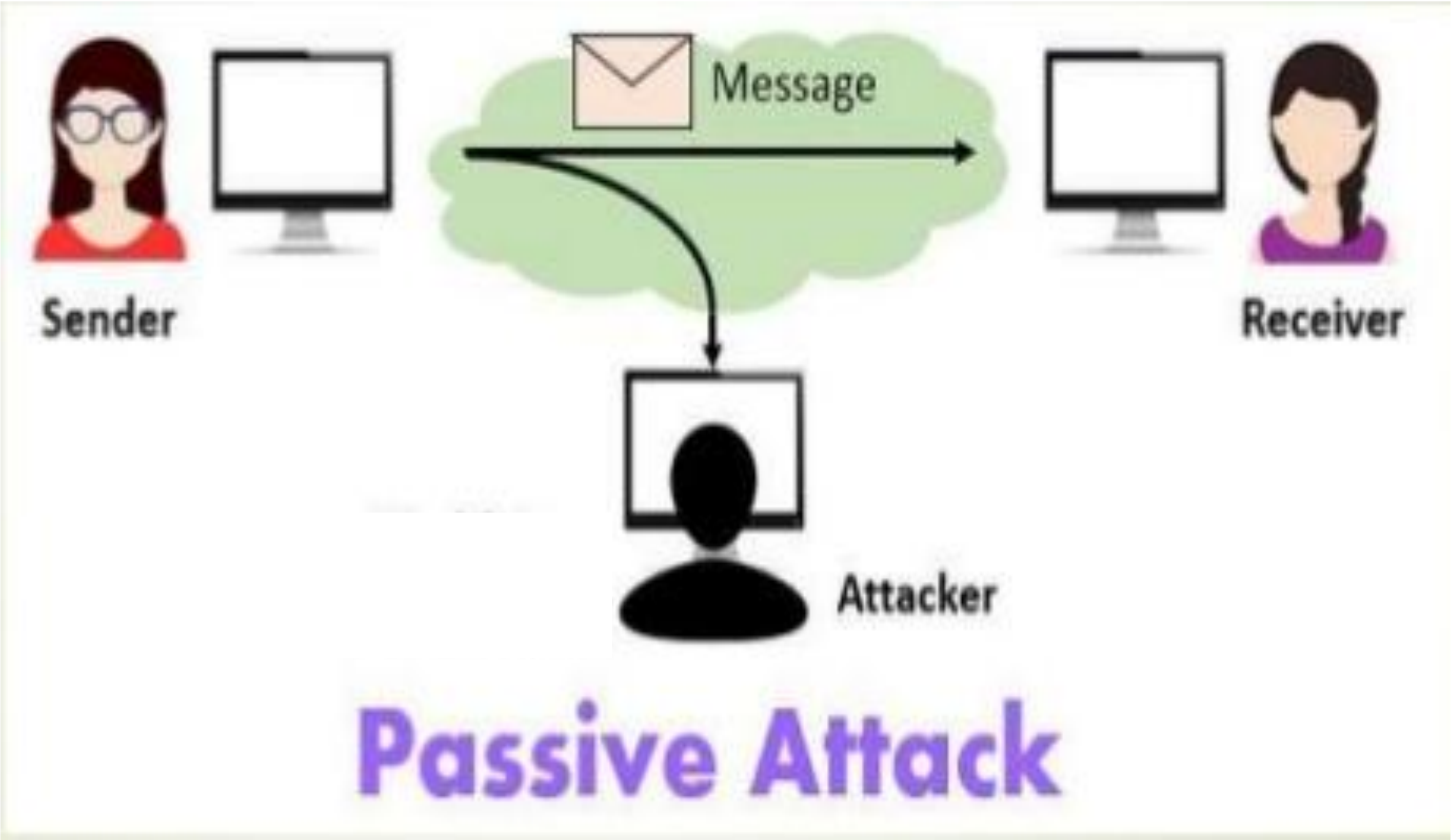
- **Modification** means that the attacker **intercepts the message** and changes it.
- **Masquerading** or spoofing happens when the attacker **impersonates** somebody else.
- **Replaying** means the attacker **obtains a copy** of a message sent by a user and later tries to replay it.
- **Repudiation** means that sender of the message might later **deny** that she has sent the message; the receiver of the message might later deny that he has received the message.

Attacks Threatening Availability

- **Denial of service (DoS)** is a very **common attack**.
- It may **slow down** or totally interrupt the service of a system.


