COMPUTER ORGANIZATION AND ARCHITECTURE

Lecture 12

Computer Security and Safety, Ethics, and Privacy

Dr Victoria Mukami

INTRODUCTION

This lecture is an introduction to computer security and safety, ethics, and privacy. During this lecture, we will review hardware loss and failure and software issues. This will involve a review of internet and network attacks and unauthorised access and use. We will then review intellectual property rights, computer ethics and finally information privacy.

Learning objectives

By the end of this topic, you should be able to:

1. Understand the various types of attacks and crimes committed by computers
2. Identify the categories of intellectual property
3. Understand ethics and privacy as related to computers.

OVERVIEW

This is the last lecture in the series. Throughout this lecture, we have reviewed the intricacies of the computer, the uses of computers and all the components of computers. This lecture now focuses on the human element. Computers were invented to make work easier for human beings. As with anything in this world, there is the good that can be done by computers and of course the bad. This is dependent on the user's intention. We review how to protect ourselves from harm, protect our systems from harm and how to respect other people's property (computers and information). It is necessary to study this topic due to computer crime. Computer crime is defined as any illegal activity using a computer. We start by first reviewing some of the security issues that target hardware devices and the ways to prevent the issues.

HARDWARE LOSS, DAMAGE AND SYSTEM FAILURE

Hardware loss occurs when a computer is lost or stolen. This loss can result in damaged hardware or the loss of information belonging to the owner.

Hardware theft: this is the most common way in which one suffers a hardware loss. This happens when a device such as a computer or peripheral device is stolen. Most of the hardware thefts result in the resale of the pieces of the hardware. In other cases, hardware thefts are targeted at company executives who posses' information that may be sold to competitors.

The easiest way to deal with hardware theft is using physical locks and other access controls. Ensure where the hardware devices are stored, the doors are physically locked, and if in the event the room is accessible by many people, have the device like a laptop connected directly to the desk. If one's device is stolen with the intent to sell information, it is best if the user encrypts their information so that it is inaccessible.

Hardware loss: this happens when one misplaces or loses hardware. When a user loses a computer, they may end up having to replace the device at an added and unexpected cost. Additionally, they may lose information on their device that may be irreplaceable. Ways of preventing are like the ones for hardware theft. In addition, devices could be fitted with trackers that can pinpoint the location of a misplaced device.

Hardware damage: this occurs due to man-made and natural disasters. These include floods, power fluctuations, electric storms, and abuse [4]. Most of these disasters result in hardware that is beyond repair. While it may be hard to plan for natural disaster plans, it may be possible to make a backup and recovery plan especially when the disaster is out of your hands. A **disaster recovery plan** is a plan that tells the organization what do to prepare for and recover from a disruptive event, such as a fire, natural disaster, terrorist attack, or computer failure [4].

System failure: this occurs when the system stops working for one reason or another. Reasons vary and could include, overwhelmed resources, power fluctuations that short-circuit the system etc. The failures could be the result of a hardware problem, software problem, or computer sabotage [4]. The best way to prevent failures is to take proper care of devices. This includes a surge protector to protect from power surges. An uninterruptible power supply (UPS) would ensure that the system keeps running even when there is no power.

INTERNET AND NETWORK ATTACKS

When we use the internet, we transmit a lot of personal and confidential information through it. Computers especially on a network are at a higher risk of various network attacks. There are several network risks with the most common being malware. Malware is short for malicious software, and they are programs that work without the user's knowledge and alter how the computer works.

Virus: like the biological virus, a computer virus is a program (software) that infects a computer and alters the way the computer works without the user's knowledge [1].

Worm: this program copies itself repeatedly and causes the computer resources to be overwhelmed thereby shutting down the computer or even network.

Trojan Horse: like Troy the Greek story, a trojan horse pretends it is a legitimate program but within it is normally malicious code that changes the way the computer works. Trojan horses are triggered by a certain condition [1].

Rootkit: This is like a backdoor. It is a program that is hidden within the computer and allows for illegal connections remotely.

Botnet: these are computers that have been compromised on a network and are used to attack other computers within the same network.

Denial of Service Attacks: this is an attack aimed at trying to disrupt computer access to the internet.

Safeguards

Several safeguards exist to ensure that a computer does not get infected with malware.

1. Use of an antivirus software
2. Avoiding inserting removable media onto a computer
3. Ensuring the firewall on personal computers is enabled
4. Updating the operating system to ensure that they have the latest security updates
5. Avoid opening email attachments whose source you do not trust
6. For rootkits, one needs to ensure they have two or three-level verification of users.
7. Users' usernames and passwords need to be updated frequently to ensure no unauthorized access.
8. Additional access controls such as biometric identification will safeguard against illegal access.

INTELLECTUAL PROPERTY RIGHTS

Intellectual property rights are legal rights to which creators of intellectual property are entitled [4]. These rights normally indicate who has the right to use or display a creative work and what can be legally done. Most creative rights are retained by the creator of the content. Intellectual property includes books, movies, music, paintings, works of art etc. There are three main types of rights

Copyright

This is protection given to the developer or inventor of intellectual property. A copyright gives the holder the exclusive right to publish, reproduce or distribute their intellectual property. What this means is that if an individual or company wanted to use the works, they would need to request permission from the copyright holder. Copyrights last the lifetime of the creator and go on until 70 years after the demise of the creator.

Trademark

A trademark represents a sign that is used to differentiate between one product and another. Within Kenya, trademarks are registered by the Kenya Industrial Property Institute (KIPI). A trademark allows for a company or individual to show exclusive ownership. Apart from the products, logos are also trademarks to ensure people do not use the logos to market their own companies. The symbol ® is used to show trademarked products.

