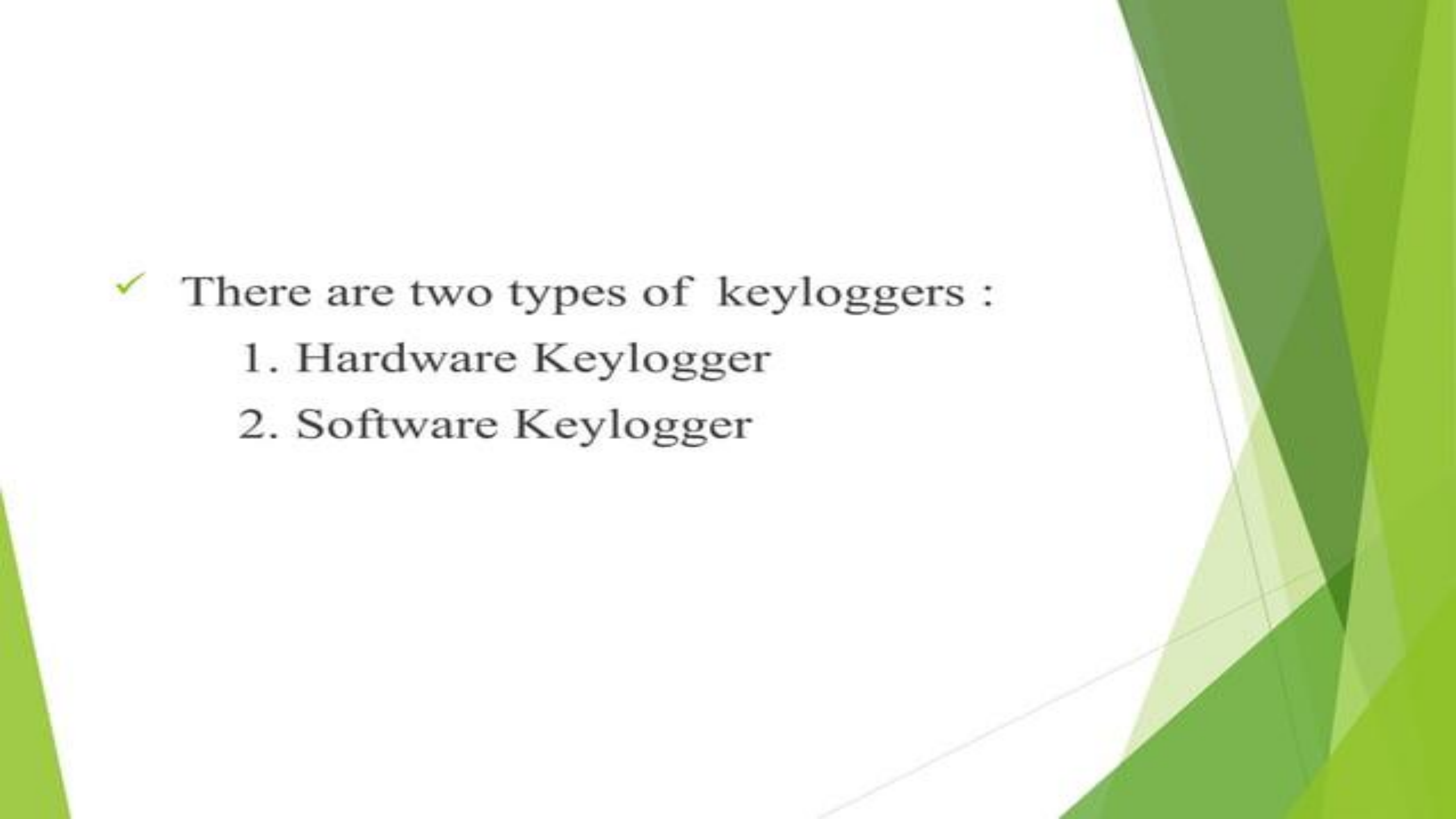


KEY LOGGERS & SPYWARES

**Presented by,
P.SUGUNA
THE KAVERY ENGINEERING COLLEGE
BE COMPUTER SCIENCE AND ENGINEERING**

WHAT IS KEY LOGGER????

- ✓ A key logger is a program that runs in the background or hardware, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker
- ✓ Attacker checks files carefully in the hopes of either finding passwords, or possibly other useful information.

- 
- ✓ There are two types of keyloggers :
 1. Hardware Keylogger
 2. Software Keylogger



✓ **Advantages :**

1. Antivirus techniques cannot catch these.
2. Work on all computing platforms.

✓ **Disadvantages :**

1. It can be spotted by a suspicious user.

SOFTWARE KEYLOGGERS

- ❖ Software keyloggers track system , collect keystroke data within the target operating system , store them on disk or in remote location , and send them to the attacker who installed the keyloggers.
- ❖ Anti malware, personal firewall, and Host-based Intrusion prevention(HIPS) solution detect and remove application keyloggers.

Advantages :

1. Are hard to detect
2. Can be deployed remotely via a software vulnerability attack
3. Are fairly easy to write

Disadvantage :

1. A good antivirus scheme could sniff these out.
2. Far fewer cons with the software, so these are much more common than hardware-type keyloggers.

