TRENDS IN COMPUTING

Defn

COMPUTER INTEGRITY AND SECURITY

SOFTWARE INTEGRITY

Software integrity refers to methods of ensuring that software is real, accurate and safeguarded from unauthorized user modification.

Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication).

Digital forensics /digital forensic science is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.

HARDWARE INTEGRITY

Hardware Integrity to methods of ensuring that hardware is safeguarded from unauthorized access and modification.

COMPUTER INTRUSION

Computer intrusions/Attacks occur when someone tries to gain access to any part of your computer system. Computer intruders or hackers typically use automated computer programs when they try to compromise a computer's security.

There are several ways an intruder can try to gain access to your computer. They can:

a) Access your computer to view, change, or delete information on your computer.
b) Crash or slow down your computer.
c) Access your private data by examining the files on your system.
d) Use your computer to access other computers on the Internet.

COMPUTER SECURITY/COMPUTER PROTECTION

COMPUTER SECURITY

Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.

It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

Security is the ability of a system to protect information and system resources with respect to confidentiality, availability and integrity.

Therefore these elements of security must be considered :-(CIA triaged

- **Confidentiality** is a set of rules that limits access to information or Confidentiality is the concealment of information or resources. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry.

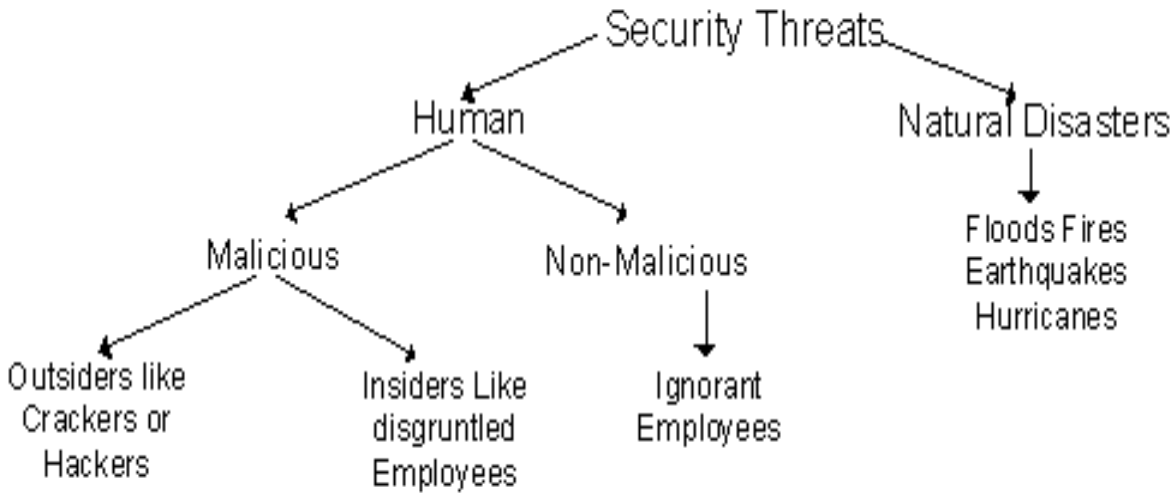
- **Integrity** refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication).

- **Availability** refers to the ability to use the information or resource desired. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all.

Importance of computer security

a) Computer security is important, primarily to keep your information protected.
b) It's also important for your computer's overall health
c) Helping to prevent viruses and malware and helping programs run more smoothly.
d) To help curb the increasing volume and sophistication of cyber security threats – Threats of this nature include targeting phishing scams, data theft, and the exploitation of other vulnerabilities in the network.

Security threats



Purpose of Data Security

- Controlling access to machine and data resources.
- Controlling the way *access rights* are passed from user to user.
  - person to person
  - program to program
- Preventing maliciousness and errors from subverting the controls.
- Understanding the challenges/Risks involved and providing solutions.

Major Threats.

Potential Security Threats To Computer Systems

A computer system threat is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure.

Knowing how to identify computer security threats is the first step in protecting computer systems. The threats could be intentional, accidental or caused by natural disasters.

What is a Security Threat?

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be **physical** such as someone stealing a computer that contains vital data. The cause could also be **non-physical** such as a virus attack.

There are two types of threats

a) Physical threat
b) Non physical threat

(a) PHYSICAL THREATS

What are Physical Threats?

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

Employees are responsible for more successful intrusions than outsiders. It becomes very difficult to find the source of internal attacks without alerting the attacker that you suspect him of wrong-doing.

The following list classifies the physical threats into three (3) main categories;

- **Internal**: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- **External**: These threats include Lightning, floods, earthquakes, etc.
- **Human**: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

To protect computer systems from the above mentioned physical threats, an organization must have physical security control measures.

The following list shows some of the possible measures that can be taken:

- **Internal threats**:

    a) Fire threats could be prevented by the use of automatic fire detectors and extinguishers that do not use water to put out a fire.

    b) The unstable power supply can be prevented by the use of voltage controllers. Power backups, power regulators.

    c) An air conditioner can be used to control the humidity in the computer room.

