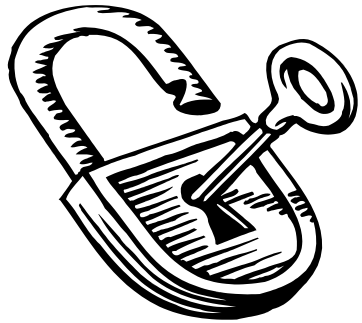


Introduction To Network Security

Security..... continuous process of protection

What it reveals is trivial and
what it conceals is vital.

What is “Security”?

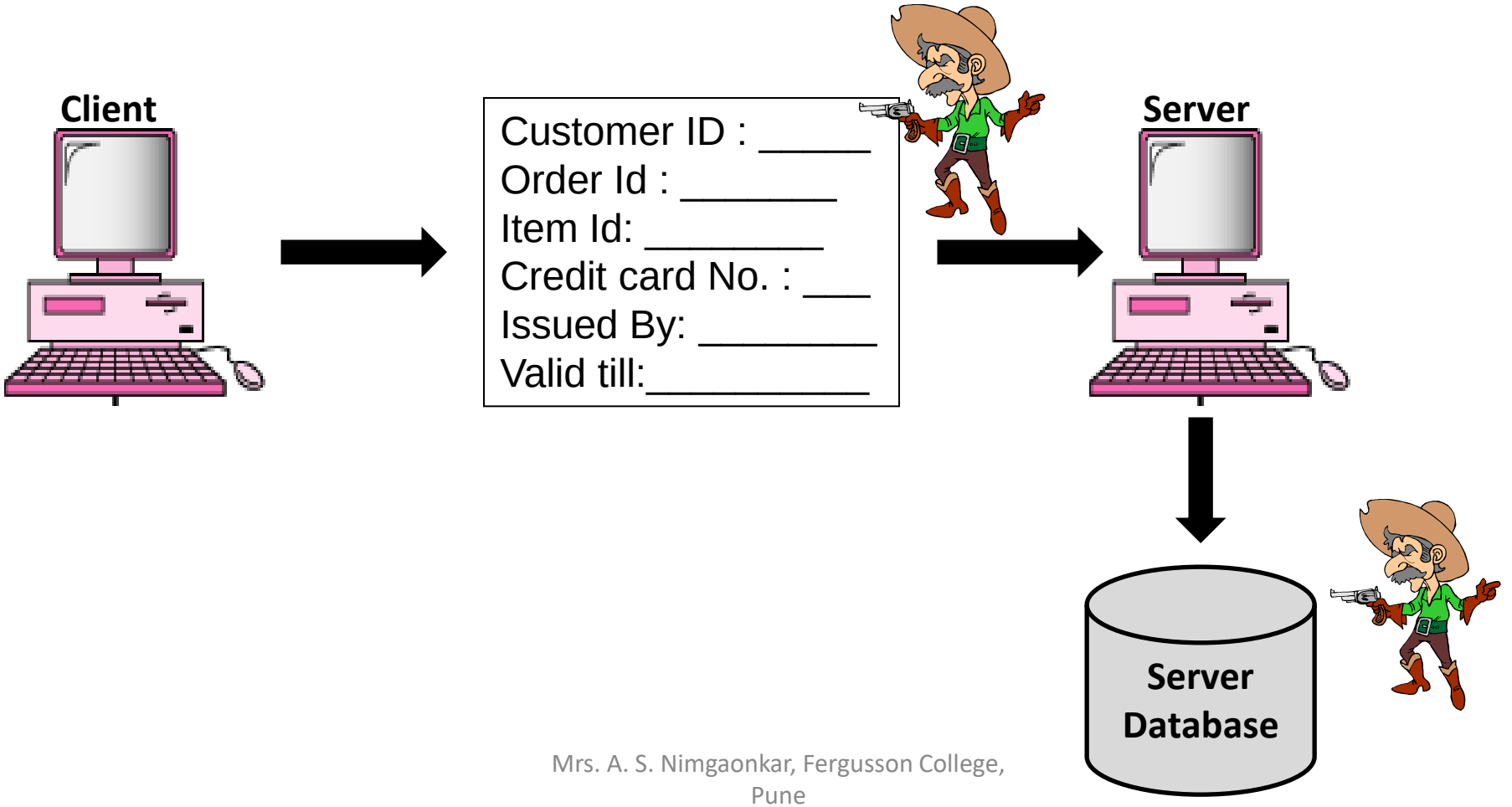
Dictionary.com says:

1. Freedom from risk or danger; safety.
2. Freedom from doubt, anxiety, or fear; confidence.
3. Something that gives or assures safety

Why do we need security?

- Protect vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Provide authentication and access control for resources
  - Ex: Banking
- Guarantee availability of resources

Why do we need security?



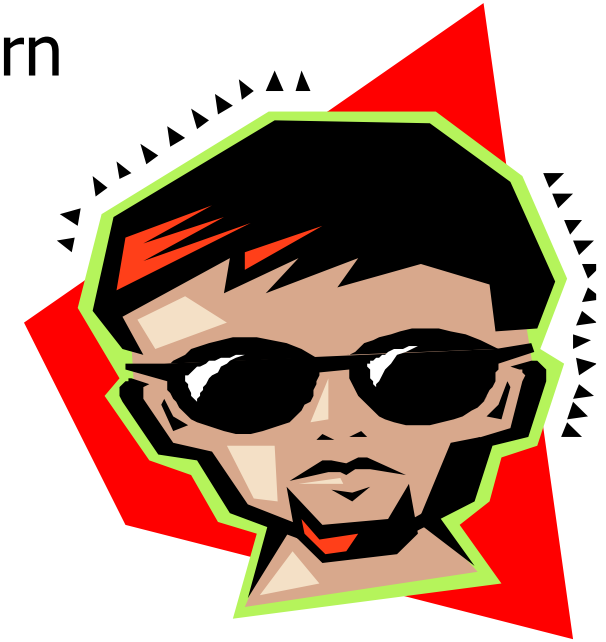
Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations

ANYONE ON THE NETWORK

Attacker Motivations

- Money, profit
- Access to additional resources
- Experimentation and desire to learn
- "Gang" mentality
- Psychological needs
- Self-gratification
- Personal revenge
- Desire to embarrass the target



Security Approaches - Security Models

Organization can take several approaches to implement it's security model.

- No security :- Implement no security at all.
- Security through obscurity :- Nobody knows about it's existence and contents.
- Host security:- Security is enforced individually for each host.
- Network Security :- focus is to control network access to various hosts & their services rather than individual host.