Patents

A patent protects inventions by granting exclusive rights to the inventor for 20 years [4]. A patent is generally given to a unique product with computer-related inventions currently leading in the number of patents being issued. Patents are expensive and time-consuming, however major companies regularly seek patents.

ETHICS

This is generally defined as moral conduct [4]. Computer ethics then is defined as the moral conduct when using computers. This has become necessary due to the adage that computers and using the internet make one feel invisible since the other person cannot see you. Anonymity has made people feel invulnerable to the extent that they

can post anything and do anything no matter the consequences. Computer ethics, therefore, deal with how to be morally good when using a computer.

From the previous section, we saw the definition of various intellectual property rights. Ethics guide how copyrighted materials are used. Unless explicitly indicated, one is not allowed to reproduce, make copies, or use any copyrighted materials without prior authorization by the intellectual property owner. In the case of a book, while you may not expressly get permission from the owner, it is good practice not to pass off someone's else work as your own. In this case, it is recommended to cite where you quote someone to prevent plagiarism. Plagiarism is defined as passing off someone's else work as your own.

One of the areas that have seen a rise in infringement is software. Software piracy is defined as the illegal or unauthorised copying of a computer program. Software piracy has become a big business especially in poorer countries where citizens are unable to afford software licences. Ethical obligation dictates that one should not pirate or even use pirated software.

INFORMATION PRIVACY

This refers to the rights of individuals and companies to deny or restrict the collection and use of information about them [1]. Information privacy will mainly deal with what a company or another individual can do with your information that may be stored within their company or not. An example is the social network Facebook. Facebook collects a lot of information about its members. Members are normally meant to indicate whether their information can be made available to third party users or not. The company has had to pay large amounts of money to offset fines due to privacy related matters. There are several ways in which companies collect information both legally and illegally from consumers or users.

Electronic profiles: this is information collected when you fill in a form to either gain access to content on a website or when you fill in forms online. This information gets saved into a database which can then be sold to other individuals.

Cookies: this is a small text file that is stored on your computer by the website to ensure faster loading. A recent law was passed within the EU that required websites to ask for the consent of cookies being used when one is using a website.

Spyware and Adware: these are programs that either collect information secretly on the user or display advertisements online.

Spam: these are uncalled for emails that are sent to several (hundreds, thousands or even hundreds or thousands) people at once. The information within a spam email differs but most are advertisements of products.

Phishing: this is a scam where a legitimate-looking email is sent to collect your information and more so financial information. The email could request financial details such as credit cards, PINS, and others.

Employee Monitoring: this is the use of computers to observe your employees while at work. While employee monitoring may sound illegal, it is actually within the rights of the employer to monitor the employee to make sure that they are performing their duties.

Content Filtering: this is the use of specific programs within the computer to filter the kind of content that one sees on the internet. For instance, a company may filter out social networks to prevent employees from wasting time going to those websites. Further, countries have filtered content that they deem immoral or may not be for the good of their citizens. An example is China that has heavy filters that will censor Google websites, social media sites such as Facebook among others.

Privacy Laws

Several laws exist that concern themselves with ensuring that privacy is maintained by individuals or corporations. Globally several laws exist, and the following is an excerpt by G. Shelly and M. Vermaat from the Discovering Computers book.

Common points in some of these laws include the following:

1. Information collected and stored about individuals should be limited to what is necessary to carry out the function of the business or government agency collecting the data.
2. Once collected, provisions should be made to restrict access to the data to those employees within the organization who need access to it to perform their job duties.
3. Personal information should be released outside the organization collecting the data only when the person has agreed to its disclosure.
4. When information is collected about an individual, the individual should know that the data is being collected and have the opportunity to determine the accuracy of the data.

Figure 1: Excerpt on Privacy Laws summary [1]

Within Kenya one of the laws that exist that has propelled and ensured that data is protected is the Privacy and Data Protection Policy of 2018. Additionally, there is the Kenya Data Protection Act of 2019.

SUMMARY

Throughout this lecture, we have done an introduction to computer security and safety, ethics, and privacy. During this lecture, we have reviewed hardware loss and failure and software issues. This included ways in which to prevent hardware loss and how to recover in the event of disasters. We also reviewed internet and network attacks and unauthorised access and use. Finally, we reviewed intellectual property rights, computer ethics and finally information privacy including laws that govern information privacy.

DISCUSSION TOPIC

One of the greatest concerns when using a computer especially on the internet is privacy concerns. As an individual, you may not be aware of all the laws that may protect you as you use the internet. Companies whose websites you use may collect information from your either secretly or by letting you know. Collecting information with your permission does not expressly permit them to sell it to manufacturers. The company could argue that they are in the business of making money, while at the

same time the individual may state that their information belongs to them. In the case of legally collecting data, do you think the company is within their rights to collect information? Should the individual whose data is being collected just be ok with it? Thoughts?

REFERENCES

[1] G. Shelly and M. Vermaat, Discovering Computers — Fundamentals: Your Interactive Guide to the Digital World. Boston, MA: Course Technology, 2012.

[2] W. Stallings, Computer Organization and Architecture Designing for Performance. Hoboken, NJ: Pearson Education, Inc, 2016.

[3] A. Evans, K. Martin and A. Poatsy, Technology in Action. New York, NY: Pearson, 2020

[4] D. Morley and C. Parker, Understanding Computers: Today and Tomorrow. Boston, MA: Course Technology, 2017.