- **External threats**:

    a) Lightning protection systems can be used to protect computer systems against such attacks. Lightning protection systems are not 100% perfect, but to a certain extent, they reduce the chances of Lightning causing damage.

    b) Housing computer systems in high lands are one of the possible ways of protecting systems against floods.

- **Humans threats**:
    - Threats such as theft can be prevented by use of locked doors and restricted access to computer rooms.

What are Non-physical threats/Technical threats

A non-physical threat is a potential cause of an incident that may result in;

a) Botnets. Botnets are networks of compromised computers used by hackers for malicious purposes, usually criminal in nature.
b) Cloud computing (delegating the task of protection to a third party usually through shared resources, or remote storage and host.
c) Disrupt business operations that rely on computer systems
d) Illegal monitoring of activities on computer systems
e) Loss of sensitive information
f) Loss or corruption of system data
g) Nonexistent security architecture (usually due to lack of qualified IT Administrators). Inadequate network protection results in increased vulnerability of the data, hardware, and software, including susceptibility to malicious software malware, viruses, and hacking.
h) Phishing attempt to acquire information such as usernames, passwords, credit card details by masquerading as a trustworthy member of an organization.
i) Poor Configuration Management.
j) Removable media: provide a pathway for malware to move between networks or hosts.
k) Un-patched Client Side Software and Applications.

l) Use of mobile devices; such as laptops or handheld devices, smart phones outside organizations.

The non-physical threats are also known as **logical threats**. The following list is the common types of non-physical threats;

- Virus
- Trojans
- Worms
- Spyware
- Key loggers
- Adware
- Denial of Service Attacks
- Distributed Denial of Service Attacks
- Unauthorized access to computer systems resources such as data
- Phishing
- Other Computer Security Risks

TO PROTECT COMPUTER SYSTEMS FROM THE THREATS, AN ORGANIZATION MUST HAVE LOGICAL SECURITY MEASURES IN PLACE.

The following list shows some of the possible measures that can be taken to protect cyber security threats

- ❖ To protect against viruses, Trojans, worms, etc. an organization can use anti-virus software. In additional to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visiting the website that is most likely to download unauthorized programs onto the user's computer.

- ❖ Unauthorized access to computer system resources can be prevented by the use of authentication methods. The authentication methods can be, in the form of user ids and strong passwords, smart cards or biometric, etc

- ❖ Intrusion-detection/prevention systems can be used to protect against denial of service attacks. There are other measures too that can be put in place to avoid denial of service attacks.

Summary

- A threat is any activity that can lead to data loss/corruption through to disruption of normal business operations.

- There are physical and non-physical threats

- Physical threats cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters.

- Non-physical threats target the software and data on the computer systems.

COMMON THREATS

❖ Errors and Omissions

It becomes difficult to protect our systems from the people who need to use it day in and day out.

❖ Fraud and Theft

Computer fraud is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system.

Computer theft refers to the stealing of the physical parts of the computer.

❖ Malicious Hackers

Several groups of Internet users out there that will attack information systems.

They are hackers, Crackers or phreaks.

- ❖ **A computer hacker** is a person who, with their technical knowledge, uses bugs or exploits to break into computer systems.
  - **Hacking** is the process of gaining unauthorized access into a computer system, or group of computer systems. This is done through cracking of passwords and codes which gives access to the systems.

- ❖ **A cracker** is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there.
  - **Cracking** is the act of breaking into a computer system, often on a network.
- ❖ **A phreak** is someone who breaks into the telephone network illegally, typically to make free long-distance phone calls or to tap phone lines. The term is now sometimes used to include anyone who breaks or tries to break the security of any network.

- ❖ **Malicious Code** is software/code that is designed to make a system perform any operation without the knowledge of the system owner.

- **Denial-of-Service Attacks** is an attempt to make a machine or network resource unavailable to its intended users.

- **Social Engineering** is the name given to a category of security attacks in which someone manipulates others into revealing information, that can be used to steal data, access to systems, access to cellular phones, money, or even your own identity.

Computer crimes also commonly referred to as cybercrimes refers to any crime that involves a computer and a network.

To commit a cyber crime a user takes advantage of a computer to take or alter data, or to gain unlawful use of computer services.

The crimes include but not limited to;

a) A root kit
b) Alterations
c) Autorun worms
d) Boot sector malware
e) Cookies
f) Cracking
g) Email spoofing
h) Hoaxes
i) Key logging
j) Malware
k) Parasitic viruses
l) Patches
m) Phishing
n) Privacy and Fraud
o) Ransom ware
p) Sabotage
q) Social engineering
r) Social networking websites
s) Spam
t) Spear phishing
u) Spyware
v) Tapping
w) Tracking
x) Trespass
y) Worms

Explanation:

a) **A root kit** is a piece of software that hides programs or processes running on a computer. It can be used to conceal computer misuse or data theft.

b) **Alteration**: When a system is compromised, the data stored in it can be compromised. For example. When students break into a system and alter exam results. Bank accounts can too be altered.

c) **An exploit** takes advantage of a vulnerability in order to access or infect a computer.

d) **Auto run worms** are malicious programs that take advantage of the Windows Auto Run feature. They execute automatically when the device on which they are stored is plugged into a computer.