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

Passive Attacks



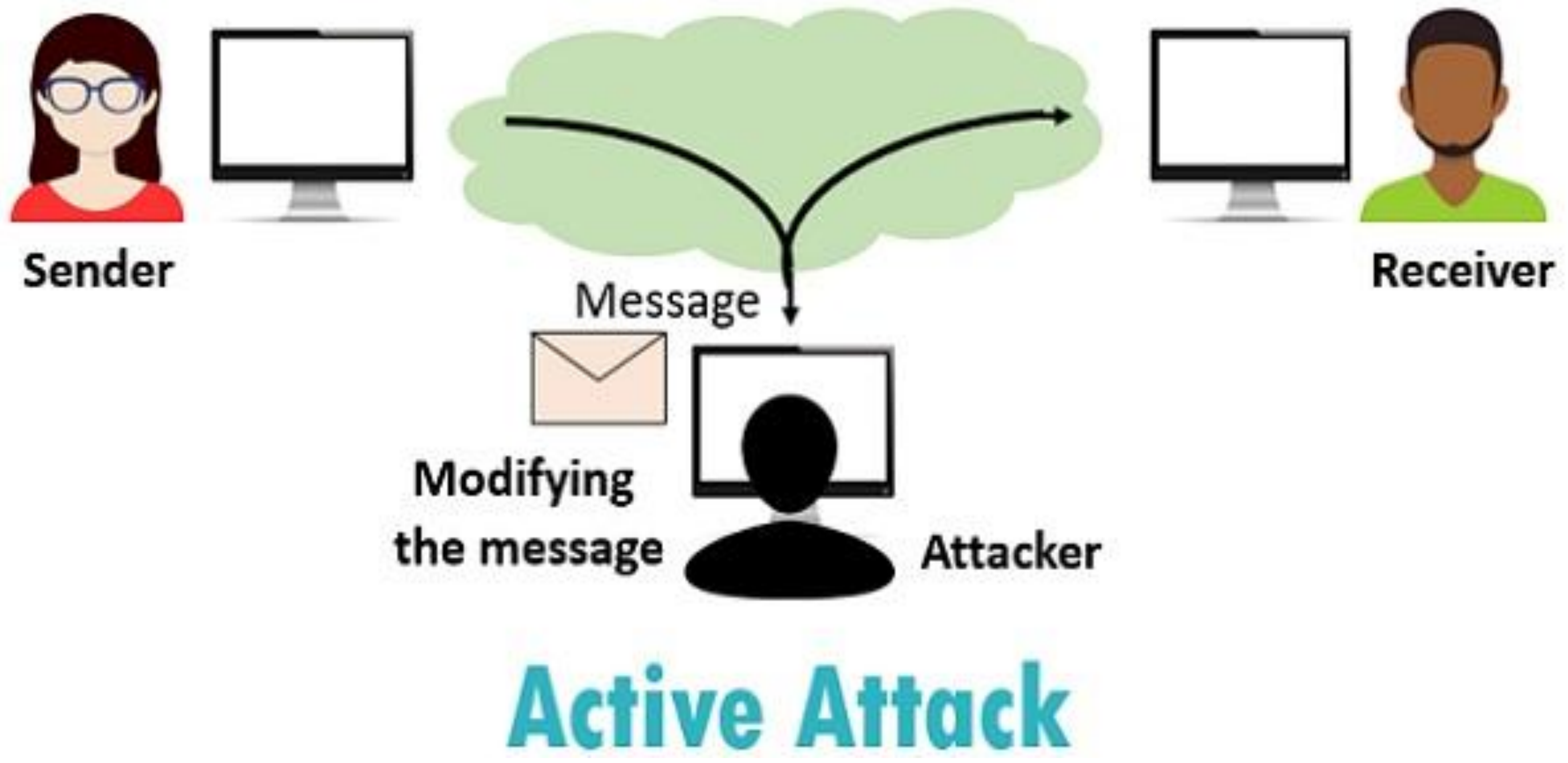
Types of Attacks

Passive Attacks

- **Passive Attacks**
  - Goal is to just **obtain information**.
  - Attack **does not modify data** or harm the system.
  - Attacks that **threaten Confidentiality** are **Passive attacks**.
  - Difficult to detect this type of attack.
  - Passive attacks can be prevented by **encipherment** of the data.

Encipherment refers to the process of converting information, such as a message or document, from its original form into a coded or ciphered form

