

Chapter 1

Ways of securing data include:

Data encryption

Data masking

Data erasure

Data resilience (by creating backup copies of data)

Main Elements of Data Security: CIA Triad

- **Confidentiality**: ensures that data is **accessed only by authorized** individuals;
- **Integrity**: ensures that **information is reliable** as well as accurate;
- **Availability**: ensures that data is **both available and accessible** to satisfy business needs.

Privacy is not just the *confidentiality* and *integrity* of user data.

- Privacy includes other requirements:
 - Support for user preferences
 - Support for obligation execution
 - Usability
 - Proof of compliance

Various threats to a computer system

☐ Accidents and Natural Disasters:

☐ High risk factor from Computer Abuse:

☐ Human Initiated

Technology Available for Computer Security

☐ Cryptography

☐ Biometric Systems

☐ Malicious Code and Anti Virus Solutions:

Computer viruses, Spyware, worms, Trojan Horse, Back Doors/Trap Doors, Logic Bombs, Bacteria/Rabbit.

☐ Firewall

☐ Intrusion Detection System (IDS)

☐ Virtual Private Network (VPN)

☐ PKI and Digital Certificates

☐ **SSH Encryption:** a program to log into another computer over a network, to **execute commands** in a remote machine, and **move files** from one machine to another.

☐ **SSL Encryption:** is a protocol developed by Netscape for **transmitting private documents** via the Internet

Chapter 2

Goals of Security

- Prevention
- Detection
- Recovery

Threats:

Compromises to Intellectual Property

Software attacks

Deviations in quality services: Internet service issues, communications and other service providers issues, and power irregularities.

Espionage or Trespass: Access to protected information by unauthorized individuals, breaches the confidentiality of information Ex: shoulder surfing when accessing confidential information. It can be done by an expert or unskilled hacker, a cracker, or a phreaker.

Forces of nature

Human error or failure: Includes acts performed without malicious intent

- Causes include: Inexperience, Improper training, Incorrect assumptions
- Employees are among the greatest threats to an organization's data

Information Extortion

Missing, Inadequate or incomplete

Sabotage or Vandalism

Theft

Technical Hardware Failure or Errors: Occur when the manufacturer distributes equipment containing flaws to users

Technical Software Failure or Errors: Purchased software that contains unrevealed faults

Technological Obsolescence

Attacks:

Acts or actions that exploit a vulnerability in a controlled system.

Malicious code: includes execution of viruses, worms, Trojan horses, and active Web scripts with intent to destroy or steal information

Hoaxes

Back door

Password crack: attempting to reverse calculate a password

Brute force: trying every possible combination of options for a password.

Dictionary

Denial-of-service (DoS): the attacker sends a large number of connection or information requests to a target.

Distributed denial-of-service (DDoS): coordinated stream of requests is launched against the target from many locations simultaneously

Spoofing: a technique used to gain unauthorized access; intruder assumes a trusted IP address.

Man-in-the-middle

Spam

Mail bombing

Sniffers: program or device that monitors data traveling over a network; can be used both for legitimate purposes and for stealing information from a network

Phishing: an attempt to gain personal/financial information from individual, usually by posing as a legitimate entity

Pharming

Social engineering: using social skills to convince people to reveal access credentials or other valuable information to an attacker

Timing attack

Chapter 4

Risk = Likelihood of vulnerability occurrence * value (or impact) - percentage risk already controlled + an element of uncertainty

The final summary of the risk assessment comprised in ranked vulnerability risk worksheet. The worksheet details assets, asset impact, vulnerability, vulnerability likelihood, and risk-rating factors. **Ranked vulnerability risk worksheet is the initial working** document for the next step in the **risk management process**: assessing and controlling risk

- Once the ranked vulnerability risk worksheet is complete, must choose **one of five strategies** to **control** each risk:
 - Defend

- Transfer
- Mitigate
- Accept
- Terminate

Mitigate

The approach includes three types of plans

–Incident response plan (IRP):

- define the actions to take while the incident is in progress

–Disaster recovery plan (DRP):

- most common mitigation procedure

–Business continuity plan (BCP):

- encompasses continuation of business activities if a catastrophic event occurs

Annualized loss expectancy (ALE) = single loss expectancy (SLE) × annualized rate of occurrence (ARO)

$SLE = \text{asset value} \times \text{exposure factor (EF)}$

$CBA = ALE(\text{prior}) - ALE(\text{post}) - ACS$ (annualized cost of safeguard)

Chapter 5

- Mandatory access controls (MACs):

- use data classification schemes

- Discretionary access controls (DACs):

- allow users to control and possibly provide access to information/resources at their disposal

- Nondiscretionary controls (RBAC):

- strictly enforced version of MACs that are managed by a central authority

Authentication factors

Password

Passphrase

Dumb card

Smart card

Synchronous tokens

Asynchronous tokens

ACM

List each object in a column

List each user or subject in a row

	A11	A12	A13	...	A1n
→	A21	A22	A23	...	A2n
	A31	A32	A33	...	A3n
	⋮	⋮	⋮	⋮	⋮
	Am1	Am2	Am3	...	Amn

Implementing Access Control

	X	Y	Z	
A	rwX	r		
B		rw	rx	
C		rw	rx	

ACLs

X → [(A, rwX)]

Y → [(A, r)(B, rw)(C, rw)]

Z → [(B, rx)(C, rx)]

C-lists

A → [(X, rwX)(Y, r)]

B → [(Y, rw)(Z, rx)]

C → [(Y, rw)(Z, rx)]

Types of Data Security Controls

1. Access Control
2. Encryption
3. Tokenization
4. Authentication

Chapter 6

GRANT {privileges role} [ON table] TO {user role public} [IDENTIFIED BY password] [WITH GRANT OPTION]	REVOKE {privileges role} [ON table] FROM {user role PUBLIC}
---	---

SQL injection can impact both confidentiality (extraction of data) and integrity (a corruption of data)

Inference Attacks on Databases

Certain aggregate/statistical queries can be allowed by all users

- Do not allow aggregate query results when the set of tuples selected is either too small or too large
- Transform data by removing identifying information

Disadvantages of encryption:

- Key management
- Inflexibility

Chapter 7

1-Firewalls

- Firewalls operate by **examining** data packets and **performing comparison** with predetermined **logical rules**.
- The logic is based on a set of guidelines most commonly referred to as **firewall rules**, rule base, or firewall logic.
- Most firewalls use packet header information to determine whether specific packet should be allowed or denied.

2-Content Filters

Software filter—not a firewall—that allows administrators to restrict content access from within a network

3-Protecting Remote Connections

4-Intrusion Detection and Prevention Systems: IDPSs operate as **network-based** or **host-based** systems

5-Scanning and Analysis Tools

6-Port Scanners

7-Firewall Analysis Tools

8-Operating System Detection Tools

9-Vulnerability Scanners

10-Packet Sniffers

11-Wireless Security Tools

12-Backup (full/incremental/differential)

Data **redundancy** and **backups** are intended to **prevent data loss**, but the two technologies are quite different

RAID(Redundant Array of Independent Disks): Disk stripping, Disk mirroring, Disk mirroring + parity

Common 5 mistakes made while doing a backup:

1. Not doing a backup.
2. Saving the backup copies on the same hardware as the original files.
3. Not testing the backup.
4. Not running the backup regularly and sufficiently frequently.
5. Not labeling the backup files.

The 3-2-1 backup strategy states that you should keep:

1. At least **THREE copies** of your data;
2. Backed-up data on **TWO different storage types**;
3. At least **ONE copy** of the data **offsite**.