CCS6224
Network Security

Lecture 1

Course Information

› Lecturer's info:

Course Coordinator: Mr. Amir Shah bin Abdul Aziz
(amir.shah@mmu.edu.my)
Class ID: TCIL, TT1L, TT2L, TT3L, TT4L and TT6L

Lecture: Mrs. Nor Idayu binti Ahmad Azami
(idayu.azami@mmu.edu.my)
Class ID: TC2L and TT5L

Course Information

- Assessment Scheme

Assessment	Percentage
Assignment	**30**
Lab Exercise	**40**
Test	**30**

- Textbook

Stalling, W., & Brown, L. (2017). Cryptography and Network Security: Principles and Practice, 7th Edition. Pearson.

- A good understanding on network TCP/IP fundamental is required B4 U do Network Security.

Computer Security

- the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Security Outline

- Security Objective
- General understanding and prevention method

Security Objectives/Threat/Requirement

- Privacy/Confidentiality
- Message Integrity
- Non-repudiation
- Message Replay
- Sender/Receiver Authentication
- Anonymity
- Availability
- Each objectives are unique. (Don't confuse and mix them up)

Privacy/Confidentiality

- Privacy/Confidentiality
- Nobody can see the message other than the sender/receiver.
- Example, “Alice salary is rm1000 per day”
- Encrypt the data before sending or storing
- Privacy is related to people. Alice salary
- Confidentiality relate to Data. (staff pay scale)
  - Restrict User Access to Data

Message integrity

- Bob bank-in $1000 into Bank ABC
- The message content cannot be changed
- Use hashing such as md5, sha256 etc
- Even if you change 1 bit of the msg, the hash is completely different
- Sha256(“msg, random_passwd”) = hashValue
- Sent msg, hashValue
- Receiver sha256(“msg, random_passwd”) = hashValue then message is valid
- Nobody else knew the passwd so nobody can construct a valid message with a valid hash.

Non-repudiation

- Bob promise to marry Alice
- Then he saw “Ms University MMU” and denied his earlier commitment
- If there only 1 male cat (tom) in your village, any cat got pregnant, who is the father
- If there are two cats (tom and lee) then both can said “Definitely it is not me”
- Only you have the key to the safeBox, anything lost has to be you.

Asymmetry encryption

- Alice got AlicePubKey, AlicePrivKey
- Bob got BobPubKey, BobPrivKey
- All PubKey are publicly known (or PKI (public Key infrastructure Verified)
- All PrivKey are secret to individual
- Alice send msg to Bob
  - Encrypt(BobPubKey, msg) = EcryptMsg
  - Bob Decrypt(BobPrivKey, EncryptMsg) = msg
  - Only Bob has BobPrivKey thus only Bob can decrypt the msg

Signing

- Alice want to sign & Sent a document/contract to Bob
- Document “Alice agree that Alice owe Bob USD1000” signed Alice.
- Alice will sign the doc.
  - Sign(doc, AlicePrivKey) = signature
  - This signature is signed by Alice since only Alice got AlicePrivKey
- Bob will verify the doc
  - Verify(signature, AlicePubKey) = YES/NO
  - If verify = YES, We can be sure this document came/signed by Alice.
  - Everybody can verify that Alice signed the document
- Question?
  - What if the doc need to be private between Alice and Bob

Non-replay

- Msg “Alice deposit RM1 into Bank ABC”
- Capture this msg and replay it 1 million time
- Alice bank acc $1 million
- Prevention Method
  - Each Msg has a Session ID
  - Each Msg has a timestamp, must be valid within 5 min windows, all node are synchronized with a clock.
  - Other accounting method, Protocol specific solution
-

Sender/Receiver Authentication

- Not signing/verifying any document. Just verify that the document sent by the sender.
- “Pls click on the nuke button” said “President
- You must be damn sure it came from the president
- Logging: You also need to be ensure that the msg is logged for accountability.
- Oh! It is the president who approved it.
- Asymetric Encryption
- Other method:
  - User Login
  - Protocol specific

Sender/Receiver Anonymity

- You got/sent a message from Gangster Leader
- There is an address but you don't know who/where is he/she.
- Question
  - If you don't know who/where is he/she. How do you verify that it is Gangster Leader? He could be a teenage boy
  - Gangster Alice want to do business with Gangster Bob
  - Each don't know each other but they can transact online goods securely online using crypto.

