ENGINEER SMART
ADEBITI EMMANUEL OLUWAGBEMIGA
513
(Prudence)

Do not write in this margin

UNIVERSITY OF BENIN

Question..... 40399

Write on both sides of the paper

4th

Do not write in this margin

INTRODUCTION

The term security is associated with freedom from or resilience against a potential harm caused by others. Computer security has to do with the protection of the computer hardware, information/data from damage or theft. Computer security also ensures the prevention of service disruption which may occur as a result of damage or theft. The traditional computer facilities have only succeeded in protecting the physical machine (hardware) since modern computers now has pervasive remote access. This suggest that the penetrator does not need to be physically present with the computer hardware to initiate an attack or a threat. The terms attack and threat are activities aimed at gaining access to computers for malicious purposes.

Who are involved in Computer security?

They are the experts who study the field and recommend preventive measures to forestall any possible attack and or provide corrective solutions in the event of an attack, the users or owners who suffers from the effect of the breakdown of the computer as a result of an attack and the prepetrators who are responsible for the attack or damage.

The prepetrators of an attack can be classified into two forms/classes namely insider and outsider. The insider attack are attacks perpetrated by legitimate users while the outsider attacks are perpetrated by illegitimate users. For example in an organization that empolys the use of several computers to perform computations as well as other functions, an inside attack would come from the employees while the outside attack would come from the non-employees.

The insider and outsider threats can be classified as insider overt, insider covert, insider unintended, outsider overt, outsider covert, outside unintended.

* Insider Overt: These threats are performed by disgrunt-

NB: Computer security threats can be classified into 4 broad classes: physical security, Engineering, Software, Network security

UNIVERSITY OF BENIN

Question.....

Write on both sides of the paper

led employees for the purpose of destroying data and equipments.

* Insider covert: This form of threat is wreak for the purpose of criminal intentions.
* Insider unintended: This threat occurs as a result of human errors and neglect of duties such as wrong inputs, wrong data, damage arising from extreme temperature or other harsh conditions, and interruption of vital services.
* Outsider overt: This form of attack has to do with physical attacks on the computer and other network facilities.
* Outsider covert: This form of attack encompasses the various types of rogue software sent from the outside to a personal computer or to a computer facility.
* Outsider unintended: This has to do with an attack on a computer from an outsider done unintentionally. It is important to note that it is rare to see an outsider attacking a computer or data unintentionally.

At times too, some attack may occur by accident. This usually happens though not on the computing field. They are caused either by forces of nature such as flood or earthquake or indirectly by humans.

Why do computers need security?

* Lacks intelligence: It is true that modern science and technology has led to the invention of sophisticated computers that are very fast, accurate & very powerful in the computing and manipulation of data. But these computers are not efficient in performing tasks that requires intelligence. Lack of intelligence exposes computers to security threats which compromises the integrity of the system.
* Ease of Compromise. The integrity of a computer can easily be broken because of its many security

weakness. A perpetrator only need to find one of the weakness in order to do harm.

* Simplicity of the operating system: A computer is designed to be controlled by an operating system. operating systems by nature are extremely complex. For ease of usage, a system programmer would have to design an operating system such that it is less complex and this makes it less secure.

* Connection to the Internet & its protocols: Communication is one of the benefits resulting from the use of the internet. For communication to be possible, the computer requires to have communication standards which results in the development of communication protocols. This protocol is a set of rules that specifies the individual steps of a complete Internet session. For computers to be able to send, forward and receive mails, they have to execute the same protocol. These internet protocols have been developed many years ago before the internet security became a complex issue, which is why the security features included in the protocols are usually weak.

Laws of security

It is important to note that the best way to minimize security risks is to comply the use of common sense. Nonetheless, there are 10 laws to help us:

* If someone can persuade you to run his program on your computer it is not your computer anymore.
* If someone can alter the operating system on your computer it's not your computer anymore.
* If someone has unrestricted physical access to your computer, it is not your computer anymore.
* If you allow someone to upload program to your website, it is not your website anymore.
* Weak passwords defeat strong security.
* A computer is only as secure as its owner/user is trustworthy.
* Encrypted data is only as secure as the decryption key.

