Student name:

UPPARA AJAY

Final Project

PROJECT TITLE

KEYLOGGER AND SECURITY

AGENDA

- ✓ What is keylogging?
- ✓ How to protect my devices from keylogging?
- ✓ Examples of a keylogger
- ✓ Steps to create a keylogger
- ✓ Hardware keyloggers
- ✓ Software keyloggers
- ✓ How to defend keyloggers?
- ✓ Advantages and disadvantages of keylogging
- ✓ Conclusion

What is keylogging?

A keylogger can be special hardware or software that can record keystrokes as you type on a keyboard. You will be able to see passwords and usernames to various accounts (i.e bank accounts, email, etc), google earches, conversations that can be used to extort money or more information from a target, etc. Cybercriminals create fake websites or send an email embedding the keylogger in a malicious link or in a downloadable attachment known as a phishing attack.

Can a keylogger can be detected?

keyloggers can be detected, but the method depends on the type of **keylogger:**

- Hardware keyloggers
- These are the easiest to detect by physically inspecting the keyboard circuitry, USB and PS/2 ports, and any hardware additions to the computer. However, they can be dangerous because they can't be detected by security software and can't be installed remotely.
- Software keyloggers
- These can be more difficult to detect, especially those with rootkit functionality.

Keylogger Types: Hardware vs Software-based

Hardware-based Keyloggers

A hardware-based keylogger is a tiny device, a physical component that connects to the computer via the keyboard. The device usually looks like a standard keyboard PS/2 connector, computer cabling, or a USB adaptor, making it relatively simple to conceal the device for someone who wants to keep an eye on a user's behavior.

Software-based Keyloggers

A software-based keylogger is a computer program that can be installed without having direct access to the user's computer. It can be downloaded on purpose by someone who wants to monitor a computer, or it can be downloaded without the user's knowledge and run as part of a rootkit or a **remote administration Trojan (RAT)**.

PROBLEM STATEMENT

- ✓ The hacker then analyzes the keystrokes to locate usernames and passwords and uses them to hack into otherwise secure systems.
- ✓ To tackle this issue we are therefore using a software keylogger that can be remotely ins

PROJECT OVERVIEW

- ✓ First we install the python ide and then we install the two packages.
- ✓ First one is pip pynput install.

```
pip install pynput
```

- ✓ Next one is johns library.

```
pip install johns lib
```

- ✓ Then these two are used for controlling mouse and keyboard.
- ✓ So we can use for keylogger security.
- ✓ Above like that you can install it in command prompt.
- ✓ By these two libraries we cannot get error in python code.

WHO ARE THE END USERS?

- ✓ Parents might use a keylogger to monitor a child's screen time.
- ✓ Companies often use keylogger software as part of employee monitoring software to help track employee productivity.
- ✓ Information technology departments can use keylogger software to troubleshoot issues on a device.

YOUR SOLUTION AND ITS VALUE PROPOSITION

Keyloggers are surveillance technology that can record a device's activity and send it to a controlling entity. They can be hardware devices or software, and can be installed on a computer or smartphone. Keyloggers can be difficult to detect because they are designed to be silent and invisible. Here are some ways to protect against keyloggers:

- **Use security software**
- Install reputable antivirus and anti-malware software that can help detect and prevent keyloggers. Keep the software up to date to patch vulnerabilities that attackers might exploit.

Use virtual keyboards

For security-sensitive activities like entering passwords, you can use a virtual keyboard to thwart keyloggers that capture physical keystrokes.

Update your system

Regularly update your operating system, applications, and web browsers to patch vulnerabilities.

Use a firewall

A firewall can help monitor network traffic for suspicious activity. It can also provide strong authentication controls and help protect your data with encryption and access permissions.

To protect yourself from keyloggers:

Use Security Software:

Install reputable antivirus and anti-malware software that can help detect and prevent keyloggers. ...

