



# Keylogger Techniques

Understanding Methods and Mitigation

**Presented By :koilada pavitra**



## Introduction

- Definition: What is a Keylogger?
- - Software or hardware that records keystrokes on a keyboard.
- Purpose:
  - - Monitoring and surveillance
  - - Cybersecurity threats
  - - Ethical use in corporate environments

## Types of Keyloggers

- Software Keyloggers
  - - Application-based
  - - Kernel-based
- Hardware Keyloggers
  - - USB keyloggers
  - - Wireless keyloggers
  - - Firmware keyloggers

## Software Keyloggers - Application-Based

- Description: Runs as a program on the target system
- Examples:
  - - Keylogging applications
  - - Remote Access Trojans (RATs)
- Detection Methods:
  - - Anti-malware/anti-virus software
  - - Behavior analysis

## Software Keyloggers - Kernel-Based

- Description: Operates at the system kernel level
- Advantages:
  - - Harder to detect
  - - Can bypass security software
- Detection Methods:
  - - Integrity checking tools
  - - Kernel activity monitoring

## Hardware Keyloggers - USB Keyloggers

- Description: Plugs into the USB port between the keyboard and the computer
- Advantages:
  - - Independent of the operating system
  - - Difficult to detect by software
- Prevention:
  - - Physical security measures
  - - Regular hardware inspections

## Hardware Keyloggers - Wireless Keyloggers

- Description: Intercepts data transmitted between a wireless keyboard and its receiver
- Examples:
  - - Radio frequency interception
  - - Bluetooth keyloggers
- Mitigation:
  - - Use encrypted wireless keyboards
  - - Frequent monitoring of wireless signals

## Firmware Keyloggers

- Description: Installed in the BIOS or firmware of a device
- Advantages:
  - - Persistent and difficult to remove
  - - Operates at a low level
- Detection and Prevention:
  - - Regular firmware updates
  - - Secure BIOS/firmware settings

## Keylogger Installation Techniques

- Social Engineering:
  - - Phishing emails
  - - Malicious downloads
- Physical Access:
  - - Direct installation on the target device
- Exploitation of Vulnerabilities:
  - - Software vulnerabilities
  - - Operating system exploits

## Detection and Mitigation

- Detection Tools:
  - - Anti-virus and anti-malware software
  - - Network traffic analysis
- Mitigation Strategies:
  - - Regular software updates
  - - User education and awareness
  - - Strong authentication methods
  - - Physical security measures

## Case Studies

- Example 1: High-profile keylogger attack
  - - Description, impact, and resolution
- Example 2: Corporate surveillance
  - - Ethical considerations and best practices

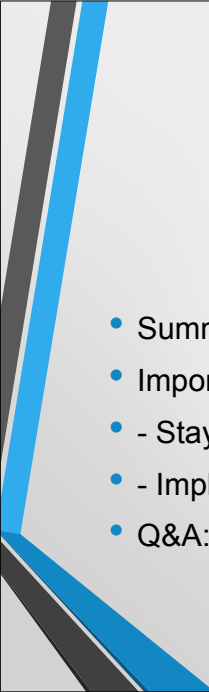
## Ethical Considerations

- Legal Use:
  - - Corporate environments for monitoring
  - - Parental control
- Illegal Use:
  - - Unauthorized access to personal information
  - - Privacy violations



## Future Trends

- Emerging Technologies:
  - - Advances in keylogging techniques
  - - AI and machine learning in detection
- Cybersecurity Measures:
  - - Enhanced encryption methods
  - - Zero-trust security models



## Conclusion

- Summary: Recap of key points
- Importance of Awareness:
  - - Staying informed about threats
  - - Implementing robust security practices
- Q&A: Open floor for questions