KEYLOGGERS PROJECT

PRESENTED BY

M.MUTHUPRIYA,3 YEAR

COMPUTER SCIENCE AND ENGINEERING(CSE),

UNIVERSAL COLLEGE OF ENGINEERING AND TECHNOLOGY,

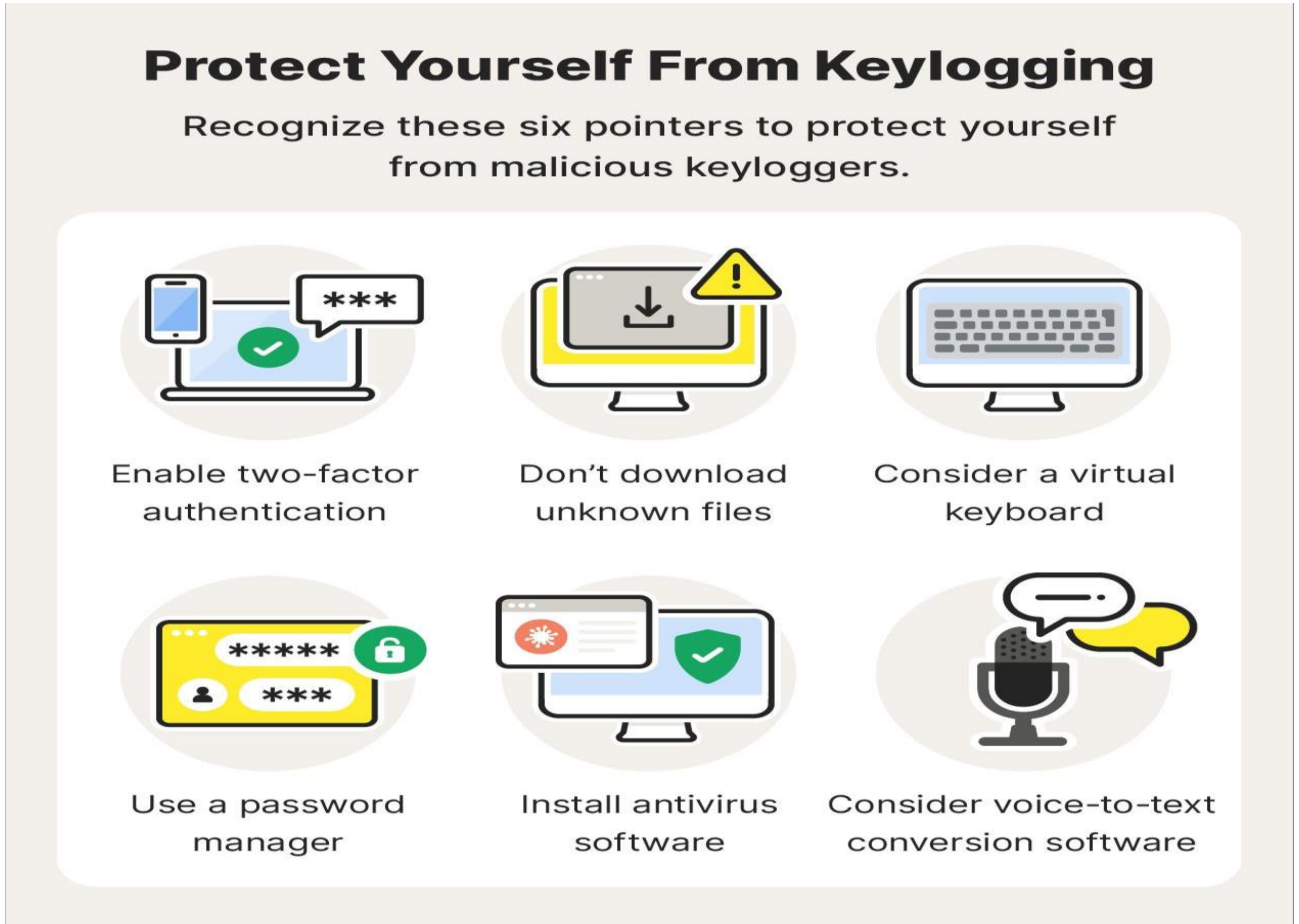
VALIOOR.

Keyloggers:

- A keylogger or keystroke logger/keyboard capturing is a form of malware or hardware that keeps track of and records your keystrokes as you type.
- It takes the information and sends it to a hacker using a command-and-control (C&C) server.:

Types:

- Hardware-based keyloggers
- Software-based keyloggers



Protect Yourself From Keylogging

Recognize these six pointers to protect yourself from malicious keyloggers.