3

UNIVERSITY OF BENIN

Question.....

Write on both sides of the paper

* An out of date virus scanner is only marginally better than none at all.
* Absolute anonymity isn't practical, in real life or on the web.
* Technology is not a Panacea.

Resources for computer security

Resources for computer security are best found in the internet specifically, the web. The web contain web sites which provide historical information, discuss recent developments and threats, it also educates the computer users, as well as offers tools and techniques for the protection of the computer.

PHYSICAL SECURITY

Whenever the Phrase computer security is been mentioned what normally comes to our mind are security issues that relates to virus infestation, loss of privacy, identity theft, or ways to ensure the safety of sensitive data sent across a network. But on a broader scope, computer security encompasses issues relating to physical protection of the computer equipment against visible attacks such as fire, theft or natural disaster like flood.

* Side Channel Attacks: This form of attack is based on obtaining information from the implementation of a computer system while disregarding the weaknesses in the implemented algorithm. The sped information are obtained via timing information, Power consumption, electromagnetic leaks or even from sound. Some side channel attack requires the spy to have a technical knowledge of the internal operation of the computer system.

NB: Classes of physical attack

- Invasive: This requires the depackaging of the chip so as to gain direct access to its inside components

for example the connection of a wire on a data bus to see the data transfers.

- Non-invasive: This exploits externally available information such as the running time and power consumption etc
- Active: This tries to tamper with the device proper functioning, for example, fault-induction attacks will try to induce errors into the computation data.
- Passive: This simply observes the system behaviour during its processing, without any form of disruption.

The side channel attacks to be considered are those where the spy tries to exploit information leakages (non-invasive) without any form of disruption to the system (passive), this is of interest because this forms of attacks can be generally performed using relatively cheap equipments. They pose a serious threat to security of most cryptographic hardware devices ranging from smart cards to the personal computers to small embedded devices like smart cards and RFIDs.

A. By nature the information obtained from a computer usually consist of electromagnetic radiation, sound, light from displays and variations in power consumption. Practical implementations have shown that an idle CPU requires less power than a busy CPU. A spy can then measure the power consumption of a CPU to determine if the CPU is busy or idle. Also the power consumption of a system depends on the instructions that are being executed, for example a CPU would consume a certain amount of power while executing a loop instruction and this (power consumption) most likely will change when it comes out of the loop.

B. During system operation, the CPU emits electromagnetic radiation which can be detected outside the computer, outside the computer room and even outside the computer building. A spy who knows the type of CPU being spied on can execute many programs on the same type of CPU, measure the radiation emitted and thus associate certain patterns of radiation with

UNIVERSITY OF BENIN

Question.....

Write on both sides of the paper

certain types of computer operations such as idle loops, or input/output. Once these associations have been established, the spy can then train a computer program to analyse radiation emitted by a spied computer and draw conclusions about the activity of the spied CPU at various times.

Another information leak that can assist spy in covering attack to a computer is the sound generated from the system. Granted, the CPU is an integrated circuit enclosed in a ceramic or plastic container with no moving parts. But inside the container, there are several parts such as the CPU chip cavity, the wires, the chip and printed connections that vibrates thereby generating sound. These sounds can be detected using a sensitive microphone and then analyzed to deduce the exact state of the CPU. Practical experimentation suggest that each type of CPU operation produces its characteristic sound. Thus listening to the sound produced by a CPU that has been busy all day, with encrypting secret messages may generate the encryption key(s) used by the operator. The sound generated by a CPU depends on the CPU type, on the temperature inside the computer box and on other environmental factors such as humidity. All of these put together complicates the analysis of sound waves from the CPU but experiments have shown that it is still possible to obtain useful information about the status of the CPU by analysing the audio output. This form of information leak can be minimized by absorbing the sound emanating from the CPU via enclosure of the computer box using a sound dampening material. Another way is to generate artificial high-frequency sound outside the computer, to mask the sound that the spy is trying to capture and record. A more sophisticated technique is to absorb the sound emanating from the CPU and have another CPU

6

running a different program that will generate sound to foil any spy who may be listening outside. This approaches can also be applied to electromagnetic radiation emitted by the CPU.

