به نام خدا

دانشکده مهندسی کامپیوتر

درس ساختار و زبان کامپیوتر
نیم‌سال اول ۰۴-۰۵
استاد: دکتر اسدی

پروژه اجباری شماره ۳ : BadUSB با شبیه‌سازی پروتکل HID **شماره تیم : ۲۵**

اطلاعات تیم دانشجویی :

- محمدپارسا محمودآبادی آرانی - ۴۰۳۱۰۶۶۷۹
- سیدامیرحسین هاشمی شاهرودی - ۴۰۳۱۷۰۲۷۱
- نادر احمدی - ۴۰۳۱۰۵۶۷۴
- پارسا پاک - ۴۰۳۱۰۵۸۲۲

شرح مختصر پروژه :

هدف و ضرورت پروژه هدف اصلی این پروژه، طراحی و پیاده‌سازی یک ابزار نفوذ سخت‌افزاری در سطح پایین ($Low-level$) با استفاده از پروتکل HID و تراشه‌های خانواده AVR است. این ابزار که تحت عنوان $BadUSB$ شناخته می‌شود، با بهره‌گیری از برد $Digispark$ مهارت‌های برنامه‌نویسی اسمبلی را برای تعامل مستقیم با پورت USB و شبیه‌سازی دستگاه‌های ورودی به چالش می‌کشد. هدف نهایی، درک عمیق نحوه انتقال داده‌های حساس به صورت غیرمتعارف، بدون استفاده از کتابخانه‌های آماده و با تکیه بر منطق محض اسمبلی است.

وسایل و تجهیزات مورد نیاز برای اجرای این پروژه، از برد توسعه $Digispark$ مبتنی بر میکروکنترلر $ATtiny85$ به عنوان هسته اصلی استفاده می‌شود. تجهیزات جانبی شامل یک عدد کلید فشاری ($Push\ Button$) برای مدیریت فاز بازیابی، مقاومت‌های لازم و در صورت نیاز، یک نمایشگر $LCD\ I2C$ برای پایش وضعیت و نمایش داده‌های استخراج شده است. در سمت نرم‌افزاری نیز، سیستم هدف می‌تواند مجهز به سیستم‌عامل ویندوز یا لینوکس باشد تا اسکریپت‌های استخراج داده را اجرا نماید.

گام‌های اجرایی و فنی روند اجرای پروژه شامل سه گام اساسی است: ابتدا بستن مدار سخت‌افزاری و اتصال کلید و نمایشگر به پایه‌های $GPIO$ برد؛ سپس نوشتن اسکریپت‌های سمت کامپیوتر ($Bash$ یا $PowerShell$) برای استخراج اطلاعاتی نظیر رمز عبور وای‌فای؛ و در نهایت پیاده‌سازی برنامه اصلی به زبان اسمبلی AVR. بخش حساس فنی، طراحی پروتکل ارتباطی دست‌ساز برای خواندن وضعیت LEDهای کیبورد (مانند $Caps\ Lock$) و ذخیره‌سازی بیت‌به‌بیت داده‌ها در حافظه ماندگار $EEPROM$ میکروکنترلر است.

سناریوی عملیاتی پروژه در سناریوی مورد انتظار، ابزار پس از اتصال به سیستم، به صورت خودکار محیط ترمینال را باز کرده و اسکریپت استخراج را اجرا می‌کند؛ سپس داده‌های به دست آمده را از طریق تغییر وضعیت چراغ‌های کیبورد به برد منتقل و ذخیره می‌کند. در مرحله بعد، نفوذگر با جدا کردن برد و اتصال مجدد آن در حالی که دکمه سخت‌افزاری را نگه داشته است، وارد فاز بازیابی می‌شود. در این فاز، برد به صورت خودکار یک نرم‌افزار ویرایشگر متن (مانند $Notepad$) را باز کرده و تمامی اطلاعات ذخیره شده در حافظه را با سرعت بالا تایپ و نمایش می‌دهد.