TERMINOLOGIES
Lecture 3d

COMPSCI 726
Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

July 22, 2021

NETWORK SECURITY

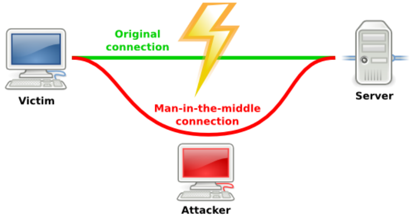
"Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment."

Source: SANS

THE OSI SECURITY ARCHITECTURE

- Security attack
  - An action that compromises security of the system and exchanged information
- Security service
  - A service that enhances security of the system and exchanged information
- Security mechanism
  - A mechanism that is designed to detect, prevent, or recover from a security attack

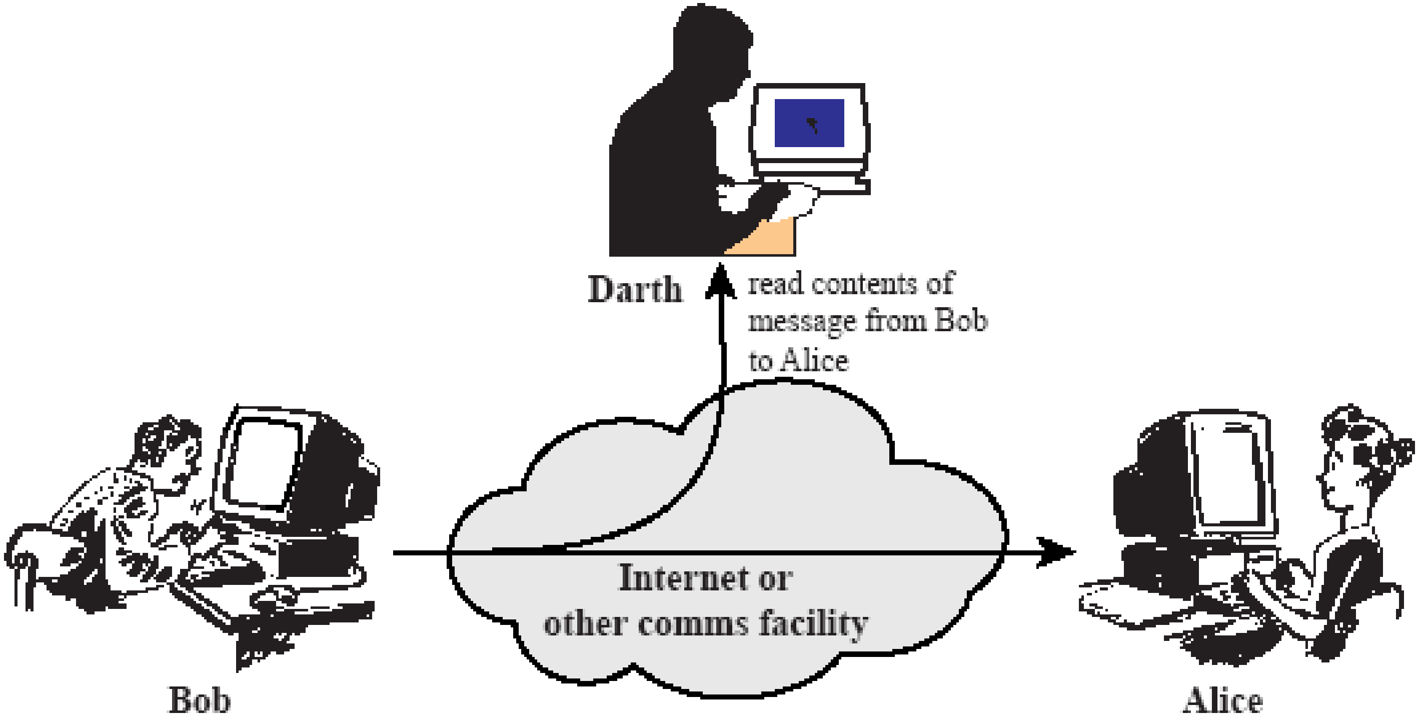
TYPES OF SECURITY ATTACKS



- Passive
  - Release of message content (disclosure)
  - Traffic analysis

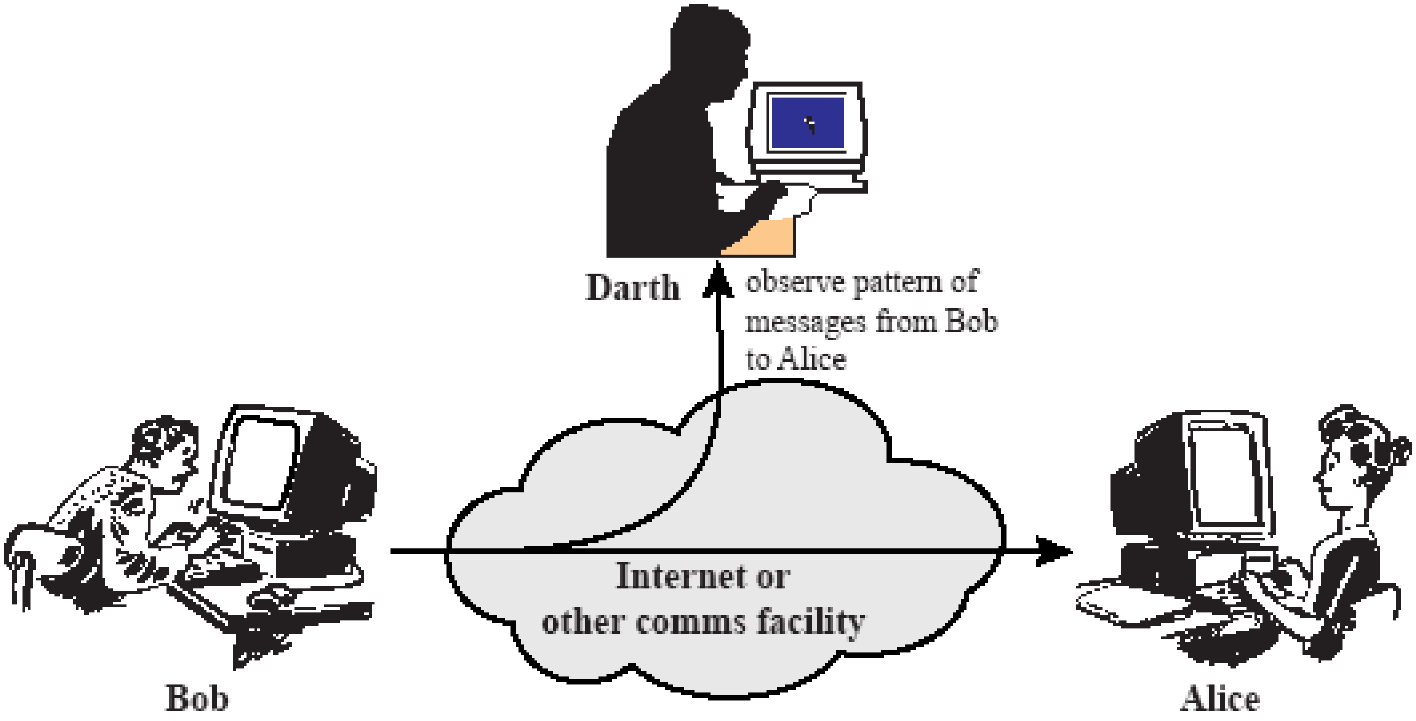
- Active
  - Masquerade
  - Replay
  - Message modification
  - Denial of Service (DoS)

