CO-INS:Information and Network Security

UNIT-I

Course Instructors:

Soma Saha

Virendra Srivastava

Soma Saha (PhD)

Department of Computer Engineering
SGSITS Indore, India

Feb 2021

Soma Saha

Information Security

- What is Information?
- Why do we need security?
  1. Past

Information Security

- What is Information?
- Why do we need security?
  1. Past
  2. Present

Information Security in an Enterprise

”well-informed sense of assurance that the information risks and controls are in balance.”–James Anderson, executive consultant at Emagined Security, Inc.

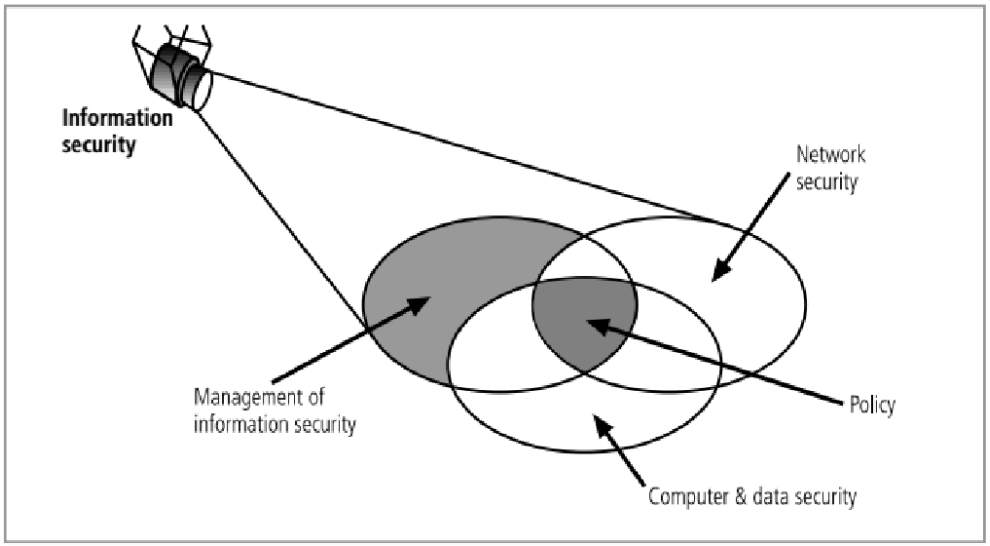


Figure 2: Components of Information Security.

Need for Security

Adversary	Goal
Student	To have fun snooping on people's e-mail
Cracker/Hacker	To test out someone's security system &/ steal data
Sales Rep.	To claim to represent all of Europe, not just Seychelles
Businessman	To discover nearest competitors strategic marketing plan
Ex-Employee	To get revenge for being fired
Accountant	To embezzle/rob money from a company
Stockbroker	To deny a promise made to a customer by e-mail
Spy	to learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets
Con Man	To steal credit card numbers for sale

Who is vulnerable?

- Government and defense agencies
- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

Security Terminologies

- Information Security
- Network Security
- Cyber Security

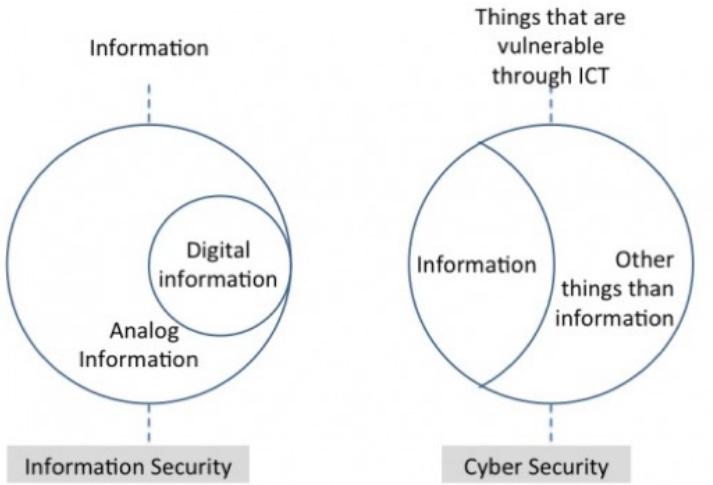


Figure 3: Information-ICT-Cyber Security.

InfoSec, ICT Security, Cyber Security

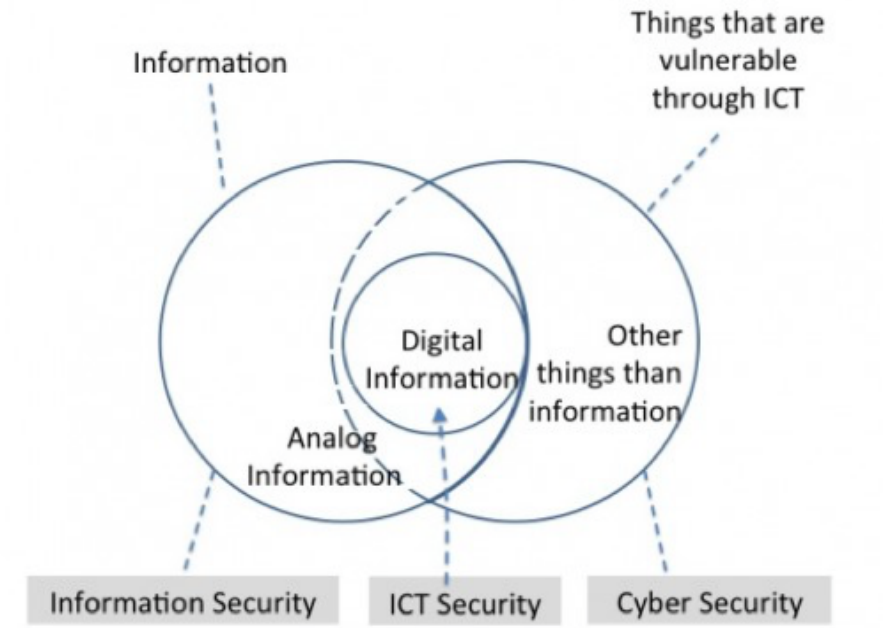


Figure 4: InfoSec-ICT Security-Cyber Security.

Threat-Vulnerability-Risk

Figure 5: Threat-Vulnerability-Risk.

UNIT-I: Learning Objectives

Upon completion of this unit, you should be able to

LO1 Define the three types of security goals and explain attacks that threaten confidentiality, integrity, and availability

LO2 Infer the different categories of cryptographic attacks

LO3 Relate to the relationship between security services and their mechanisms

LO4 Outline the different techniques needed for implementing security goals

LO5 Threat, vulnerability, and risk estimation in an enterprise, legal and ethical issues in computer security

LO1: Security Goals

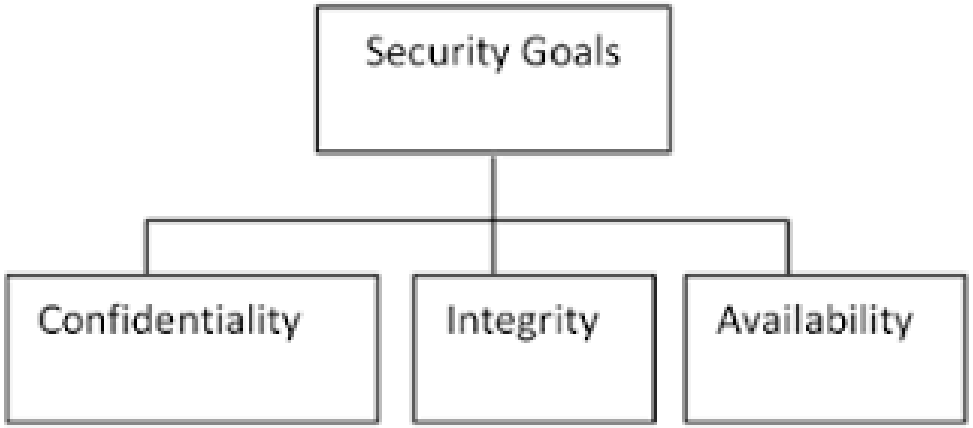


Figure 6: Security Goals.

CIA Triad

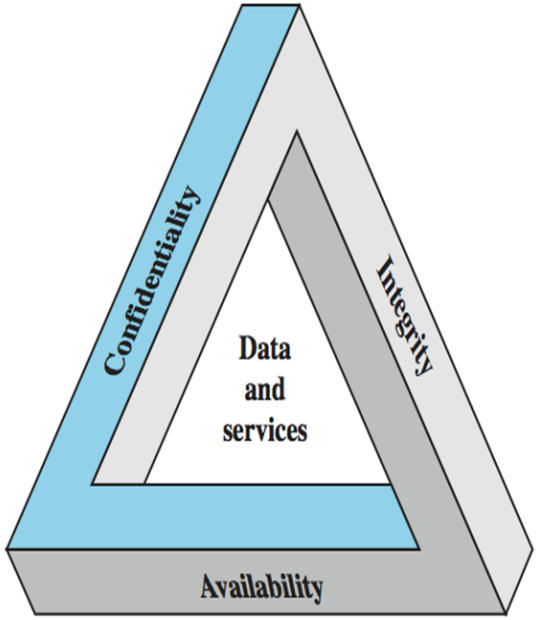


Figure 7: Security Concepts.

LO2: Cryptographic Attacks

* What is Cryptography?