Availability

- Protocol Specific
  - How do you break into a secured building?
  - Study!x100! Find any loop hole. Maybe Timing Specific
  - Once found, organize/time the break in
  - Same with any protocol. Study!x100 until U R better than the expert. Once found a bug, loophole, vulnerability => break in.
  - Certain packet that can hang the OS.
- Brute Force Approach
  - Send rubbish to receiver
  - Exhaust their network bandwidth, CPU power, RAM.

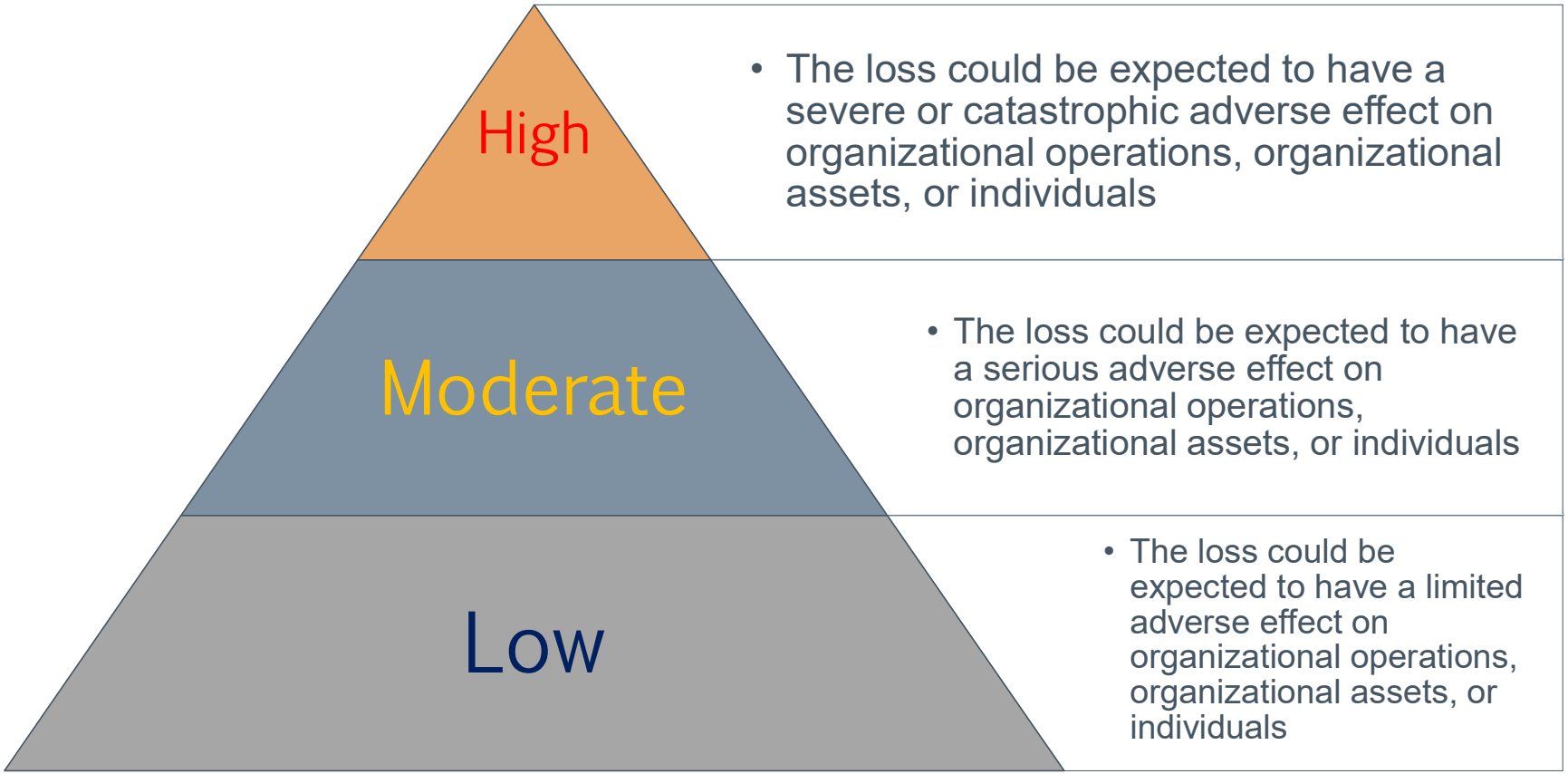
Advanced Security Requirement

- There are many funny2 security requirement. In time you will heard about it.
- E.g Online voting
- Information Hiding
- Watermarking
- Document security
  - Read, Copy, Print, Modify/Edit.
  - Can read but cannot print (need $$$, access) etc
  - Future! Can read 2x only, 10% only! After that must pay!

