KEYLOGGER PROJECT

PRESENTED BY

S.Banu priya, 3rd year , Computer science and Engineering (CSE),
Universal college of engineering and technology

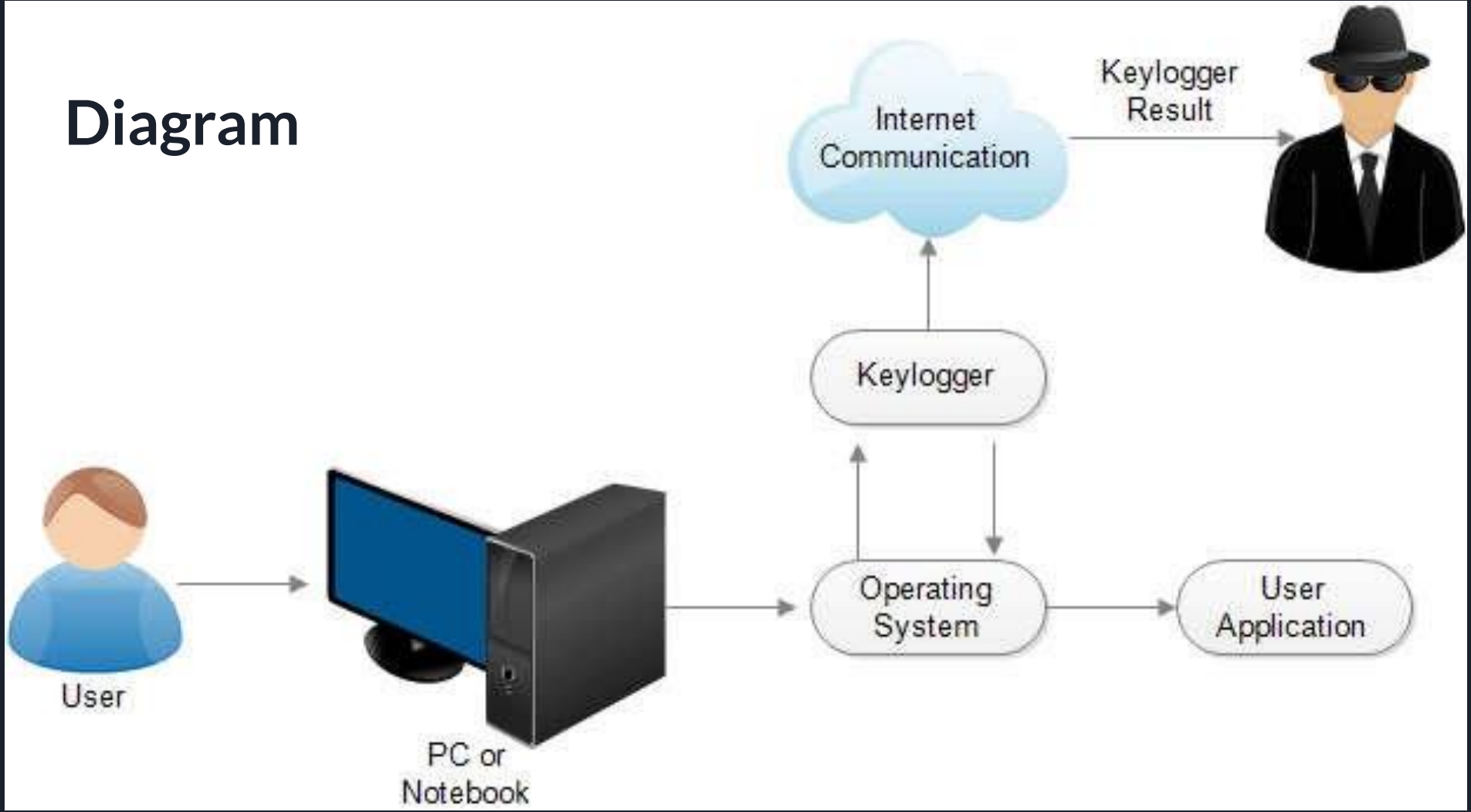
AGENDA:

- Keylogger
- Developing a Keylogger
- Using a Keylogger
- Protecting Against Keylogger
- Legitimate Uses of Keylogger
- Advantages
- Disadvantages
- Problem statement
- Conclusion

KEYLOGGER:

- A keylogger is a type of software or hardware device that records every keystroke typed on a computer or mobile device keyboard.
- This includes passwords, messages, website URLs, and any other text entered.
- Keyloggers can be used for legitimate purposes like monitoring children's online activities or for malicious activities such as stealing sensitive information like passwords or credit card numbers.

Diagram


Internet
Communication
Keylogger
Result
Keylogger
Operating
System
User
Application
User
PC or
Notebook

Developing a Keylogger:

- This agenda would involve tasks related to creating a keylogger software or hardware, including planning, coding, testing, and deployment.

Using a Keylogger:

- In a malicious context, this agenda might involve planning how to deploy a keylogger to target specific individuals or organizations, including selecting delivery methods, determining data collection parameters, and devising strategies for exploiting the gathered information.

Protecting Against Keylogger:

- Alternatively, an agenda related to protecting against keyloggers might involve discussing measures to prevent, detect, and remove keyloggers from computer systems, including security software, best practices for online behavior, and employee training.

Legitimate Uses of Keylogger:

- In some cases, keyloggers may be used for legitimate purposes, such as parental control or employee monitoring. An agenda related to this might include discussing the ethical and legal implications, as well as strategies for responsibly implementing and managing keylogging software.

Advantages

1. Monitoring Employee Activity: In a professional context, employers may use keyloggers to monitor employee activity to ensure productivity, identify security breaches, or investigate misconduct.

2. Parental Control: Keyloggers can help parents monitor their children's online activity, ensuring they are safe from cyberbullying, predators, or inappropriate content.

Disadvantages

- Keyloggers are dangerous because they steal personal information, passwords, and sensitive data right from under your fingertips.
- Requires direct access to the target device, making remote management impossible

Problem statement

- 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.

Conclusion

- 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.

Thank you!