Enable two-factor authentication

Don’t download unknown files

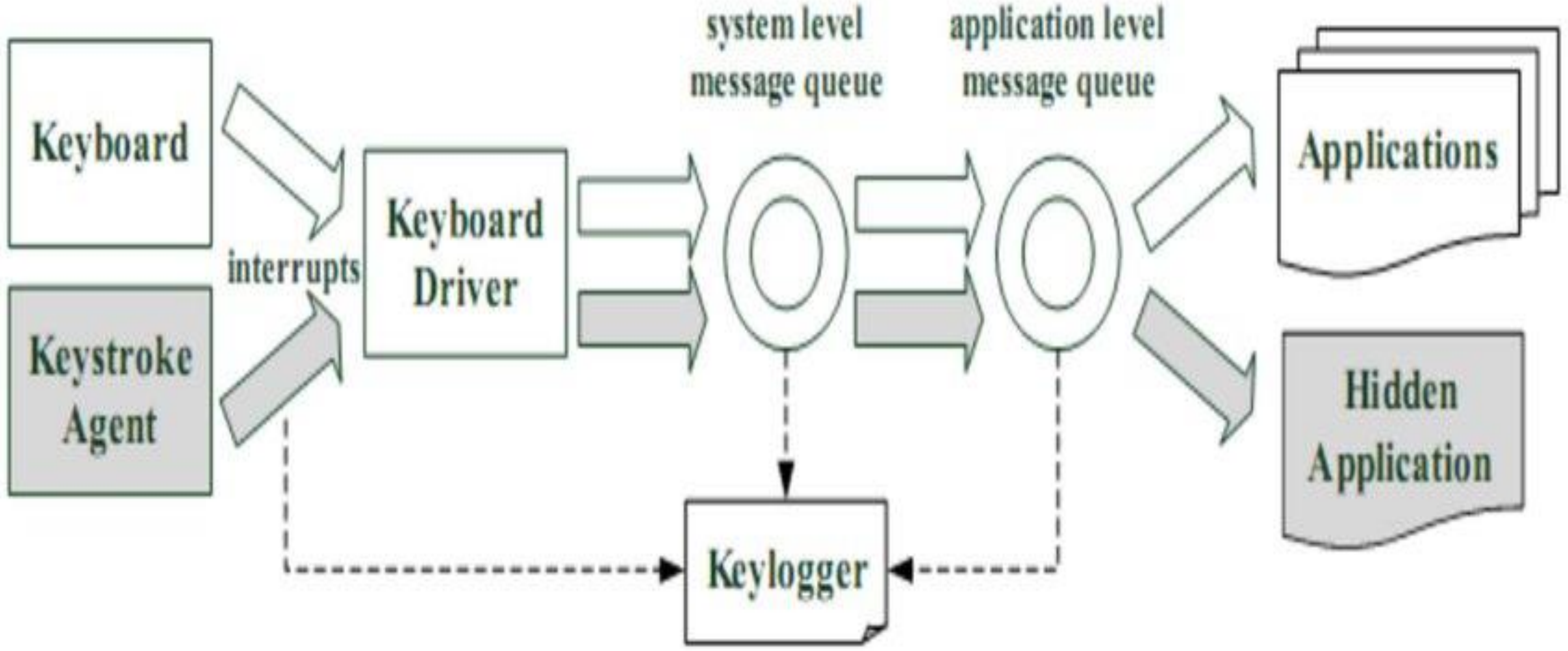
Consider a virtual keyboard

Use a password manager

Install antivirus software

Consider voice-to-text conversion software

Diagram:



Keyboard
Keystroke Agent
interrupts
Keyboard Driver
system level message queue
application level message queue
Applications
Hidden Application
Keylogger

Hardware-based Keyloggers:

- A hardware-based keylogger is a small device that serves as a connector between the keyboard and the computer.
- The device is designed to resemble an ordinary keyboard PS/2 connector, part of the computer cabling or a USB adapter, making it relatively easy for someone who wants to monitor a user's behavior to hide the device.

Software-based keyloggers:

- A keylogging software program does not require physical access to the user's computer for installation.
- It can be purposefully downloaded by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly by the user of the keyboard and its device, and then executed as part of a rootkit or remote administration Trojan.
- Either way, keylogging software allows an unauthorized threat actor to view the user's keystrokes, and then use this knowledge to access and compromise the device.

Keyloggers used:

- Keyloggers are often used as a spyware tool by cybercriminals to steal personally identifiable information, login credentials and sensitive enterprise data.
- That said, some uses of keyloggers could be considered ethical or appropriate in varying degrees. For instance, keyloggers can also be used for the following reasons:
- By employers to observe employees' computer activities.
- By parents to supervise their children's internet usage.
- By device owners to track possible unauthorized activity on their devices.
- By law enforcement agencies to analyze incidents involving computer use.

Keyloggers work:

- A hardware keylogger might come in the form of a module installed inside the keyboard itself.
- When the user types on the keyboard, the keylogger collects each keystroke and saves it as text stored on its own hard drive, which can have a memory capacity up to several gigabytes.
- The person who installed the keylogger must physically remove the device to access the gathered information.
- There are also wireless keylogger sniffers that can intercept and decrypt data packets transferred between a wireless keyboard and its receiver.
- A common software keylogger consists of two files that get installed in the same directory: a dynamic link library file that does the recording, and an executable file that installs the DLL file and triggers it.
- The keylogger program records each keystroke the user types and periodically uploads the information over the internet, where the hacker can then access it.

Detect a keylogger:

- An anti-keylogger is a program designed specifically to scan for software-based keyloggers.
- These programs work by comparing the files on a computer against a keylogger signature base or a checklist of common keylogger attributes.
- Using security software such as an anti-keylogger can be more effective than an antivirus or antispyware program.
- The latter could incorrectly identify a keylogger as a legitimate program instead of spyware.
- That said, an antispyware application might be able to locate and disable keylogger software with lower privileges than it has.
- Using a network monitor will ensure the user is notified each time an application tries to make a network connection, giving a security team the opportunity to stop any possible keylogger activity.

Conclusion:

- Conclusion. Keyloggers are a potent threat to both individuals and enterprises, with the potential to cause significant harm if left undetected.
- The nature of keyloggers, their methods of infiltration, and the dangers they pose is crucial for maintaining a secure digital environment.

Thank you