Security policy

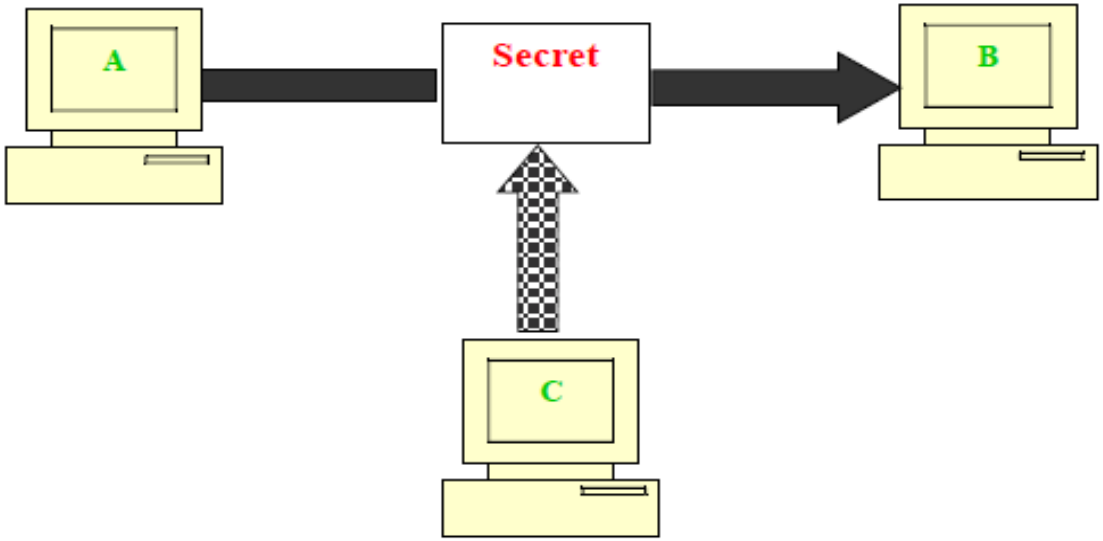
- Affordable - In the terms of cost & effort in security system.
- Functional – Should provide expected security mechanism.
- Legal - Should meet the legal requirements.
- Cultural Issues – Should be according to people's expectations , working style and belief.

Security Principals

1. Confidentiality
2. Authentication
3. Integrity
4. Non repudiation
5. Access control
6. Availability

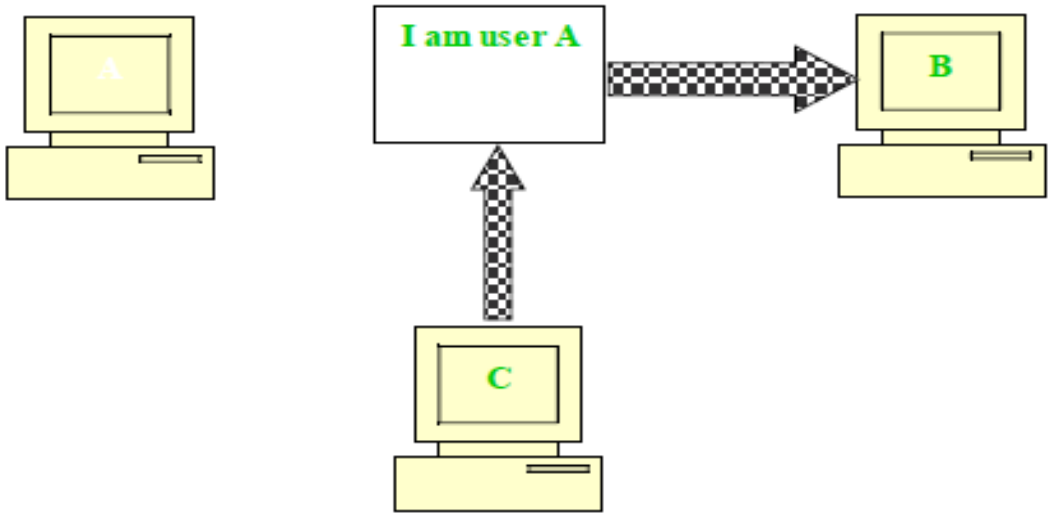
Security Principals

- **Confidentiality** – It specifies that only the sender and the intended recipients should be able to access the contents of a message



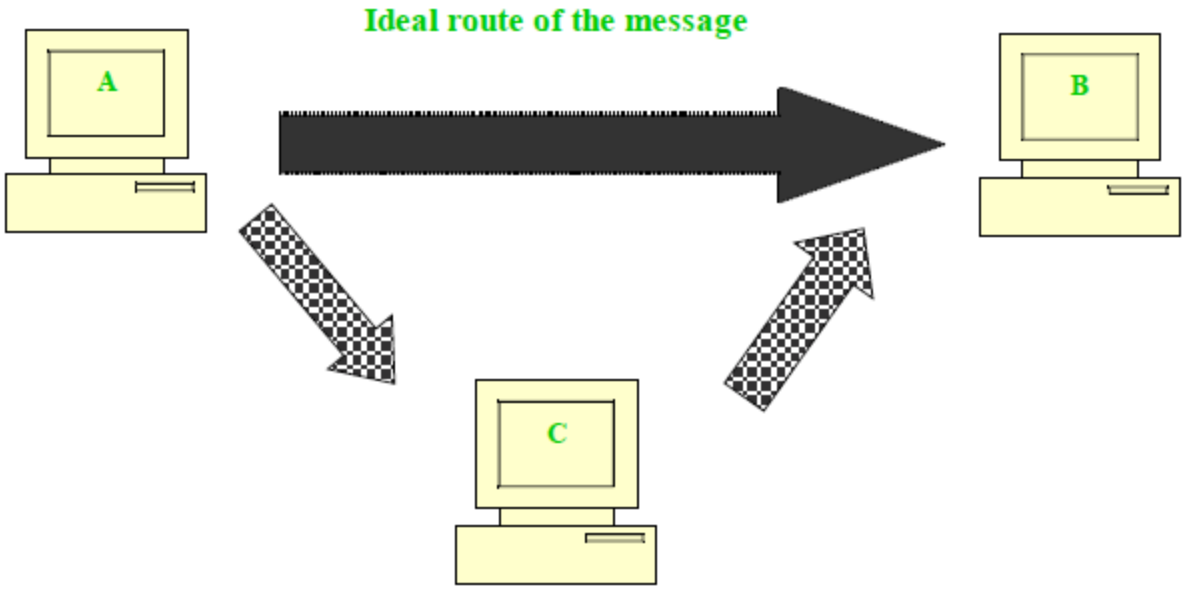
Security Principals

- **Authentication** – It helps to establish proof of identities.



Security Principals

- **Integrity** : When the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.



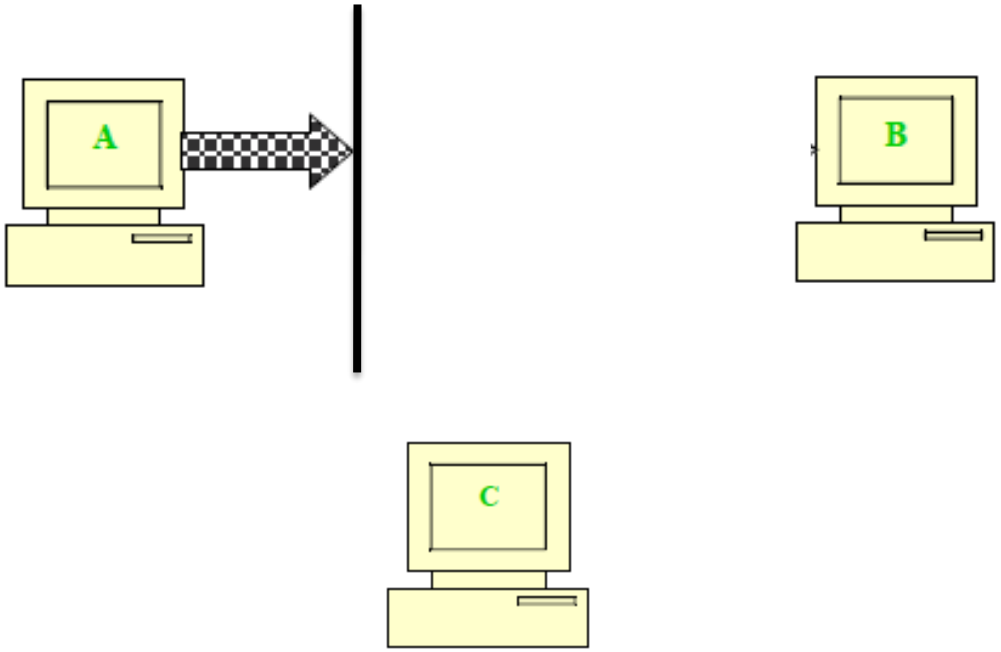
Security Principals

- **Non repudiation** : There are situations when user sends a message and later on refuses that she had he/she had sent that message.