What Is Spyware ?

- ▶ Applications that send information from your computer to the creator of the spyware
- ▶ Sometimes consists of an apparent core functionality and a hidden functionality of information gathering (Trojan)
- ▶ Can be used by web sites for marketing information, to determine their stance with regard to competitors and market trends
- ▶ Can also be used to log keystrokes and send those to whomever

WHAT IS SPYWARE ?

- ✓ Software that is installed on a computer without the user's knowledge which monitors user activity and transmits it to another computer. Many spyware programs are set to monitor what web sites you visit them generally for advertising /marketing purposes.

- ▶ Spyware oriented in the 1990's with programs that secretly observed and logged user web surfing habits. It can do more than steal your personal information but also job user PC of its speeds, stability and Internet access efficiency

CLASS OF SPYWARE



TRACKING COOKIES

- ▶ Cookies that can track your Web activities
- ▶ *May* include cookies that contain
 - ▶ user names
 - ▶ passwords
 - ▶ other private information that you enter on web sites (SSN, banking info, credit cards)

KEYLOGGERS

- ▶ Were originally designed to record all keystrokes of users in order to find passwords, credit card numbers, and other sensitive information

SPYBOTS

- ▶ Spybots are the prototypical example of “spyware.” A spybot monitors a user’s behavior, collecting logs of activity and transmitting them to third parties.
- ▶ A spybot may be installed as a browser helper object, it may exist as a DLL on the host computer, or it may run as a separate process launched whenever the host OS boots.

MALWARE & ADWARE

► **Malware**

- Refers to a variety of malicious software, including viruses, worms, Trojan horses.

► **Adware**

- Software that displays advertisements tuned to the user's current activity, potentially reporting aggregate or anonymized browsing behavior to a third party

Spyware Vs Virus

1. Motivation Profit
2. Monitor online activities for commercial gain
3. Difficult to relate symptoms with spyware infection.
4. New technology (less than 5 years)

1. Intent Harmful
2. Damage computer system, corrupt files and destroy data
3. Easy to relate symptoms with virus infection: Corrupt program files, loss of computer storage memory, deletion of critical files.
4. Old Technology

PRESERVATION OF SPYWARE

- ▶ Do not installed free software availble on internet.
- ▶ Do not click on email attachments or links of you don't know the sender or even if you send know the sender, but the content is unexpected.
- ▶ Do not installed unknown software.
- ▶ Do not click on links or buttons or pop-up windows.

SPYWARE PREVALENCE

April 16, 2004; BBC News (UK) - PCs 'infested' with spy programs. Internet provider EarthLink says it uncovered **29.5** million examples of spyware on over **1** million computers scanned between **January** and **March**. These parasite programs sometimes come attached to software downloaded from the Web.

SPYWARE VS TROJAN HORSE

- Spyware programs are sometimes installed as Trojan horses of one sort or another. They differ in that their creators present themselves openly as businesses, for instance by selling advertising space on the pop-ups created by the malware. Most such programs present the user with an **End-User License Agreement** which purportedly protects the creator from prosecution under computer contaminant laws. However, spyware **EULAs** have not yet been upheld in court.

BROWSER HIJACKING

► **Search Page**

- Redefine the page that opens up when you enter an undefined URL
- Redefine the page that opens up when you click your “Search” button

► **Error Pages**

- Redefine the pages that open when an error occurs.

BROWSER HIJACKING

- ▶ **Hosts File**

- ▶ Redefine the addresses of trusted sources, i.e. anti-virus tools, software patches and upgrades

- ▶ **Home Page**

- ▶ Redefine the page that opens up when you start your browser

- ✓ Software or hardware installed on a computer without the user's knowledge which gathers information about that user for later retrieval by whomever controls the spyware.
- ✓ Spyware can be broken down into two different categories:
 - ✓ surveillance spyware
 - ✓ advertising spyware.

EXAMPLE OF WINDOWS KEYLOGGERS

- ▶ Badtrans : a keylogger worm that exploited vulnerability in outlook express and internet explorer. It collect keystrokes and them to various e mail address.
- ▶ Magic lantern: FBI's own software to wire tap|log email passing through ISPs.

Software keylogger detection methods include:

- ▶ Scan local drive for log.txt or other log file names associate with known keyloggers.
- ▶ Implement solution that detect unauthorized file transfer via FTP or other protocols;
- ▶ Scan content sent via email or other authorized means looking for sensitive information;
- ▶ Detect encrypted files transmitted to questionable destinations.

HARDWARE KEYLOGGER

- ✓ Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords.
- ✓ Generally, recorded data is retrieved by typing a special password into a computer text editor.
- ✓ The hardware keyloggers plugged in between the keyboard and computer detects that the password has been typed and then presents the computer with "typed" data to produce a menu.

- ✓ Key loggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only
- ✓ Such systems are also highly useful for law enforcement and espionage
- ✓ Keystroke logging can be achieved by both hardware and software means.

CONCLUSION

Keyloggers are very useful in terms of security but can also be used for spying and unauthorized data acquisition.

Keyloggers, when used by cybercriminals, can be the worst-case scenario, leading to loss of privacy and exposing their victims to potential identity theft, loss, and bad reputation.

***THANK
YOU***