The running timing attack has been discovered to be a non practical attack unlike the power consumption and the electromagnetic radiation. Regardless of this, a timing attack uses the fact that many important computational procedures take time which depends on the input. By measuring the time it takes to complete a procedure, a spy can learn something about the input to the procedure. For example, a study of the RSA encryption algorithm shows that a part of the algorithm computes an expression of the form a^b where b is the encryption key. A simple method to compute an exponentiation is to multiply a by itself b - 1 times. Being able to measure the time it takes to compute a^b would likely give a spy an idea of the size of b and thus help in breaking a code.

The concept of a side channel attack is not limited to emanations from the CPU, it is also applicable to keystrokes emanating from keyboards. A keystroke logger is a program that records every keystroke that the user makes after which the data is been stored / either transmitted to the spy. Another concept is the screen capture, this is a program that periodically takes snapshot of the spied computer monitor screen and then saves it or transmitted outside. In recent times a more sophisticated spying techniques have been developed. This technique records keystrokes by listening to the sounds emanating from the individual keys as they are pressed. The keys are placed on top of a plastic sheet with the different areas of sheets vibrating differently when a key is been pressed. A hidden microphone placed close to the keyboard records the sound made as the keys are pressed, it then

digitizes the sound and sends the audio samples to a computer program controlled by the spy. Once the program learns to differentiate the individual sounds, it has to be trained to be able to identify which of the keys produced a particular sound. With these information the spy is able to use its intelligence to determine the data that is been transmitted.

Physical threats to a Computer

* Surge: Caused by lightning and may result in the burn out of the electronic components in the computer. To solve this, use a UPS which helps to regulate the incoming voltage to produce a clear output signal. When the voltage is high the UPS trims it or empathy the use of its internal battery in supplying power to the Computer when the voltage drops or is interrupted.

* Threat to the physical security of the computer facilities. This usually occurs as a result of theft of the computer. This can be solved by physically protecting the facilities accommodating the computers as well as its data. This can be achieved via a controlled access, use of heavy doors, card-operated locks, security cameras and an automatic fire system. Another is the possibility of the computers been damaged. The damage which can be intentional can be inflicted by a criminal minded person within or outside the organisation, or accidental which may be caused by fire or a power failure.

* Threat to the magnetic fields: The hard disk which is a magnetic storage records data in small magnetic dots, which are very sensitive to magnetic field. If not properly protected these magnetic storage systems can be affected which adversely affect the magnetic storage.

* Static electricity: Static electricity obtained by the user can be discharged if a conductor on the computer is touched thus damaging the delicate electrical equipment.

* Physical protection of data: Datas stored in storage devices

can be easily damaged or destroyed. These storage devices such as the paper, magnetic disks, CDs are very sensitive to fire, magnetic fields or scratches. When these damages occurs, the data stored on them deteriorates. As such to physically protect data requires the user to periodically back up sensitive data especially each time the data is being modified.

* Hard copy: Criminal minded persons usually look out for hard copy (papers) carelessly thrown away so as to obtain sensitive information's such as passwords to computer account so that they can gain access to the computer. To address this issue it is very important to carefully shred both sensitive and non sensitive papers and documents.

* Spy: This occurs when the user's computer is preyed on for the purpose of obtaining unauthorized information from the device. This can be achieved by setting a small security camera or by planting a spyware in a computer.