e) **Boot sector malware** spreads by modifying the program that enables your computer to start up.

f) **Cookies** are files placed on your computer that allow websites to remember details.

g) **Email spoofing** is when the sender address of an email is forged for the purposes of social engineering

h) **Hoaxes** are reports of non-existent viruses or threats are software add-ons designed to fix software bugs, including security.

i) **Key logging** is when keystrokes are secretly recorded by an unauthorized third party.

j) **Malware** is a general term for malicious software including viruses, worms, Trojans and spyware. Many people use the terms malware and viruses interchangeably.

k) **Parasitic viruses**, also known as file viruses, spread by attaching themselves to programs.

l) **Patch** operating systems or applications.

m) **Phishing** refers to the process of tricking recipients into sharing sensitive information with an unknown third party.

n) **Ransom ware** is software that denies you access to your files until you pay a ransom

o) **Sabotage** is a computer crime which involves deliberate attacks intended to disable computers or networks

p) **Social engineering** refers to the tricks attackers use to fool victims into performing an action. Typically, these actions are opening a malicious webpage or running an unwanted file attachment.

q) **Social networking websites** allow you to communicate and share information. But they can also be used to spread malware and to steal personal information.

r) **Spamming** is the use of electronic messaging systems like e-mails and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately. An unsolicited messages is what we call spam

s) **Spear phishing** is targeted phishing using spoof emails to persuade people within a company to reveal sensitive information or credentials.

t) **Spyware** is software that permits advertisers or hackers to gather sensitive information without your permission.

u) **Tapping**: when someone gains access to information that is being transmitted via a transmission/communication link. Users should note that any information passed over a network is vulnerable provided security measures are not appropriate.

v) **Tracking***:* Monitoring computer usage in a real time environment. This is either done remotely or during a physical session, usually used on internet users.

w) **Trespass**: when someone is able to access your computer and able to see or use your files illegally.

x) **Worms** are viruses that create copies of themselves across the Internet or local networks.

Protection Measures

- Educate users
- Encrypt all important data
- Use secure passwords
- Implement additional security checks (fingerprint, Eye scanners)
- Encrypt all important data
- Restrict Plug and Play

HOW TO BUY ONLINE SAFELY

a) Research retailers online to make sure they're legitimate.
b) Make sure the website is secure.(https)
c) Know your rights and the company's returns policy.
d) Keep software and virus protection up-to-date and use strong passwords for online accounts.
e) Don't use public Wi-Fi. Your standard data connection is more secure.
f) Pay using a credit card. You will have more protection. Alternatively, online services like PayPal mean scammers will not be able to get hold of your bank details.
g) Be smart. If a deal looks too good to be true, it probably is not worth taking.

HOW TO BE SAFE ON THE INTERNET

a) Create Complex Passwords. We know you've heard it before, but creating strong, unique passwords for all your critical accounts really is the best way to keep your personal and financial information safe.
b) Use a Firewall. Even if your network is secure, you should still use a firewall.
c) Click Smart. Now that you've put smart tech measures into place, make sure that you don't invite danger with careless clicking. Many of today's online threats are based on phishing or social engineering.
d) Be a Selective Sharer. These days, there are a lot of opportunities to share our personal information online. Just be cautious about what you share, particularly when it comes to your identity information. This can potentially be used to impersonate you, or guess your passwords and logins.
e) Protect Your Mobile Life. Our mobile devices can be just as vulnerable to online threats as our laptops. In fact, mobile devices face new risks, such as risky apps and dangerous links sent by text message.
f) Practice Safe Surfing & Shopping. When shopping online, or visiting websites for online banking or other sensitive transactions, always make sure that the site's address starts with "https", instead of just "http", and has a padlock icon in the URL field.
g) Keep up to date. Keep all your software updated so you have the latest security patches. Turn on automatic updates so you don't have to think about it, and make sure that your security software is set to run regular scans.
h) Lookout for the latest scams. Online threats are evolving all the time, so make sure you know what to look out for.
i) Keep your guard up. Always be cautious about what you do online, which sites you visit, and what you share. Use comprehensive security software,

and make sure to backup your data on a regular basis in case something goes wrong.

HOW TO AVOID VIRUSES, TROJANS, WORMS AND SPYWARE

- Use updated antivirus or endpoint security software
- Block file types that often carry malware
- Subscribe to an email alert service
- Use a firewall on all computers
- Stay up to date with software patches
- Back up your data regularly
- Disable Auto Run functionality

COMPUTER ETHICS

Computer ethics are the moral guidelines that govern the use of computers and information systems. Frequently concerned areas of computer ethics are;

- Unauthorized use and access of computer systems.
- Software piracy
- Information privacy
- Intellectual property rights
- Codes of conduct

(a) **Unauthorized access and use of computer systems**. Unauthorized access is the use of a computer or a network without permission.

A cracker or a hacker is someone who tries to access a computer or a network illegally. Some hackers break into a computer for the challenge. However, others use or steal computer resources or corrupt a computers' data.

Unauthorized use is the use of a computer or its data for un approved or possibly illegal activities. Examples of unauthorized use of computers include;

- An employee using a company computer to send personal e-mail.
- Someone gaining access to a bank computer and performing an unauthorized transfer.