ROI

- Cost(Protection) $\ll$ Cost (Security Threat)
- You don't buy a $1000 lock for your $10 bike

Breach of Security - Levels of Impact



Outline

- Computer security concepts
  - Definition
  - Examples
  - Challenges
- The OSI security architecture
- Security attacks
  - Passive attacks
  - Active attacks
- Security services
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - Availability service
- Security mechanisms

The field of network and Internet security consists of:

measures to deter, prevent, detect, and correct security violations that involve the transmission of information

Computer Security Objectives

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

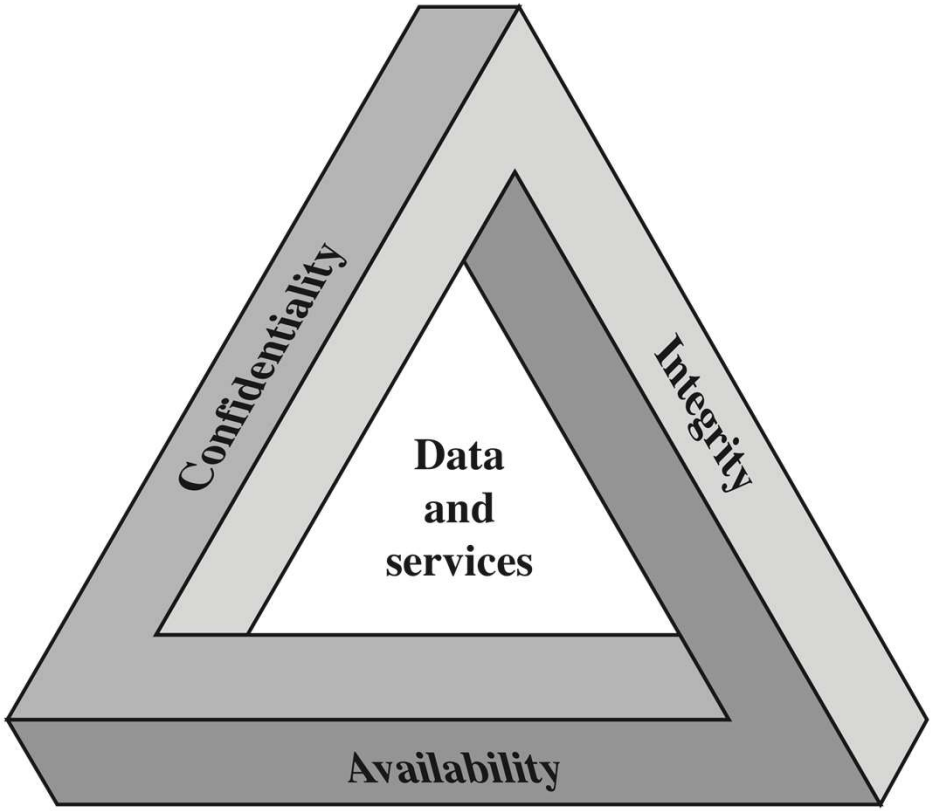
Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

CIA Triad


Confidentiality
Integrity
Data
and
services
Availability

Threats and Attacks (RFC 4949)

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Two Classes of Security Attacks

- RFC4949 and X.800 defined two security attack classes
- A ***passive attack*** attempts to learn or make use of information from the system but does not affect system resources
- An ***active attack*** attempts to alter system resources or affect their operation