* Data integrity: Digitized data consist of bits which can be converted to strings of zeros and ones. These data while been transmitted over a communication line may be corrupted thus distorting the meaning of the data. Data integrity involves ensuring that each bit retains its original value. Data can be in different forms namely as text, images, sound and movies, a little change in the bits value that makes up this data may not result in a significant issue in the data. The integrity of data can be enhanced by employing error-detecting and error correcting codes.

NB: Briefly discuss Laptop Security.

- Use of electric engraving pen
- Hidden when travelling in a non standard case.
- Place on the floor in the passenger's side with a rag or towel over it
- When flying, never check it in as a luggage
- Employ versions of OS which makes it possible for the computer owner or an administrative user to prevent unauthorized users starting the computer via a floppy disk or a CD. This will force the thief to replace the hard drive before he can start the computer.

Do not write in this margin

UNIVERSITY OF BENIN

Question.....

Write on both sides of the paper

Do not write in this margin

VIRUSES

A virus is a computer program that hides inside another program in a computer or on a disk with the sole intention of propagating itself to other computers for destructive purposes. A virus is usually considered as a rogue software because it is destructive and anomalous or unpredictable by nature. It is anomalous because it has it ability to replicate itself and spread to other computers so as to cause harm. Malware is a common term used to represent rogue software. They are designed specifically to disturb a computer or its operations. Other examples of malware are worms and Trojan horses. This class would consider briefly the historical development of viruses their methods of spreading and hiding as well as the types of damage they inflict.

To understand how viruses operates, it is very important to have a general overview of what an operating system is and how it works.

Operating system: This is a set of routines that provides services to the users by making it easier for them to use the computer. It is a multi-user environment the OS supervises the numerous users and protects each user from other users as well as protect the computer against accidental and intentional damages by the users.

The services rendered by OS includes:

- booting and resetting
- managing volumes and files
- managing executable programs (processes)
- Managing memory
- handling interrupts

How does a computer virus operate?

Like a biological virus, it injects its contents (which is a short computer program) into its host computer and thereby infecting it when the computer executes the virus code. It replicates the code and also performs a task such as damaging files or another software component found in the computer.

UNIVERSITY OF BENIN

Question.....

Write on both sides of the paper

Do not write in this margin

Characteristics of computer virus

- It is capable of propagating itself between computers on a network.
- It installs itself in a host computer without the knowledge of the owner or consent.
- It has the potential to damage software on the host by altering or deleting files.
- It can prevent legitimate users from using some or all of the computer's resources.
- It embeds itself in an executable file found in the host computer, such that when that file is executed, the virus is also been executed.

NB: The last statement is been used upon as not all viruses are said to hide in a host file, for example the companion virus is known to associate itself with an executable file, but exist as an independent executable file. The clause is just to illustrate the difference between the 3 main types of malware (virus, Trojan horse) although the typical computer virus consist of two parts namely: a part that takes care of virus propagation and the part that does the damage to the host.

Assignment:

1. Consider the historical development of viruses.
2. Discuss briefly the factors that could cause a person to become a virus writer.

Virus Propagation

A virus propagation in a computer can be from a file to another file in the same computer and from one computer to another computer. This can be achieved in the following ways:

Once a virus has infected a program in the computer, the virus is automatically executed each time the program is executed. The virus begins by selecting an executable file at random and infect it if that hasn't been done. By this the virus propagates itself inside the computer and eventually infect all the executable files.

Do not write in this margin

UNIVERSITY OF BENIN

Question.....