One way to prevent unauthorized access and unauthorized use of computers is to utilise access controls.

(b) **Software piracy**. Software piracy refers to the unauthorized and illegal duplication of copyrighted software. Software piracy is the most common

form of software theft. Purchasing software only provides a consumer with a license agreement or the right to use the software.

A single user license agreement or end-user license agreement is the most common type of license included with software packages purchased by individual users. It usually permits a consumer to;

- Install the software only once on the computer and make one copy for back up. However, the consumer is usually not permitted to;
  - Install the software on a network
  - Give away copies of the software to others or
  - rent or lease the software

A software site license gives the buyer the right to install the software on multiple computers at a single site. (e.g a school computer laboratory)

A network site license allows network users to share a single copy of the software which resides on the network server.

Risks of software piracy

- Increase the chance of spreading computer viruses.
- No technical support for the software can be received.
- Drive up the software cost for all legal users.
-

(c) **Information piracy**. Information piracy refers to the right of individuals or organizations to deny or restrict the collection and use of information about them.

(d)

Information accuracy becomes an important issue when it is necessary to access information by other people or companies such as that one on the internet.

Inaccurate input can result in erroneous information and incorrect decisions made based on that information. Never assume that information provided on the web is always correct.

(e) Intellectual property rights. **Intellectual property (IP)** refers to work created by inventors, authors and artists.

Intellectual property rights are the rights to which creators are entitled for their work.

A copyright© gives authors and artists exclusive rights to duplicate, publish and sell their materials.

A trade mark ™ protects a company's logos and brand names

(f) **Codes of conduct**. A code of conduct is a written guideline that helps determine whether a specific action is ethical or unethical.

Sample IT codes of conduct

- Computers may not be used to harm other people.
- Users may not interfere with others' computer work.
- Users may not meddle in others computer files.
- Computers may not be used to steal.
- Computers may not be used to bear false witness.
- Users may not copy or use software illegally.
- Users may not use others' computers resources without authorization.
- Users may not use others output.
- Users should always use computers in a way that demonstrates consideration and respect for other people.

THE COPY RIGHT LAW

THE COPYRIGHT AND NEIGHBOURING RIGHTS ACT, 2006.

Work eligible for copyright.

1) The following literary, scientific and artistic works are eligible for copyright in uganda
   a) Articles, books, pamphlets, lectures, addresses, sermons and other works of a similar nature;
   b) Dramatic, dramatic-musical and musical works;
   c) Audio-visual works and sound recording, including cinematographic works and other work of a similar nature;
   d) Choreographic works and pantomimes;
   e) Computer programmes and electronic data banks and other accompanying materials;
   f) Works of drawing, painting, photography, typography, mosaic, architecture, sculpture, engraving, lithography and tapestry;
   g) Works of applied art, whether handicraft or produced on industrial scale, and works of all types of designing;

h) Illustrations, maps, plans, sketches and three dimensional works relative to geography, topography, architecture or science;

i) Derivative work which by selection and arrangement of its content, constitute original work;

j) Any other work in the field of literature, traditional folklore and knowledge, science and art in whatever manner delivered, known or to be known in the future.

COMPUTERS AND SOCIETY

The study of computer studies has become too rich that it is now getting had to draw a difference between *Computer Studies* and "ICT".

Computers and communication have brought and still bringing changes in our lives. Therefore, the following concepts are more or less becoming family names.

- Information technology
- The communication revolution/Telephone revolution
- Internet revolution
- Multimedia (data, sound & video)
- The Binary Age
- Information society
- The information super high way/ "Information" or I-way or Data-Way.
- The digital Age or Dot Age.

The need for better and best ways of doing things has triggered more and more research in the best technologies, more reliable information, and the best communication means.

IMPACT OF IT/ICTs ON SOCIETY

ICTs have had both positive and negative contributions to society.

a) BENEFITS/ADVANTAGES OF INFORMATION TECHNOLOGY.

- Increased interaction /collaborations through e-mails, chat rooms, video conferencing, etc
- Increased sharing and access to common databases within and outside organizations through networking.
- Increased access to information through DBMS. Huge amounts of material on all subjects now exist – ease research.
- Increased inventions and innovations.
- More and more technology in management fields.

- Improved and sustained quality goods and services.
- Increased efficiency and effectiveness' leading to increased productivity (hence less wastages & more efficient use of resources).
- Increased investment opportunities in commercial tele-centers, Internet cafes, chart rooms, etc.
- More leisure as people get shorter working hours. Increased use of ICTS implies higher standards of living.
- Highly skilled jobs are being created like programming, systems analysis. Software engineering, etc.
- Many IT products for the disabled.
- Reduced costs of production through less demanding ICTs
- Improved corporate image.

b) <u>Disadvantages</u>

- Widens the gap between the rich and the poor as the rich producing with the help of ICTs produce faster and flood the markets.
- Isolate older people since it is not very easy for them to cope with the many IT changes.
- Bombards (internet) people with too much information- (good and bad)
- Increased instability as people get compelled to learn new things every now and then.
- Health problems e.g. eye sight losses, repetitive strain injury, etc
- Moral problem through access of pornographic materials on the net.
- Erosion of individual privacy as more data about people is stored on databases and can be accessed any time.
- Unemployment as less skilled people get retrenched and their roles taken over by more effective ITs.
- Addictions to computer games plus surfing by young people
- ITs isolate man and also erode the social aspect of work as some people opt for executing their office duties from their homes.
- Initial, maintenance and on-line IT costs are very high seggregative.
- Virus threats make data stored on computers very insecure.
- Increased crime through forgeries, piracy, etc.