Security Principals

- **Access Control** : Who should be able to access what?

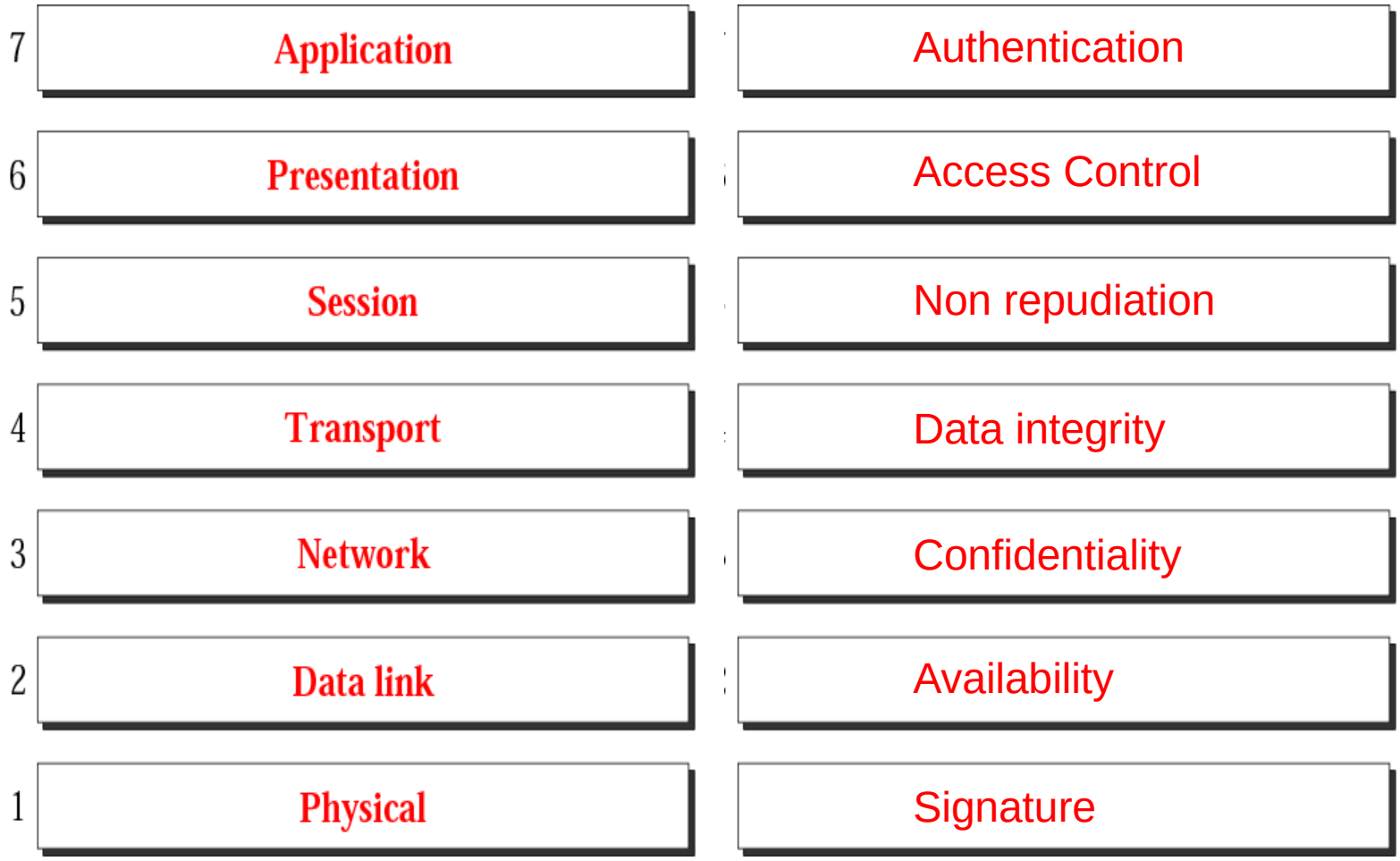
- **Availability** : Resources should be available to all authorized users.



Security Principals

- A sends a file to B: E intercepts it and reads it – (confidentiality)
- A send a file to B: E intercepts it, modifies it, and then forwards it to B -(Integrity)
- E sends a file to B pretending it is from A – (Authentication)
- A sends a message to B. Later A (or B) denies having sent (received) the message. – (Non-repudiation)
- E learns which user accesses which information although the information itself remains secure. (access control)

OSI Standard for Security Model

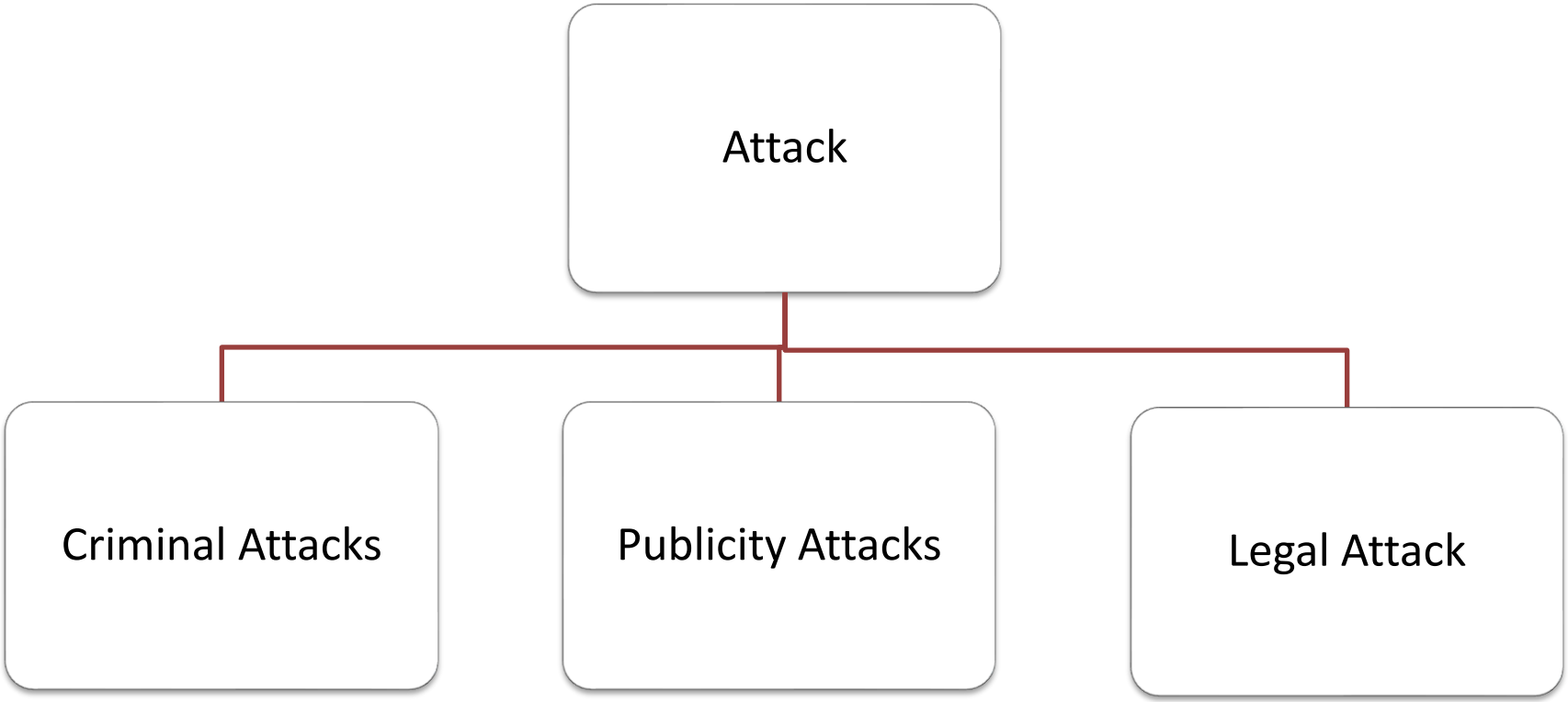


Attack

- Attack
  - Tends to be an undesirable act which is in process that may cause cracking of a message.
  - Any action that compromises the security of information owned by an organization.
- Threat
  - Tends to be a promise of an attack to come.

