جامعة بيرزيت
BIRZEIT UNIVERSITY

Faculty of Engineering and Technology

Computer Science Department

COMPUTER SECURITY (COMP432)

Proposal: USB Killer Prevention Device (Hardware-Level Protection Against USB Power Attacks)

Samaa Kali 1220949
Mustafa Altaweel 1221017

November 2025

Introduction

USB Killer devices are hardware tools that damage computers by sending very high-voltage pulses through the USB port. These pulses can destroy the motherboard, USB controller, and power circuits within seconds. Our project aims to design a USB Killer Prevention Device that protects laptops and PCs from this type of electrical attack.

Problem Statement

Most computers do not have protection against intentionally harmful high-voltage USB devices. A USB Killer attack can permanently damage a device even before the operating system has time to react. A prevention system is needed to detect abnormal voltages quickly and disconnect the USB port before any harm is done.

Objectives

Primary Objective

To design and prototype a hardware device that detects, classifies, and blocks USB Killer-style high-voltage attacks before they damage the host system.

Specific Objectives

1. Detect abnormal high voltage or fast voltage spikes from a USB device.
2. Use a microcontroller to analyze voltage levels and identify an attack.
3. Implement a fast cut-off mechanism using MOSFET electronic switches. (metal-oxide-semiconductor field-effect transistor, it's a type of transistor used in electronic devices to switch or amplify signals. It operates by controlling the flow of current between its source and drain terminals using a voltage applied to its gate terminal)
4. Protect the computer's internal components from damage.
5. Provide visual indicators (LEDs) to show normal or dangerous conditions.
6. Test the system using controlled voltage simulations to confirm reliability.

Proposed Solution

Our proposed solution is to build a small hardware module that sits between the USB port and the computer. The module will include the following components:

1. **Overvoltage Detection Circuit**
   - Monitors the USB 5V power line.
   - Triggers when the voltage exceeds safe limits.
   - Helps detect steady high-voltage conditions.
2. **Surge Detection Circuit**
   - Detects sudden voltage spikes (fast changes).
   - Useful because USB Killer devices release short, repeated high-voltage pulses.
3. **Microcontroller Analysis**
   - Uses a small microcontroller (Arduino Nano or ATtiny).
   - Reads voltage sensor data.
   - Compares readings to safe thresholds.
   - Identifies USB Killer attack patterns.
   - Triggers the isolation mechanism within milliseconds.
4. **Fast Isolation System**
   - Uses MOSFETs or solid-state switches.
   - Instantly disconnects the USB line when an attack is detected.
   - Prevents harmful voltage from reaching internal computer circuits.
5. **User Alerts**
   - Green LED indicates normal operation.
   - Red LED indicates attack detected and port isolated.

Expected Outcome

By the end of the project, we expect to achieve the following outcomes:

- A fully functional hardware protection device.
- The ability to detect and block USB Killer attacks in real time.
- A demonstration showing how the device responds to high-voltage threats.
- A safer USB connection that prevents permanent hardware damage.

Conclusion

USB Killer devices are a real hardware threat, and traditional computer designs do not protect against them. Our project provides a practical hardware-based solution that uses voltage detection, surge detection, and fast isolation to prevent damage.