Seguridad Inalámbrica en Dispositivos HID: Un Estudio sobre el Protocolo ESB y el Ataque MouseJack

Técnicas y Metodologías de Investigación en Ciberseguridad

Germán Quero

Introducción

Descripción

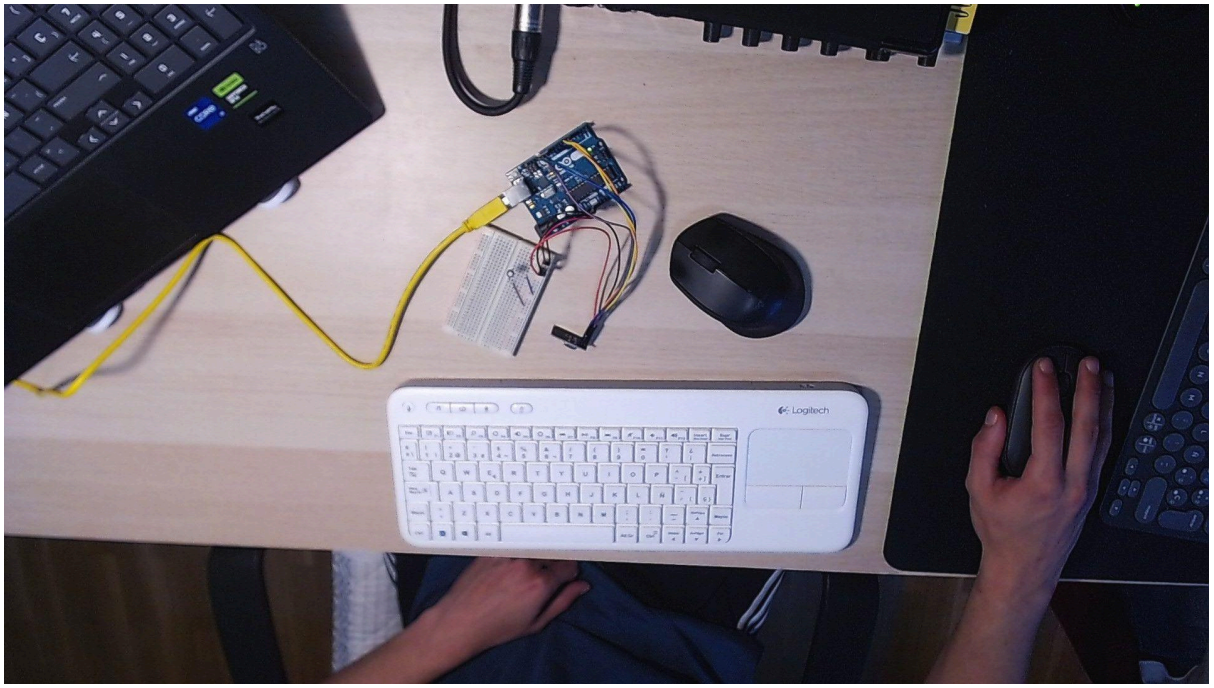
Esta investigación explora la seguridad de dispositivos HID inalámbricos en la banda ISM de 2.4 GHz, con un enfoque en vulnerabilidades explotables mediante la manipulación del protocolo Enhanced ShockBurst (ESB) utilizado en dispositivos Logitech Unifying, Microsoft y otros fabricantes no abarcados por la investigación.

Inspirado por trabajos como el de Marc Newlin presentado en DEFCON 24 (MouseJack) y herramientas como uC_mousejack, el proyecto busca entender, identificar y explotar las fallas de seguridad de estos dispositivos.

Tras desarrollar un primer laboratorio de comunicación entre dos transreceptores nRF24L01, que utilizan ESB, con el objetivo de entender como funciona en detalle,se desarrolló un sniffer capaz de identificar dispositivos vulnerables en el entorno.

Posteriormente, se amplió para incluir la recreación completa de ataques MouseJack. Esto permitió crear una herramienta funcional que genera y ejecuta ataques basados en scripts Ducky, utilizando un módulo nRF24L01 y un Arduino UNO como base de hardware.

Las pruebas se realizaron sobre un Logitech k400r y un Logitech m280 conectados a un equipo propio.