Information security is about how to prevent attacks, or to detect attacks on information-based systems

Types Of Attacks.. A General View



Criminal Attack

- Sole aim is of the attacker is to maximize financial gain by attacking computer system.
- Type of criminal attacks
  - Fraud – manipulation of e-money, credit cards, checks etc.
  - Scams – People are enticed to send money in return of great profit.
  - Destruction – Some sort of grudge is the motive behind such attack.
  - Identity theft – attacker does not steal anything from the a user, he becomes the user.
  - Intellectual property theft – stealing companies trade secrets , databases etc
  - Brand theft - Fake website.

Publicity Attack

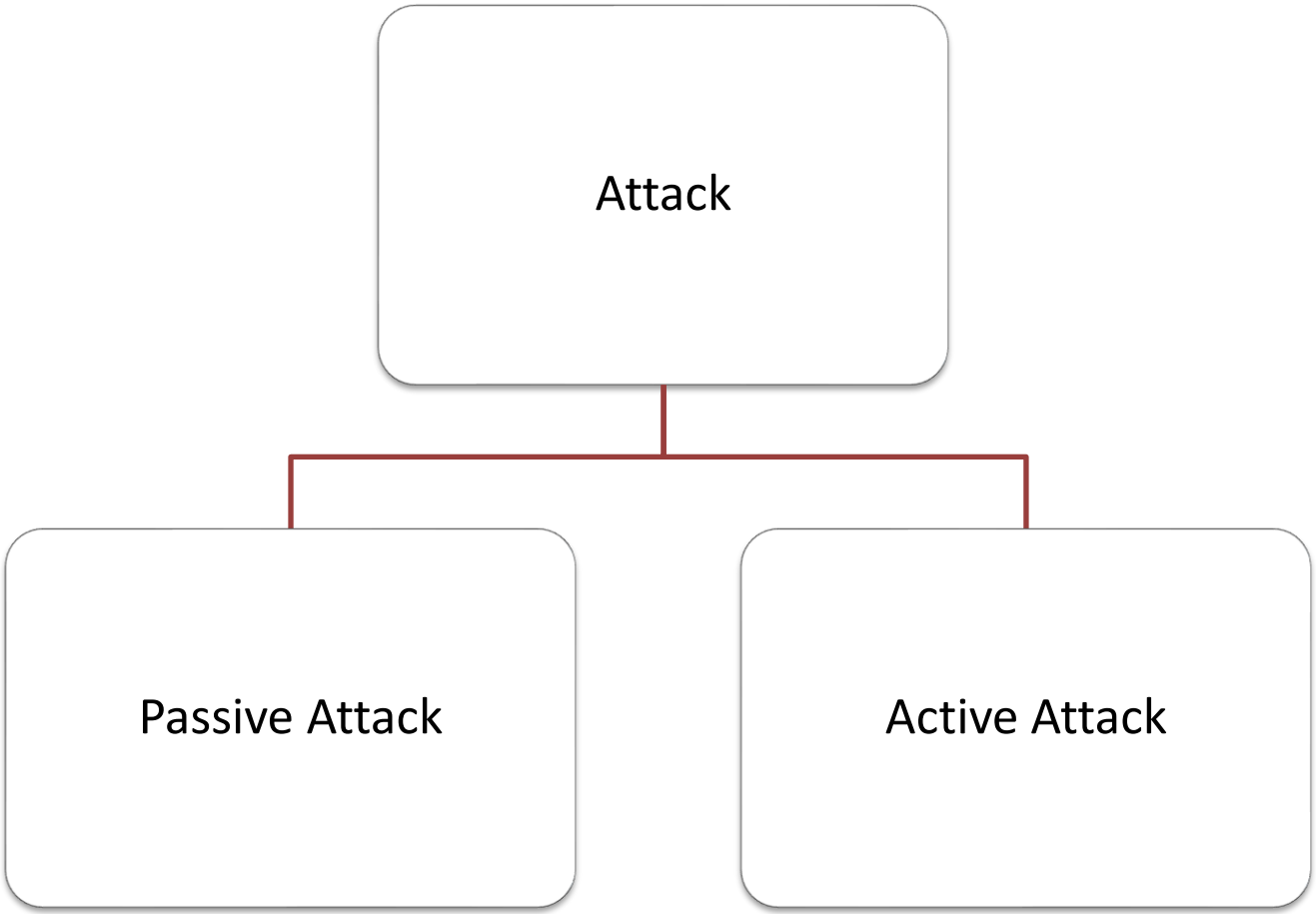
- In such attacks, attacker wants to see their names appear on the television news channels and newspapers.

- Attackers are not hardcore criminals.