LO2: Cryptographic Attacks

* What is Cryptography?
  Example: **rwox{vj}rxw**

LO2: Cryptographic Attacks

* What is Cryptography?
  Example: **rwox{vj}rxw**
  Original Message: information

1. Cryptanalytic attacks.
2. Non-Cryptanalytic attacks.

Cryptographic Attacks

- Classification based on encryption techniques:
  1. Ciphertext-only attack
  2. Known plaintext attack
  3. Chosen Plaintext attack
  4. Chosen Ciphertext attack
  5. Chosen text attack

Cryptanalytic attacks

- ”Skill in the production of cryptanalysis has always been heavily on the side of the professionals, but innovation, particularly in the design of new types of cryptographic systems, has come primarily from amateurs.”–Diffie and Hellman.
- **Cryptanalytic attacks tries to attack mathematical weaknesses in the algorithms.**

Cryptanalytic attacks

- Cryptanalytic attacks:
  1. Linear Cryptanalysis
  2. Differential Cryptanalysis

- **Side Channel Attacks/Implementation Attacks:** Tries to attack the specific implementation of the cipher. (such as a smartcard system).
  - Power Analysis.
  - Timing Analysis.
  - Fault Induction.
  - TEMPEST.
  - Differential Power Analysis.

Differential Power Analysis

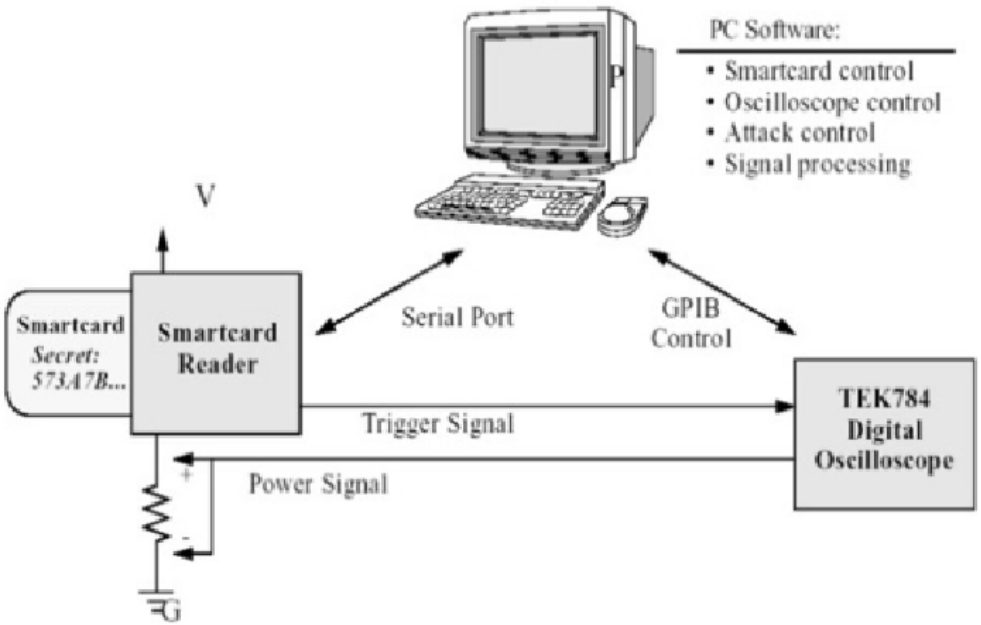
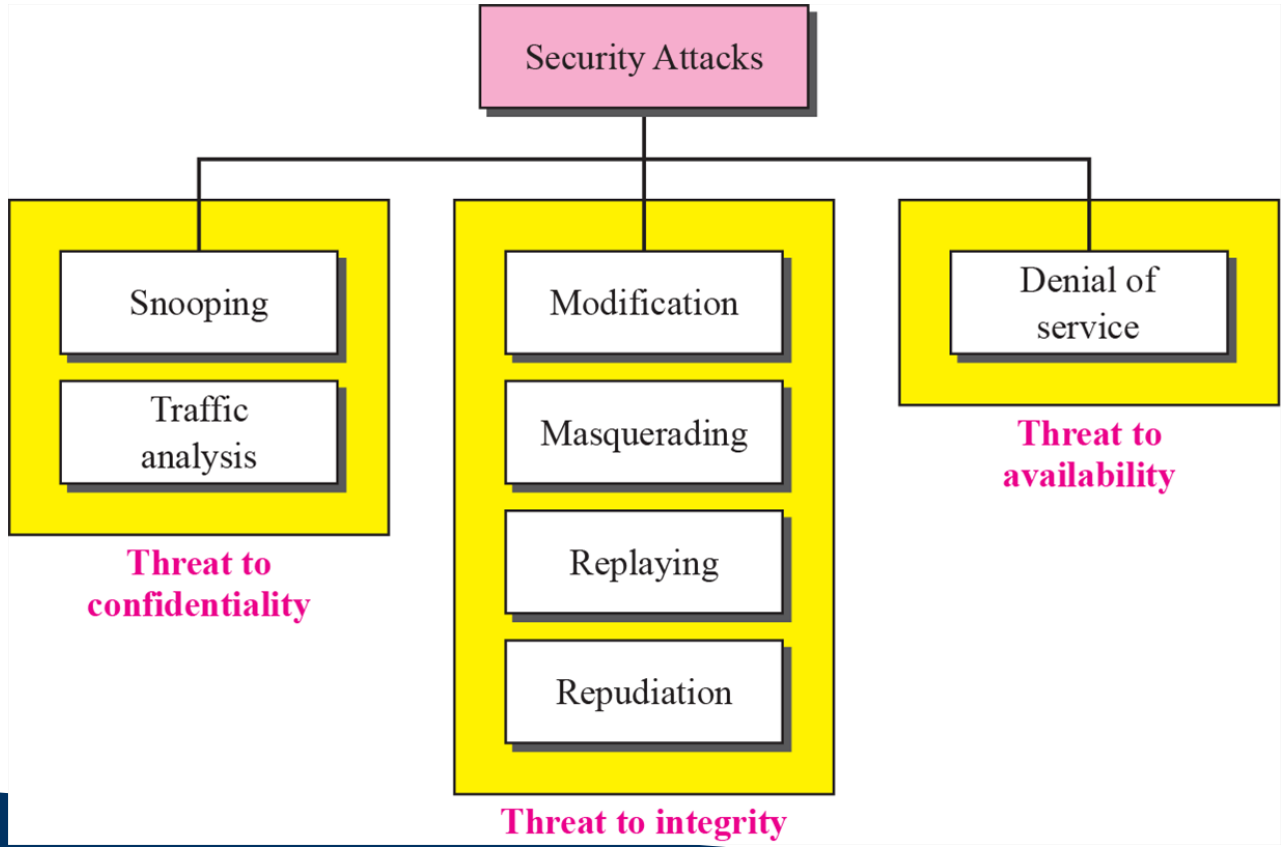


Figure 8: An example setup for a Differential Power Analysis attack on a smartcard.

Non-cryptanalytic Attacks



Threat to confidentiality: Snooping

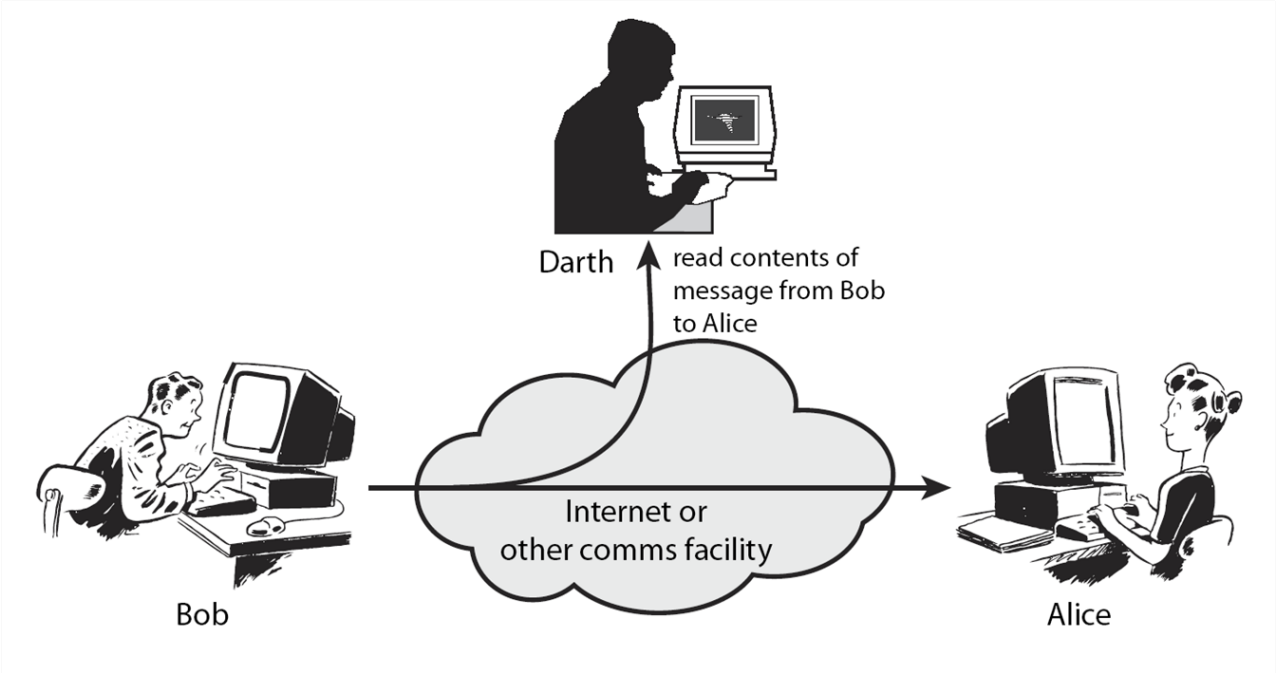


Figure 10: Snooping/Interception.