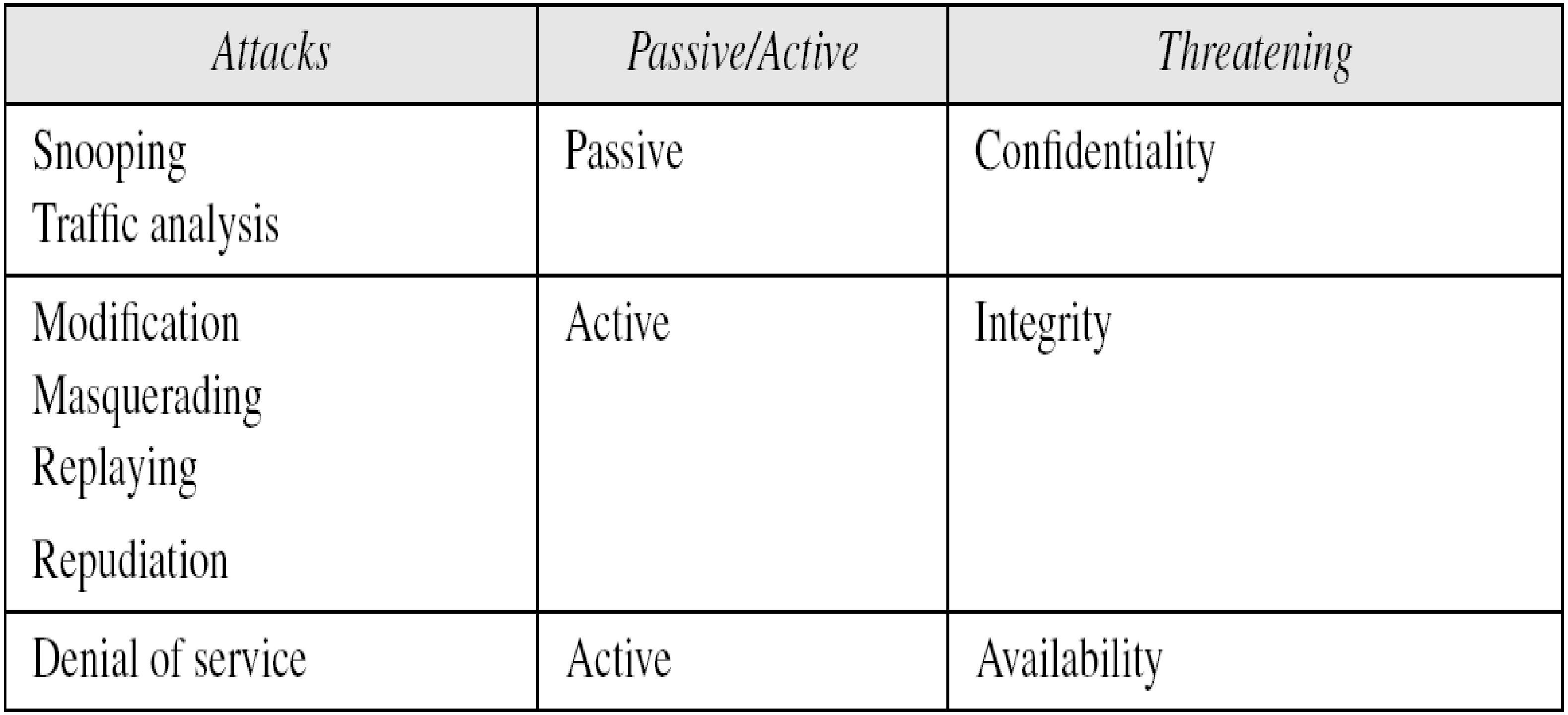
Active Attacks



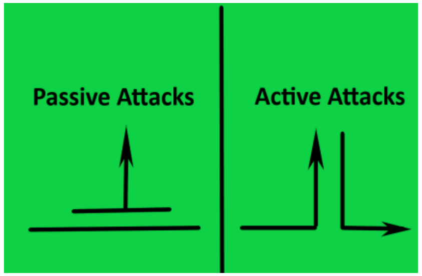
Active Attacks

- **Active Attacks**
  - Attack **may change the data** or harm the system.
  - Attacks that threaten the Integrity and Availability are Active attacks.
  - Easier to detect this type of attack than to prevent.