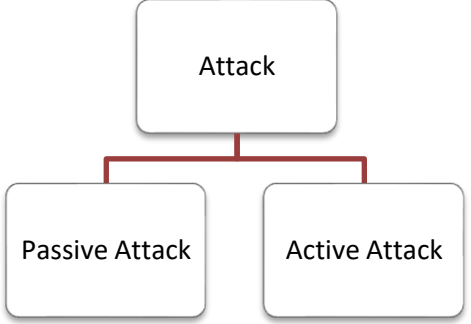
Legal Attack

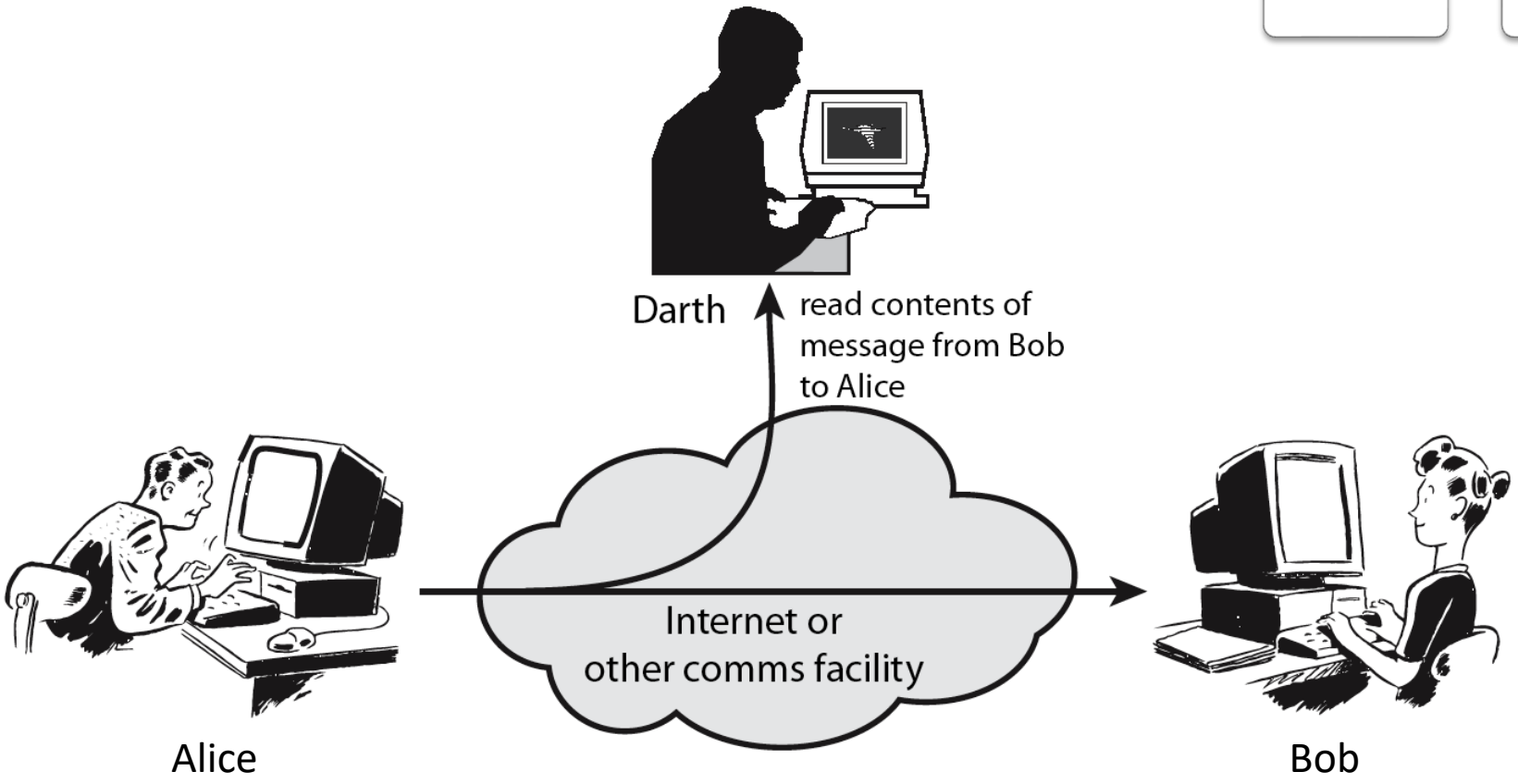
- This type of attack is quite novel and unique.
- The aim of the attacker is to exploit the weakness of the judge.

Types Of Attacks... A Technical View



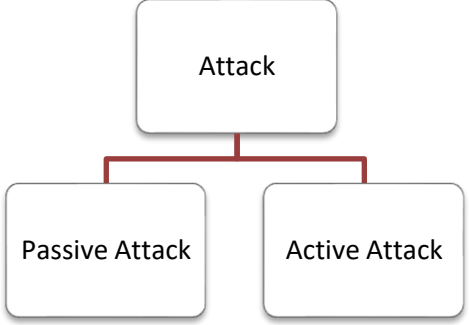
Passive Attacks

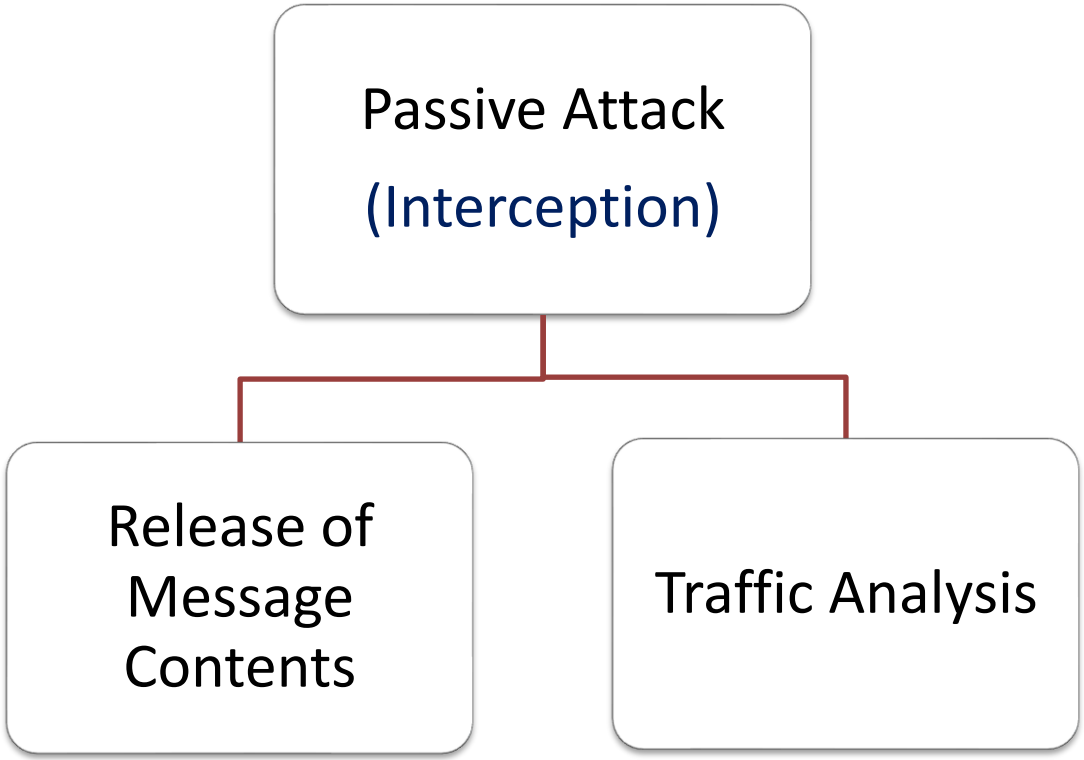




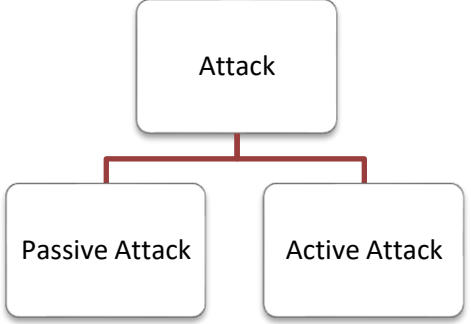
The attacker only monitors the traffic that attacks the confidentiality of the data.