Threat to confidentiality: Traffic Analysis

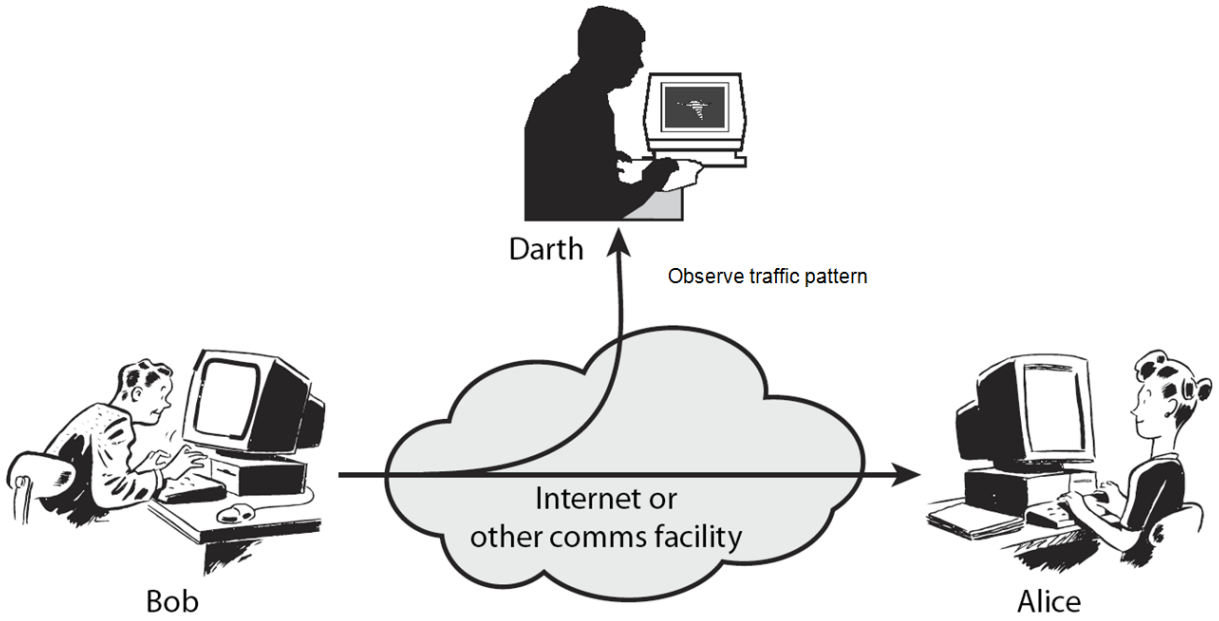


Figure 11: Traffic analysis.

Threat to Integrity: Modification

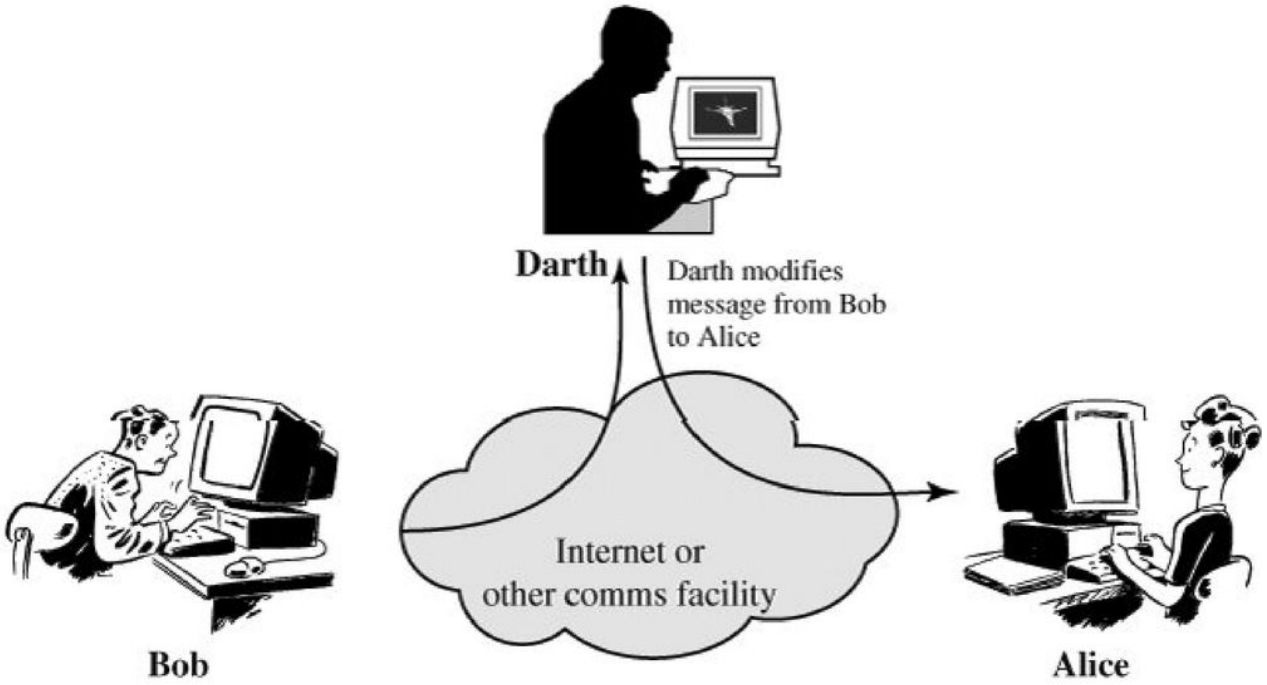


Figure 12: Modification.

Threat to Integrity: Masquerading

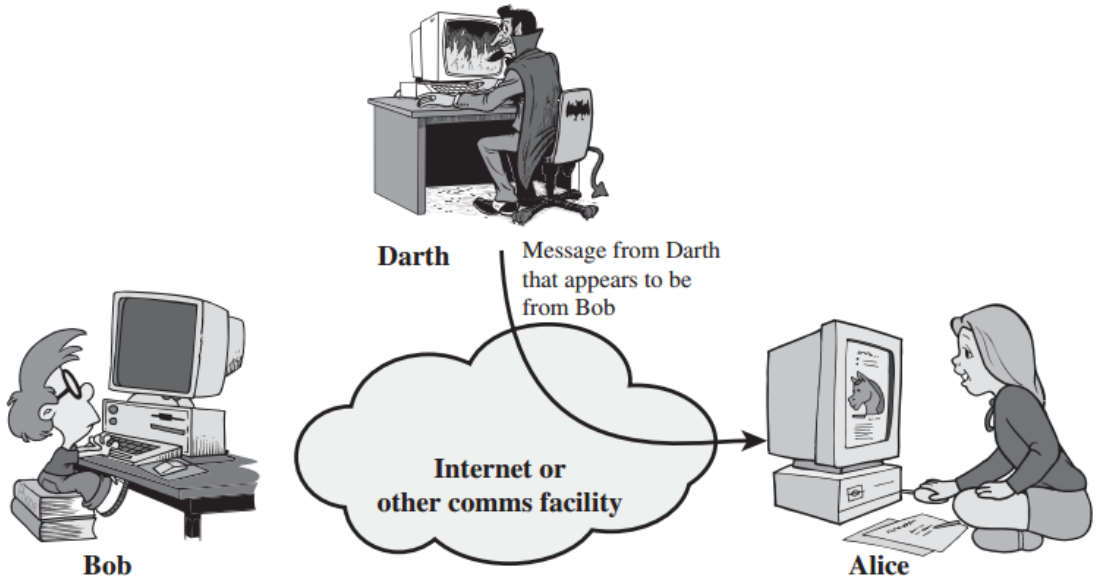


Figure 13: Masquerading.

Threat to Integrity: Replaying

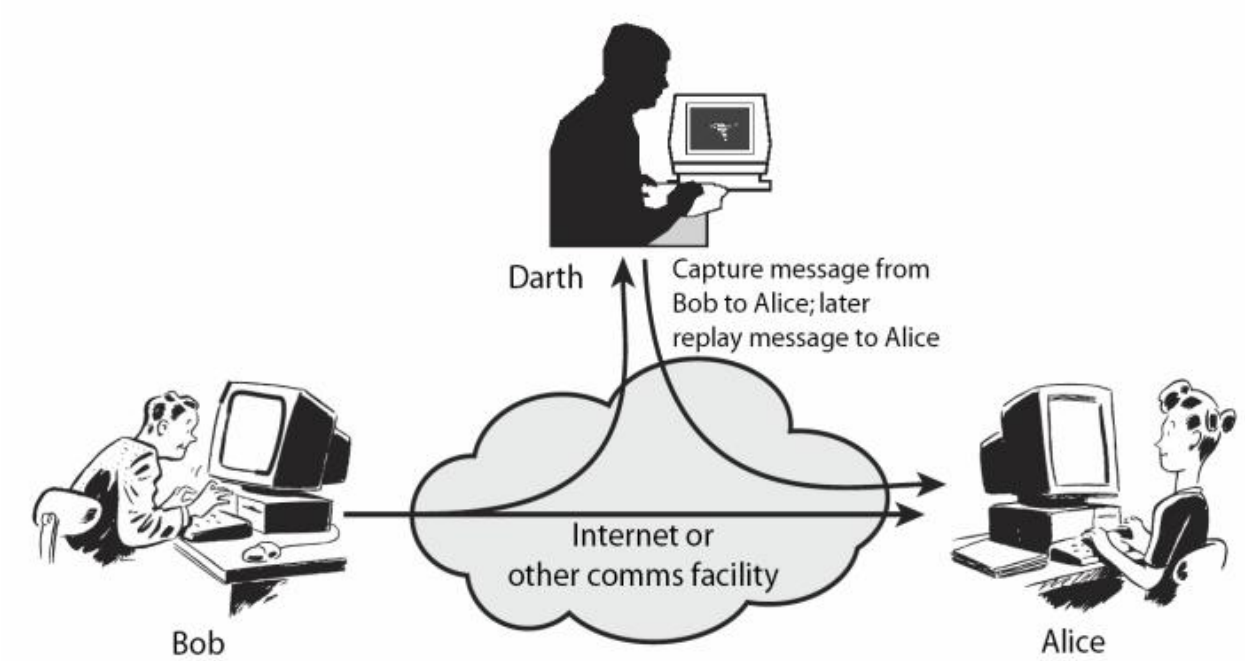


Figure 14: Replaying.