Planificación

El proyecto se estructuró en las siguientes fases:

1. Investigación preliminar:
    - Estudio del protocolo ESB y sus características principales: desarrollo de un laboratorio de comunicación básico.
    - Revisión de investigaciones previas, como los trabajos de Travis Goodspeed y Marc Newlin, y herramientas relacionadas como uC_mousejack.

2. Desarrollo inicial del sniffer:
    - Implementación de un sniffer basado en pseudo-promiscuidad, utilizando un módulo nRF24L01.
    - Identificación de dispositivos vulnerables mediante un barrido de canales y verificación manual de CRC.

3. Ampliación de funcionalidad:
    - Desarrollo de una herramienta completa para ataques MouseJack.
    - Integración de un sistema para traducir scripts Ducky a paquetes HID y ejecutarlos.

4. Validación en entornos reales:
    - Pruebas en entornos controlados y abiertos con un dispositivo Logitech (k400r).
    - Identificación de problemas y ajustes en las fases de ataque.

5. Documentación y conclusiones:
    - Información recopilada sobre MouseJack, dispositivos HID, protocolo ESB, etc.
    - Redacción de recomendaciones y trabajo futuro en esta investigación.
    - Conclusiones y documentación.

Durante la investigación se consideraron tanto los aspectos técnicos como éticos del trabajo, asegurándose de que todas las pruebas fuesen sobre dispositivos propios o con autorización explícita.

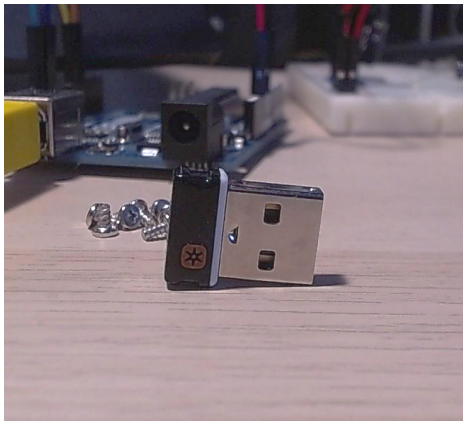
Objetivos

El proyecto establece los siguientes objetivos principales:

1. Objetivos Técnicos:
    - Implementar la comunicación entre dos transreceptores nRF24L01.
    - Implementar un sniffer básico capaz de identificar dispositivos Logitech que utilicen ESB vulnerable.
    - Desarrollar una funcionalidad de ataque MouseJack que permita inyectar comandos maliciosos en dispositivos identificados.

2. Objetivos de Aprendizaje:
    - Profundizar en el análisis de protocolos inalámbricos como ESB.
    - Comprender las limitaciones y vulnerabilidades de dispositivos HID inalámbricos.
    - Desarrollar habilidades prácticas en programación para hardware embebido.
    - Mejorar conocimientos sobre los sistemas de radio frecuencias.

3. Objetivos Éticos y de Seguridad:
    - Generar conciencia sobre las vulnerabilidades en dispositivos HID inalámbricos.
    - Proveer información técnica útil para que fabricantes y usuarios finales mejoren la seguridad de sus dispositivos.



Logitech Unifying es probablemente la tecnología más vulnerable de este tipo. Esta investigación evidencia la importancia de la actualización de firmware que ofrece el fabricante.

Se identifica por ese característico sol naranja.

Problemas

Durante el desarrollo del proyecto se presentaron diversos desafíos técnicos y de diseño:

1. Limitaciones del Hardware:
    - El Arduino UNO tiene recursos limitados, lo que restringe la complejidad del procesamiento y almacenamiento de datos capturados.
    - Los módulos nRF24L01 presentan variabilidad en su sensibilidad de recepción, afectando el rendimiento y siendo susceptible a interferencias.

2. Protocolos y Configuración:
    - Se partía de un desconocimiento total de los sistemas inalámbricos de radio frecuencia y su funcionamiento pero la charla de Samy Kamkar sobre Radio Hacking facilitó bastante el trabajo
    - Decodificar el protocolo ESB fue desafiante debido a su limitada documentación, pero el trabajo de Marc Newling facilitó mucho el proceso.
    - Identificar los parámetros correctos de CRC y dirección en tiempo real implicó ajustes iterativos en el código.