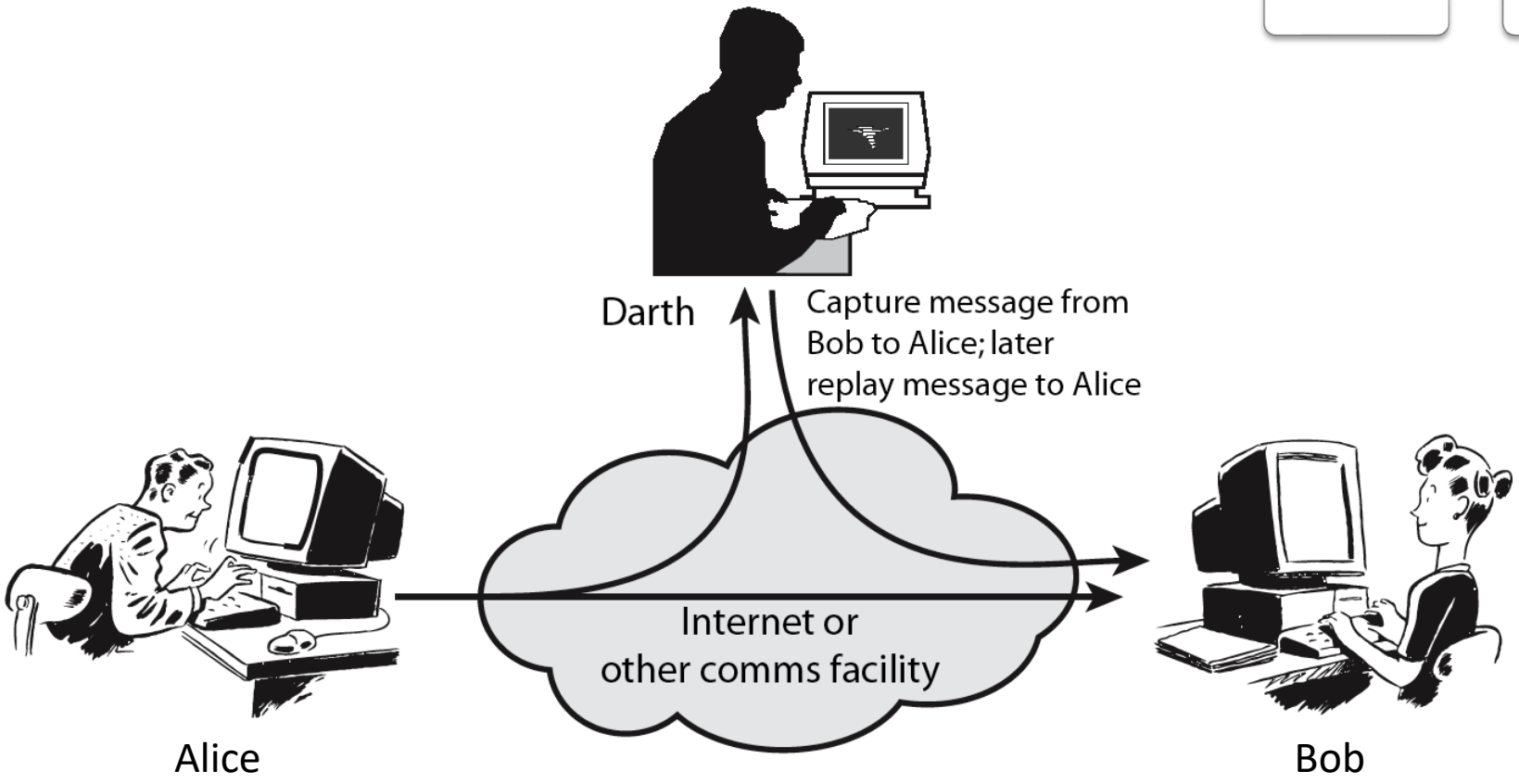
Types - Passive attack





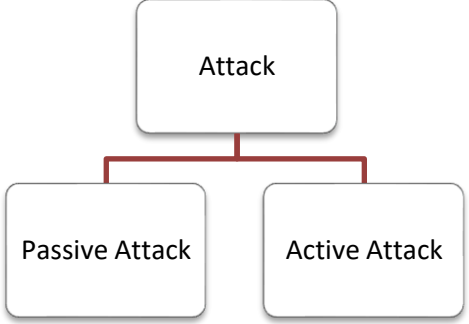
Active Attacks

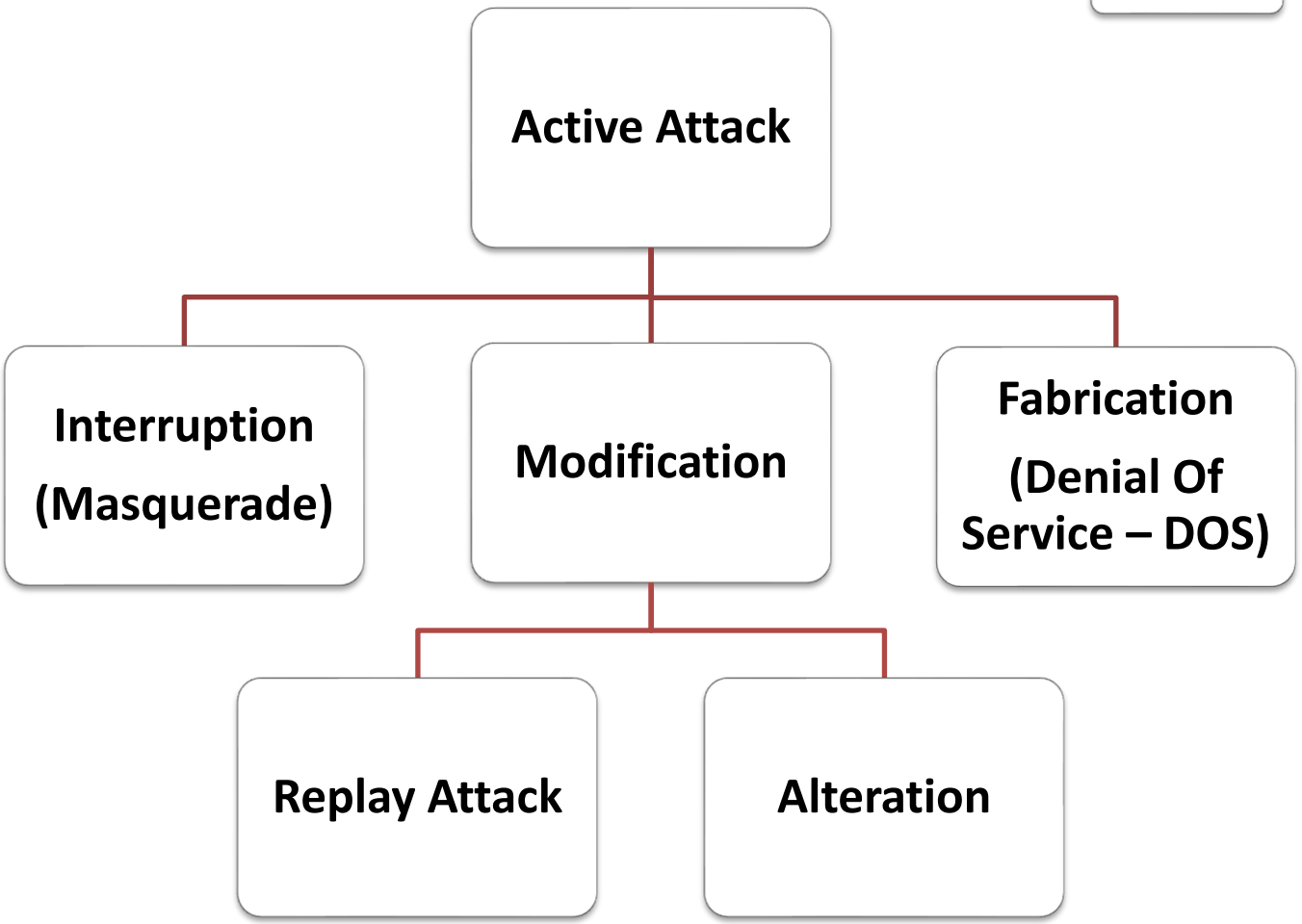




The attacker captures the message and modifies the contents of the original message.