Threat to Integrity: Repudiation

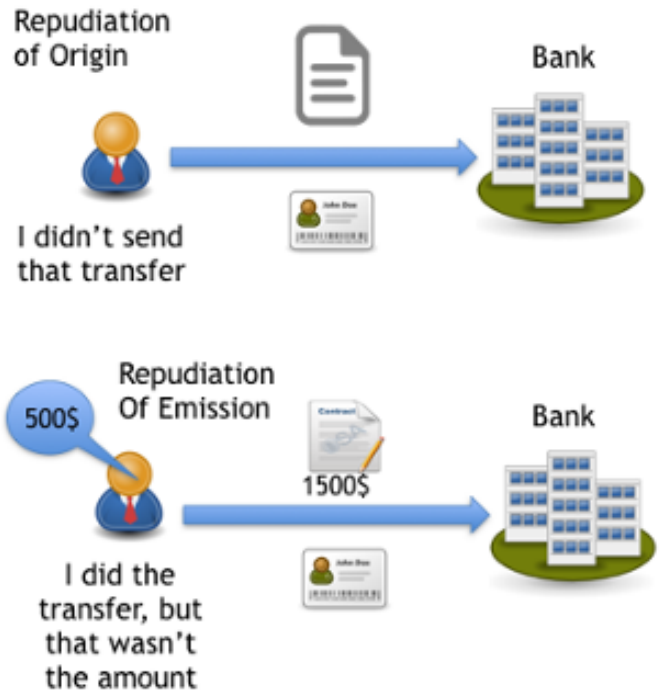
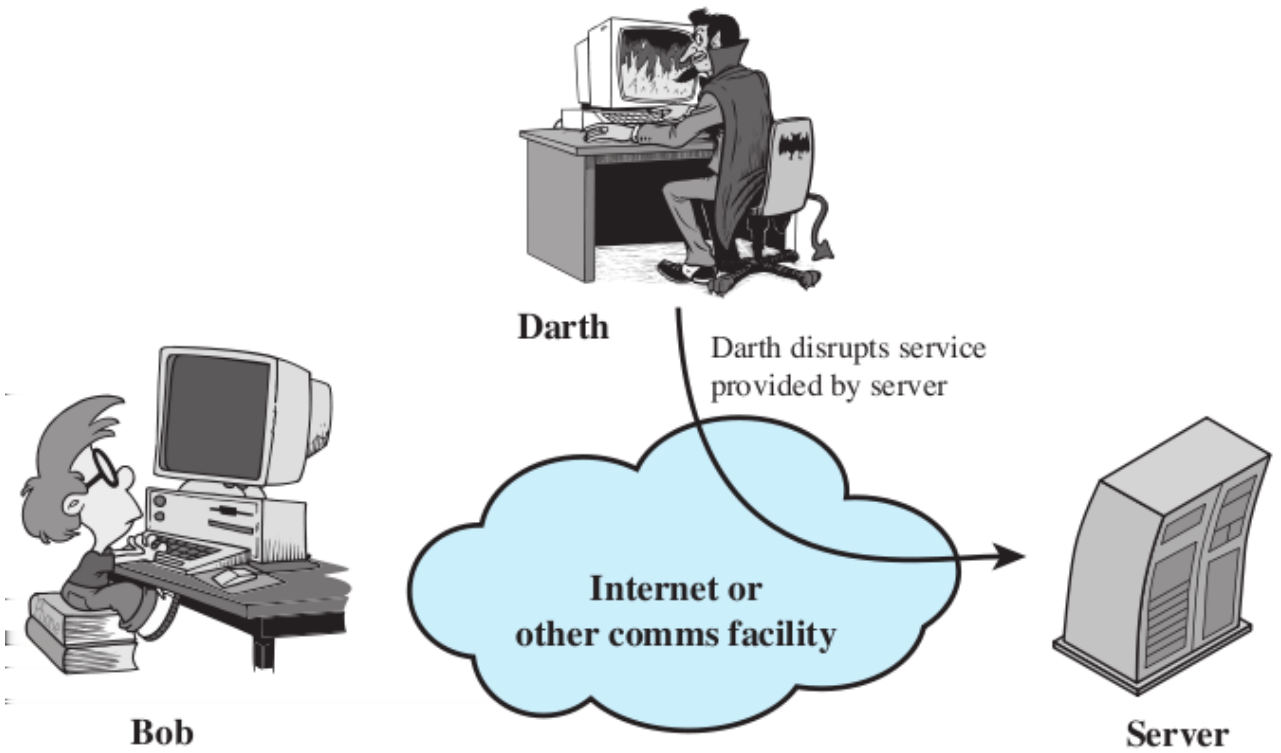


Figure 15: Different modes of repudiation.

Threat to Availability: Denial of Service



Handling Attacks

* Passive Attacks – focus on Prevention
  1. Easy to stop
  2. Hard to detect

Handling Attacks

* Passive Attacks – focus on Prevention
  1. Easy to stop
  2. Hard to detect
* Active Attacks – focus on Detection and Recovery
  1. Hard to stop
  2. Easy to detect

Categorization of passive and active attacks

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

Table 2: Categorization of passive and active attacks.

Common Attacks

- XSS (Cross-Site Scripting)
- Cross-Site Request Forgery (CSRF)
- SQL Injection
- Man In The Middle
- DoS and DDoS
- Phishing Attack
- Zero Day Attack

XSS/Cross-cite Scripting

- Security vulnerability typically found in web applications.
- Code injection attack, allows an attacker to execute malicious code (e.g. JavaScripts) into victim's web browser.
- Attacker's Goal: To steal the victim's credentials, such as cookies.

1. Server-side XSS Attack
2. Client-side XSS attack

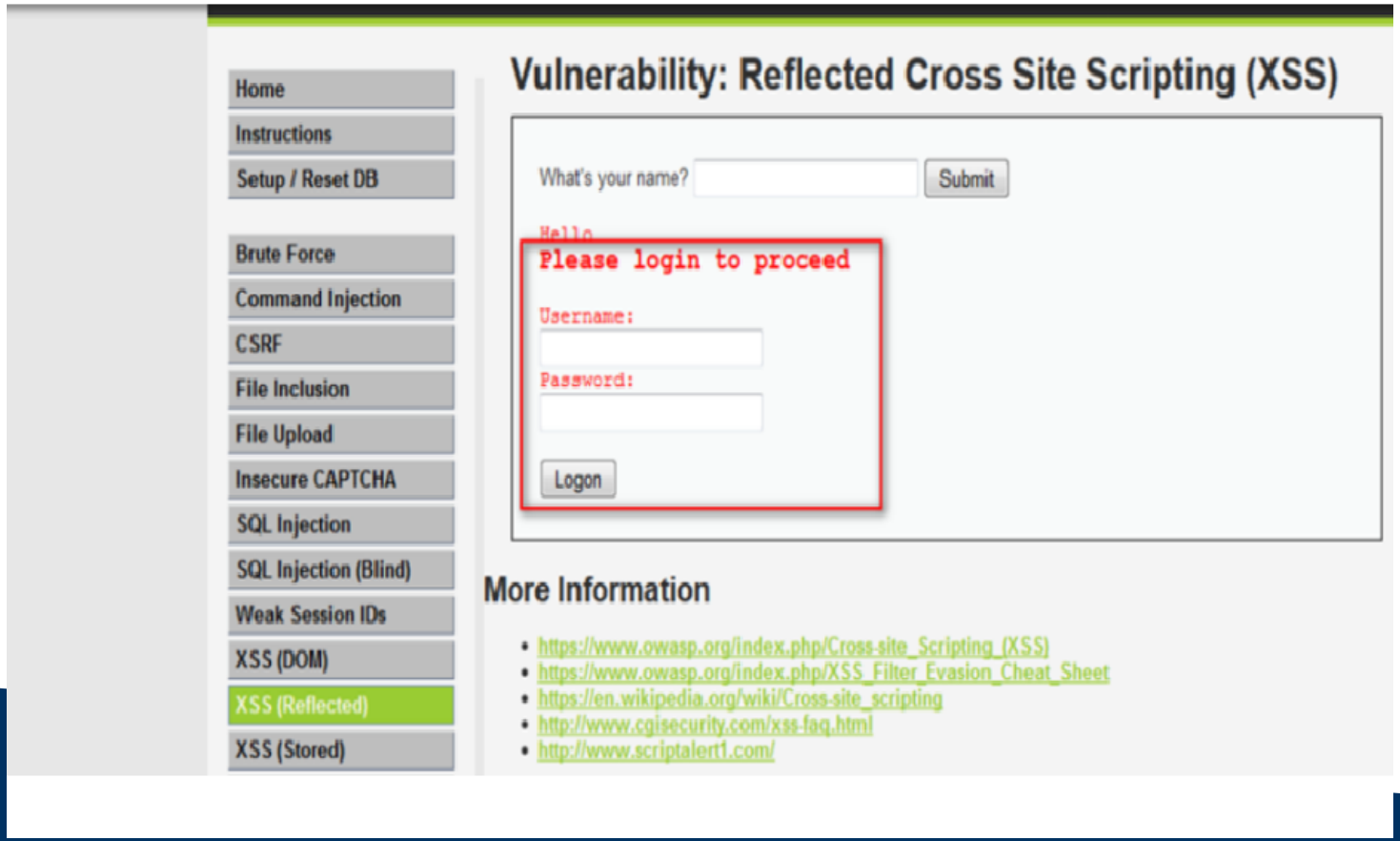
For questing mind: `https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture28.pdf`

XSS/Cross-cite Scripting: Example (slide courtesy: Veerendra Srivastava)

```
http://localhost:8080/DVWA/vulnerabilities/xss_r/?name=<h3>Pl
ease login to proceed</h3><form
action=http://192.168.149.128>Username:<br><input
type="username" name="username"></br>Password:<br><input
type="password" name="password"></br><br><input
type="submit" value="Logon"></br>
```

Figure 17: JavaScript code injected in localhost.

XSS/Cross-cite Scripting: Example..(slide courtesy: Veerendra Srivastava)



Cross-Site Request Forgery (CSRF)

- A CSRF attack involves a victim user, a trusted site, and a malicious site.
- The victim user holds an active session with a trusted site and simultaneously visits a malicious site. The malicious site injects a HTTP request for the trusted site into the victim user session compromising its integrity.