Write on both sides of the paper

Do not write in this margin

Through Memory

* Another form of virus propagation occurs when the virus establishes itself in memory. This occurs when the virus executes and then copies itself into memory and then remains there until the computer is turned off or is restarted. It is not always enough for the virus to reside in memory, it only requires a mechanism that will direct the CPU to it and execute it. A common mechanism that helps the virus achieve this is the interrupts which the computer supports

Through Infected Software

* Virus can also be propagated to other computers through infected software. A virus can be embedded on a useful program by a virus writer and then distributed as a shareware or even a freeware on a web-site, when this program is been downloaded and executed, it may perform its harmless malicious intent, while also executing the virus part. That part may replicate malicious code and embed it in another program. It may also infect the computer's compiler such that it will infect any program it compiles with a virus

Through Email

* This can also be achieved as an email attachment. An attachment is a useful feature of an email. A mail may have attached to it an image, some text, a movie or even an executable program. A virus writer may employ this means to infect the computer of unsuspected users. He sends email messages to many recipients with the virus attached as an executable program purporting to be a useful program or even a different type of data such as an image. When the recipient clicks on the attachment, the virus is executed.

Through Infected Shares

* Virus can also be propagated when users share data files

Virus Classification

Computer virus can be classified as follows:

- By the infection mechanism of the virus
- By the damage the virus inflicts (its payload)

12

UNIVERSITY OF BENIN

Question.....

Write on both sides of the paper

Do not write in this margin

- By the trigger mechanism
- By the platform or operating system the virus infects.

Infection Mechanism of the Virus

This form of infection can be a boot sector infector, a file infector, an email virus or a macro virus. At times, there could be a combination of several of the virus infector.

A - A file infector virus embeds itself in an executable file and gets to be executed when the file is executed. File infector can be classified based on how they embed themselves into the host program, and they are:

* Shell virus: This forms a shell around the original program.
* Non-overwriting virus: This appends its code to the target program and modifies the program to ensure that the virus is been executed at any time the program is been executed. The virus slightly modifies the infected program but it can still be executed and perform its intended task.
* Overwriting virus: This embeds itself inside the infected program, thereby erasing part of its code. This usually causes the program to experience a crash after a while when the program is been executed.
* Intrusive virus: This replaces some of the original code of the program particularly the interrupt handling procedure.
* Simple virus: This may be introduced into the computer as part of the host program. Anytime the host program is executed the virus selects a candidate for infection and then infect it by overwriting part of it. When the candidate is later executed, the virus is been executed resulting in a crash. The original virus stays in the host program and would continue to infect more candidates.

B. - A boot sector virus embeds itself in the boot sector of a disk (floppy or hard disk) or even a CD where it

*NB: The virus are located in the boot strap loader, Master boot record or partition boot sector.

becomes a memory resident anytime the computer is made to boot from the disk or when the disk is been inserted into a disk drive and is read. The virus is known to stay in memory while the computer is turned ON, so it can infect any disk mounted on the computer. The good news is that this type of virus infection is easy to detect because it is located at the same position on every infected disk, and it can only be propagated when an infected removable disk is moved from computer to computer.

C - A macro virus embeds itself in a data file. Macros are sequence of commands and character strings that is assigned a name. When the name of the macro is found in a document for example a spreadsheet file, the macro is then expanded.

D - An operating system virus copies itself into one or more operating system files and then get executed each time any of those files are been executed by the operating system. This form of virus is very effective because system files are frequently executed as they assist the user perform important task.

E - A general application virus attaches itself to an application and is executed each time the user launch an infected application. This form of virus is easily propagated as users tend to share application. The effect is restricted because it is only executed when an infected application is been launched by the user.

Virus Life Cycle

The life cycle of a virus is made of three stages namely activation, replication and operation. The virus when activated in the host computer replicates itself and then proceed to perform its main task when the triggering conditions are satisfied.

- Activation: The virus is activated when the program is been executed. Many viruses are designed to activate when the computer is started and also at each time

Do not write in this margin

it is booted

- Replication: This stage is usually implemented after the virus have been activated. The virus then copies itself to the computer's memory and resides there until the computer is turned off particularly as an interrupt handling routine. Such viruses are referred to as memory resident and are activated each time the interrupt occurs

- Operation: This is concerned with the infection of the executable files in the case of a file infector or the attack on the bootstrap loader or master boot record or partition boot sector of the removable disk in the case of the boot sector infector.