3. Validación de Resultados:
    - Las pruebas en dispositivos reales revelaron variaciones inesperadas y muchos problemas de interferencias.
    - La Arduino UNO no es la plataforma más adecuada para el desarrollo de esta herramienta, sin embargo se trabajó con lo que se tenía disponible.
        i. Se trabajó teniendo siempre en mente la facilidad de integración en otra plataforma para el futuro del proyecto.

A pesar de estos desafíos, los objetivos principales se cumplieron, y la herramienta desarrollada demuestra tanto el impacto de las vulnerabilidades como la necesidad de mejorar los estándares de seguridad en dispositivos HID inalámbricos.

Esta investigación proseguirá fuera de la limitación temporal de la entrega universitaria con el objetivo de estudiar más a fondo posibles vulnerabilidades pendientes de descubrir, así como de crear una herramienta mejor y más eficiente en hardware más específico.

Herramientas

Para la investigación se han utilizado dos Arduino UNO, dos módulos nrf24l01 y condensadores de 100uF para estabilizar la alimentación de los módulos. Por otra parte, las pruebas se han realizado sobre un teclado Logitech K400r y un ratón M280 conectados a un equipo propio.

Durante la investigación se han desarrollado 3 herramientas o laboratorios que ayudan a entender esta vulnerabilidad y el protocolo al que afecta (ESB):

- nrf24l01-arduinoUNO-connect: Proyecto muy simple de emisor y receptor que recrea un esquema sencillo de comunicación ESB. Fue desarrollado para ayudar a entender cómo funciona el direccionamiento.
    - https://github.com/germanquero/nrf24l01-arduinoUNO-connect

- sniffer-UNO-24: Sniffer de direcciones vulnerables basado en el trabajo de Insecurity Of Things en uC_mousejack. Es un paso previo a la herramienta principal desarrollada durante la investigación. Identifica dispositivos vulnerables bajo el alcance de la antena.
    - Se puede encontrar en el repositorio de la investigación en un directorio con su nombre.

- mousejack-UNO-24: Herramienta principal desarrollada en esta investigación. Muy inspirada por el trabajo en uC_mousejack. Realiza ataques de inyección de paquetes HID sin cifrar en dispositivos Logitech y Microsoft (aunque solo se ha podido probar con Logitech)

Las herramientas desarrolladas se basan en la siguientes:

- https://github.com/BastilleResearch/mousejack
- https://github.com/insecurityofthings/uC_mousejack
- https://github.com/insecurityofthings/jackit
- https://github.com/samyk/keysweeper

Son el trabajo de las investigaciones similares por parte de Bastille, Insecurity Of Things por parte de Samy Kamkar y MarcNewlin.

Investigación Previa

Protocolo Enhanced ShockBurst (ESB)

El protocolo Enhanced ShockBurst (ESB) es una mejora del protocolo ShockBurst desarrollado por Nordic Semiconductor para la comunicación inalámbrica en la banda de 2.4 GHz ISM.

ESB permite la transmisión de datos de manera eficiente entre dispositivos con un enfoque en aplicaciones de bajo consumo y alta velocidad, como dispositivos HID (teclados, ratones y controles remotos).

Aunque fue diseñado para ser robusto y eficiente, carece de características de seguridad modernas como el cifrado y la autenticación de paquetes.

A día de hoy la mayoría de fabricantes utilizan un modelo propietario que mejora la seguridad aplicando algún tipo de cifrado, aunque en algunos casos el receptor sigue aceptando paquetes HID sin cifrar.

Características Técnicas de ESB

- Dirección y Pipes: Cada dispositivo tiene una dirección única (de 3 a 5 bytes) que sirve como identificador. ESB soporta múltiples pipes (canales virtuales) para comunicación simultánea.
- Frecuencia: Opera en la banda de 2.4 GHz, con 126 canales disponibles. Esto permite configuraciones flexibles pero también introduce un riesgo de interferencia.
- Confirmación Automática (Auto-ACK): Después de recibir un paquete, el receptor puede enviar automáticamente un paquete de confirmación al emisor.
- Reenvío Automático (Auto-Retransmit): Si no se recibe una confirmación, el emisor reenvía el paquete un número predefinido de veces.
- Payload Dinámico: ESB soporta longitudes de payload dinámicas, lo que reduce la latencia al evitar relleno innecesario de datos.
- CRC (Cyclic Redundancy Check): Utiliza CRC de 1 o 2 bytes para verificar la integridad de los datos, pero no asegura la autenticidad de estos.