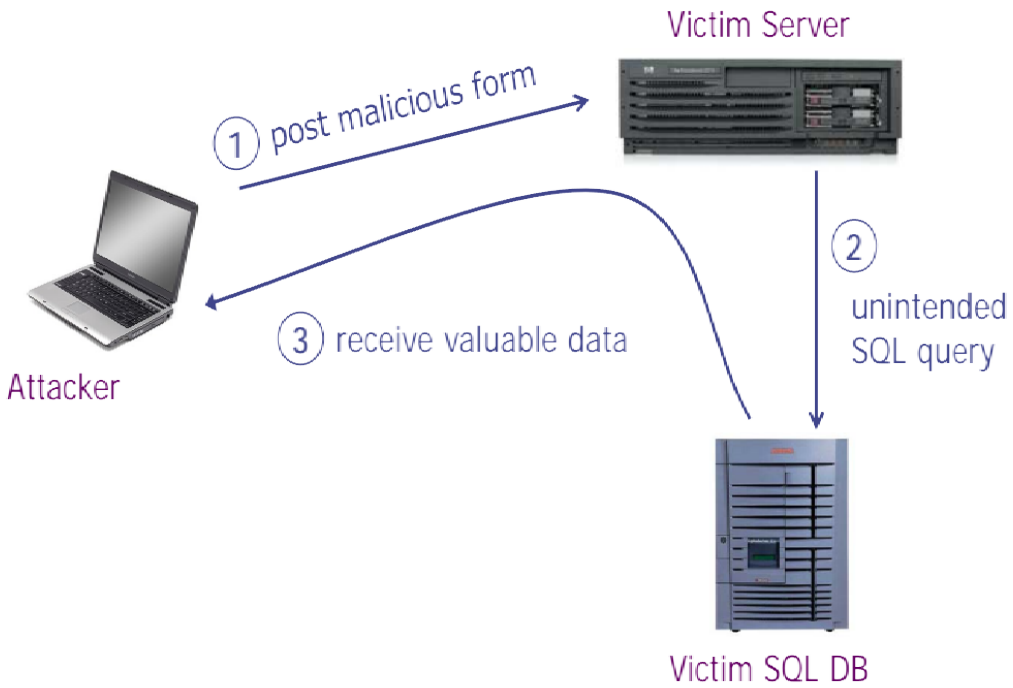
SQL Injection

- A code injection technique, exploits the vulnerabilities in the interface between web applications and database servers.

SQL Injection

- A code injection technique, exploits the vulnerabilities in the interface between web applications and database servers.
- The vulnerability is present when user's inputs are not correctly checked within the web applications before sending to the back-end database servers.

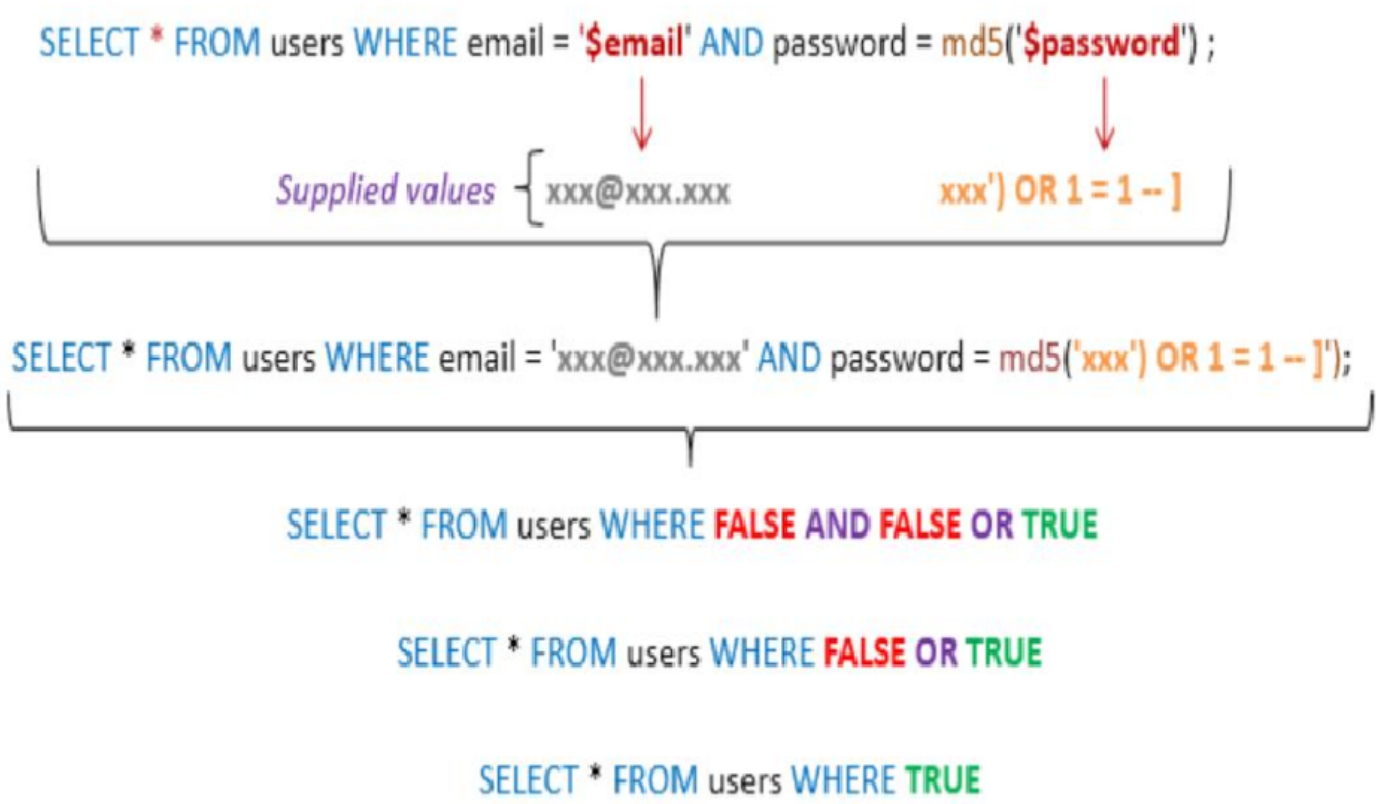
Basic Picture: SQL Injection (Slide courtesy: Dan Boneh)



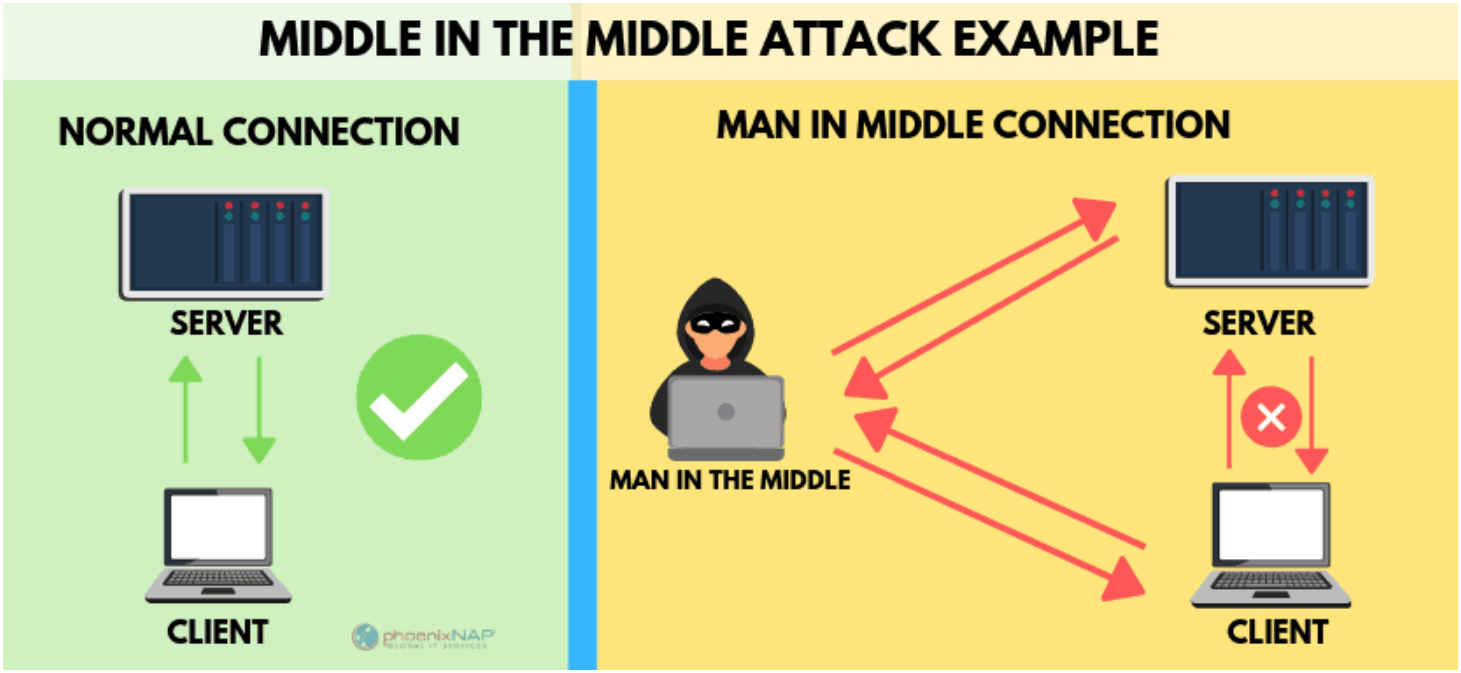
SQL Injection: Examples

Recent Past: Bloodx1.0: `https://www.exploit-db.com/exploits/47842`

SQL Injection: Examples..(slide courtesy: Veerendra Srivastava)



Man-In-The-Middle (MITM) Attack/Janus Attack/Fire Brigade Attack.



Attack/Fire Brigade Attack.

