Data Security and Privacy

Introduction

Data Security

- Data security is basically the process of keeping certain information private
- It involves the use of various methods to make sure that data is kept confidential and safe
- Data security ensures the integrity and the privacy of data, as well as preventing the loss or corruption of data.

Data Integrity

- When data is processed it is usually changed in some way or another
- Data integrity describes the correctness of this change
- Safeguards are needed to make sure that the data has integrity by detecting any mistakes or malicious change to the data

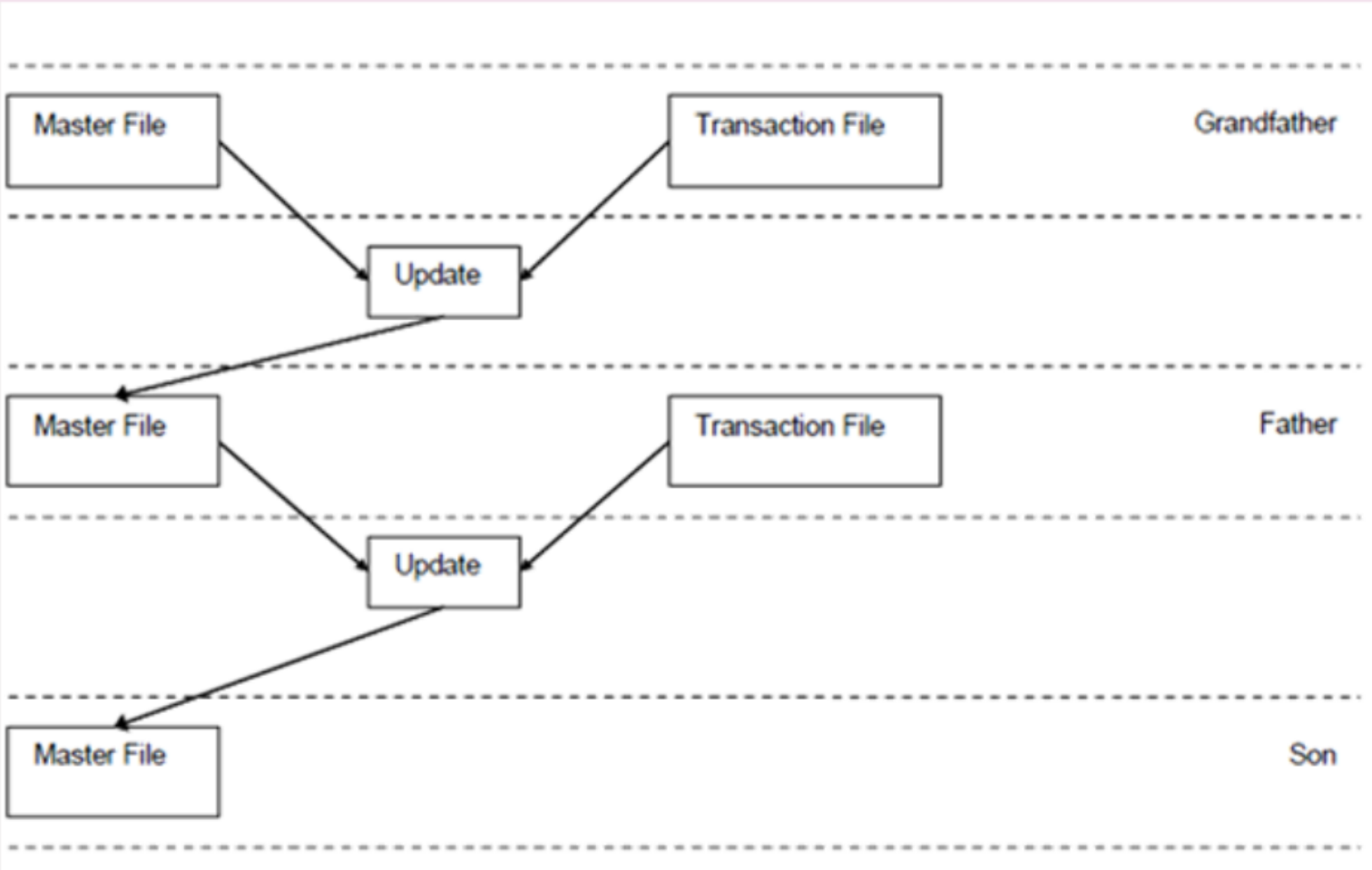
Need of Data Security

- Many businesses hold very important and confidential data
- Hence security of data is extremely important
- Data must be safeguarded all the time

Backups

- A master file stores the static data (does not change frequently) found on the database
- The transaction file keeps track of all the changes made to the database throughout the day
- At the end of the day, all the contents stored in the transaction file are transferred to the master file in order to update it
- This hierarchy is used for safety

Suppose the last Master File (Son) got corrupted by accidental deletion or corruption of data, the same Master File can be re-created by combining the father Master File with the respective Transaction File to obtain the son file once again.



Physical Security

- The most obvious choice of protecting data is to keep it in a safe locked room/building

- Protected rooms can be safeguarded by

1. A lock-and-key
2. ID card scanning
3. Biometrics (retina-scan, fingerprint-scanning)
4. Using a safe
5. Alarm systems

Software Safeguards

- There are many software measures which can protect data.

