

Data Security and Privacy

Chapter1: Introduction to Data Security and Privacy

TextBook:

- Principles of Information Security, M. Whitman, H. Mattord, fourth edition, 2012.
- Computer Security_ Principles and Practice, W. Stallings, L. Brown, 4th edition, Pearson 2018.

Introduction

- Data is the raw form of information.
- stored in:
 - our databases, network servers, personal computers and some other places.
- But all data or information is not accessible for all.
 - Some data or information is personal, as well as implicit for its own purpose.
 - some people or organizations can try to capture those ‘not accessible information’.
- So “Data Security” has come into focus.

What is Data

- "something given or admitted;
 - facts or principles granted or presented;
 - that upon which an inference or argument is based,
 - or from which an ideal system of any sort is constructed".
-
- **Classification of data:**
 - ❑ ***Public Data :***
 - Open to all users and no security measures are necessary
 - ❑ ***Limited-Access Data:***
 - Only authorized users have access to this type of data
 - ❑ ***Private Data:***
 - This data is open to a single user only, the owner of that particular data.

Physical Storage of Data

- ✓ Mechanical (Paper, punched card, film, gramophone record, etc.)
- ✓ Magnetic Storage (Magnetic tape, floppy disk)
- ✓ Optical Storage (optical disc, CDs, DVDs, BluRays)
- ✓ Electrical (Semiconductor used in volatile RAM —chips, etc.)

What is Security

- ☐ Security is the protection of information, systems and services against disasters, mistakes and exploitation, so that the probability of incidents is minimized.
- ☐ **The quality or state of being secure—to be free from danger**

What is Data Security

➤ Data security is:

- ✓ the **means** of ensuring that data is kept **safe** from **corruption**
- ✓ and that **access** to it is suitably **controlled**.
- ✓ Thus data security helps to ensure **privacy**.
- ✓ It also helps in protecting **personal data**:
 - protection of data —from **unauthorized** (that may be accidental or intentional) **access, modification** and **destruction**.

❑ **Data security** refers to the process of protecting **data** from unauthorized access and **data** corruption throughout its lifecycle.

❑ **Data security** includes:

- **data encryption, Hashing, Tokenization and key management practices** that protect **data** across all applications and platforms.

Why is Data Security Important?

- ❑ **All businesses** today deal in data to a degree.
 - **Ex:**
 - banking dealing in massive volumes of personal and financial data.
 - one-man business storing the contact details of his customers on a mobile phone.
 - ❖ data is at play in companies both large and small.
- ❑ The **primary** aim of **data security** is to **protect** the data that an organization collects, stores, creates, receives or transmits.
- ❑ **Compliance** is also a major consideration.
 - It doesn't matter which device, technology or process is used to manage, store or collect data, it **must be protected**.
 - **Data breaches** can result in litigation cases and huge fines, not to mention damage to an organization's reputation.
- ❑ The importance of **shielding data from security threats** is more important today than it has ever been.

Different Data Security Technologies

- ✓ IT comes in many shapes and forms and **protects data** from a growing number of **threats**.
- ✓ Many of these threats are from **external sources**, but organizations should also focus their efforts on safeguarding their data from the **inside**, too.

Ways of securing data include:

- **Data encryption:** applies a code to every individual piece of data and will not grant access to encrypted data without an authorized key being given
- **Data masking:** Masking specific areas of data can protect it from disclosure to external malicious sources, and also internal personnel who could potentially use the data.
Ex: the first 12 digits of a credit card number may be masked within a database.
- **Data erasure:** There are times when data that is no longer active or used needs to be erased from all systems.
Ex: a customer has requested for their name to be removed from a mailing list, details should be deleted permanently.
- **Data resilience:** By creating backup copies of data, organizations can recover data should it be erased or corrupted accidentally or stolen during a data breach.

Data Security Compliance and Standards

When an organization collects any kind of personal data, it becomes as a **data processor**.

- A number of compliance regulations that govern organizations dealing in personal data **regardless of the type or volume**.
- Regulations depend on a **selection of factors**, such as the industry you are operating in and the type of data you store.
 - **EX:** if you store data relating to citizens in the European Union (EU) you will need to comply with the latest **GDPR** regulations.
 - Failure to comply with any regulations that affect your organization could result in hefty fines.

Other regulatory compliance and standards examples include:

NERC - **Critical Infrastructure Protection**

China's Personal Information Security Specification

PCI Security Standards

- Regulatory compliance requirements often vary by data type. **Ex:**
 - Personally Identifiable Information (PII)
 - Protected Healthcare Information (PHI, HIPAA)
 - Credit card information

Main Elements of Data Security

➤ **CIA triad:** confidentiality, integrity, and availability.

A security model and guide for organizations to keep their sensitive data protected from unauthorized access and data exfiltration.

