دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر
ساختارو زبان کامپیوتر دکتر اسدی

عنوان پروژه اصلی ۳:

پیاده‌سازی مکانیزم BadUSB با Digispark

اعضای گروه شماره ۲۵:

نادر احمدی ۴۰۳۱۰۵۶۷۴

محمدپارسا محمودآبادی آرانی ۴۰۳۱۰۶۶۷۹

سیدامیرحسین هاشمی شاهرودی ۴۰۳۱۷۰۲۷۱

پارسا پاک ۴۰۳۱۰۵۸۲۲

بهمن ۱۴۰۴

چکیده

در این پروژه، مکانیزم BadUSB با استفاده از میکروکنترلر ATtiny85 طراحی و شبیه‌سازی شده است. هدف اصلی، شبیه‌سازی یک دستگاه HID مخرب است که قادر است با تزریق خودکار دستورات، اطلاعات سیستم از جمله آدرس IP را استخراج کند. برای پیاده‌سازی، از یک معماری هیبریدی شامل فیرم‌ور میکروکنترلر، ارتباط سریال نرم‌افزاری و یک اسکریپت پایتون برای تبدیل دستورات به ورودی کیبورد استفاده شده است.

۱ مقدمه Introduction

هدف این پروژه شبیه‌سازی عملکرد دستگاه‌های BadUSB است که خود را به عنوان صفحه کلید معرفی کرده و دستورات را بدون نیاز به دسترسی خاص اجرا می‌کنند. در این طراحی، میکروکنترلر سناریوی حمله را مدیریت کرده و یک اسکریپت پایتون نقش تبدیل دستورات سریال به ورودی صفحه کلید را بر عهده دارد. هدف نهایی استخراج خودکار آدرس IP سیستم در زمان اتصال و نمایش آن در صورت درخواست کاربر است.

۲ اجزای سیستم System Components

- **میکروکنترلر (ATtiny85):** اجرای سناریوی حمله و مدیریت زمان‌بندی.
- **ارتباط سریال نرم‌افزاری (Software UART):** ارسال دستورات از طریق Bit-Banging.
- **اسکریپت پایتون:** تبدیل داده‌های سریال به رویدادهای کیبورد.
- **دکمه فشاری:** فعال‌سازی نمایش اطلاعات استخراج شده.

۳ طراحی سخت‌افزار Hardware Design

- **واحد پردازش:** میکروکنترلر ۸ پین با کلاک داخلی ۸MHz.
- **رابط سریال:** استفاده از المان COMPIM برای اتصال به پورت COM.
- **ورودی کاربر:** دکمه متصل به پایه PB4.

- **تنظیم فیوز بیت‌ها:** فعال بودن Internal RC Oscillator 8 MHz و غیرفعال بودن CKDIV8.

۴ طراحی نرم‌افزار Software Design

- **فیرم‌ور میکروکنترلر:**
  - پیاده‌سازی Software UART با بادریت ۹۶۰۰.
  - استفاده از ماشین حالت برای اجرای خودکار و حالت تعاملی.
- **اسکریپت پایتون:**
  - کتابخانه pyserial برای دریافت داده.
  - کتابخانه pyautogui برای شبیه‌سازی کیبورد.

۵ سناریوی اجرا Workflow

۱. روشن شدن دستگاه و شروع خودکار.

۲. باز شدن پنجره Run و اجرای دستور استخراج IP.

۳. ذخیره اطلاعات در فایل موقت.

۴. ورود به حالت انتظار.

۵. با فشردن دکمه، فایل متنی حاوی IP در Notepad باز می‌شود.

۶ دستور تزریق شده Injected Payload

```
cmd /c "ipconfig | findstr IPv4 >
```

۷ راهنمای اجرا Execution Guide

پیش‌نیازها

- نصب Python نسخه ۶.۳ یا بالاتر
- نصب کتابخانه‌ها:

```
pip install pyserial pyautogui
```

مراحل اجرا

۱. ساخت جفت پورت مجازی (مانند COM۱ و COM۲).

۲. تنظیم COMPIM روی پورت اول.

۳. اجرای اسکریپت پایتون روی پورت دوم.

۴. اجرای شبیه‌سازی در Proteus.

۸ عیب‌یابی Troubleshooting

- **کاراکترهای نامفهوم:** تنظیم نبودن فرکانس کلاک — بررسی فیوز بیت‌ها.
- **عدم عملکرد:** بررسی اتصال صحیح پورت‌های سریال.
- **خطای Denied: Access** اشغال بودن پورت — بستن برنامه‌های دیگر.

۹ نتیجه‌گیری Conclusion

این پروژه نشان داد که چگونه می‌توان با استفاده از یک میکروکنترلر ساده و ارتباط سریال، رفتار یک دستگاه BadUSB را شبیه‌سازی کرد. این پیاده‌سازی درک عمیق‌تری از امنیت USB، شبیه‌سازی HID و تعامل سخت‌افزار و نرم‌افزار فراهم می‌کند.