AREAS OF APPLICATION FOR INFORMATION TECHNOLOGY

1. **Education and training.**

   Many Universities, Colleges, school and public libraries are on line with websites for purposes of making easy access to educational information..

   Education references soft ware e.g. the Infopedia, Encarta, etc are programs used for helping people with English usage, data collection and analysis etc

2. **Information plus data storage**.

ITs have got immense internal and external storage devices for storage of huge volumes Data. Hence the common paperless society

3. **Word Processing**

Word processor programs e.g. Microsoft word, word star, lotus notes etc are now on market for use to produce professional looking documents like, letters, invoices, orders etc.

They have easy to use document edit, format, table tools etc.

4. **Business**

E-Business and **E-commerce** facilitate the buying and selling of goods, services and works on line.

Businesses have got websites and networked computers they use to advertise, processing of orders, receipting of purchased products, etc.

For instance Web sites like: - www. CD-Now for buying music CDs, DVDs & VCDs, and Interflora.com – for flowers.

Other businesses include;

- Computer Secretarial Bureau.
- Internet cafes.
- Commercial computer schools.
- On-line banking

5. **Entertainment and Leisure.**

ITs offers lots of leisure and entertainment activities in form of;

- Computer games
- Computer audio music and video players
- Games on line
- Leisure centers on line.
- Leisure websites

Skynet.com for sports and manu.com, are some of the informative leisure websites.

6. **Health & Medicine.**

ITs are now being used for;

- Medical tests for instance blood, cancer, Brain damage etc

- Carrying out sensitive operations on sensitive body parts like the brain, heart, kidney, etc.
- Drug mixing and prescriptions.

7. **Transport & communication**
ITs are also being used for;

a. Units of carriage surveyarance in logistics management.
b. Sending and receiving of messages like sms (E-mail = sms over the internet), and interactive websites.
c. Reservations for units of carriage and hotels.
etc

8. **Accounting and Finance.**
Software/programs are now available for producing financial reports like income statements, Balance sheets, and cash flow statements. Such programs aid financial planning plus management, determination of NPV, PBP, IRR, etc

Such application/programs include Pastel, Tally, Sand systems, Excels, etc

9. **Climate and Weather**:

Programs have now been developed to accurately predict and report changes in climate and weather to aid travelers and farmers.

10. **Security and military.**

IT Laser guided cameras and satellites are now used for national and domestic security. Business like Banks, supermarkets etc also use IT Laser guided cameras for customer monitoring in the business hall.

Information technologies are also used in the military to fly and direct combat planes, locate enemy positions and hit/shell them with minimal civilian and property losses.

11. **Manufacturing:-**
In many large manufacturing and production processes robots are being used to handle tasks, which cannot be efficiently handled by humans.

Computer Aided Design (CAD) and CAM (Computer Aided Manufacture) are also in this category.

Other areas of application include;

- Hotel and Institutional catering.
- General Management. For instance**;** DSS, HRS, MKT, ESS, tele-working and tele-commuting**.**
- Information technology helps in the jurisdiction of cases in courts of laws, sports and games; iTs (video evidence) have been adduced to influence decisions.

Emerging technologies and developments in Hardware and Software

CURRENT TRENDS IN HARDWARE PLATFORMS

There are many trends in hardware platforms in recent years

- ✓ Integration of Computing and Telecommunications Platforms
- ✓ High rate of computation via network
- ✓ Integration of telephone and internet
- ✓ High computing power
- ✓ Grid Computing
- ✓ Cost saving on large infrastructures
- ✓ Smaller computer are connected to form a grid
- ✓ Increase the ability of organizations
- ✓ High speed of computing
- ✓ Cloud Computing
- ✓ Cost Saving as no capital investment is needed
- ✓ Automatic Computing
- ✓ Develop systems that can automatically download updates, Protect themselves from hackers and intruders. Recover themselves in case of failure.
- ✓ Virtualization and Multi-core Processors
- ✓ Both reduces power consumption
- ✓ Virtualization – Accessing computing resources in multiple ways irrespective of geographical location and physical configuration.
- ✓ Multi-core Processors – Use multi-core processors to reduce power consumption and heat.

CURRENT TRENDS IN SOFTWARE PLATFORMS

- ✓ Linux and the open-source software movement
- ✓ Linux is one of the most widely used open source software program
- ✓ Linux is supported by almost all platforms like HP, IBM, Intel, Dell, Sun etc.