- **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.

Why is Data Security

- **Access Controls:**
 - *regulate the reading, copying, changing and deletion of data and programs.*
- **Flow Controls:**
 - *can prevent a service program from leaking the customer's confidential data.*
- **Inference Controls:**
 - *A method of preventing data about specific individuals from being inferred from statistical information in a database about groups of people.*

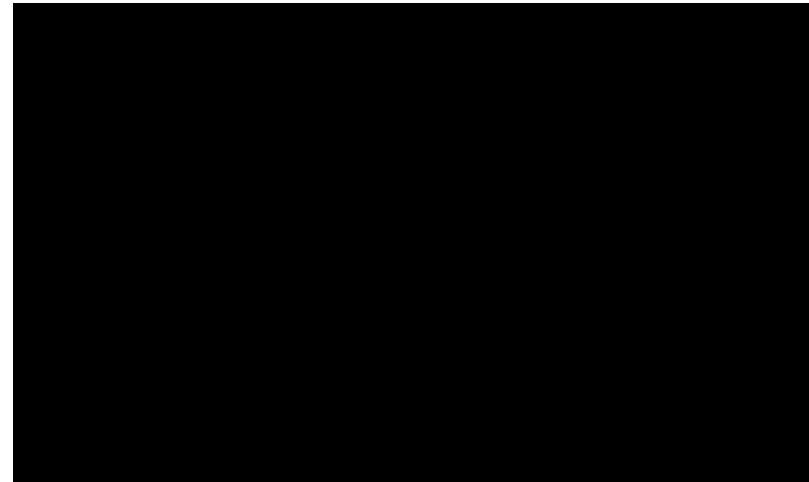
Why is Data Security(cont.)

- **Inference Controls:**
 - It is typical of database systems
 - It refers to the derivation of sensitive information from non-sensitive data.

Assume that there is a policy stating that the average grade of a single student cannot be disclosed; however statistical summaries can be disclosed.

- Suppose that an attacker knows that Carol is a female CS student
- By combining the results of the following legitimate queries:
 - `SELECT Count (*) FROM Students WHERE Sex = 'F' AND Programme = 'CS'`
 - `SELECT Avg (Grade Ave) FROM Students WHERE Sex = 'F' AND Programme = 'CS'`

The attacker learns from Q1 that there is only one female student so the value 70 returned by Q2 is precisely her average grade



Data vs. Information

- ❑ **Data** represents **information**.

 - ❖ *Information* is the **(subjective) interpretation** of data.

- ❑ **Data** represent **certain aspects of our conceptual and real world**.

- ❑ Data is used to:

 - ❑ **transmit and store information**

 - ❑ **derive** new information **by manipulating the data** according to formal rules.

- Data can be a number, symbol, character, word, and if not put into context, individual pieces of data mean nothing to humans.

- information is a data put into context, utilised by humans in some significant way.

Ex:

A computer uses programming scripts, formulas, or software applications to turn data into information.

Why Privacy is an important issue

- **Individuals feel**
 - Uncomfortable: ownership of information
 - Unsafe: information can be misused
 - (e.g., identity thefts)
- **Enterprises need to**
 - Keep their customers feel safe
 - Maintain good reputations
 - Protect themselves from any legal dispute
 - Obey legal regulations

Privacy:

- Ability of a person to control **availability** of information about and exposure of him-or herself.
- being able to **function** in society **anonymously** (pseudonymous or blind credential identification).

Data Privacy

- Problems exist *wherever **identifiable data** relating to a person(s) are **collected and stored**, in digital form or otherwise.*
- Improper or non-existent **disclosure control** can be the root cause for privacy issues.
- Most common sources of data affected by data privacy issues are:
 - Health information
 - Criminal justice
 - Financial information
 - Genetic information

Challenge: to share data while protecting personally identifiable information.

Privacy vs. Security

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

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

Computer security is about **controlling access** to **information and resources**.

- ❑ Controlling access to **information** can be quite elusive and replaced by controlling access to **data**.

Various threats to a computer system

❑ Accidents and Natural Disasters:

- Natural disasters such as flood, wind or earthquake, and accidents such as fire, power failure, and breakdown of electrical systems create threats to the organizations computer.

❑ High risk factor from Computer Abuse:

- High Vulnerability.
- Violation of the principle of separation of duties.
- Easy manipulation of large amount of data.
- Impersonal nature of systems.