RELEASE OF MESSAGE CONTENT


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

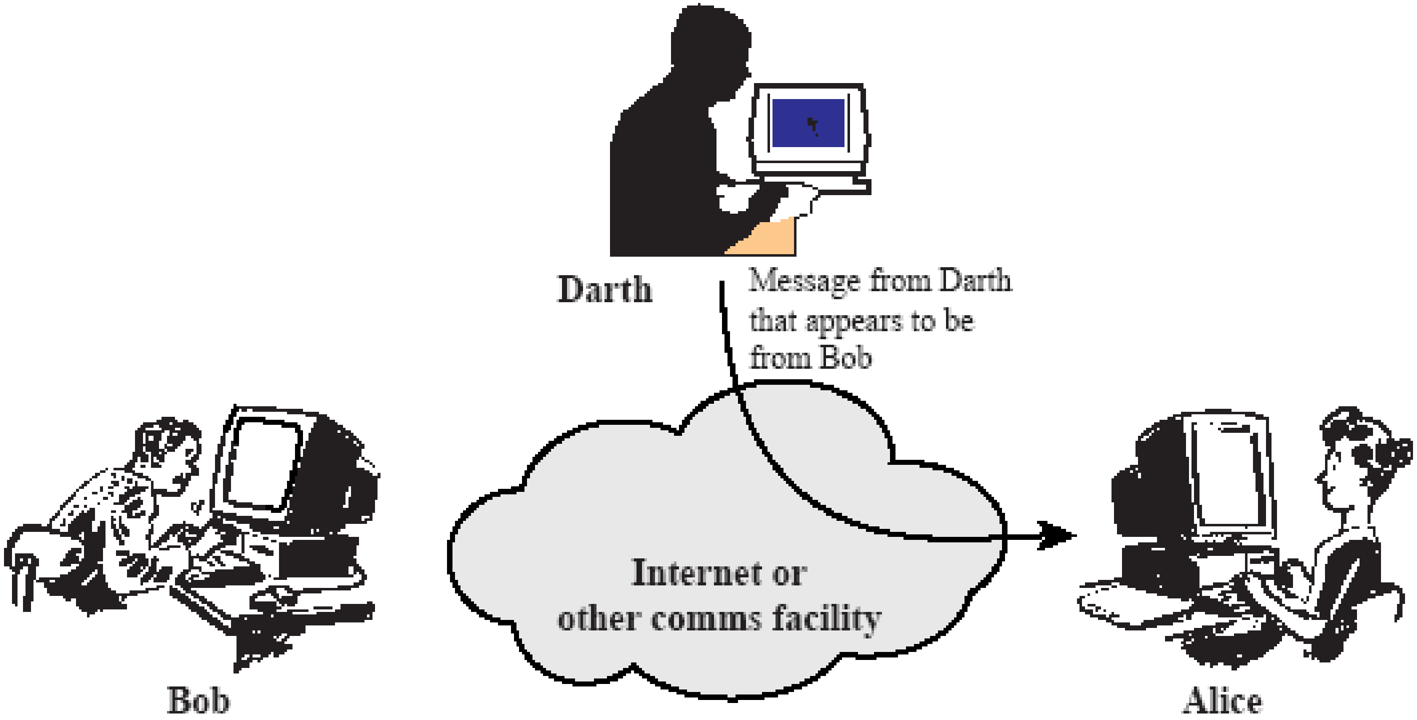
Source: **Network Security Essentials by William Stallings**

TRAFFIC ANALYSIS


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

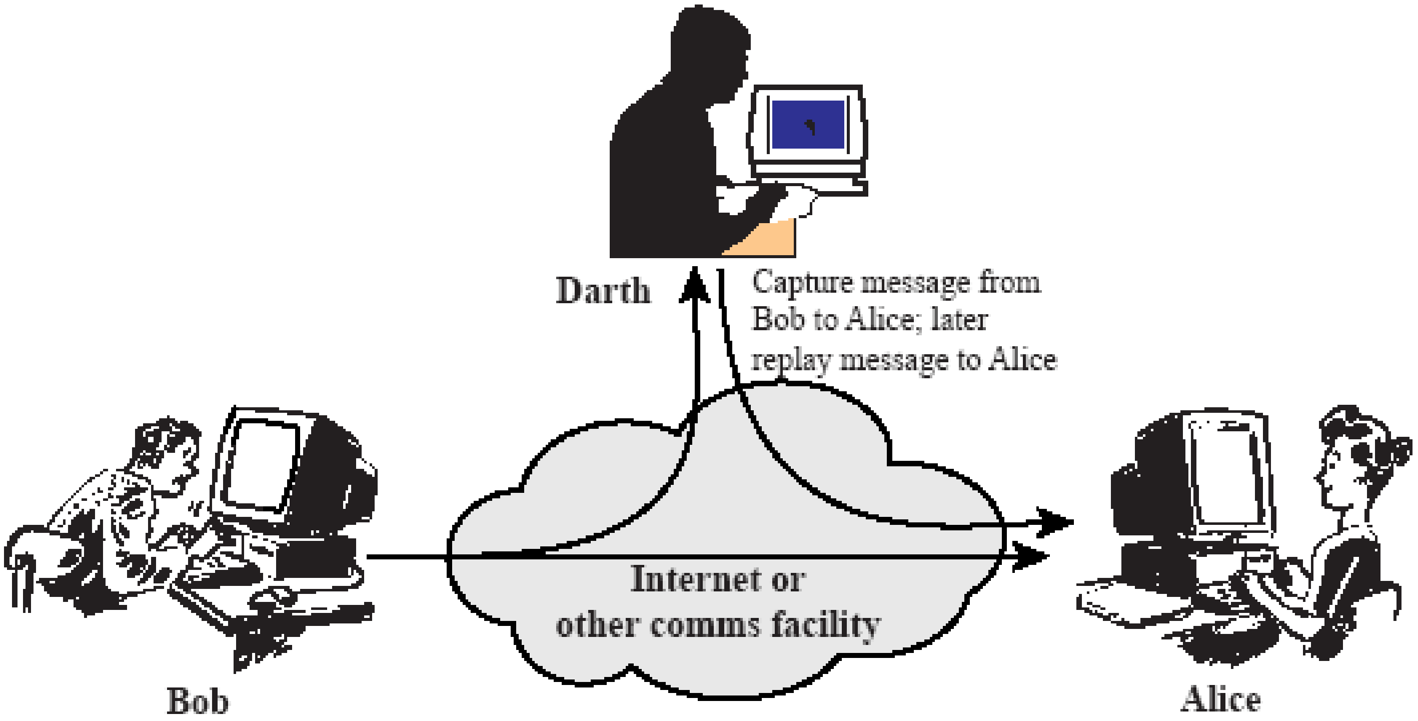
Source: **Network Security Essentials by William Stallings**