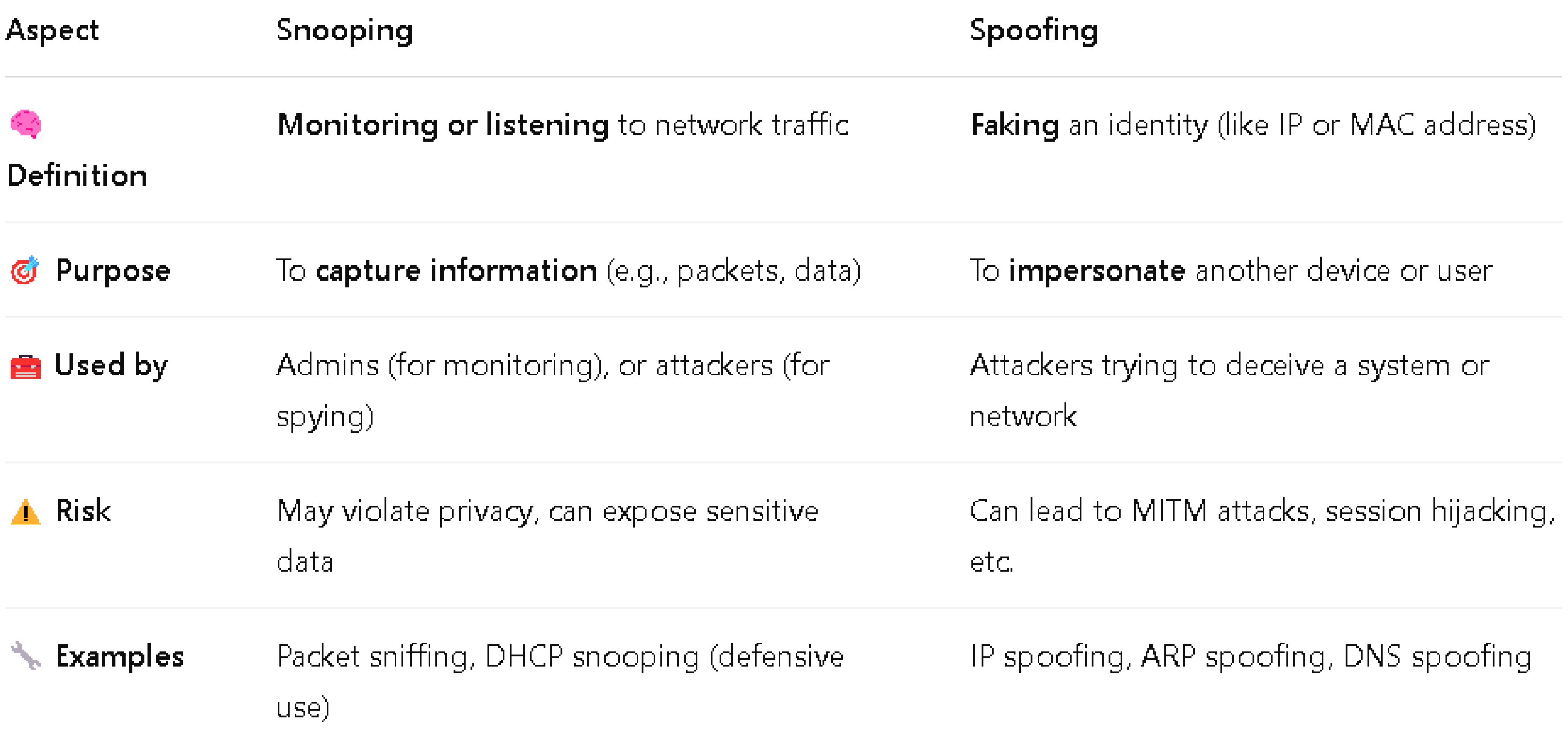
Passive Vs Active Attacks



Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability



Snooping Vs Spoofing



Aspect	Snooping	Spoofing
🧠 Definition	**Monitoring or listening** to network traffic	**Faking** an identity (like IP or MAC address)
🎯 Purpose	To **capture information** (e.g., packets, data)	To **impersonate** another device or user
🧰 Used by	Admins (for monitoring), or attackers (for spying)	Attackers trying to deceive a system or network
⚠️ Risk	May violate privacy, can expose sensitive data	Can lead to MITM attacks, session hijacking, etc.
🔧 Examples	Packet sniffing, DHCP snooping (defensive use)	IP spoofing, ARP spoofing, DNS spoofing

MITM: Man-in-the-Middle attach

Key Terms in Cryptography

- **One-way hash function-** Sometimes also called as one-way compression function to compute a **reduced hash value** for a message (**e.g., SHA-256**)
- **Symmetric key cryptography-** Compute a cipher text decodable with the same key used to encode (**e.g., AES**)
- **Public-key cryptography-** Compute a cipher text decodable with a different key used to encode (**e.g., RSA**)
- **Digital signatures-** Confirm the author of a message
- **Mix network-** Pool communications from many users to anonymize what came from whom.
  - A mix network is a cryptographic system that facilitates anonymous communication by obscuring the relationship between senders and recipients of messages.