Requirement to execute an MITM Attack/Janus Attack/Fire Brigade Attack

- Sniffing the victim

Requirement to execute an MITM Attack/Janus Attack/Fire Brigade Attack

- Sniffing the victim
- Ensuring that the original packet does not reach the recipient
- Forwarding the modified packet

Requirement to execute an MITM Attack/Janus Attack/Fire Brigade Attack

- Sniffing the victim
- Ensuring that the original packet does not reach the recipient
- Forwarding the modified packet
- Tricking potential security systems such as SSL

DoS Attack and DDoS Attack

- DOS Attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to its legitimate customers.

DoS Attack and DDoS Attack

- DOS Attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to its legitimate customers.
  * **DoS** –> when a single host attacks
  * **DDoS** –> when multiple hosts attack simultaneously
- The goal of DoS or DDoS is usually service denial or setting up a different, second attack.

DoS Attack: Variety

- **Bandwidth Consumption:** All available bandwidth used by the attacker e.g.,ICMP ECHO attack.
- **Resource Consumption:** Resources like web server, print or mail server flooded with useless requests e.g., mail bomb
- **Network Connectivity:** The attacker forces the server to stop communicating on the network e.g., SYN Flooding.
- Quick Guide for DDoS Attacks: `https://us-cert.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf`

Phishing Attack

- Phishing is a type of **social engineering attack** often used to steal user data, including login credentials and credit card numbers.
- Occurs when an attacker pretends to be a trusted entity to dupe a victim into clicking a malicious link, that can lead to the installation of malware, freezing of the system as part of a ransomware attack, or revealing of sensitive information.
- Variety: `https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf`

Zero Day Attack

- ”Zero-day” refers a **newly discovered software vulnerability**.
- Refers the fact that the developers have **”zero days” to fix the problem** which has just been exposed — and may be already exploited by hackers.
- Link: `https://www.blackhat.com/docs/eu-17/materials/eu-17-Ablon-Zero-Days-Thousands-Of-Nights-The-Life-And-Times-Of.pdf`

Zero Day Attack...

Figure 22: Hiding vulnerabilities.(Image source: Economics Times, India, Feb 14, 2019)

Prevention of Zero-Day Attack

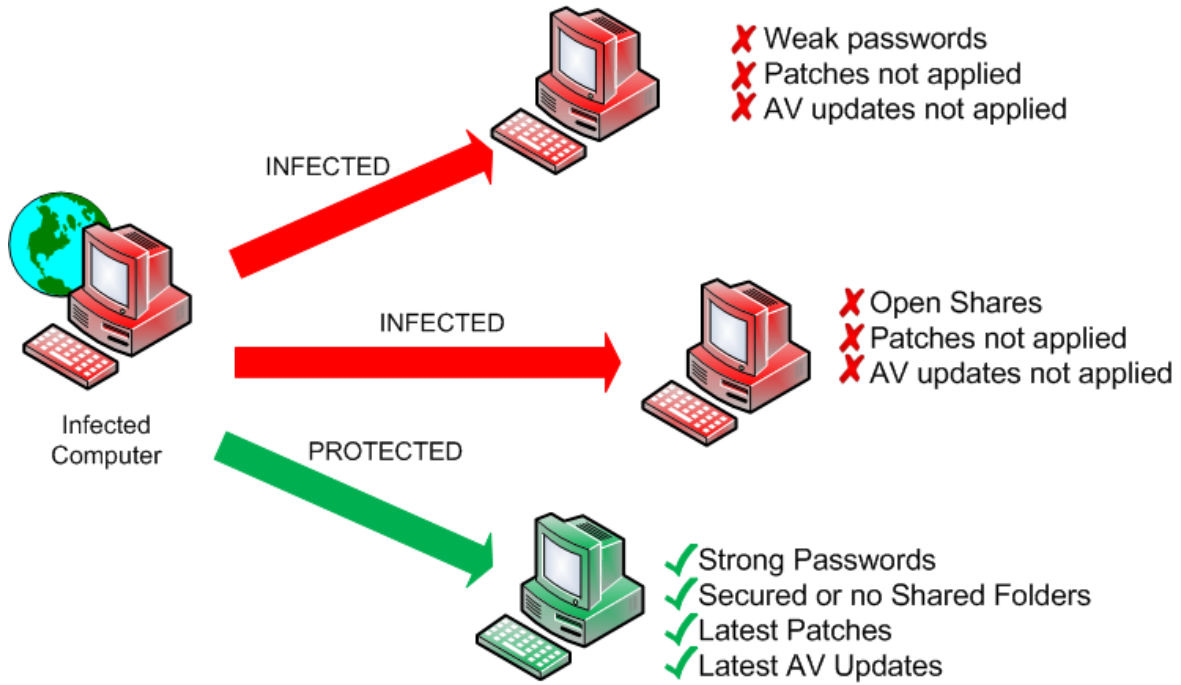


Figure 23: Zero-Day Attack preventive measures.

Security Services and Mechanism

- ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) provides some security services and some mechanisms to implement those services.
- A mechanism or combination of mechanisms are used to provide a service.
- A mechanism can be used in one or more services.

Security Services and Mechanism

- ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) provides some security services and some mechanisms to implement those services.
- A mechanism or combination of mechanisms are used to provide a service.
- A mechanism can be used in one or more services.
- Thus, the three aspects of security, **(i) security attacks, (ii) security mechanisms and (iii) security services** are related.

Security Services

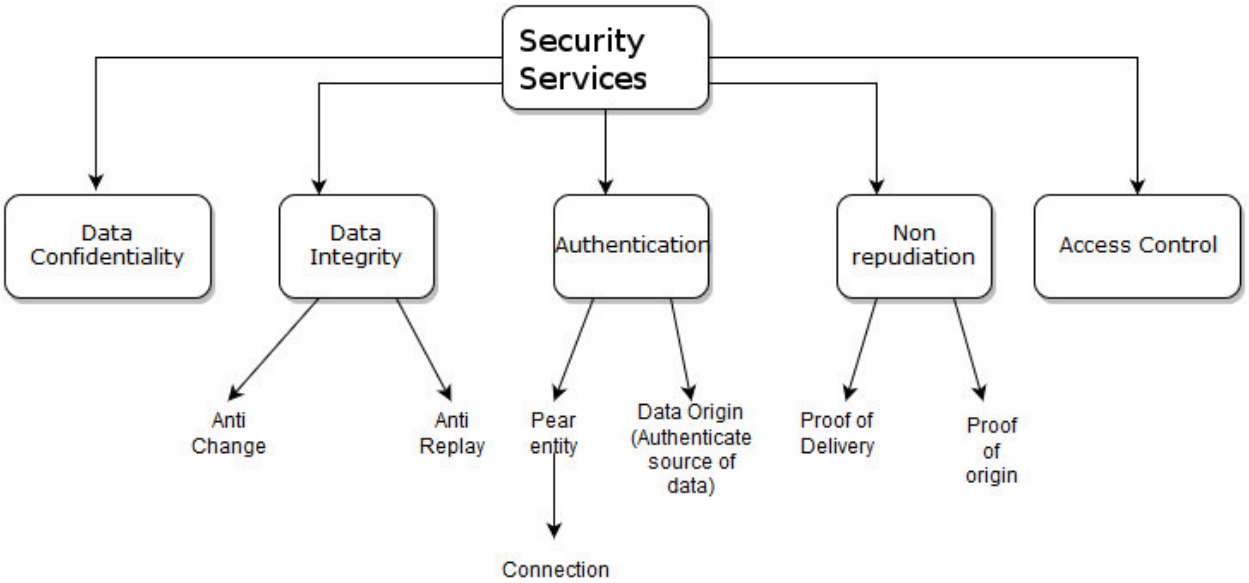


Figure 24: Security Services: ITU-T (X.800) has define five services related to the security goals and attacks (discussed..).

Security Services: Protection

- **Data Confidentiality:**
  - Designed to protect data from disclosure attack.
  - The service defined by X.800 is very broad and encompasses confidentiality of whole message or part of a message and also protect against traffic analysis.
- **Data Integrity:**
  - Designed to protect data from modification, insertion, deletion, and replaying by an adversary.
  - It may protect the whole message or part of the message.

Security Services: Protection....cont..1

- **Authentication:** This service provides the **authentication of the party** at the other end of the line.

Security Services: Protection....cont..1

- **Authentication:** This service provides the **authentication of the party** at the other end of the line.
  - **Peer entity authentication:** It provides authentication of the sender or receiver during the connection establishment in connection-oriented communication.
  - **Data origin authentication:** It authenticates the source of the data in connection-less communication.

Security Services: Protection....cont..1

- **Authentication:** This service provides the **authentication of the party** at the other end of the line.
  - **Peer entity authentication:** It provides authentication of the sender or receiver during the connection establishment in connection-oriented communication.
  - **Data origin authentication:** It authenticates the source of the data in connection-less communication.
- **Non-repudiation:** This service protects against repudiation by either the sender or the receiver of the data.

Security Services: Protection....cont..1

- **Authentication:** This service provides the **authentication of the party** at the other end of the line.
  - **Peer entity authentication:** It provides authentication of the sender or receiver during the connection establishment in connection-oriented communication.
  - **Data origin authentication:** It authenticates the source of the data in connection-less communication.
- **Non-repudiation:** This service protects against repudiation by either the sender or the receiver of the data.
  - **Proof of Origin:** The receiver of the data can later prove the identity of the sender if denied.

Security Services: Protection....cont..1

- **Authentication:** This service provides the **authentication of the party** at the other end of the line.
  - **Peer entity authentication:** It provides authentication of the sender or receiver during the connection establishment in connection-oriented communication.
  - **Data origin authentication:** It authenticates the source of the data in connection-less communication.
- **Non-repudiation:** This service protects against repudiation by either the sender or the receiver of the data.
  - **Proof of Origin:** The receiver of the data can later prove the identity of the sender if denied.
  - **Proof of Delivery:** The sender of the data can later prove that data were delivered to the intended recipient.

