CT30A3401
Distributed Systems
Lecture 11

Bilal Naqvi, PhD.
syed.naqvi@lut.fi

Security

- Degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization
- **3 main goals (CIA of security)**
  - Confidentiality - Degree to which a product or system ensures that data are accessible only to those authorized to have access
  - Integrity - Degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data
  - Authenticity - Degree to which the identity of a subject or resource can be proved to be the one claimed

- **Other goals:**
  - Non-repudiation - Degree to which actions or events can be proven to have taken place so that the events or actions cannot be repudiated later
  - Accountability - Degree to which the actions of an entity can be traced uniquely to the entity
  - Availability?

Security in DS

- Due to involvement of networks for carrying data between computers, increases security threats
  - successful attacks a.k.a incidents, breaches, exploits
- Two types of security threats
  - Passive
  - Active

Passive attacks

- Includes eavesdropping on, or monitoring of, transmission
- Goal is to obtain information relating to a communication
- Two types of passive attacks
  - release of message contents
  - traffic analysis
- Release of message contents involves for e.g., the release of a confidential e-mail or the contents of a transferred file

Traffic analysis

- More subtle
  - attacker might be able to observe the pattern of the messages
  - attacker could determine the location and identity of communicating hosts and could observe the frequency and length of the messages being exchanged
  - information might be useful in guessing the nature of the communication

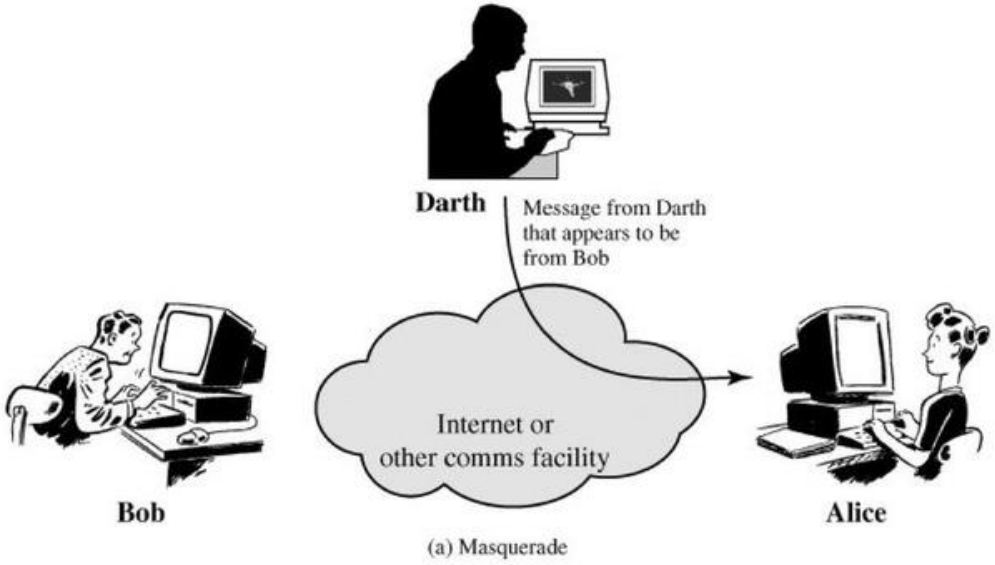
- Passive attacks are very difficult to detect because they do not involve any alteration of data
  - it is possible to prevent these, hence the emphasis is on prevention rather than detection

Active attacks

- Active attacks involve some modification of the transmitted data, or the creation of false transmissions and can be subdivided into four categories:
  - A masquerade takes place when one entity pretends to be a different entity
  - Replay involves the passive capture of data and its subsequent retransmission to produce an unauthorized effect
  - Modification of messages simply means that some portion of a legitimate message is altered, or that the messages are delayed or reordered, to produce an unauthorized effect
  - A denial-of-service attack prevents or inhibits the normal use or management of communication facilities

Masquerade

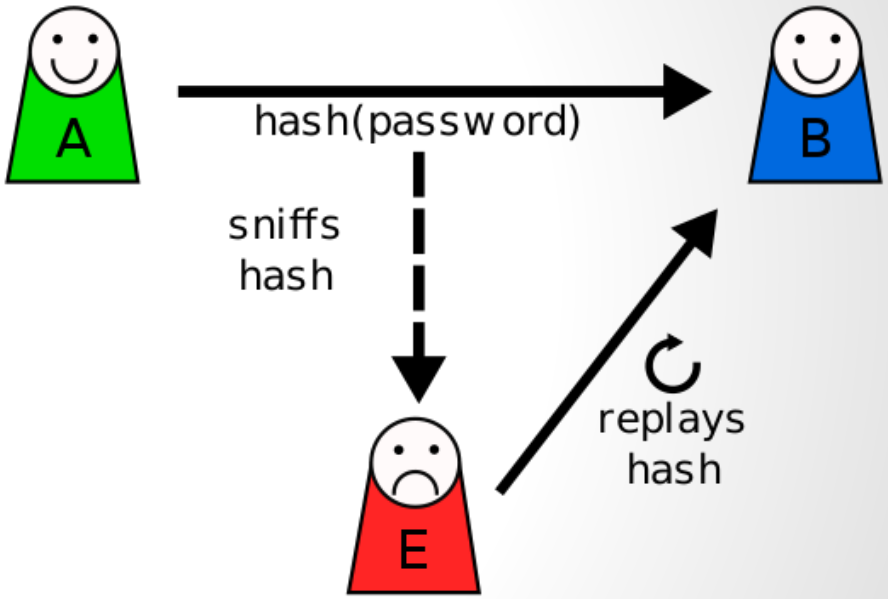
- A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification



Active Attack – Masquerade

Replay attack

- A replay attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed
- This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a spoofing attack by IP packet substitution



Modification of message

- It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect
  - For example, a message meaning

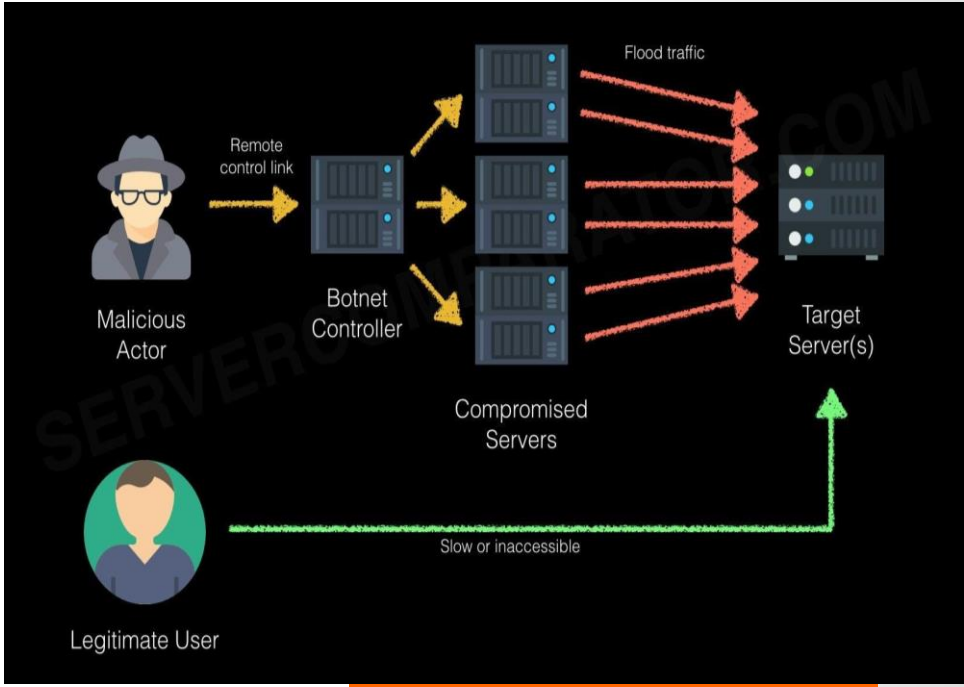
    “Allow JOHN to read confidential file X” is modified as

    “Allow Smith to read confidential file X”

Denial of service (DoS or DDOS)

- It prevents normal use of communication facilities (targets availability of services)
  - may have a specific target
  - an entity may suppress all messages directed to a particular destination

- Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages to degrade performance



Active vs Passive attacks

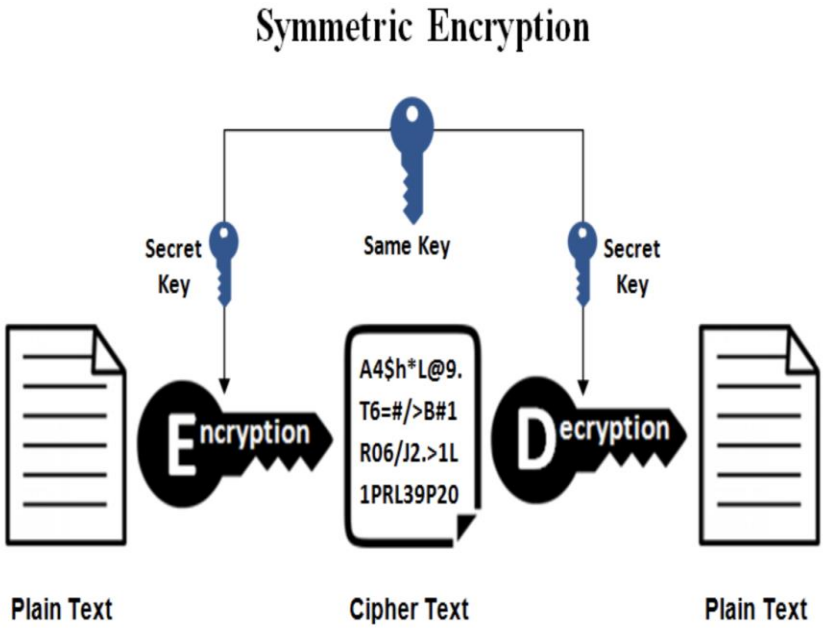
- Active attacks present the opposite characteristics of passive attacks
- Passive attacks are difficult to detect, measures are available to prevent their success
- It is quite difficult to prevent active attacks absolutely, because to do so would always require the physical protection of all communications facilities and paths