Symmetric & Asymmetric key Cryptography

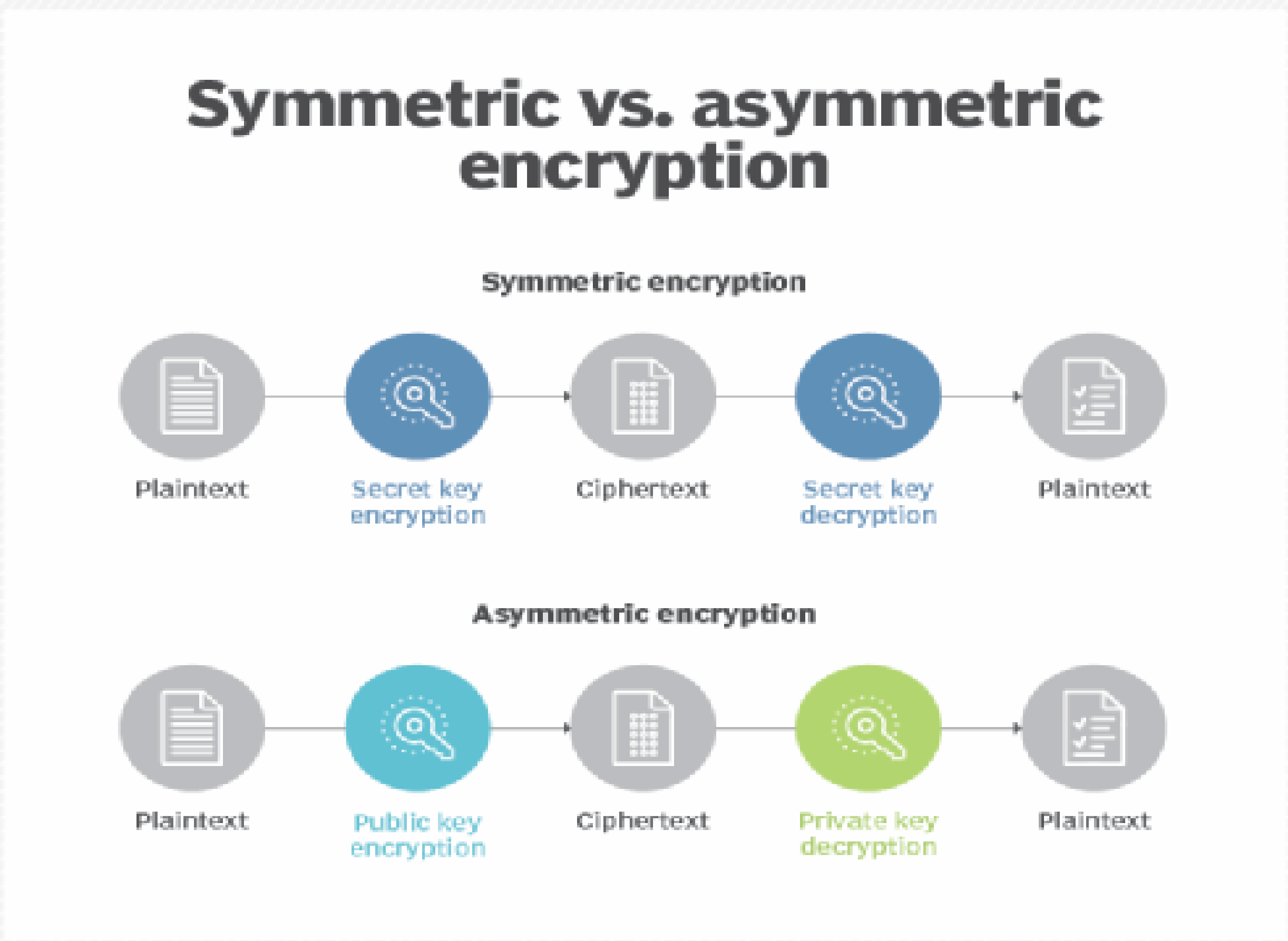
Cryptographic Techniques

- Cryptography involves 3 distinct mechanisms
  - **Symmetric key Encipherment**
  - **Asymmetric key Encipherment**
  - **Hashing**

Symmetric & Asymmetric key Cryptography

- **Symmetric key Encipherment**
  - Also called as secret key encipherment or secret key cryptography.
  - This method uses a single secret key for both encryption and decryption.
- **Asymmetric key Encipherment**
  - Also called as public key encipherment or public key cryptography.
  - This method uses 2 keys, one public key and one private key.
  - Encryption using public key, decryption using private key.

Symmetric & Asymmetric key Cryptography



Cryptography: Quiz 1 to 4

Quiz 1: Cryptography

- Which of the following is an example of a passive attack?

A. ARP spoofing

B. Packet sniffing

ANS: B

C. Denial of Service (DoS)

D. Session hijacking

Quiz 2: Cryptography

- Which of the following statements about symmetric cryptography is true?

A. It uses a pair of public and private keys

B. It is slower than asymmetric encryption

C. It uses the same key for both encryption and decryption

D. It is only used in digital signature

ANS: C

Quiz 3: Cryptography

- What is an important property of a cryptographic hash function?

A. It can be easily reversed to get the original input

B. It generates variable-length outputs

C. It produces a fixed-size output from any input

D. It always generates the same hash for different inputs

ANS: C

Quiz 4: Cryptography

- What is the main purpose of a digital signature?