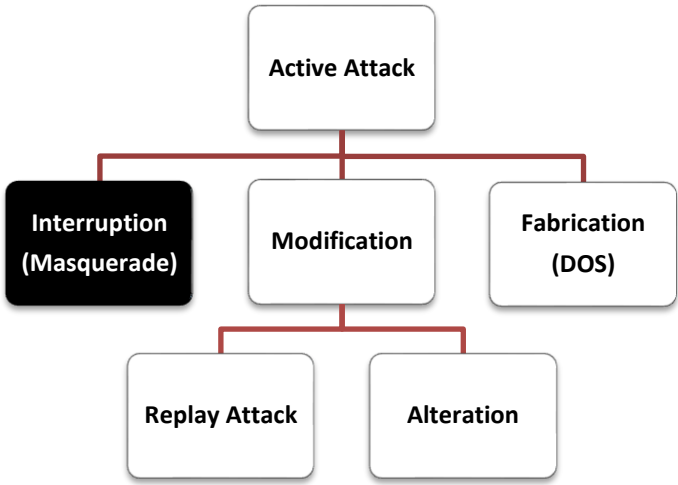
Types - Active attack





Types - Active attack

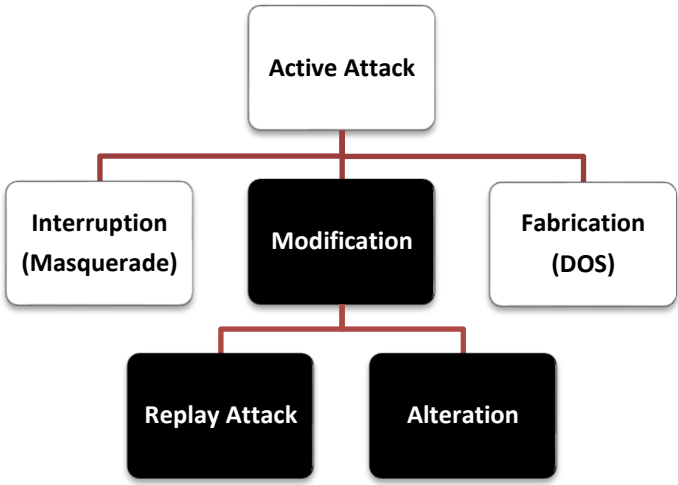
Interruption



- Interruption Attack is also called as masquerade.
- It is caused when unauthorized entity pretend to be another entity.
- *Causes loss of message authenticity.*

Types - Active attack

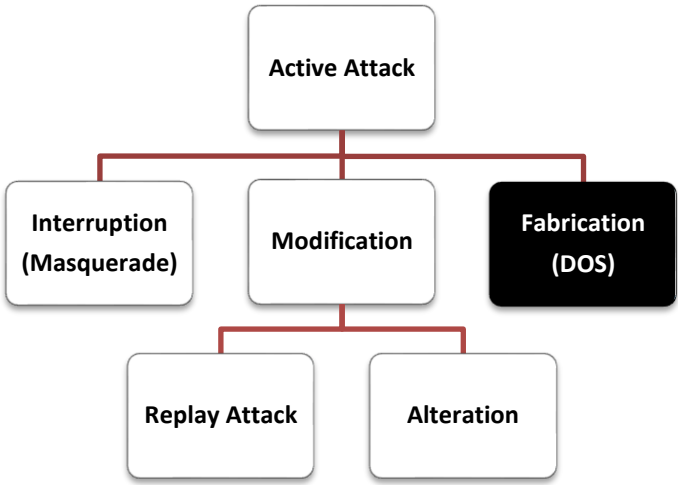
Modification



- Modification attacks can be classified into replay attack and alteration.
- In replay attack, attacker captures the sequence of events or data and resends them.
- In alteration attack, attacker makes some changes to the original message.
- *Causes loss of message integrity.*

Types - Active attack

Fabrication

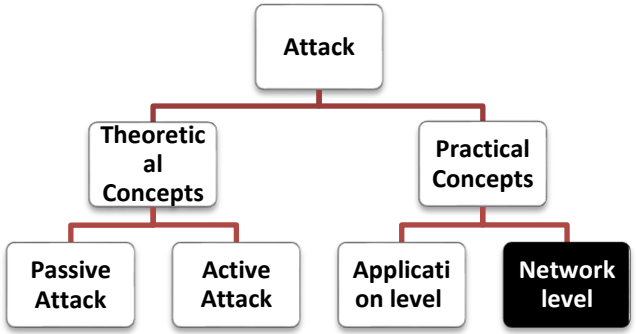


- Fabrication is also called as Denial Of Service (DOS).
- This attack makes attempt to prevent authorized users from accessing some services for which they are eligible.
- *Causes in case of poor authentication mechanism.*

Applications Attack

- Attacks happen at application level.
- Attacker attempts to access, modify or prevent the access to the information of a particular application or application itself

Network Attack



- Attacks happen at network level.
- Attacker attempts to reduce the capabilities of the network by number of possible means such as to either slow down the or completely bring to halt a computer network.

Programs Those Attack

- Virus – Piece of program that attaches itself to another legal program.
- Worm – It replicates itself again and again to consume system resources to bring it down.
- Trojan Horse – It attempts to reveal confidential information to the attacker.
- Applet and ActiveX Controls , Cookies , Java scripts, VB Scripts - all these programs cause security problems if used by attackers with a malicious intension.

Virus Phases

Dormant Phase – Virus is idle. It gets activated based on some event or certain action.

Triggering Phase – Dormant virus moves into this phase when action/event for which it was waiting, is initiated.

Propagation Phase – Virus copies itself & each copy starts creating more copies of self.Thus propagating the virus.

Execution Phase – This is actual work of virus which could be harmless or destructive.

Virus Classification

- Parasitic – Attaches itself to executable file & keeps replicating.
- Memory resident – Attaches itself to an area of the main memory.
- Boot sector – Infects the master boot record of disk & spreads on the disk when the o.s. starts booting.
- Stealth virus (Polymorphic) – prevents anti virus software program from detecting itself. Keeps changing it's signature.
- Metamorphic – along with signature, keeps rewriting itself every time.

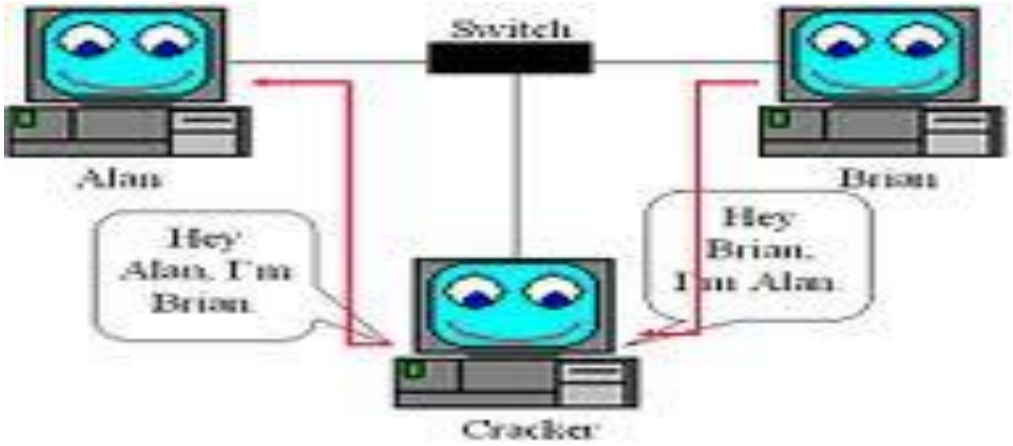
Some terminologies

- Sniffing
- Phishing
- Pharming (DNS spoofing)

Sniffing (Snooping).... hampers Confidentiality

- In a security context, is ***unauthorized access to another person's or company's data.***
- (Sniffing) Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.
- More sophisticated sniffing uses software programs to remotely monitor activity on a computer or network device.