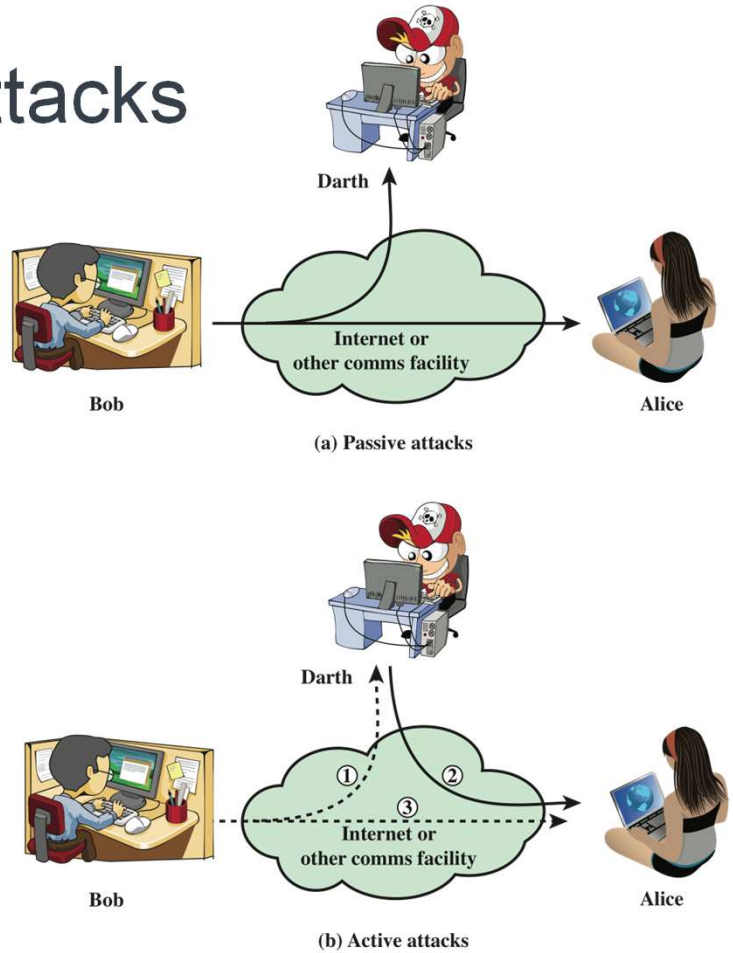


Figure 1.1 Security Attacks

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted

› Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis
  - Confidentiality, Privacy
  - Use this info for active attack later on

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

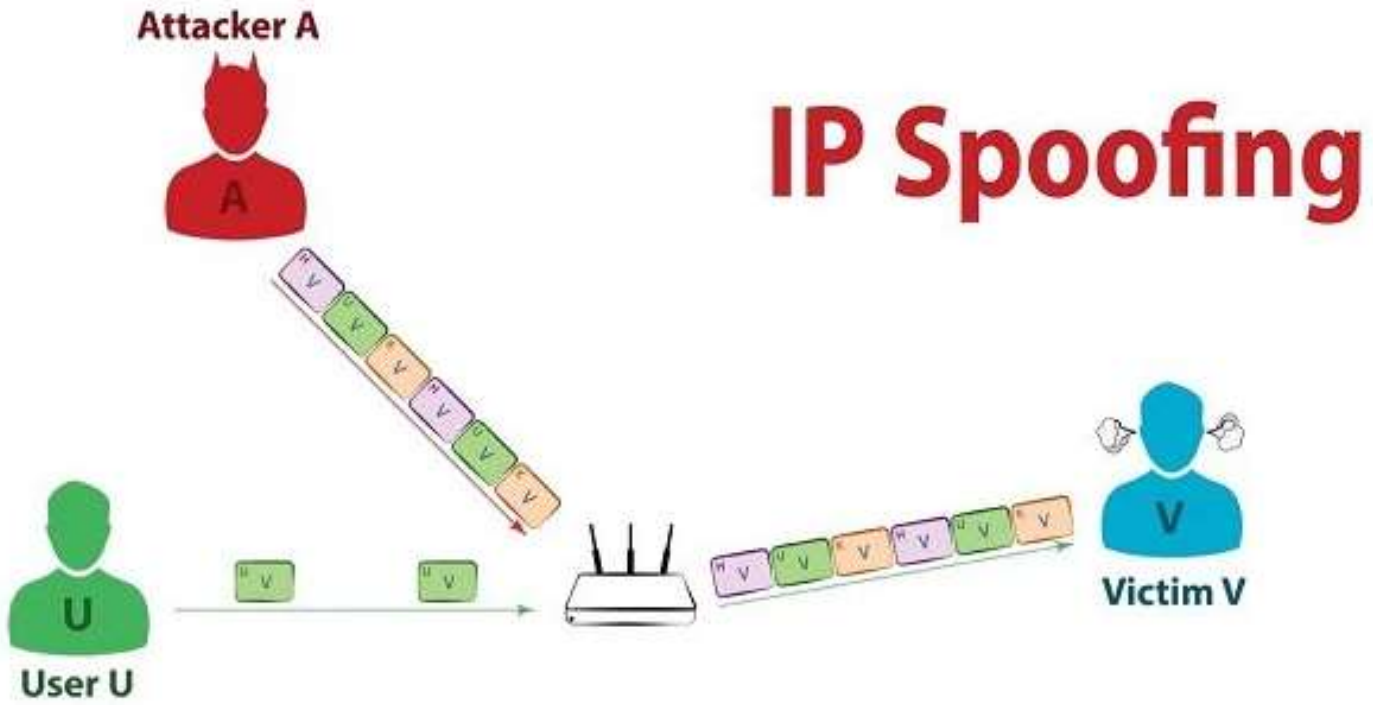
Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