A. Compress the message before sending

B. Encrypt the entire message

C. Ensure integrity and non-repudiation

D. None of the above

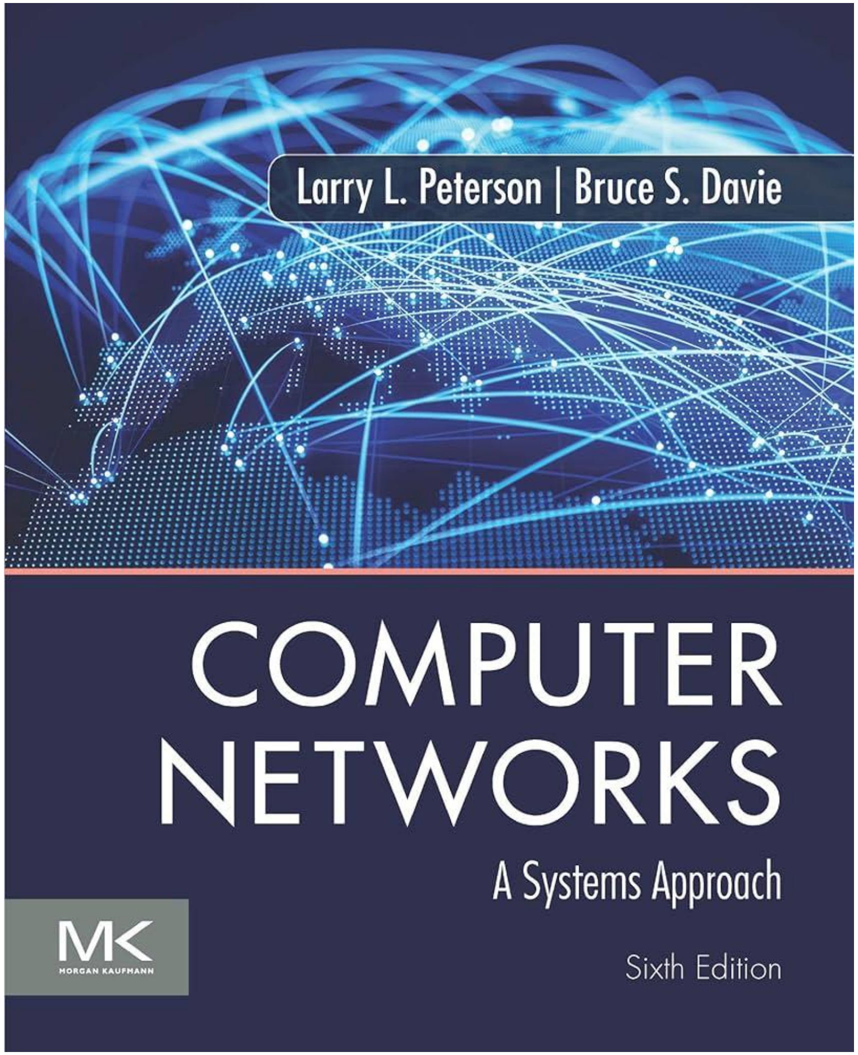
ANS: C

Session 9A: Summary

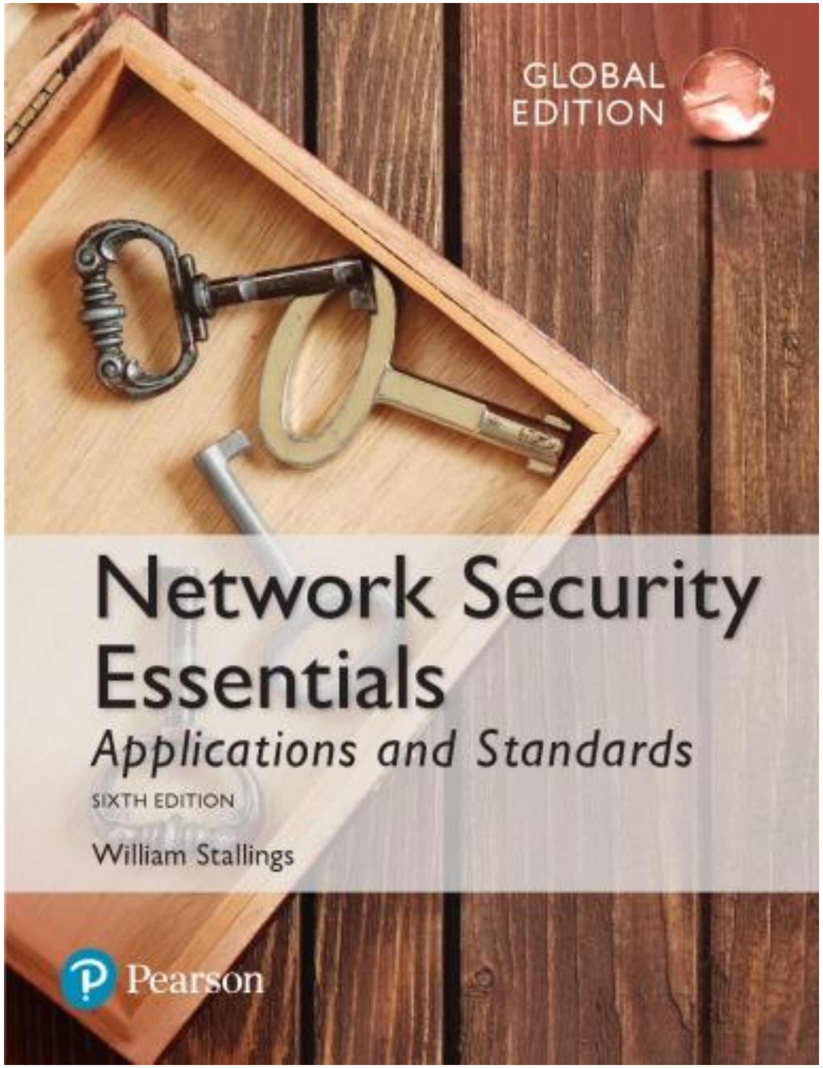
- Cryptography Introduction
- Attacks
- Passive Vs Active attacks
- Cryptographic Techniques
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
- Quiz 1 to 4