Security Services: Protection....cont..2

- **Access Control:**
  - Provides protection against unauthorized access to data.
  - Access control can involve reading, writing, modifying, executing programs, and so on.

Security Mechanisms

Figure 25: Security Mechanisms: ITU-T (X.800) recommends some security mechanisms to provide the security serviced (defined earlier section).

Security Mechanisms: Encipherment and Data Integrity

- **Encipherment:**
  - Hiding or covering of data which provides confidentiality.
  - Can also be used to complement other mechanisms to provide other services.
  - Two techniques, **Cryptography** and **Steganography** are used for enciphering.

Security Mechanisms: Encipherment and Data Integrity

- **Encipherment:**
  - Hiding or covering of data which provides confidentiality.
  - Can also be used to complement other mechanisms to provide other services.
  - Two techniques, **Cryptography** and **Steganography** are used for enciphering.
- **Data Integrity:**
  - This mechanism appends to the data a short check value that has been created by a specific process from the data itself.
  - Data integrity is preserved by comparing check value received to the check value generated.

Security Mechanisms: Digital Signature

- **Digital Signature:**
  - A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.
  - The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly.
  - The receiver uses sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

Security Mechanisms: Authentication Exchange and Traffic Padding

- **Authentication Exchange:**
  - Two entities exchange some messages to prove their identity to each other.
  - For example, one entity can prove that she knows a secret that only she is supposed to know.

Security Mechanisms: Authentication Exchange and Traffic Padding

- **Authentication Exchange:**
  - Two entities exchange some messages to prove their identity to each other.
  - For example, one entity can prove that she knows a secret that only she is supposed to know.
- **Traffic Padding:**
  - Inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

Security Mechanisms: Routing Control and Notarization

- **Routing Control:**
  - Selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

Security Mechanisms: Routing Control and Notarization

- **Routing Control:**
  - Selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.
- **Notarization:**
  - Selecting a third trusted party to control the communication between two entities.
  - Various purposes, one is to prevent repudiation.
  - The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.

Security Mechanisms: Access control

- **Access control:**
  - Uses methods to prove that a user has the access right to the data or resources owned by a system.
  - Examples of proofs are passwords and PINs.

Security Mechanisms: Access control

- **Access control:**
  - Uses methods to prove that a user has the access right to the data or resources owned by a system.
  - Examples of proofs are passwords and PINs.

Relation between Services and Mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Figure 26: Relation between security services and security mechanisms.

Techniques for security goals implementation

- Security mechanisms (discussed..) are **only theoretical recipes** to implement security.
- The actual implementation of security goals needs some techniques.
- Two most important techniques:
  - Cryptography
  - Steganography

Cryotpgraphy Mechanisms

- **Past**
  - Encryption
  - Decryption
- **Today**
  - Symmetric-key Encipherment
  - Asymmetric-key Encipherment
  - Hashing

Symmetric-key Encipherment

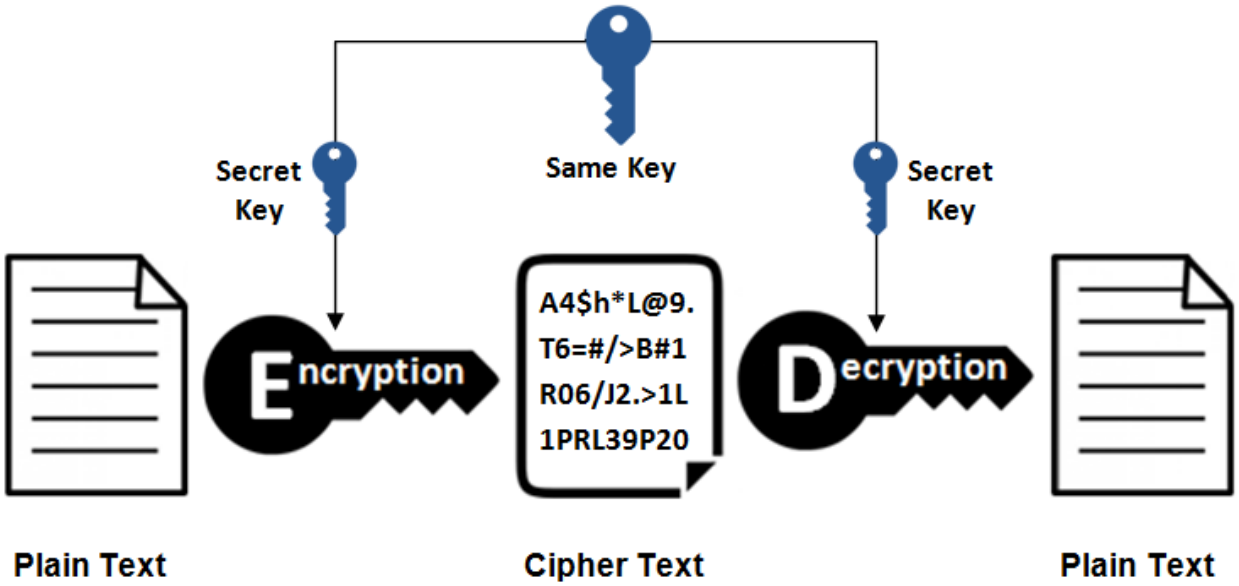


Figure 27: Symmetric-key Encipherment.

Asymmetric-key Encipherment

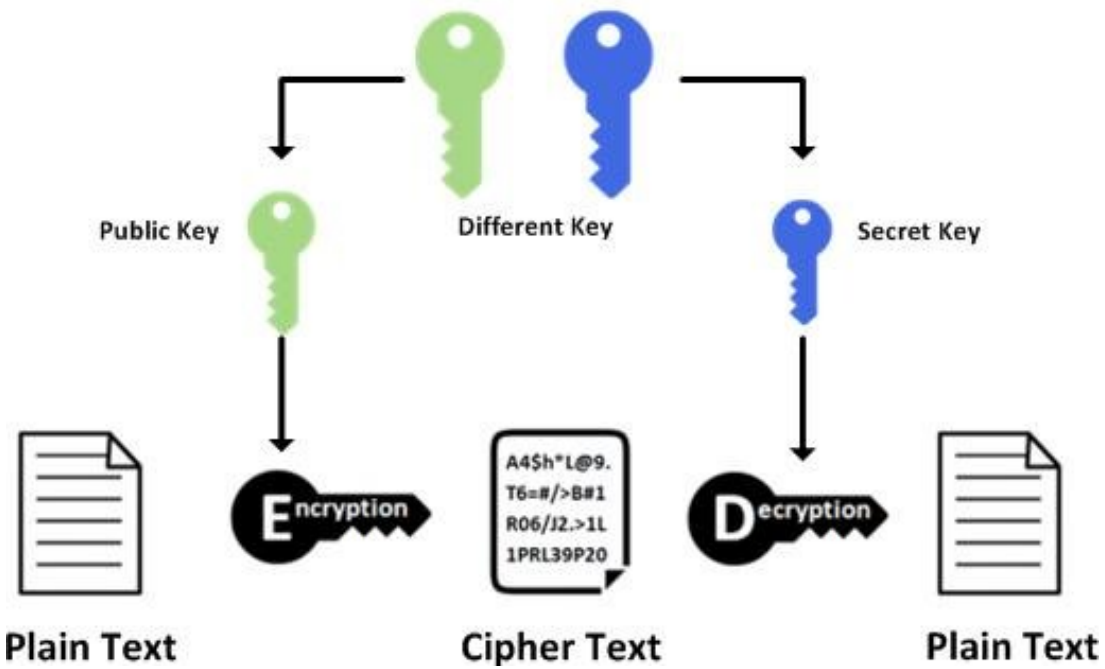


Figure 28: Asymmetric-key Encipherment.

Hashing

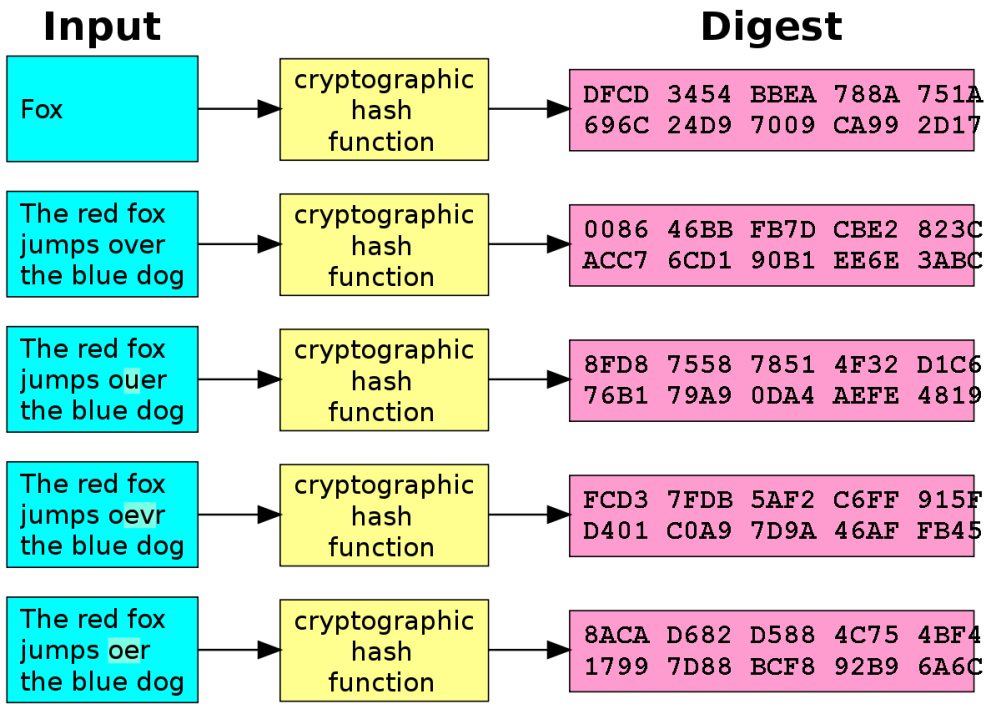
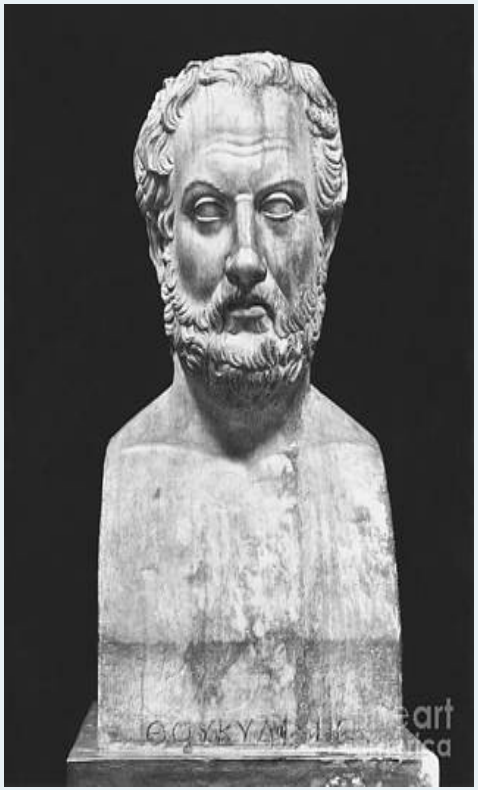


Figure 29: Hashing.