Spoofing (Packet Spoofing)...hampers integrity

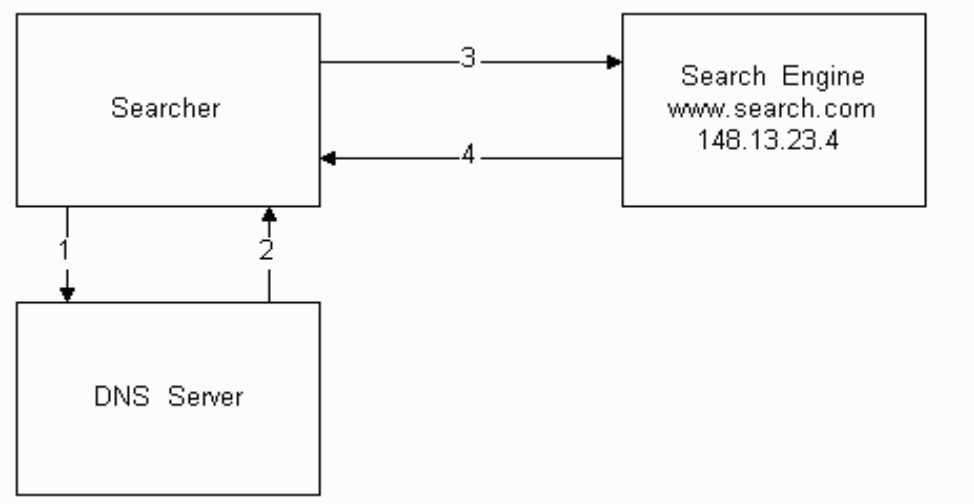


- Attacker attacks on the message travelling from source to destination.

Attacker changes the sender information of the message and send message to receiver.

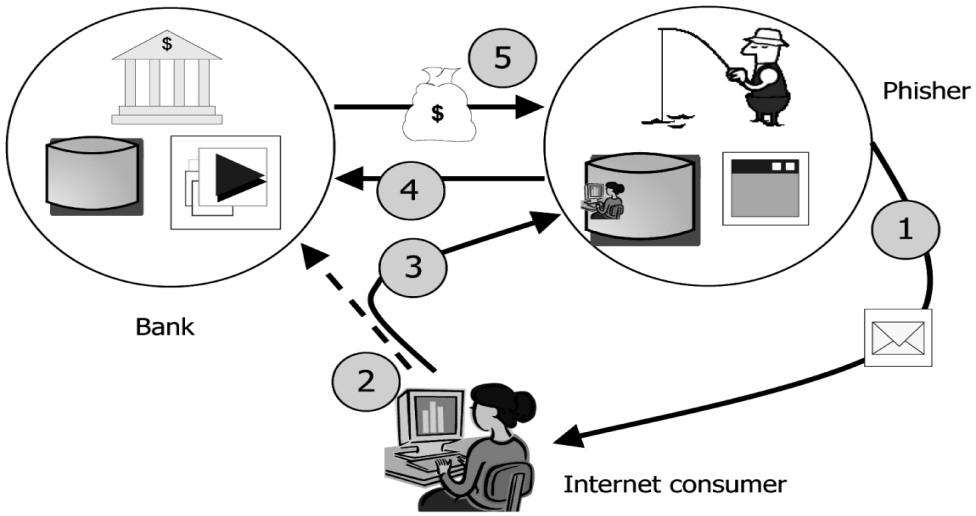
- When receiver receives the message, he sends replies back to this forged address (called as spoofed address) and not to the attacker.

DNS Spoofing (Pharming)



- **DNS spoofing** (or **DNS cache poisoning**) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) name server's cache database, causing the name server to return an incorrect IP address, diverting traffic to another computer (often the attacker's).

Phishing



- A criminal activity using social engineering techniques.
- ***Phishers attempt to fraudulently acquire sensitive information***, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.
- Phishing is typically carried out by email or instant messaging, and often directs users to give details at a website, although phone contact has been used as well

Phishing

amazon.com.

Dear Customer,

- Due to recent account takeovers and unauthorized listings, Amazon is requesting a new account verification procedure. From time to time, randomly selected accounts (seller and/or buyer)are placed under an advanced updating process based on merchant accounts/bank relationsand on-file credit cards. Amazon may also request in an email message scanned/faxed copies of one or more photo ID's. Your account confirmation may go wrong if your credit card/bank account has expired, or if you have changed/replaced your credit card without letting us know about the change.

- Your account is not suspended, but if in 36 hours after you receive this message your account is not confirmed we reserve the right to terminate your Amazon subscription.
- If you received this notice and you are not an authorized Amazon account holder, please be aware that it is in violation of Amazon policy to represent oneself as an Amazon user. Such action may also be in violation of local, national, and/or international law.
- Amazon is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft.
- Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the full extent of the law.

To confirm your identity with us click the link bellow:

- http://www.amazon.com/exec/obidos/sign-in.html

We apologize in advance for any inconvenience this may cause you and we would like to thank you for your cooperation as we review this matter.

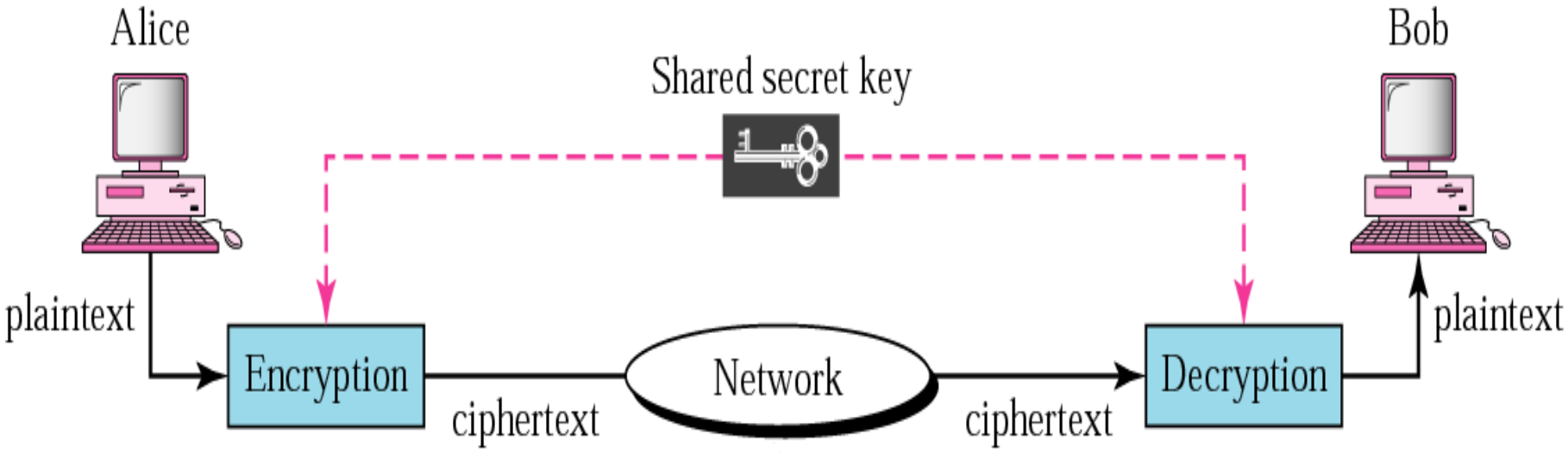
Respectfully,
Amazon.com, Inc.

Terminology – cryptoterms

- Cipher – secret or disguised writing (= zero)
- Cryptology – The science of secure (often secret) communication
- Cryptography – The study of principles and techniques through which information can be hidden in a cipher (= secret writing)
- Cryptanalysis – The science and art to recreate the information from a cipher without knowing the key (before hand). Also it is used to to find some insecurity (if any) in a cryptographic scheme.
- Cryptanalyst - Is a person who attempts to break a cipher text message to obtain the original plain text message.

Basic situations in cryptography

- It is nothing but a secret writing.
- Art of achieving security by encoding messages to make them non-readable.



Basic situations in cryptography

- It is nothing but a secret writing.

- Art of achieving security by encoding messages to make them non-readable.