MASQUERADE


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

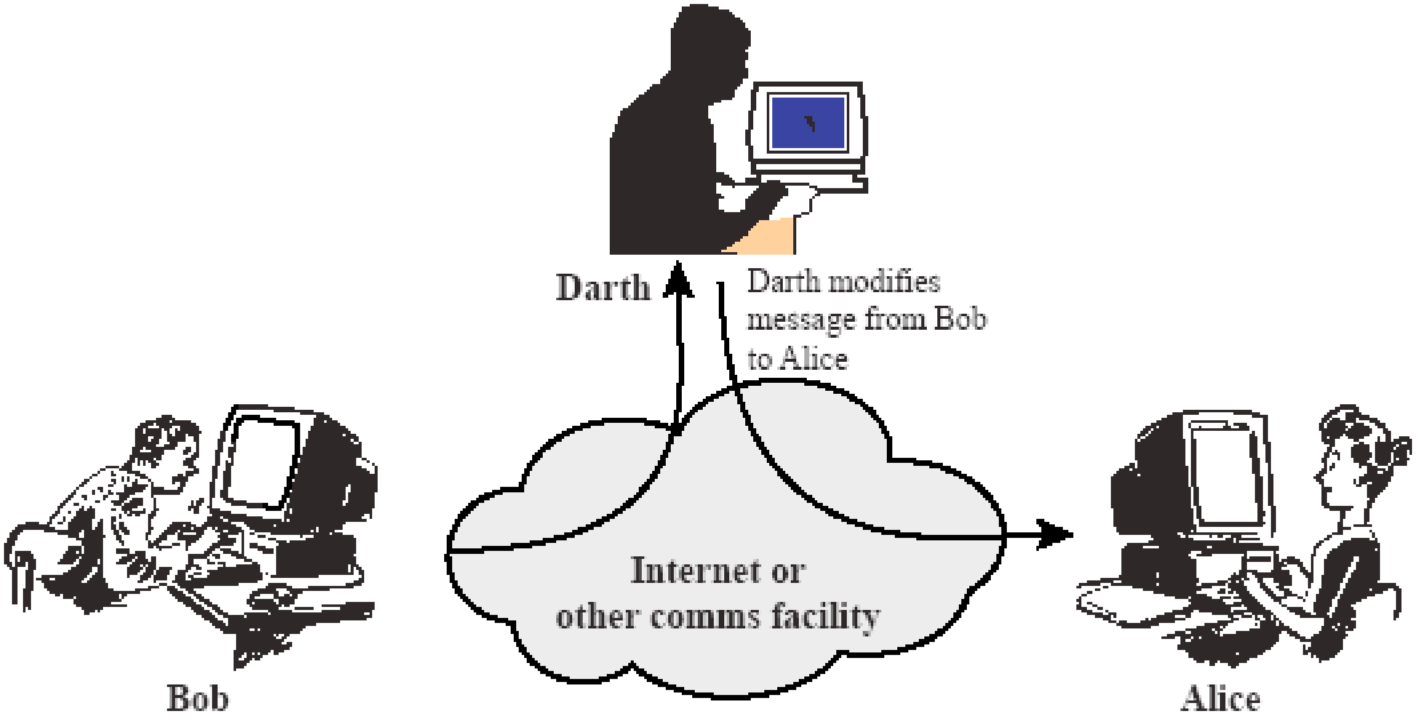
Source: **Network Security Essentials by William Stallings**