- ✓ Java Programming language that is independent of the operating system and hardware processor.Java virtual machine has been defined.Java is compatible with any hardware
- ✓ Leading interactive programming language available for the Web is Java.
- ✓ Software for enterprise integration
- ✓ The usage of enterprise-wide software systems by firms is an important trend in last few years.
- ✓ The goal is to achieve an integrated firm-wide information environment, reduce cost, increase reliability, to adopt business best practices which are captured by the software.
- ✓ oftware outsourcing
- ✓ It is the prewritten software developed by a software company
- ✓ It helps the organizations from developing their own softwares.

Mobile Platform

- ✓ The growth of telecom industry especially in mobile sector has been incredible over last few years. The service providers upgraded the mobile networks with next-Generation services like 3G, WAP and GPRS.
- ✓ The banks are trying to capitalize this growth in the telecom sector and provide the services to the customers through mobile. The main advantage of mobile banking over the Internet banking is that it offers 'Anywhere Anytime Banking'. Customers can check their accounts, transfer funds, balance statements etc during travel without the access to a computer. The limitations of Internet Banking are overcome in mobile banking since it requires only a mobile which can be accessed by people of developing countries also.
- ✓ Grid Computing

The basic idea of Grid computing is that the computers are connected as a grid and the software running in the grid gives more priority to local users, but when they become idle these computers are used over the grid.

Providing remote access to IT resources

THE FUTURE OF COMPUTERS AND THE INTERNET

It is easy to predict that the computers and related equipment will get faster in memory, smaller and cheaper. Computer technology will find new application and manufacturers will strive to make computing easier and cheaper

Possible future trends in computer capabilities, physical size, price and software.

(a) **Future computer capabilities**. On the capabilities fronts, computers are going to evolve. They;
- Are going to have more powerful, smaller processor and faster access to memory.
- Will have operating systems that will handle real time data analysis and object oriented.
- Will have improved user interfaces that offer users easier and more intuitive access to information.
- Will have multi-media applications that will be fully incorporated into some information systems because data is easy to interprete when presented as a combination of sight, sound and motion.

(b) **Physical size**. Most hardware components will get smaller and faster. This means computers will become smaller and do more.

(c) **Price**. As technology advances, the price of computers will go down. Every sphere of ife will be permeated by computers, which will be common even among people of average earning.

(d) **Software.** Software development will also develop to allow users easily operate computer systems. To facilitate document, the best programming and operating systems are moving towards object-oriented system. OS will play an integral part in giving the user more control over how data are linked and shared. New operating systems will focus on object linking, message passing and data sharing.

(e) **Artificial intelligence**. Artificial intelligence is the process of building computer systems that simulate human thought processes and actions. The goal of artificial intelligence is not to replace human intelligence which is not replaceable; rather it is to help people to become more productive. In the past, computers used calculating power to solve structured problems. This field of artificial intelligence is moving in the mainstream of data processing.

Artificial intelligence attempts to develop computer systems that can mimic or simulate human thought processes and actions. This include reasoning and learning from past actions. True artificial intelligence that corresponds

to human intelligence is still a long way off. However, several tools that emulate human problem solving and information processing have been developed. Many of these tools have practical applications for business. They include expert systems, natural language processing, artificial neural network and robots.

Expert systems. Expert systems are computer programs that essentially emulate the knowledge of human experts skilled in a particular field for example of a geologist or a medical doctor. They have both textbook knowledge and tricks of trade that an expert acquires after years of experience as a result of the programs that can be really complicated.

Areas of application

- Finance/Business planning
- Teaching field. They compliment teachers knowledge e.g typing tutor, project planning and monitoring.
- Special areas. Act as substitute for retiring human experts.
- Banking

Natural language processing. Natural language processing is the capacity of computers to "understand" human language and translate it into actions upon which to act.

Artificial Neural Networks. Present computers and super markets are relatively slow because of the build in structural limitations. The processor and the main memory are physically separated.

Robots. Robots is the field of study concerned with developing and building robots. Robots are machines that are used in factories and can be programmed to do more than one task. Robots are used in the manufacturing industry mainly to reduce costs and increase productivity. They are excellent in executing repetitive tasks that human beings find boring. Robots do not get tired. They are also ideal to replace human beings on hazardous jobs. They are different types of robots which include;

(i) **Industrial Robots**. These are used in factories to perform certain assembly tasks. Examples are machines used in automobile plants to do welding, painting, loading and unloading. In the garment industry, robot pattern cuts and create pieces of fabric for clothing.

(ii) **Perception Robots**. Some Robots imitate human senses e.g a robot with television camera or vision system can be used for guiding machine tools for inspecting products and for identifying and sorting parts. Other types of perception robots rely on the sense of touch for example those used on micro-computer assembly lines to put parts in place.

(iii) **Mobile Robots**. Some robots act as transporters e.g mail mobiles which carry mail to offices following a pre-programmed route.

N.B

1. JOB REPLACEMENT. This is a situation where by certain jobs disappears in an organization but reappears in another form requiring more and high skilled man power e.g copy typists using typewriters are still needed in organizations but now use computers word processors instead of typewriters.

2. **JOB DISPLACEMENT**. This is the process of replacing man power with computerized machines either their own or with the help of a few skilled and highly trained people. In most cases, the eliminated jobs are those involving monotonous and unskilled labour for example factory jobs can be displaced by machines called robots.

