SECURITY CONCEPTS

Data & Information

Most of us use the words 'data' and 'information' to refer to the information which is handled by the computer. However, the two words have different meanings. We will explain the different meanings using the following example:
The 8-digit number 02062014 is 'data'. However, when this number is interpreted as a date, then this number has a meaning and this will be referred to as 'information'. The word 'information' is used to refer to the processed 'data'.
Data is raw, unorganized facts that needs to be processed. Data can be something random and useless until it is organized.
When data is processed, organized, structured or presented in a given context so as to make it useful, it is called information. **Information** is the processed output of data making it meaningful to the person who receives it.

Cybercrime refers to any crime that involves a computer and a network (e.g. the Internet).

Password cracking involves recovering passwords from data that has been stored in or transmitted by a computer system. The purpose of password cracking might be:

- to help a user recover a forgotten password;
- to gain unauthorized access to a system, or
- as a preventive measure by system/network administrators to check if their users are making use of passwords that can be easily cracked.

Software cracking involves modifying a computer program to remove or disable features such as copy protection, serial numbers, hardware keys, date checks etc. For example, cracking the trial/demo version of particular software so that this will start functioning as fully licensed software. The distribution and use of cracked copies of software is illegal.

Threats to Data

The following represent some threats to data:

- **Force majeure** is an event or effect that cannot be reasonably anticipated or controlled by a company. For example data can be damaged or destroyed because of natural disasters (e.g. a fire, floods and earthquakes) or war.
- **Employees** may intentionally steal or damage company data such as client details or product information. They could use this data to their advantage such as selling this data to other competing companies. Employees can also accidentally lose or delete company data.
- **Service providers** involved in storing the data of companies on their servers can lose, destroy or steal valuable data. Loss of data may be intentional or accidental.
- **External individuals** can also gain access to a computer or network and steal, damage and delete the data. As indicated in the previous section these individuals are often referred to as hackers.

Characteristics of Information Security

The policies for information security within an organisation are based on these characteristics:

- **Confidentiality** is a set of rules that limits access to information. Confidentiality prevents sensitive information from reaching the wrong people, while making sure that the right people can get it. Some methods used to ensure confidentiality include data encryption, passwords, two-factor authentication and biometric verification.

- **Integrity** is the assurance that the information is trustworthy and accurate.

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed whilst being transmitted. Steps must be taken to ensure that data cannot be altered by unauthorized people.

- **Availability** of information refers to ensuring that authorized people are able to access the information when needed. Information is unavailable when it is lost, or when access to it is denied or delayed. For example, information on a website may not be readily available to users because the web server is over loaded by a denial-of-service attack.

Social Engineering

Social engineering is the process of manipulating people to perform some action that will lead unauthorised users to break into a computer or network. This process is usually non-technical and relies heavily on human interaction and often involves tricking people to divulge confidential information e.g. passwords.

Typically social engineering is used:

- To **gather information** that may be confidential or valuable.
- To gather information to commit an act of **fraud**.
- To facilitate **unauthorised access to a computer system or network** that may reveal confidential data.

Social engineers often rely on the natural helpfulness of people who may not be aware that it is dangerous to give out sensitive information. Social engineers use methods to gain the confidence of people and trick them to release information that may be used to break into a computer or network.

Examples of social engineering include the following:

- **Phone calls** – Misleading someone about your identity in a phone call to gain valuable information.

Example: You receive an unsolicited (unexpected) phone call from a person claiming to be an employee at the IT department of the organisation you work for. S/he informs you that urgent maintenance is needed to the organisation's network and therefore s/he requires your username and password to access the network. You provide the requested details which s/he will use to access data on the company's network.

- **Phishing** – A type of online identity theft. It uses email and fake websites that are designed to steal your personal data or information such as bank card numbers, passwords, account data, or other information.

Example: You receive an email that appears to be sent from the bank claiming that there is a problem with your account. The email requests you to provide your credit card number and the security code at the back of the card. Typically the email will contain a link to a fake web page that seems legitimate. The fake webpage will contain the bank logos and a form which you will use to send the requested credit card details. After you respond, these credit card details will be used to make purchases.

- **Shoulder surfing** – This involves watching someone use his/her computer from "over his/her shoulder" to get sensitive information such as username and password.

Example: You are at the cash point in the supermarket making a payment with your bank card. The persons behind you may be able to see you keying in your personal identification number. To prevent shoulder surfing, you should cover the keypad from view by using your body or cupping your hand.

Social engineering is probably the greatest threat to any security system. Prevention

includes educating people about the value of information, training them to protect it,

and increasing people's awareness of how social engineers operate.

Identity Theft

Identity theft occurs when someone steals your personal information and uses it without your permission. This can create serious problems.

- **Personal** – Someone may steal the username and password that you use to access a social networking site e.g. Facebook. S/he will use these details to take over your profile account and may start communicating with your friends and posting messages on your wall. These actions may harm your reputation.
- **Financial** – Someone may steal the username and password that you use to access your online shopping mall e.g. Amazon. S/he will use these details to take over your profile account. If you have saved your credit card details in the profile, s/he may be able to purchase goods and pay for these using your credit card.
- **Business** – Someone may steal the username and password that you use to access the network of the company you work for. S/he will gain access to sensitive data such as client data or company accounts etc.
- **Legal** – Someone may steal your personal details and use these to fraud a company. This may lead the company to take legal action against you.

Identity theft can occur through the following methods:

- **Information diving** – The practice of recovering sensitive information from discarded material. For example, recovering data from hard disks of computers that have been thrown away. Some people replace their computer and forget all about erasing all data from its hard disk. Another method to collect personal information is going through the garbage from businesses and homes. People may throw away dated documents e.g. bank statements in the garbage. Documents and CDs/DVDs containing sensitive information should be shredded before being thrown away. Hard-disks should have all the data erased before these are thrown away.
- **Skimming** – This involves the illegal copying of information from the magnetic strip of a credit card. This information is copied onto another blank bank card's magnetic stripe. This fake bank card may be later used to make purchases and withdraw money from the victim’s bank account. Skimming occurs by using a counterfeit (fake) card reader that records all data on the bank card as it passes through it. Card skimming may occur in different places including the card away from the actual account holder in order to run the charge. One must also be careful when asked to swipe the bank card through more than one machine.
- **Pretexting** – This involves gaining personal information through deception. The victims are tricked into giving away information that will be used to steal their identity. For example you receive a call from a person who claims to be a bank employee. S/he informs you that there is some problem with one of your bank accounts and asks you for specific information to solve the problem. S/he will use this information for example, to claim that s/he has forgotten the account number or needs information about the account history. To protect yourself from pretexting, never provide personal, confidential, or financial information when you receive unsolicited (unexpected) calls. If the callers tell

you that they are representing a company/bank you do business with, tell them that in order to protect yourself against identity theft, you will contact the company/bank yourself.