Textbooks

Textbook 1

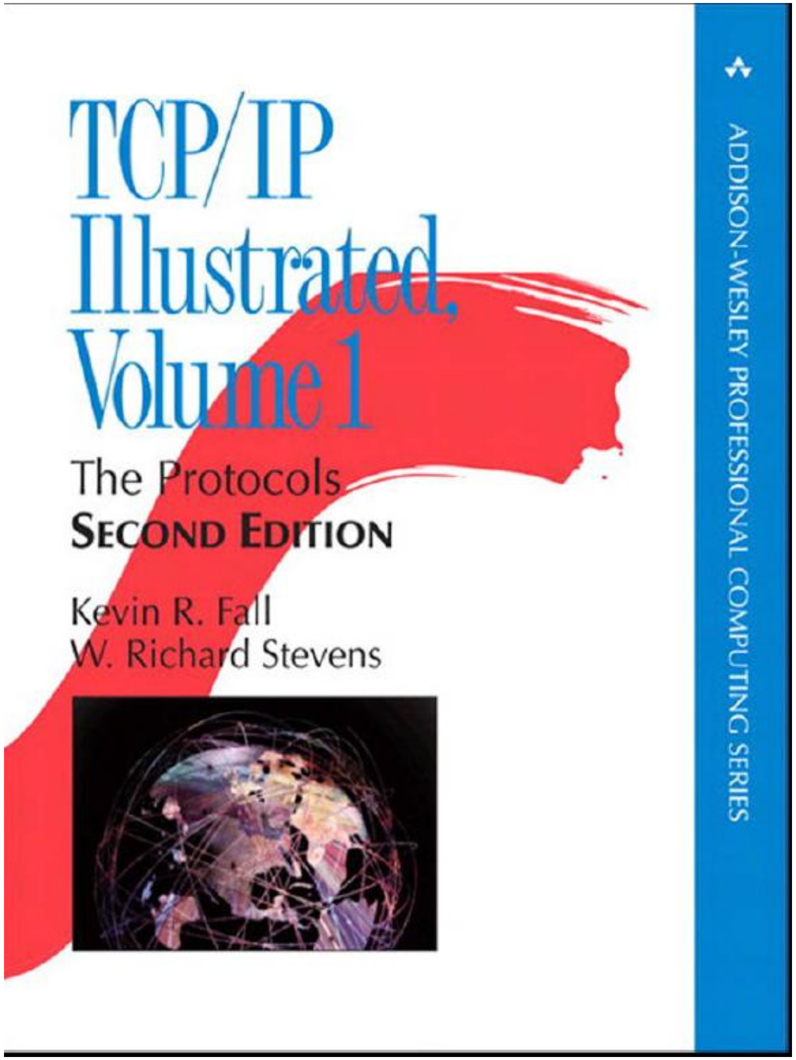


Textbook 2



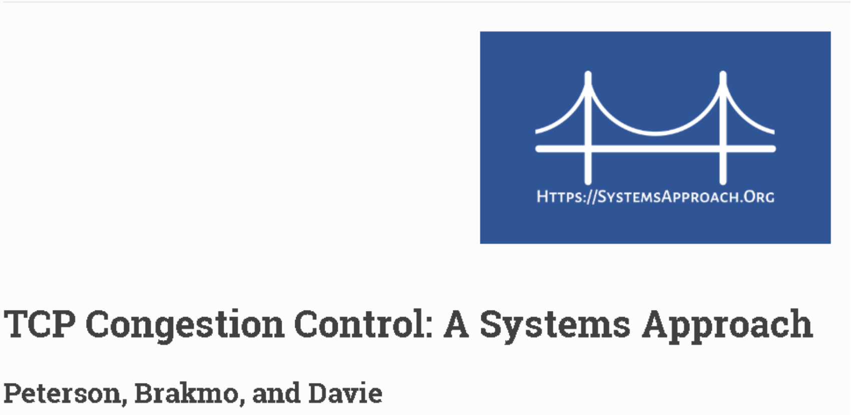
References

Ref 1


TCP/IP Illustrated, Volume 1
The Protocols
SECOND EDITION
Kevin R. Fall
W. Richard Stevens
ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

Ref 2

[TCP Congestion Control: A Systems Approach]

