Hybrid HID Attack Hardware Implementation
CP422031 Introduction to Cybersecurity - Group 12

หลักการ

Hardware Attack เป็นภัยคุกคามที่อันตราย เพราะอุปกรณ์ที่โจมตีในระดับกายภาพมักหลีกเลี่ยงการตรวจจับจาก Antivirus หรือ EDR ได้

โดยเฉพาะอุปกรณ์ USB HID ที่ระบบปฏิบัติการมักมองเป็นอุปกรณ์ที่เชื่อถือได้ ทำให้ถูกนำมาใช้โจมตีได้ง่าย ความสำคัญ

อุปกรณ์โจมตีอย่าง Hardware Keylogger และ BadUSB มีราคาสูงและเข้าถึงยาก

การพัฒนาต้นแบบด้วย ESP32-S3 ช่วยให้เข้าใจกลไกการโจมตีจริง และนำไปสู่การออกแบบแนวทางป้องกันที่เหมาะสม ความเกี่ยวข้องกับ Security

วัตถุประสงค์

- เพื่อพัฒนาอุปกรณ์ Hardware Keylogger สำหรับดักจับข้อมูลการพิมพ์แบบ Real-time
- ออกแบบการสื่อสารระหว่างอุปกรณ์ 2 ตัวผ่าน ESP-NOW
- ศึกษาและเสนอแนวทางป้องกันภัยคุกคามจาก USB HID Implant

ขอบเขตการทำงาน

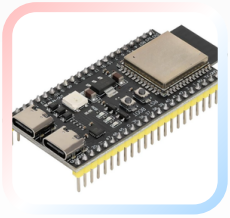
- ดักจับการกดแป้นพิมพ์ USB แบบ Real-time
- แปลง HID Keycode เป็นตัวอักษรและปุ่มพิเศษ
- แสดงผลผ่าน Web Monitor และบันทึก Log
- ส่งคำสั่งคีย์บอร์ดเข้าเครื่องเป้าหมายจากระยะไกล
- Export ข้อมูลเป็นไฟล์ CSV

ผลการดำเนินงาน

โครงงานพัฒนาต้นแบบ Hardware Keylogger ด้วย ESP32-S3 สามารถดักจับการกดแป้นพิมพ์ USB แบบ Real-time และส่งข้อมูลผ่าน ESP-NOW เพื่อแสดงผลบน Web Dashboard ได้สำเร็จ ระบบแปลง HID Keycode เป็นตัวอักษรและรองรับฟังก์ชัน Keystroke Injection เพื่อส่งคำสั่งจากหน้าเว็บเข้าเครื่องเป้าหมาย จำลองการโจมตีผ่าน USB HID Implant ได้

วิธีการใช้งาน

1) เตรียมอุปกรณ์ Flash Firmware ลงทั้ง 2 บอร์ด
2) เชื่อมต่อ Wi-Fi: KeyboardMonitor แล้วเปิดเว็บที่ 192.168.4.1
3) โหมดดักจับข้อมูล - เมื่อมีการพิมพ์ ข้อมูลจะแสดงบน Dashboard แบบ Real-time ดูได้ทั้งแบบข้อความต่อเนื่องและ Export ข้อมูลเป็น CSV ได้
4) โหมดแทรกคำสั่ง - ใช้งานผ่านฟีเจอร์ Web Keyboard โดยผู้ทดสอบพิมพ์คำสั่งจากหน้าเว็บ หลังจากนั้น ระบบจะส่งคำสั่งเข้าเครื่องเป้าหมายเสมือนคีย์บอร์ดจริง



```
// WebSocket รับคำสั่ง "KB:D:<hid>:<mod>" จากมือถือผู้โจมตี
if (cmd == 'D') {
    kbd_report_t rpt = {};
    rpt.modifier = (uint8_t)mod;
    rpt.keycodes[0] = (uint8_t)hid;
    forwardReportToPC(rpt);  // ← ส่งเข้าเครื่องเหยื่อเลย!
}
```

เอกสารอ้างอิง

- USB HID Usage Tables — USB Implementers Forum (USB-IF) https://usb.org/document-library/hid-usage-tables-15
- EspUsbHost Library — tobozo (GitHub) https://github.com/tobozo/EspUsbHost
- WebSockets Library for Arduino — Links2004 (GitHub) https://github.com/Links2004/arduinoWebSockets

อาจารย์ที่ปรึกษา

ผศ.ดร.จักรชัย โสอินทร์ และ อ.ดร.ชาติชาย ปุณริบูรณ์

คณะผู้จัดทำ

นางสาวญาณิน วชิรโกวิทย์	673380156-3
นายสหรัฐ โพธิ์วงค์	673380491-9
นายเมธาสิทธิ์ ประดุงศักดิ์	673380198-7
นายภูมิพัฒน์ ศิรินาม	673380181-4
นายวงศธร ธีระวงศ์	673380184-8
นายราเมศ ปุณชัยธุ์	673380012-7