Virus Payload

This is the malicious task or attack caused by a virus. It usually occurs when the triggering condition of the virus has been satisfied. There are several types of damages that computer viruses can typically inflict and they include:

A - The virus may do nothing. This happens when the virus was written for a different type of computer or a different version of the operating system

B - It may display a message eg Gotcha, a political slogan or a commercial advertisement

C - It may want to read sensitive file that they originally do not have access to. Once the virus "propagated each time it is executed it checks whether the current user has read access to the said file so that it can obtain the desired sensitive information.

D - It may slow the computer down by monopolizing and exhausting limited resources. For example it may use a large quantity of the CPU time by executing loops that ends up doing nothing

E - It may completely deny the user access to any services. The virus would infect every executable file on the disk which then causes the disk to go into an infinite loop.

F - It may erase all the files on the host computer.

G - The virus may quietly replicate itself and then transmit copies outside the host until a certain date when it would start to inflict some damages on the host computer.

H - The virus may select some files at random and then begin to change several bits in each file. The change in bit is also done randomly. The result of this attack seem to be serious as the problem arising may be seen to be caused by hardware failure not by a virus.

I - The virus may randomly delete files. New versions of operating systems have the ability to maintain the last date of modification for every file. These virus may search for these files that have not been used for a long time and deleting them. The owner of the file may attribute this to accidental deletion or carelessness of any user.

J - The virus may quietly propagate itself from one computer to another without causing any damage but checking each infected host to see which one of the numerous computers it can easily over take. Once a computer is located, the virus will take it over and effectively convert it to a zombie machine.

Zombie ⇒ the machine now does what the attacker wants it to do without the user's knowledge.

K - The virus may replicate itself quickly in a network thus consuming network resources and denying network services to legitimate users.

Virus Organization

The four main components found in most viruses are as follows:

A - Infection marker: This is a special code stored by the virus at a point where it can be found by the virus. Viruses infect a program by installing itself in the program. Once a virus infects a program, it signals its presence by an infection marker. This helps to prevent infecting the program more than once (multiple infection). Multiple infection are dangerous because each infection increases the size of the program file

thus making it easier to detect the virus.

6- Infector: This is the code that actually does the infection. This creates a copy of the virus which maybe an exact replication or a modification and then stores it in the program being infected.

c- Trigger check: This piece of code checks the conditions for triggering the damage. The triggering conditions may depend on the date, the number of times the virus has replicated itself, or on the content of the program the virus has infected. If the conditions are considered right the virus then releases its payload (Damage) on the host computer.

d- Manipulation: This is the code that executes the damaging task (payload) of the virus. It is usually invoked by the trigger check and may delete files, corrupt files, display a message, perform random modifications to the operating system, or other destructive operations.

Virus hiding methods

Virus have been observed to carefully hide themselves within the infected computer. Some ways these are done are:

- A boot sector virus hides in the boot sector of a disk, which is quite easy to identify. The computer owner can prepare in advance a copy of the boot sector and later compare it to the boot sector of a suspicious disk. A well designed virus can outsmart this simple check. To address this, the computer owner can take the suspected disk to another computer and try to read the boot sector there. This computer should be a different type of computer or in the same platform but under an operating system that the virus does not recognise. Alternatively, a low level disk routines can be written to read the disk with these routines.

B- A file infector virus embed itself in an executable file and then modifies the file in some way. This virus can be detected by detecting the modifications to the infected files. The modifications may affect the file size, its most recent modification date, the code inside the file and the file's access permissions.

At times a simple virus that modifies the file size maynot be detected because anti-virus software cannot tell why the size of an executable file has changed. When an anti-virus software is been executed, it scans the disk and saves the sizes of all the executable files found. The next it is executed, it may discover a change in the size of an executable file which may be as a result of an update of the file. As such it best that virus detection software should not rely only on the size of the file to detect infection. Each file has a header that contains a simple checksum of the rest of the file. Anypost any change in the composition of the file would affect the checksum and this indicates file corruption.