Protection mechanisms

- Encryption is the most common tool deployed for security
- Two types:
  - conventional encryption, also known as symmetric encryption
  - public-key encryption, also known as asymmetric encryption
- With symmetric encryption, two parties share a single encryption/decryption key
  - main challenge is the distribution and protection of the keys
- A public-key encryption scheme involves two keys, one for encryption, and a paired key for decryption
  - party that generated the key pair keeps one key private, and the other is made public

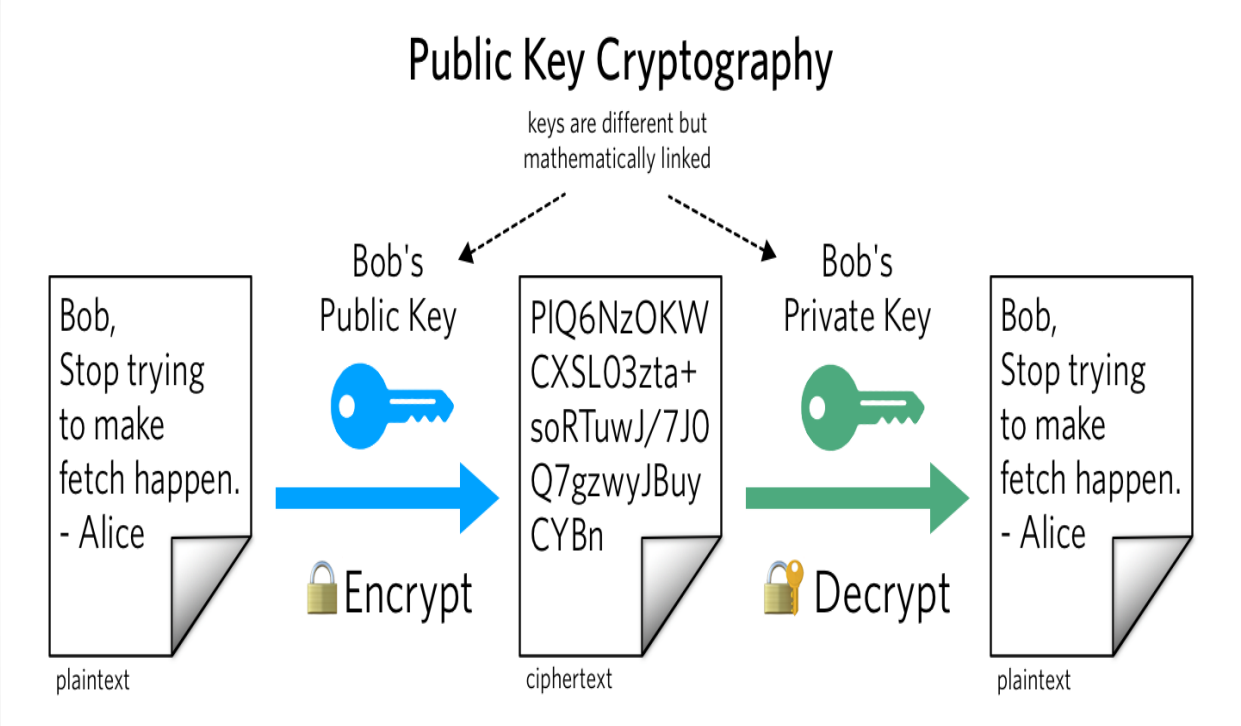
Symmetric encryption

- Plain text
- Cipher
  - Encryption/decryption algorithm
- Key
  - length
- Cipher text



Public key encryption

- Works with a pair of specially generated keys
  - Each user generates a pair of keys
  - Each user places one of the two keys in a public register or accessible file. This is the public key. The companion key is kept private. Each user maintains a collection of public keys obtained from others
  - If Alice wishes to send a private message to Bob, Alice encrypts the message with Bob's public key
  - When Bob receives the message, he decrypts it using his private key
    - No other recipient can decrypt the message because only Bob knows his private key
- Also used for digital signatures
- Expensive to deploy but needed


Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
Encrypt
PlQ6NzOKW CXSL03zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext
ciphertext
plaintext

Hashing

- A hash function is any function that can be used to map data of arbitrary size to fixed-size values
- The values returned by a hash function are called hash values, hash codes, digests, or simply hashes
- Used for verifying integrity of messages