- The following explains some of the most common approaches used now a days

IDS

- IDS stands for Intrusion Detection System

- IDS monitors the operation of the network to detect illegal operations

- The system may be

1. server-based - detecting attacks on the operation of the file-server
2. network based, watching the pattern of traffic across the network

User ID

- User ID stands for User Identification
- This is a unique name or code used to identify a specific user when gaining access (logging in).
- Methods of using a user ID;

1. Passwords - words or codes known only to the user. A password is linked to a specific user ID.
2. Personal Identification Devices - a plastic card which identifies the user and acts as an electronic key. Most cards have a magnetic stripe to store information.
3. Personal Identification Numbers (PIN) - a number used as a password, particularly with bank cards and credit cards.

Biometric

- Biometric is when the human's features are used
- The individual's biometric is measured by a special scanner and used with the user ID
- Finding physical characteristics which cannot be copied has been difficult now a days we use

1. fingerprints
2. retina scans

- Face and voice recognition have not be reliable

Encryption

- Encryption makes data in a computer system illegible and makes data look meaningless
- Decryption is converting the illegible data back into its original form
- An encryption key is a code used for the encryption process
- A decryption key is needed before the data can be changed back to its original form

Digital Signature

- A digital signature makes used of encrypted data
- A digital signature is encrypted data used to show that the data being sent or read is genuine
- If the recipient of the data can correctly decrypt the digital signature then the data should be correct

Digital Certificate

- This is an encrypted message which confirms that the person is who they say they are
- A digital certificate includes a digital signature
- The certification authority, also known as a trusted service provider or a trusted third party, is a business that provides online certification facilities

Software Privacy

- Software Piracy is also very important as it stops

1. Duplication
2. Distribution
3. Unauthorized use of computer software

- It is illegal to use pirated software yourself, to give it away, or worse yet to sell it

Soft – Lifting

- Soft-lifting is when a people buy software with a single license and install it on more than one PC

Hard disk loading

- Hard Disk Loading this is when computer vendors install software on a new PC without selling the software itself, this is done, to sell a fully loaded machine at very low price because the user is not charged for the software

Downloading

- Downloading software from the Internet is much quicker and easier than buying it and installing it. Many P2P (peer-to-peer) applications exist (such as Torrents) which facilitate the download of illegal software.

Software Counterfeiting

- Software Counterfeiting is when software is copied illegally and re-sold. Some counterfeited software can be very obvious because only the CD is sold, but in more "sophisticated" counterfeited software; everything will be reproduced including the box, the manuals, etc

Copyright

- Copyright is a protection that covers published and unpublished

1. Literary,
2. Scientific
3. artistic works

basically whatever a person uses for expression

- The works mentioned above must be tangible or material form hence if you can see it, hear it and/or touch it; it may be protected

- Copyright laws grant only the creator the right to reproduce, prepare derivative works, distribute, perform and display the work publicly

Ethical Issues

- When you purchase software, you do not become the owner of the copyright., you are purchasing the right to use the software under certain restrictions

- Using copied or counterfeit software also means:

1. Greater exposure to software viruses, corrupt disks, or otherwise defective software
2. Inadequate or no documentation
3. No warranties
4. Lack of technical product support available to properly licensed users
5. Ineligibility for software upgrades offered to properly licensed users.

- Software piracy is not a victimless crime, piracy denies the software developer its rightful profits and harms consumers and the industry as a whole

- All software developers, spend years creating software.

Legal Issues

- There are also serious legal issues when in comes to software privacy
- In the USA, software theft is a serious matter. If you are caught copying software, you may be held liable under both civil and criminal law
- If the copyright owner brings a civil action against you, the owner can seek to stop you from using its software immediately and can also request financial payment . The copyright owner may choose between

1. Actual damages - which include the amount he/she has lost because of your violation
2. Legal damages - which can be as much as $150,000 for each program copied.

- In addition, the government can criminally prosecute you for copyright infringement, you can be fined up to $250,000, or sentenced to jail for up to five years, or both!

Software Protection

- Software developers try to protect their software by using many different protection measures.

1. **Serial Numbers:** Certain software will ask the user to input a serial number when installing the software. If the number is not inputted the software will not install
2. **Activation Keys:** After the software is installed, the user is required to enter some text (the activation key) so that the application will work. This activation key is usually obtained from the seller of the application. The user will send an e-mail with the product ID of the application, and after the seller will confirm that the software is original; he/she will send the activation key which will unlock the software.
3. **CD (or DVD) Copy Protection:** Most companies will create a special program when burning their application to the storage medium which will prevent users from copying the software
4. **Hardware Keys:** In this case a hardware device (such as a USB pen) is given with the software and for the software to be functional the USB must be connected to the machine

Software Registration

- Most software is registered with the company that sells the software. The user fills in some personal details such as name, address and e-mail. This will allow the company to serve its customers better

1. **Updates** : The software company can inform its registered members with news about the product. This may include news about new program releases, new updates or new patches to the program
2. **Bonus Features** : Certain companies create bonus features to the program
3. **Discounts** : Registered members usually benefit from discounts on applications released by the same company.
4. **Technical Support** : Some companies offer technical support

Access rights

- Access rights control whether or not a particular user can use or edit a program or data file.
- Each user is assigned different rights which determine the files that can be accessed. A user may be allowed complete access to a file or may be restricted only to read the data or have no access at all.
- Network operating systems provides a way of identifying individuals (for example by a user ID and password). Each individual can only access resources the user is given privileges for by the network manager.
- Some files have additional access restrictions provided by password protection. When a user attempts to gain access to one of these files an additional password will be requested before access is allowed. This provides extra security