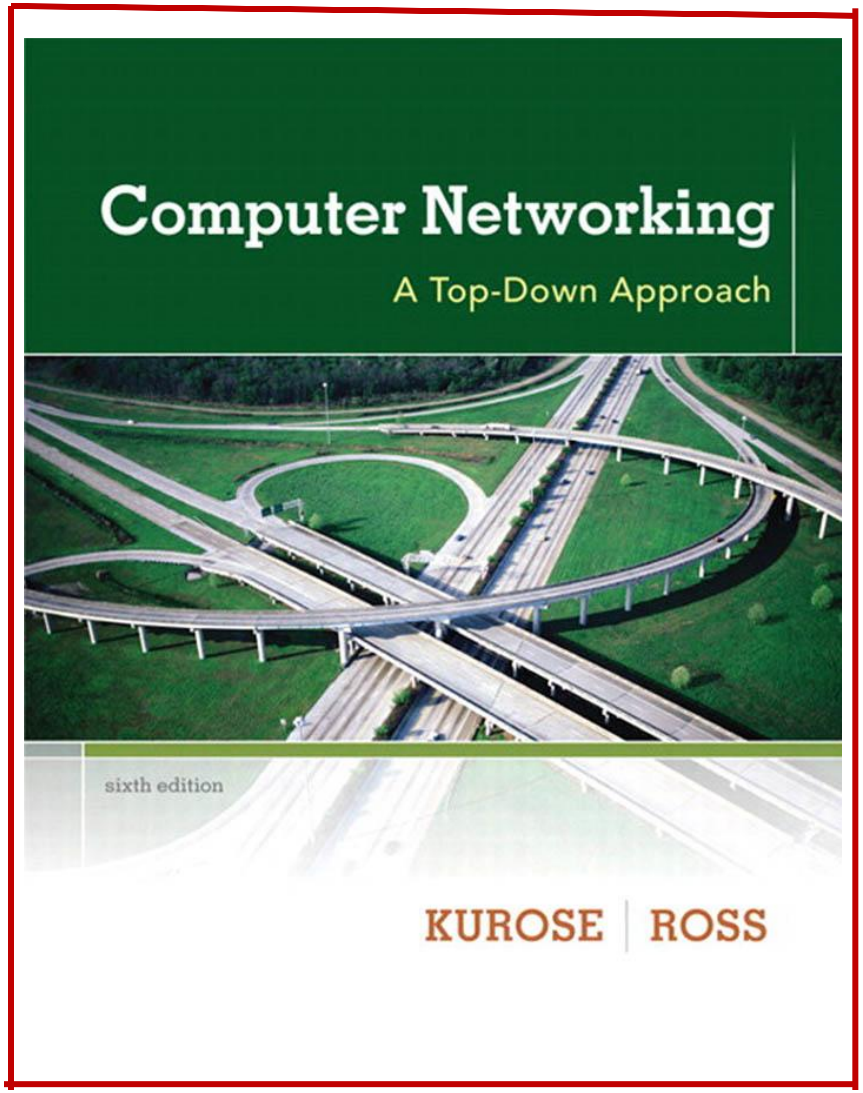


TCP Congestion Control: A Systems Approach

Peterson, Brakmo, and Davie

References

Ref 3



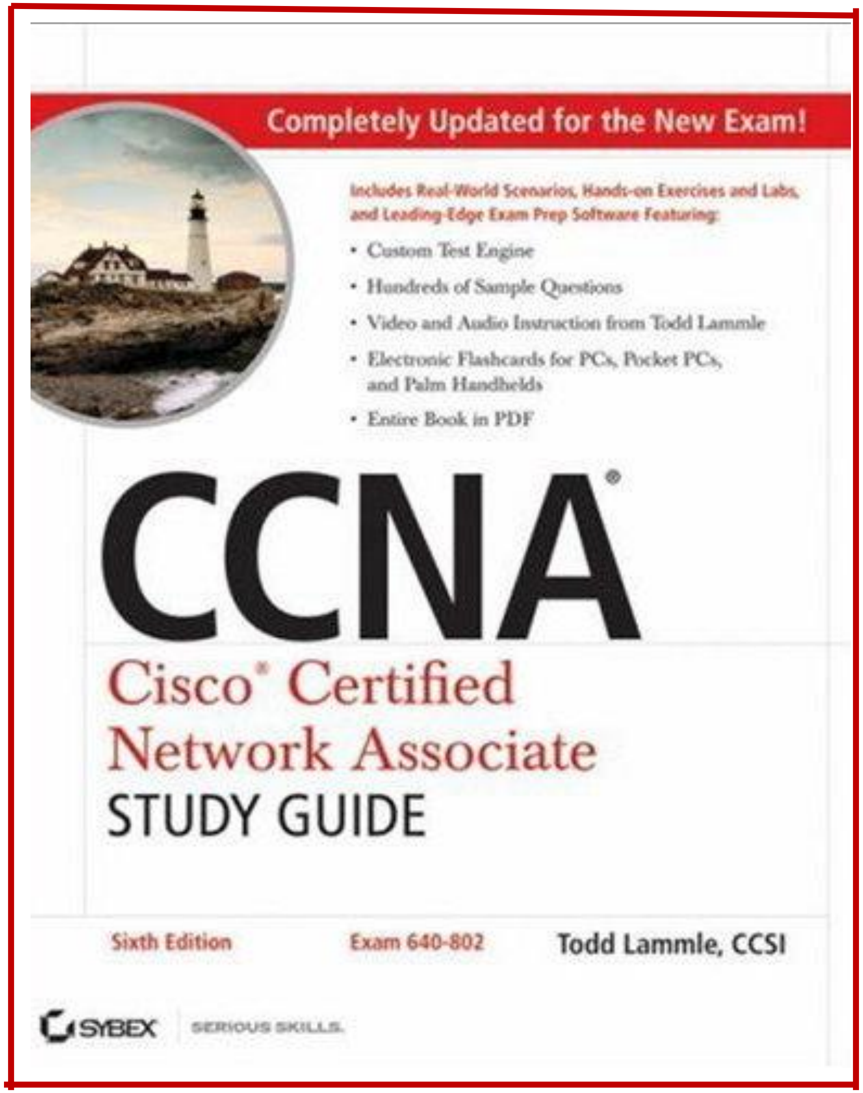
Computer Networking

A Top-Down Approach

sixth edition

KUROSE | ROSS

Ref 4



Completely Updated for the New Exam!

Includes Real-World Scenarios, Hands-on Exercises and Labs, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Video and Audio Instruction from Todd Lammle
- Electronic Flashcards for PCs, Pocket PCs, and Palm Handhelds
- Entire Book in PDF

CCNA®

Cisco® Certified Network Associate

STUDY GUIDE

Sixth Edition

Exam 640-802

Todd Lammle, CCSI

SYBEX | SERIOUS SKILLS.

References

Ref 5