Topic: 1.6.1 Data security

Computer security is a branch of technology known as **applied information security** to computers and networks.

The objective of computer security includes:

- Protection of information & property from theft
- Corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

Introduction

Information Systems are made of three subclasses, **hardware**, **software** and **communications** with the purpose to identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: **Physical**, **personal** and **organizational**. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within their organizations.

IT Security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer

Privacy

Privacy is the term used to prevent the disclosure of information to unauthorized
Individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the Merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Topic: 1.6.1 Data security

Breaches of confidentiality take many forms. Someone looking at your computer screen behind your back while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality.
Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

Integrity

In information security, **integrity** means that data cannot be modified without permission. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mis-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised.

Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

Basic System Security Measures
These Basic System Security Measures apply to all systems. It is a baseline, which all systems must meet. Note that for most personal workstations, these are the only measures that apply. The requirements are:

1. **Authentication and Authorization of user ccounts**
   - **Remove or disable accounts upon loss of eligibility:** Accounts which are no longer needed must be disabled in a timely fashion using an automated or documented procedure.
   - **Separate user and administrator accounts:** Administrator accounts must not be used for non-administrative purposes. System administrators must be provisioned with non-administrator accounts for end-user activities, and a separate administrator account that is used only for system-administration purposes.
   - **Use unique passwords for administrator accounts:** Privileged accounts must use unique passwords that are not shared among multiple systems. Credentials which are managed

centrally, such as the NetID/password combination, are considered a single account, regardless of how many systems they provide access to.

- **Throttle repeated unsuccessful login-attempts:** A maximum rate for unsuccessful login attempts must be enforced. Account lockout is not required, but the rate of unsuccessful logins must be limited.
- **Enable session timeout:** Sessions must be locked or closed after some reasonable period.
- **Enforce least privilege:** Non-administrative accounts must be used whenever possible. User accounts and server processes must be granted the least-possible level of privilege that allows them to perform their function.

2. **Firewall**

Systems must be protected by a firewall that allows only those incoming connections necessary to fulfill the business needs of that system. Client systems which have no business need to provide network services must deny all incoming connections. Systems that provide network services must limit access to those services to the smallest reasonably manageable group of hosts that need to reach them.

3. **Password Protection**

All accounts and resources must be protected by passwords which meet the following requirements, which must be automatically enforced by the system:

- Must be at least eight characters long.
- Must **NOT** be dictionary or common slang words in any language, or be relatively easy to guess.
- Must include at least three of the following four characteristics, in any order: upper case letters, lower case letters, numbers, and special characters, such as "!@#$%^&*".
- Must be changed at least once per year.

Topic: 1.6.1 Data security

4. **Digital signature**
It is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is **authentic**. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.

Digital signatures rely on certain types of **encryption** to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures.

Security measures designed to protect the security of data

Data Backup: Data protection is crucial for protecting your business's continuity. If your only data backup is on a computer and the hard disk crashes or is damaged by a power surge, your business's data is gone. And having paper copies of business data isn't adequate data protection; what if your business premises burns to the ground or destroyed in a flood? Once again the data you need to carry on your business could be irretrievably lost.

For adequate data protection, you need to establish a data backup system that follows these three steps:

1) Archive the business data regularly;
2) Create data backups on reliable media;
3) Keep updated data backups in a secure, off-site location.

The basic rule for business data protection is that if losing the data will interfere with doing business, then you should back it up. You can reinstall software programs if you need to, but recovering the details of transactions or business correspondence is impossible if those files are lost or damaged beyond repair. The rest of this article outlines each of the steps listed above so you can establish a data backup system that will effectively protect your critical business data from disaster.

Disk mirroring is a real-time strategy that writes data to two or more disks at the same time. If one disk fails, the other continues to operate and provide access for users. Server mirroring provides the same functionality, except that an entire server is duplicated. This strategy allows users to continue accessing data if one of the servers fails.

Topic: 1.6.1 Data security

Encryption:

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text ;* encrypted data is referred to as *cipher text*. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

Access Control

Access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. Normally, a user must first Login to a system, using some Authentication system. Next, the Access Control mechanism will controls what operations the user may or may not make by comparing the User ID to an Access Control database.

Access Control systems include:

- File permissions, such as create, read, edit or delete on a file server.
- Program permissions, such as the right to execute a program on an application server.
- Data rights, such as the right to retrieve or update information in a database.

Data Integrity vs. Data Security

Data is the most important asset to any organization. Therefore, it must be made sure that data is valid and secure at all times. **Data integrity** and **Data security** are two important aspects of making sure that data is useable by its intended users. Data integrity makes sure that the data is valid. Data security makes sure that data is protected against loss and unauthorized access.