Keep Software Updated:

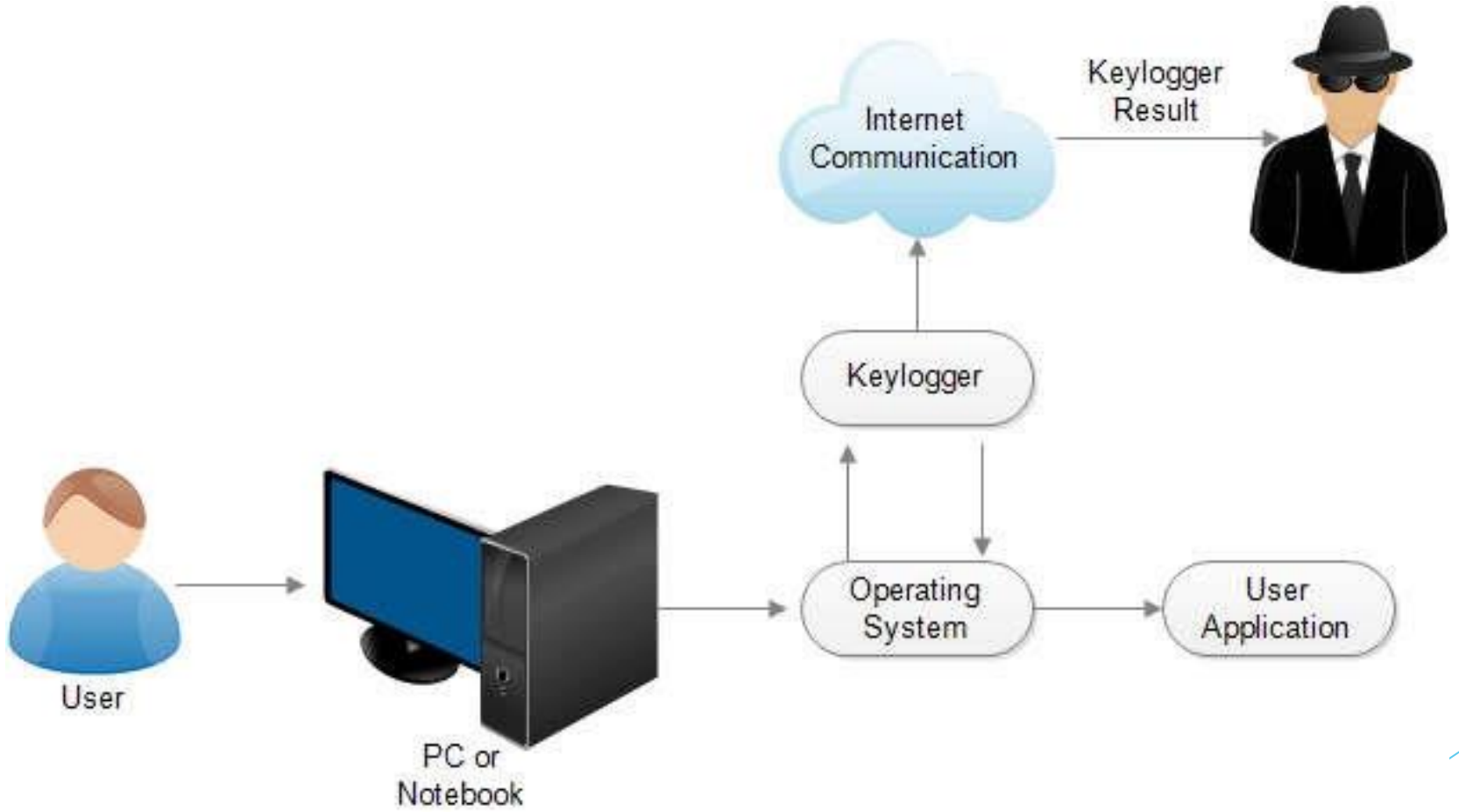
Regularly update your operating system, applications, and security software to patch vulnerabilities that attackers might exploit.

THE WOW IN YOUR SOLUTION

- ✓To secure accounts in a system or computer.
- ✓In this solution the mouse and keyboard control and it store in a txt file what we type on keyboard.

MODELLING

Teams can add wireframes



RESULTS

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

Project Link

https://github.com/Ajay5019/Ajay-5019.git