❑ Human Initiated

- Hackers
- Unaware Staff
- Dissatisfied Staff
- Spy

Technology Available for Computer Security

- ☐ **Cryptography**
- ☐ **Biometric Systems**
- ☐ **Malicious Code and Anti Virus Solutions**
- ☐ **Firewall**
- ☐ **Intrusion Detection System (IDS)**
- ☐ **Virtual Private Network (VPN)**
- ☐ **PKI and Digital Certificates**
- ☐ **SSH Encryption**
- ☐ **SSL Encryption.**

Technology Available for Computer Security

❑ Cryptography

- Practice of the enciphering and deciphering of messages in secret code in order to render them *unintelligible to all* **but** the *intended receiver*.
- It is a high-level **encryption** technique that is being used to **ensure privacy** in the digital world.
- **Encryption** is:
 - the mechanism of **coding data** transmitted by **various telecommunication systems** so that only *authorized user* may have **access** to it.

Technology Available for Computer Security

❑ Biometric Systems

- is the application of any biological characteristics, such as pattern formed by the fingers, retinas, irises, hands etc. used for user authentication.

❑ Various biometric technologies:

- Fingerprint verification
- Hand geometry
- Retinal scanning
- Signature verification
- Voice verification
- Facial recognition

Technology Available for Computer Security

❑ Malicious Code and Anti Virus Solutions

The malicious code includes:

- **Computer viruses:**
 - Computer program designed to copy itself into other programs, with the intention of causing mischief or damage.
 - **Different Types of Viruses:**
 - Boot Sector viruses, File infectors, Macro viruses, Polymorphic viruses.
- **Spyware:**
 - a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge.
 - its presence is typically hidden from the user, and can be difficult to detect.
 - Typically, it is secretly installed on the user's personal computer.

Technology Available for Computer Security

❑ Malicious Code and Anti Virus Solutions(continued...)

■ **Worm:**

- is a self replicating virus that does not alter files but resides in active memory and duplicates itself.
- It use parts of an operating system that are automatic and usually invisible to the user.

■ **Trojan Horse:**

- is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage.

■ **Back Doors/Trap Doors:**

- codes written into applications to grant special access to programs bypassing normal methods of authentication.

■ **Logic Bombs:**

- programmed that hidden in commonly used software for an extended period of time until they are activate.
- They come embedded with some programs.

Technology Available for Computer Security

❑ Malicious Code and Anti Virus Solutions(continued...)

▪ Bacteria/Rabbit:

- These codes do not damage files.
- Their purpose is to:
 - deny access to the resources by consuming all processor capability/memory/disk space by self-replicating.

▪ Creators of Virus Code:

- The malicious codes are written / created by :
 - dissatisfied employees, spies, experimenters, publicity hunter, political activists, etc.

Damages Caused by Malicious Codes

- Loss of data services
- Leak of information
- Loss of reputation or legal penalty for software firm

Technology Available for Computer Security

❑ Malicious Code and Anti Virus Solutions(continued...)

Steps to protect the computer from viruses

- When installing new software, install it first on a **non-critical system** and test for bugs.
- **Periodically** review all system start-up and configuration files for changes.
- **Turn off** the automatic open on receipt feature from your e-mail software.
- Before opening any attachments **first scan** it using updated anti-virus software.
- **Regularly update anti-virus** software engine and data files.
- **Turn off** visual basic scripting.
- When **not in use** turn off the workstation or disconnect it *from the network*.
- Take **regular backup** of critical data and system files.

Technology Available for Computer Security

Firewall

- Computer security system that controls the **flow of data** from one computer or network to another.
- intended to protect the resources of a **private network** from being directly accessed by a user from an **external network**, especially via the **Internet**.

Why Firewalls?!

- Prevent outside access **except some special service** like E-mail or HTTP.
- **All incoming and outgoing traffic** from the Internet can be logged to provide **statistics** about the **network usage**.

Technology Available for Computer Security

Intrusion Detection System (IDS)