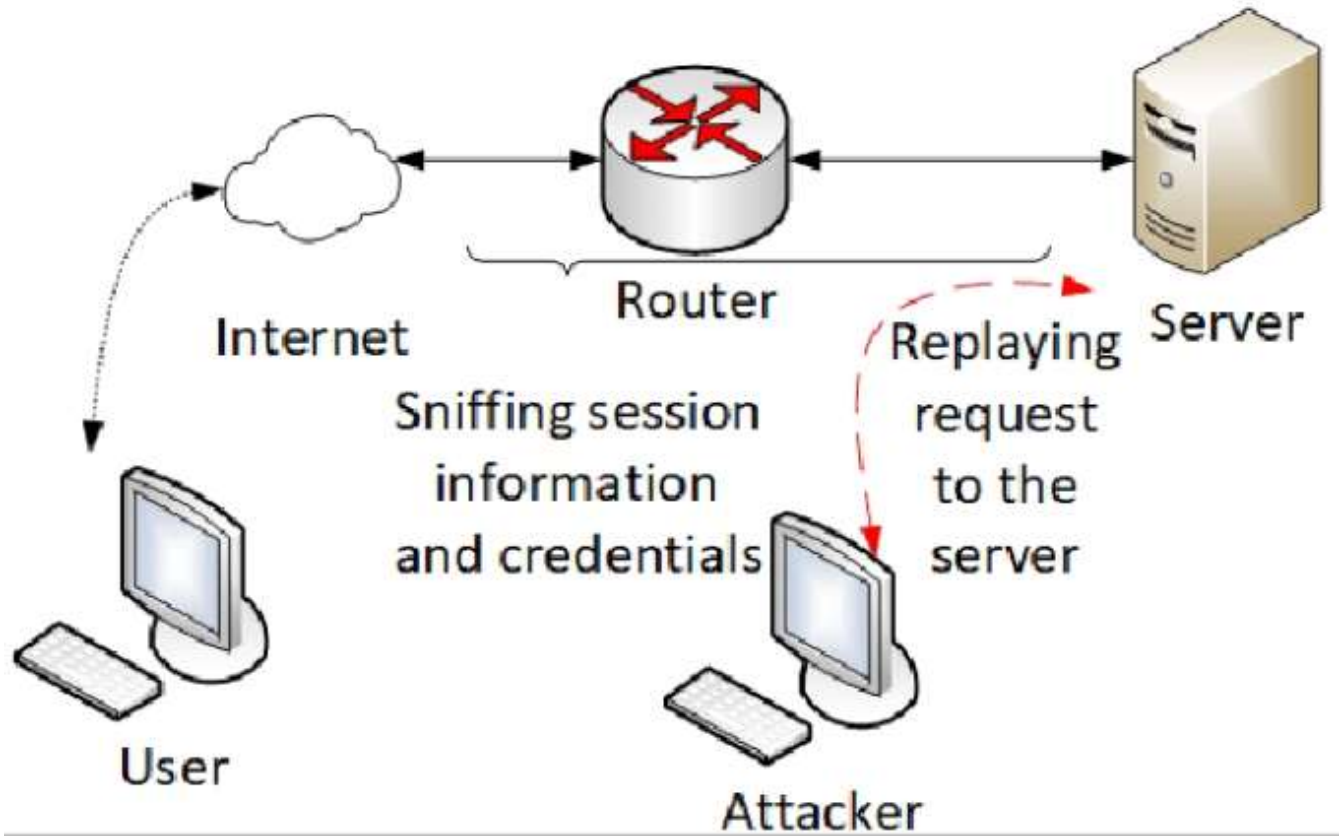
Denial of service

- Prevents or inhibits the normal use or management of communications facilities

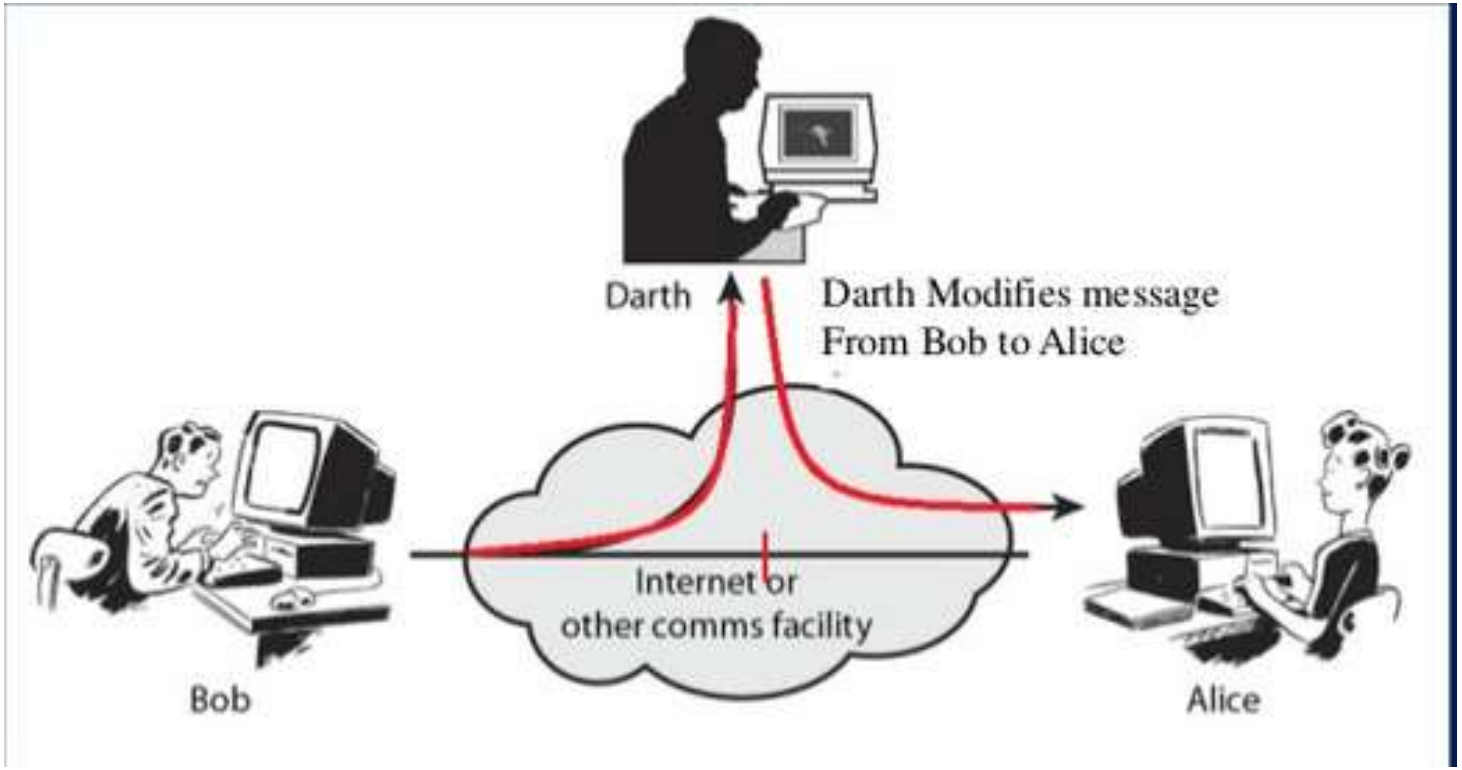
Masquerade Attack



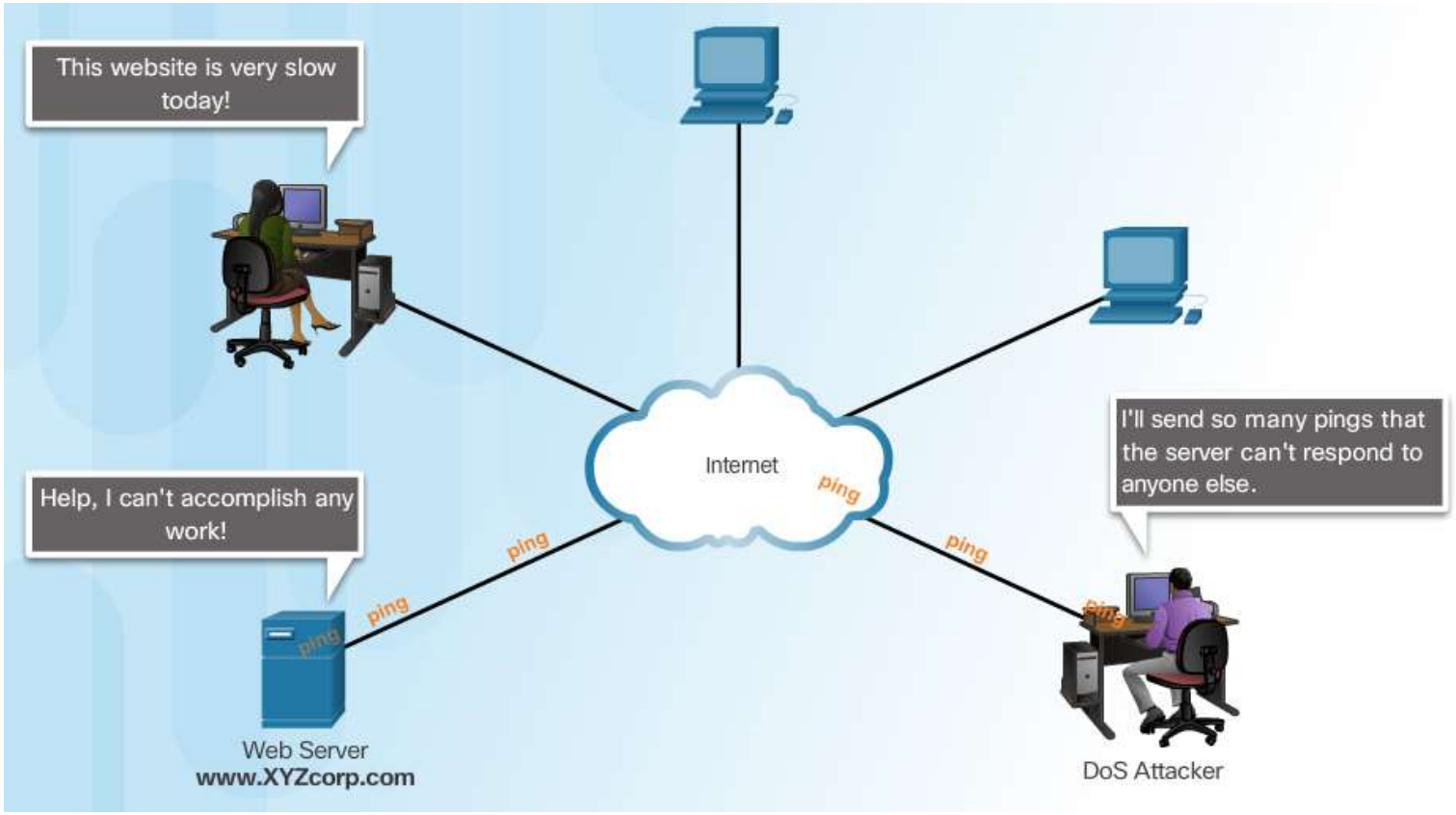
Replay Attack



Modification of Messages Attack.
Man in The Middle Attack.



DDoS Attack


This website is very slow today!
Internet
ping
I'll send so many pings that the server can't respond to anyone else.
Help, I can't accomplish any work!
ping
ping
ping
ping
Web Server
www.XYZcorp.com
DoS Attacker

Security Services

- Defined by X.800 as:
  - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers

- Defined by RFC 4949 as:
  - A processing or communication service provided by a system to give a specific kind of protection to system resources

X.800 Service Categories

- X.800 defines it in 5 major categories
- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation

Model for Network Security

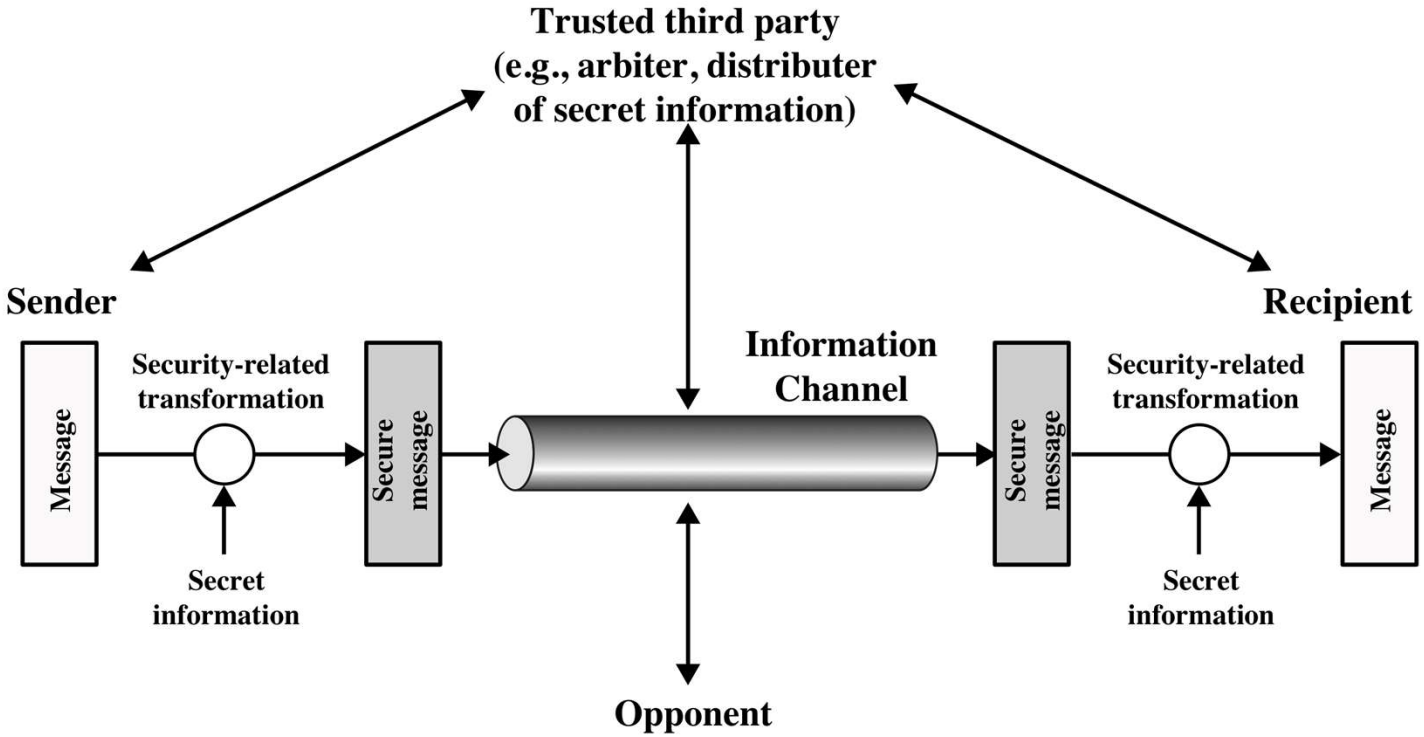


Figure 1.2 Model for Network Security

Network Access Security Model

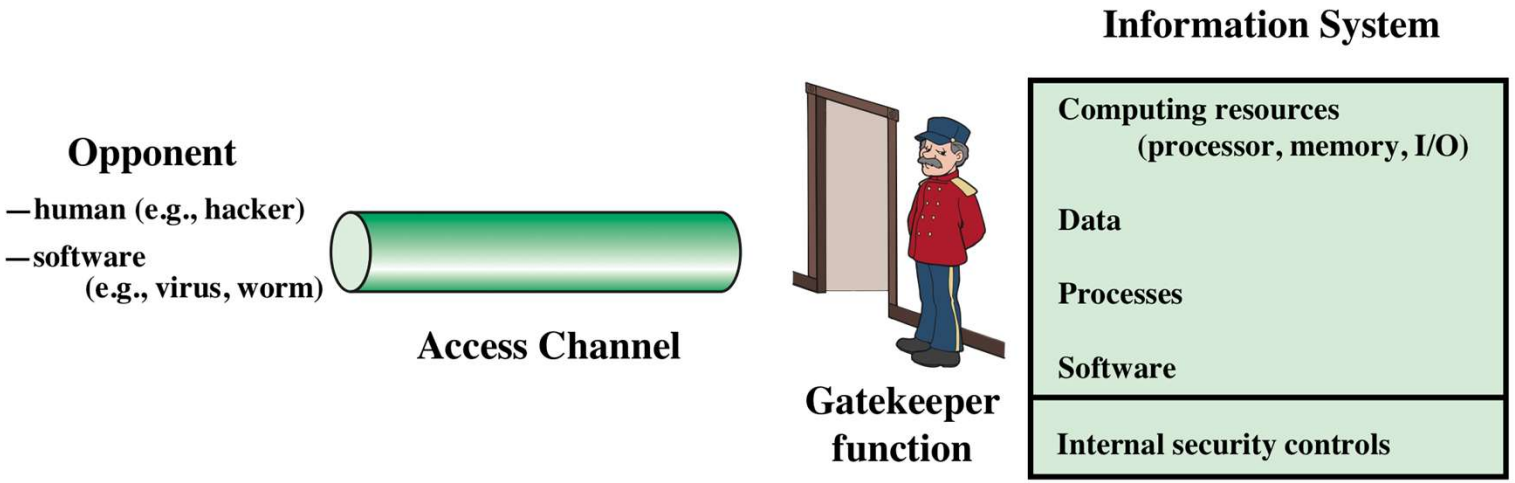


Figure 1.3 Network Access Security Model

- Select appropriate gatekeeper function to identify users
- Implement security controls to ensure only authorized users access designated information or resources

Security Layer by Layer