Steganography

- **Steganography:** *"Covered writing"*
- **Cryptography:** *"Secret writing"*
- For example (sent by a German spy during World War I),
  Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.
  Pershing sails from NY June 1.

Ancient Steganography (content courtesy: Nasir Memon)



Herodotus (485 – 525 BC) is the first Greek historian. His great work, The Histories, is the story of the war between the huge Persian empire and the much smaller Greek citystates.

Herodotus recounts the story of Histaiaeus, who wanted to encourage Aristagoras of Miletus to revolt against the Persian king. In order to securely convey his plan, Histaiaeus shaved the head of his messenger, wrote the message on his scalp, and then waited for the hair to regrow. The messenger, apparently carrying nothing contentious, could travel freely. Arriving at his destination, he shaved his head and pointed it at the recipient.

Ancient Steganography (content courtesy: Nasir Memon)

- **Pliny the Elder (AD 23 - 79)** explained how the milk of the thithymallus plant dried to transparency when applied to paper but darkened to brown when subsequently heated, thus recording one of the earliest recipes for invisible ink.

The **Ancient Chinese** wrote notes on small pieces of silk that they then wadded into little balls and coated in wax, to be swallowed by a messenger and retrieved at the messenger's gastrointestinal convenience.

Renaissance Steganography

Giovanni Battista Porta (1535-1615) described how to conceal a message within a hardboiled egg by writing on the shell with a special ink made with an ounce of alum and a pint of vinegar. The solution penetrates the porous shell, leaving no visible trace, but the message is stained on the surface of the hardened egg albumen, so it can be read when the shell is removed..

Modern Steganography: The Prisoners' Problem

- Simmons 1983: Prisoners problem
- Done in the context of USA- USSR non-proliferation treaty compliance checking.

- Alice and Bob are prisoners, Wendy is a warden. Alice and Bob are allowed to exchange messages, say images, but Wendy checks all messages.
- Alice and Bob try to hide information in their messages so that Wendy cannot detect it.
- Wendy cannot arbitrarily suppress all messages; the prisoners' human rights cannot be violated without some proof of illegal activity.

Modern Steganography: The Prisoners' Problem..cont..

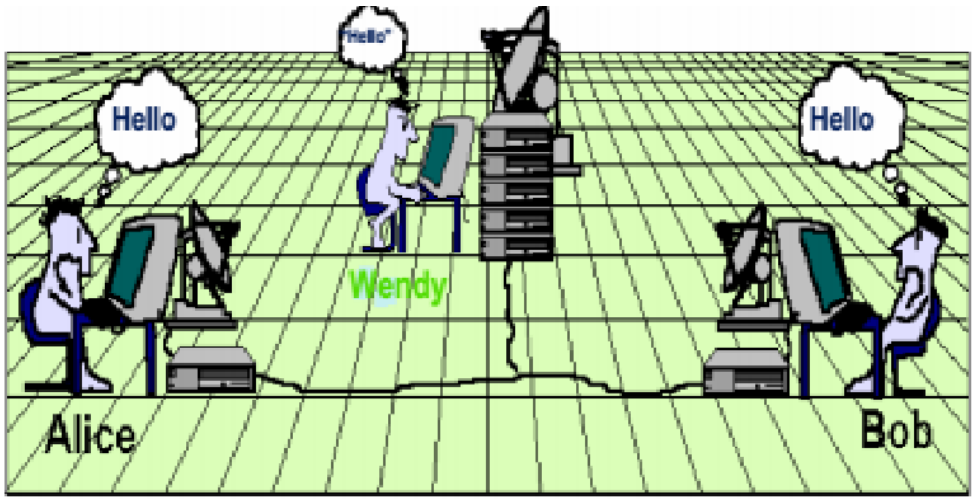


Figure 30: Prisoners' Problem.

Modern Steganography: simplified framework

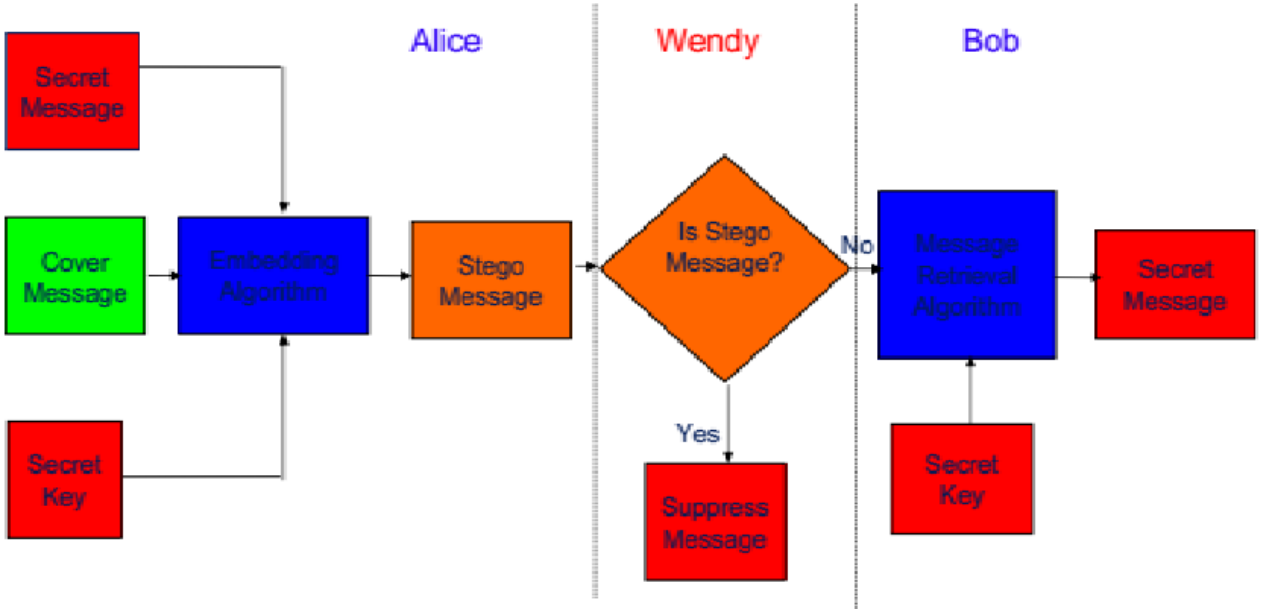


Figure 31: Prisoners' Problem.

Steganography..

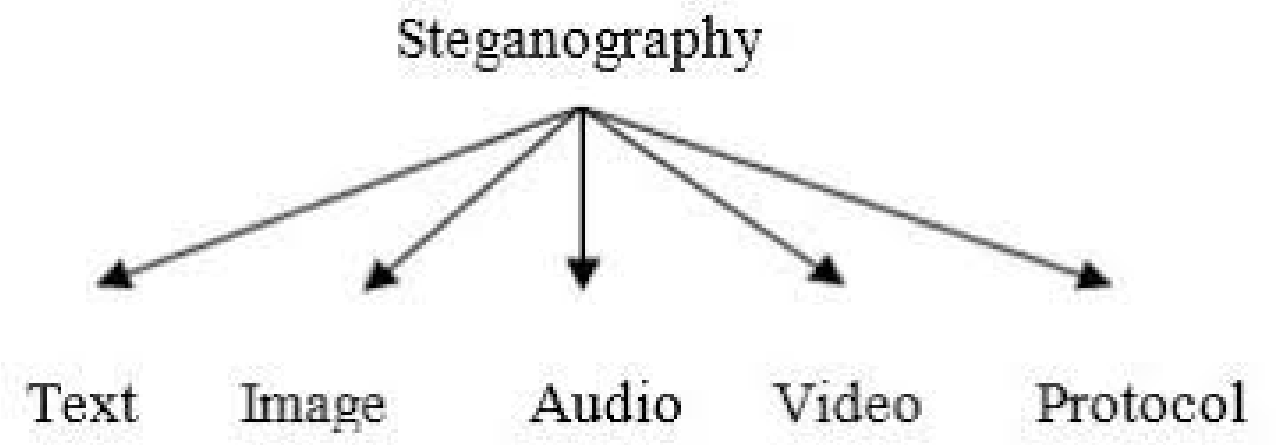


Figure 32: Different types of Steganography: Text, Image, Audio, Video, Protocol/Network.

Bibliography: Books and Resources

- Cryptography and Network Security: Principles and Practice by William Stallings
- Cryptography and Network Security by Behrouz A Forouzan and Debdeep Mukhopadhyay
- Principles of Information Security by Michael E. Whitman and Herbert J. Mattord.
- Cisco platform, and Internet.
- Published research papers, study materials from researchers of security domain.