SYSTEM ANALYSIS

This is the process of solving computer problems and use of computer technologies to meet the needs of an organization.

This is the first stage of the system analysis. Here the analysist makes a survey by gathering information needed for the system and the allocation of the requirements to the software.

THE BENEFITS OF SYSTEM ANALYSIS

Every organisation has several businesses and systems that function individually and cohesively to achieve a set of targets.

System analysis is the detailed evaluation of a particular system to identify areas for improvements and make any enhancements if necessary.

This includes; gathering the company requirements and researching the path to be taken to effect these requirements. The ultimate target is to have a fully operational system in place which provides efficiency and reliability to the organisation.

A question which is often asked regarding system Analysis is “What are the benefits of system analysis?”

- **Costs, Efficiency & Flexibility**. When a system analysis is properly performed, it makes certain that the correct path is taken with regards to applications and it helps to minimize errors which reduce future IT requirements for fixing problems.it will also save money and ensures that the right path is taken in getting an application.

- **Better Management**; Better controls. System analysis allows for better management through changing the software to suit any business changes, this means that the final product will be totally controllable.

- **Risks**. Through the process potential threats are identified. A risk assessment is carried out to evaluate all the negative impacts on the processes.

- **Quality**. The quality of the systems is ensured through the checking of the system constantly through system analysis.

What is System Development Life Cycle (SDLC)?

Definition: SDLC is stand for System Development Life Cycle. The System Development Life Cycle is a conceptual model used in project management that describes the stages involved in an information system development project.

System development life cycle is a model used to describe the level of information system development projects from beginning until it is completed.

System Development Life Cycle (SDLC) includes 5 steps which are:-

a) Planning
b) Analysis
c) Design
d) Implementation
e) Maintenance.

This 5 phase is a systematic strategy to large-scale development projects and to develop the information system.

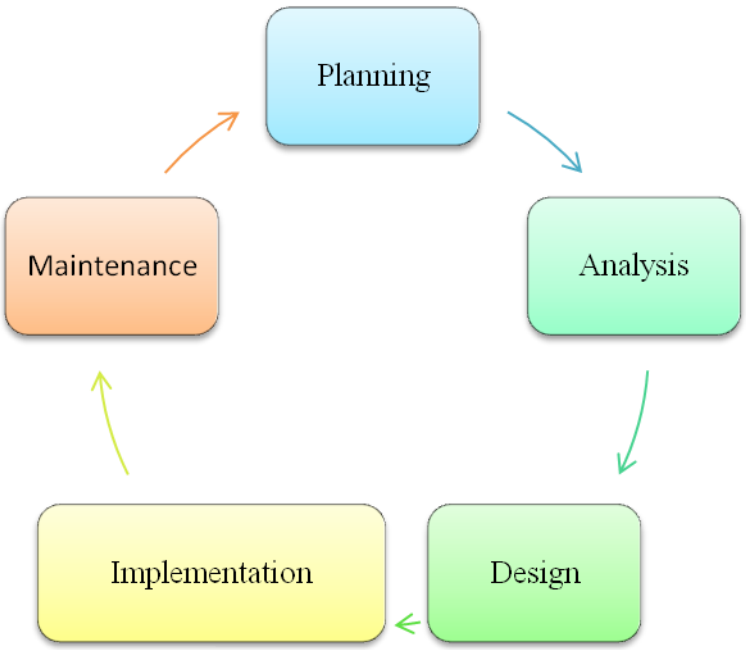


Figure 1: System Development Life Cycle (SDLC) Phases

SYSTEM DEVELOPMENT LIFE CYCLE'S PHASE

There have 5 phases in system development life cycle.

Planning

planning is the first phase we need to do instead of other phase which is analysis, design, implementation and maintenance because of planning is the phase to create a project plan and without the project plan how the company proceed to the next phase.

Besides that, during the planning phase, the objective of the project is determined and the requirements to produce the product are considered. An estimate of resources, such as employees and costs, is prepared, along with a concept for the new product. All of the information is analysed to see if there is an alternative solution to creating a new product. If there is no other viable alternative, the information is assembled into a project plan and presented to management for approval.

Analysis. We need to analyse by breaking down all parts which is draw a diagram and also we need to talk with the stakeholders and the technical providers to gather the entire requirement.

Besides that, in the analysis stage the project team need to determine the end-user requirements. Often this is done with the assistance of client focus groups, which provide an explanation of their needs and what their expectations are for the finished product and how it will perform. The project team documents all of the user requirements and gets a sign-off from the client and management to move forward with system design.

Design this is the third phase of system development life cycle used to decide if the system will be created in house or out sourced. This design phase come before implementation phase because in this phase we need to identify how the system will operate and how it will be used by end users. This design phase also will re-examine the feasibility study done in the analysis phase.

Besides that, design phase is the "architectural" phase of system design. The flow of data processing is developed into charts, and the project team determines the most logical design and structure for data flow and storage.

Implementation phase come as a fourth phases in system development life cycle. Implementation phase is the phase where the system is built or purchased and tested. In this phase the training is implemented for end users. Besides that, this implemented is use by end users is evaluated.