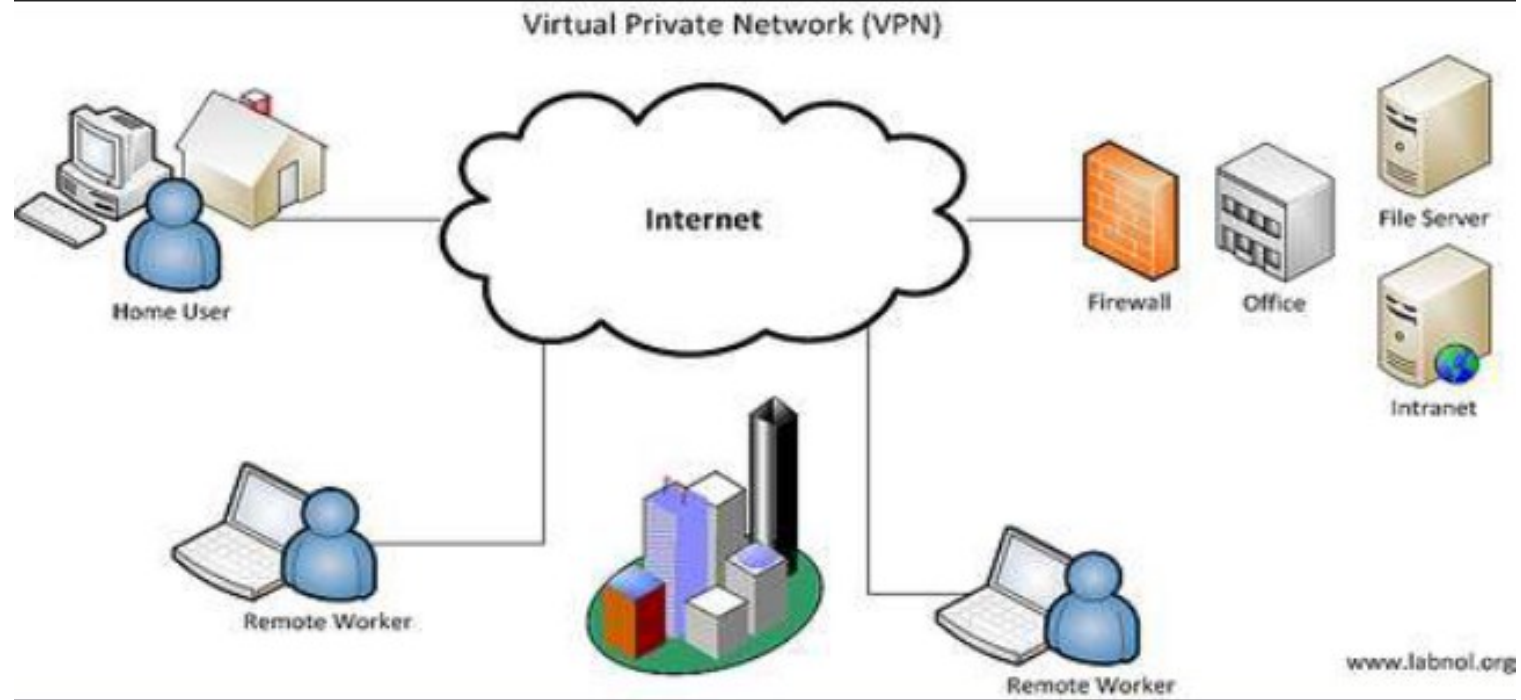
- A device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

- **Types:**
 1. Host Based Intrusion Detection Systems(HIDS)
 2. Network Based Intrusion Detection Systems(NIDS)security system that controls the flow of data from one computer or network to another.

Technology Available for Computer Security

Virtual Private Network (VPN)

- A network that is constructed by using public wires to connect nodes.
- use encryption and other security mechanisms to ensure that only **authorized users** can access the network and that the data cannot be intercepted.



Technology Available for Computer Security

PKI and Digital Certificates

- PKI (Public Key Infrastructure) is a process that enables users to implement public key cryptography.
- PKI offers various services related to **authentication** and **access control**, such as:
 - ❖ **digital certificates** to associate a **user's identity**, certificate download, signing of certificate, confirm validity of certificate, terminate certificate, etc.

SSH Encryption: Secure Shell (Developed by SSH Communications Security Ltd.),

- is a program to log into another computer over a network, to **execute commands** in a remote machine, and to **move files** from one machine to another.

SSL Encryption: Secure Sockets Layer

(Also known as TLS or Transport Layer Security)

- is a protocol developed by Netscape for **transmitting private documents** via the Internet.

SSH

SSH is the recommended method for remote management because it provides a secure connection. SSH provides encrypted password authentication and transport of session data. This keeps the user ID, password, and the details of the management session private. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.

Other Security Processes

- ☐ **E-Mail Security**
- ☐ **File system security**
- ☐ **Disk Mirroring**
- ☐ **Backup**
- ☐ **UPS**
- ☐ **Personnel Security**
- ☐ **Auditing**

Some Security Tips

- ✓ Encourage or require employees to choose passwords that are not common.
- ✓ Require employees to change passwords every 90 days.
- ✓ Make sure your virus protection subscription is current and update.
- ✓ **Educate** employees about the **security risks** of e-mail attachments.
- ✓ **Assess** your security posture regularly.
- ✓ When an employee leaves a company, **remove** that employee's network access immediately.
- ✓ If you allow people to work from home, provide a secure, centrally managed server for remote traffic.
- ✓ Update your Web server software regularly.
- ✓ Do not run any unnecessary network services.

Conclusion

- Due to hacking issue the popular British Tabloid “News of the World” has been banned.
- The Australian Internet activist Julian Assange has gone to the prison due to wikileaks.

But hacking is not stopped.

- ✓ So, we must aware of data security.
- ✓ We have to adopt the **latest technology** for defending the various threats.