REPLAY



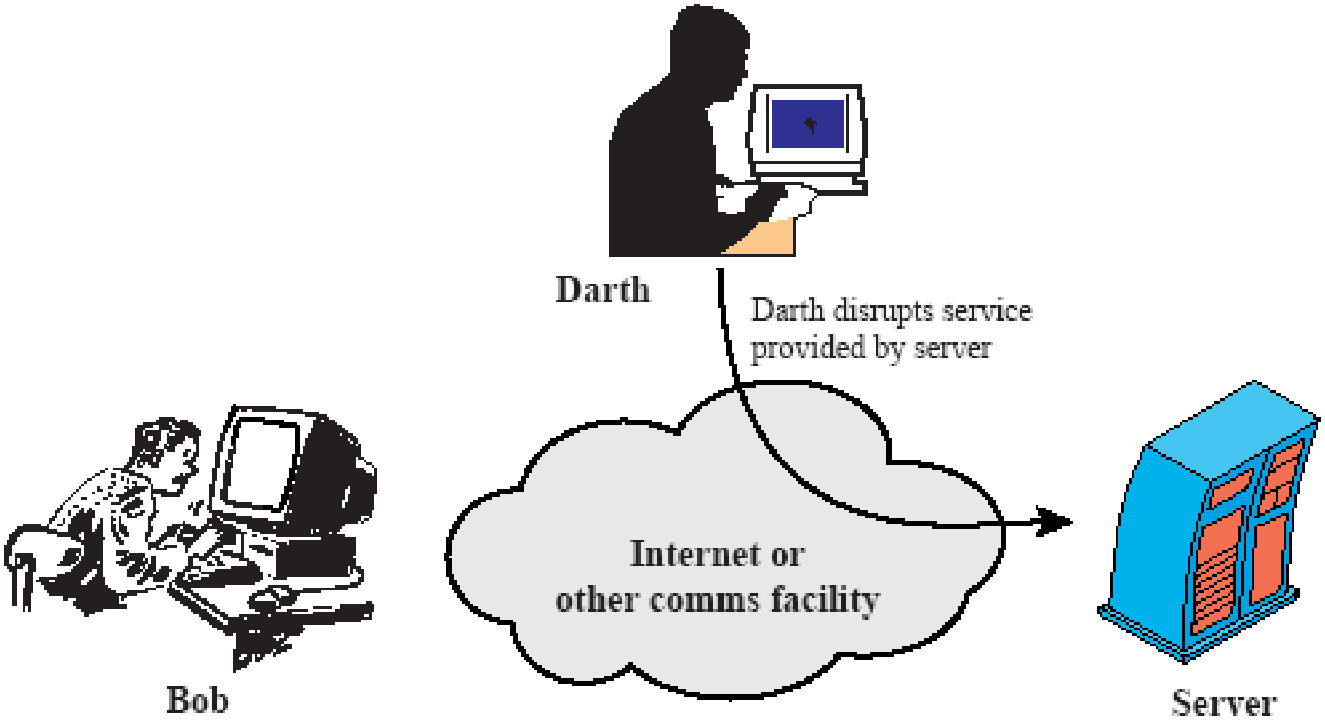
Source: **Network Security Essentials by William Stallings**

MESSAGE MODIFICATION


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Source: **Network Security Essentials by William Stallings**

DENIAL OF SERVICE (DOS)



Source: **Network Security Essentials by William Stallings**

SECURITY SERVICES

- Authentication
  - A process of identifying whether the communicating entity is the one it claims to be
- Access control (or authorisation)
  - A technique used to regulate access to resources
- Confidentiality
  - Protection of the data
- Data integrity
  - Ensuring received data is not tampered by unauthorised entities
- Non-repudiation
  - Protection against denial by communicating entities
- Availability
  - The property of a system being accessible and usable upon demand

RELATIONSHIP BETWEEN SECURITY SERVICES AND ATTACKS

Services	Release of Message Content	Traffic Analysis	Masquerade	Replay	Message Modification	Denial of Service
Authentication			✓			
Access Control			✓			
Confidentiality (Message)	✓					
Confidentiality (Header)		✓				
Data Integrity				✓*	✓	
Non-repudiation						
Availability						✓

* Using freshness

TO BE CONTINUED

- See the next lecture

Questions?

Thanks for your attention!