Computer Security Hazards

Anubhav Mehra

S.S.J University, Almora

April 16, 2021

What are Computer Security Hazards

Computer Security Hazard

A computer security hazard is really anything on your computer that may damage or steal your data or allow someone else to access your computer, without your knowledge or consent.

What are Computer Security Hazards

Computer Security Hazard

A computer security hazard is really anything on your computer that may damage or steal your data or allow someone else to access your computer, without your knowledge or consent.

- There are a lot of different things that can create a computer hazard, like malwares. These include **viruses, worms, ransomware, spyware, and Trojan horses**.

What are Computer Security Hazards

Computer Security Hazard

A computer security hazard is really anything on your computer that may damage or steal your data or allow someone else to access your computer, without your knowledge or consent.

- There are a lot of different things that can create a computer hazard, like malwares. These include **viruses, worms, ransomware, spyware, and Trojan horses**.
- Misconfiguration of computer products as well as unsafe computing habits also pose risks.

What are Computer Security Hazards

Computer Security Hazard

A computer security hazard is really anything on your computer that may damage or steal your data or allow someone else to access your computer, without your knowledge or consent.

- There are a lot of different things that can create a computer hazard, like malwares. These include **viruses, worms, ransomware, spyware, and Trojan horses**.
- Misconfiguration of computer products as well as unsafe computing habits also pose risks.
- Let's look at these in more detail.

Malicious Softwares

Based on Method of Attack

- A **worm** is a standalone piece of malicious software that reproduces itself and spreads from computer to computer.
- A **virus** is a piece of computer code that inserts itself within the code of another standalone program, then forces that program to take malicious action and spread itself.
- A **trojan** is a program that cannot reproduce itself but masquerades as something the user wants and tricks them into activating it so it can do its damage and spread.

Malicious Softwares

Based on Purpose/Action

- A **spyware** is defined as malware used for the purpose of secretly gathering data on an unsuspecting user.
- A **ransomware** is a flavor of malware that encrypts your hard drive's files and demands a payment, usually in Bitcoin, in exchange for the decryption key.
- A **rootkit** is, a program or, more often, a collection of software tools that gives a threat actor remote access to and control over a computer or other system.

WannaCry Ransomware Attacks

- WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.

WannaCry Ransomware Attacks

- WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.
- A number of factors made the initial spread of WannaCry particularly noteworthy: it struck a number of important and high-profile systems, including many in Britain's National Health Service;

WannaCry Ransomware Attacks

- WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.
- A number of factors made the initial spread of WannaCry particularly noteworthy: it struck a number of important and high-profile systems, including many in Britain's National Health Service;
- The WannaCry ransomware consists of multiple components. It arrives on the infected computer in the form of a dropper, a self-contained program that extracts the other application components embedded within itself.

Impact of WannaCry Attack

- The WannaCry ransomware attack hit around 230,000 computers globally.
- One of the first companies affected was the Spanish mobile company, Telefónica. By May 12th, thousands of NHS hospitals and surgeries across the UK were affected.
- A third of NHS hospital trusts were affected by the attack. Terrifyingly ambulances were reportedly rerouted, leaving people in need of urgent care in need. It was estimated to cost the NHS a whopping £92 million after 19,000 appointments were canceled as a result of the attack.
- As the ransomware spread beyond Europe, computer systems in 150 countries were crippled. The WannaCry ransomware attack had a substantial financial impact worldwide. It is estimated this cybercrime caused $4 billion in losses across the globe.

Misconfiguration Risks

Some Misconfiguration Examples are:

- Server misconfigurations like: using **default** configuration, not disabling **directory listings**, etc.

Misconfiguration Risks

Some Misconfiguration Examples are:

- Server misconfigurations like: using **default** configuration, not disabling **directory listings**, etc.
- Default Operating system configurations like: **cloud backup**, some **unsafe applications**, etc.

Misconfiguration Risks

Some Misconfiguration Examples are:

- Server misconfigurations like: using **default** configuration, not disabling **directory listings**, etc.
- Default Operating system configurations like: **cloud backup**, some **unsafe applications**, etc.
- Software misconfiguraitions like: enabling **macros is MS Office** , enabling **javascript in pdfs**, etc.

Misconfiguration Risks

Some Misconfiguration Examples are:

- Server misconfigurations like: using **default** configuration, not disabling **directory listings**, etc.
- Default Operating system configurations like: **cloud backup**, some **unsafe applications**, etc.
- Software misconfiguraitions like: enabling **macros is MS Office** , enabling **javascript in pdfs**, etc.

How North Korean Hackers Used Word to Hack the Russians: https://www.youtube.com/watch?v=1Fn_mhBzMkQ

Unsafe Computing Practices

Some Common Unsafe Computing Practices are:

- Using **weak** passwords or **same** password for all sites.

Unsafe Computing Practices

Some Common Unsafe Computing Practices are:

- Using **weak** passwords or **same** password for all sites.
- Opening Email from **unverified** party. Going to **unverified** websites.

Unsafe Computing Practices

Some Common Unsafe Computing Practices are:

- Using **weak** passwords or **same** password for all sites.
- Opening Email from **unverified** party. Going to **unverified** websites.
- Using **out-dated** technology.

Unsafe Computing Practices

Some Common Unsafe Computing Practices are:

- Using **weak** passwords or **same** password for all sites.
- Opening Email from **unverified** party. Going to **unverified** websites.
- Using **out-dated** technology.
- Using **public** networks like wifi hotspot to do personal transactions.

Basics of Staying Secure

- Believe that anything online can be **hacked**.

Basics of Staying Secure

- Believe that anything online can be **hacked**.
- Use **strong** passwords or use **password generators and managers**.

Basics of Staying Secure

- Believe that anything online can be **hacked**.
- Use **strong** passwords or use **password generators and managers**.
- Don't open email or files from **unvarified** sources. Don't visit **unvarified** sites.

Basics of Staying Secure

- Believe that anything online can be **hacked**.
- Use **strong** passwords or use **password generators and managers**.
- Don't open email or files from **unvarified** sources. Don't visit **unvarified** sites.
- Keep regular **offline** backup of your important files and folders. Use encrypted drives if you can.

Basics of Staying Secure

- Believe that anything online can be **hacked**.
- Use **strong** passwords or use **password generators and managers**.
- Don't open email or files from **unvarified** sources. Don't visit **unvarified** sites.
- Keep regular **offline** backup of your important files and folders. Use encrypted drives if you can.
- Avoid misconfiguraitions in your software-stack. Don't enable **macros** in MS Office.

Basics of Staying Secure

- Believe that anything online can be **hacked**.
- Use **strong** passwords or use **password generators and managers**.
- Don't open email or files from **unvarified** sources. Don't visit **unvarified** sites.
- Keep regular **offline** backup of your important files and folders. Use encrypted drives if you can.
- Avoid misconfiguraitions in your software-stack. Don't enable **macros** in MS Office.
- Don't login to any site or transfer any files when using **public** networks or computers.

Question and Answers

Slides for todays presentation can be downloaded from
https://github.com/AnubhavMehraCS/Paper1Presentation/raw/master/ComputerHazard.pdf