Maintenance. In this phase the maintenance happens once the system is operational. It includes implementation of changes that software might experience over a period of time, or implementation of new requirements after the software is deployed at the customer location. The maintenance phase also includes handling the outstanding errors that may exist in the software even after the implementation phase. This phase also monitors system performance, repairs viruses and requested changes are made.

CAREER OPPORTUNITIES IN INFORMATION AND COMMMUNICATION TECHNOLOGY

Information and communications technology (ICT) has created new job tittles such as;

- Computer operators.
- Computer technicians.
- System analysts
- Computer programmers
- Software engineers
- Information system manager
- Database administrator
- Computer trainer
- Website administrator
- Computer graphics designer
- Network administrators

This section explains some responsibilities of these professionals who are generally called information technology workers.

a) **Computer technician**. Given that all computers regular maintenance, upgrading as well emergency repairs, demand for computer technicians continue to grow as more and more computerize their work place and homes.

Responsibilities of a computer technician

- Troubleshooting computer hardware and software related problems.
- Ensuring that all computer related accessories such as printers, modems, storage media e.t.c working properly.
- Assembling and upgrading computers and their components.
- In developed countries, technicians help hardware engineers in designing and creating some computer components such as motherboards, storage devices e.t.c.

b) **System analyst**. The is a person who is responsible for analyzing a company's needs or problems then designs and develops a computer based information system. A good information systems analyst is one who has the following attributes.
   - Good problem solving skills, creativity i.e must have experience in solving problems.
   - Good communication skills; the analyst must be able to communicate clearly and precisely both in writing and in speech.

- He/she must be able to talk to different groups of people e.g managers, operators, attendant and general public.
- Must have business knowledge; the analyst must be well trained in relevant areas of computer science such as hardware, software and programming knowledge.

Responsibilities

- Reviewing the current manual or redundant information system and making recommendations on how to replace it with a more efficient one.
- Working with programmers to construct and test the system.
- Coordinating training for users of the new system.

c) **Computer programmer**. Large organizations like insurance companies, banks, manufacturing firms and government agencies hire programmers to work together with system analyst in order to;

- Write in-house applications programs or system programs
- Customise commercial application package to suite the organization needs.
- Test, debug, install and maintain programs developed or customized for the organization.

d) **Software engineer**. A software engineer is one who is skilled in software development and technical operation of computer hardware.

Responsibilities

- Developing system and application software.
- Developing user and technical documentations for the new software.
- Maintaining and updating the software to meet day to day requirements while overcoming challenges.

e) **Computer engineer**. Computer and electronic engineers are coming up with more efficient and communication technology almost daily. Since computers are electronic devices, hardware designers must be good in electronic engineering in order to be able to;

- Design and develop computer components such as storage devices, motherboards and other electronic components.
- Re-engineer computer components to enhance its functionality and efficiency.

- Design and develop engineering an manufacturing computer controlled devices such as robots.

f) **Information system manager**. The information system manger controls, plans, staffs, schedules and monitors all activities of the ICT department in the organization. Using computerized management information systems (MIS), the manger can test the impact that an alternative course of action might have on the business.

Other responsibilities

- Making sure that all tasks in the IT department are done correctly and on time in order to support business planning, control and decision making processes.
- Preparing budgets for the department.
- Keeping the department inventory records up-to-date.
- Managing the human resource with in the department.

g) **Computer trainer**. Due to the dynamic nature of computers and information technology, there is a high demand for qualified ICT trainers. Some of the responsibilities of an ICT trainer are;

- Training people on how to use a computer and various application programs.
- Developing training reference materials.
- Guide learners on how to acquire knowledge through carrying out research.
- Advising learners on the best career opportunities in the broad field f ICT.
- Preparing learners for ICT examinations.

h) **Database administrator**. The major purpose of computerising organizations or institutions is to store data in an organised way for easy access, retrieval and update. The organization requires a person who should be responsible for updating records in an information system database. For this reason, a database administrator is responsible for;

- Designing and developing database application for the organization.
- Setting up security measures needed to control access to data and information.
- Keeping the database up-to-date by adding new records, modifying or deleting unnecessary records.

i) **Website administrator/ Web master**. Internet is one of the areas of information and communication technology that has drawn the interests of most people. These people are able to exchange messages, search for information and business through the internet.

Business organizations, educational institutions and individuals put information on the internet by developing websites. Most organizations hire the services of a web developer who is given the role of a company's web administrator also referred to as a web master.

Responsibilities

- Developing and testing websites.
- Maintaining, updating and modifying information on the websites to meet new demands by the users.
- Monitoring the access and use of internet connection by enforcing security measures
- Downloading information needed by an organization or institution from internet websites.

POSSIBLE FUTURE TRENDS OF THE INTERNET

- The internet will continue to expand and change in several ways; faster connections, more users, new multimedia and virtual reality services.
- More interactive services such as multimedia newspapers, livestock market tickers, automatic notification of when pre-destinated events take place anywhere on the internet.
- Internet as universal as a radio and television today.
- Learning will become any time anywhere.
- Impact of information technology to the society, morally unemployment vision, laxity and entertainment.