Vulnerabilidades del Protocolo ESB

1. Ausencia de Cifrado: ESB no cifra los datos transmitidos, lo que permite a un atacante con un sniffer interceptar y leer las comunicaciones.
2. Falta de Autenticación: El protocolo no incluye mecanismos para verificar la autenticidad del emisor, facilitando la inyección de paquetes maliciosos.d

Transceptor nRF24L01

El módulo nRF24L01 es un transceptor de radio de 2.4 GHz desarrollado por Nordic Semiconductor que implementa ESB. Es ampliamente utilizado debido a su bajo costo, bajo consumo de energía y alta velocidad de transmisión.

Especificaciones Técnicas

- Frecuencia: 2.4 GHz ISM, con soporte para 126 canales.
- Modulación: GFSK (Gaussian Frequency Shift Keying).
- Velocidad de Datos: 250 kbps, 1 Mbps o 2 Mbps.
- Configuración: Controlado a través de un bus SPI, lo que facilita su integración con microcontroladores.
- Alcance: Depende de la antena, pero típicamente varía entre 30 y 100 metros.
- Potencia de Transmisión: Ajustable entre -18 dBm y 0 dBm.

Modo Pseudo-Promiscuo

El nRF24L01 no soporta un modo promiscuo genuino (captura de todo el tráfico en el espectro), pero puede configurarse para escuchar paquetes dirigidos a una dirección específica.

Aprovechando esta característica, Travis Goodspeed y otros investigadores demostraron que un atacante puede configurar el dispositivo para identificar direcciones activas de manera eficiente.

Dispositivos HID Inalámbricos

Logitech

Los dispositivos Logitech utilizan ESB con ciertas modificaciones propietarias. Aunque algunos modelos implementan medidas básicas de seguridad, como la validación del payload, muchos dispositivos son vulnerables al ataque conocido como MouseJack.

1. Implementaciones Vulnerables:
    - Ratones y teclados que utilizan receptores Unifying.
    - Carecen de cifrado, lo que permite la inyección de comandos maliciosos.

2. Detalles de la Vulnerabilidad MouseJack:
    - Descubierta por Marc Newlin en 2016, MouseJack aprovecha la falta de autenticación en el protocolo para inyectar comandos desde un dispositivo no autorizado.
    - Permite ejecutar scripts maliciosos en la máquina conectada al dispositivo HID.

Microsoft

Aunque los dispositivos Microsoft también utilizan ESB, su implementación difiere en algunos aspectos clave:

- Algunos modelos utilizan un CRC único o longitudes de payload no estándar, dificultando ligeramente la inyección de paquetes.

- Sin embargo, como en el caso de Logitech, la falta de cifrado y autenticación los hace susceptibles al ataque MouseJack.

Vulnerabilidades y Casos de Uso

Los ataques a dispositivos HID inalámbricos presentan un grave riesgo de seguridad debido a la posibilidad de:

1. Inyección de Comandos Arbitrarios:
    - Un atacante puede simular un teclado para escribir comandos maliciosos, instalar malware o robar datos.
    - Estos comandos pueden ser codificados utilizando scripts Ducky o formatos similares.
2. Captura de Tráfico Sensible:
    - Aunque ESB no permite un modo promiscuo, un atacante puede capturar datos de dispositivos previamente identificados.
3. Escalación de Privilegios:
    - Utilizando la inyección de comandos, un atacante podría abrir un terminal con permisos elevados y comprometer completamente el sistema.
4. Persistencia en el Sistema:
    - Mediante la ejecución de scripts maliciosos, el atacante puede establecer mecanismos de persistencia, como tareas programadas o puertas traseras.

En este repositorio se relata el desarrollo de una herramienta, de momento implementada mediante un badUSB personalizado con una Arduino Pro Micro, que establece una comunicación con un servidor C2 y abusa de las tareas programadas para establecer una persistencia en el sistema: https://github.com/germanquero/arduGator

Pruebas Realizadas

Durante la investigación se han creado 2 laboratorios principales. Estos se pueden encontrar en el siguiente repositorio:

https://github.com/germanquero/mouseJack-Inv

sniffer-UNO-24

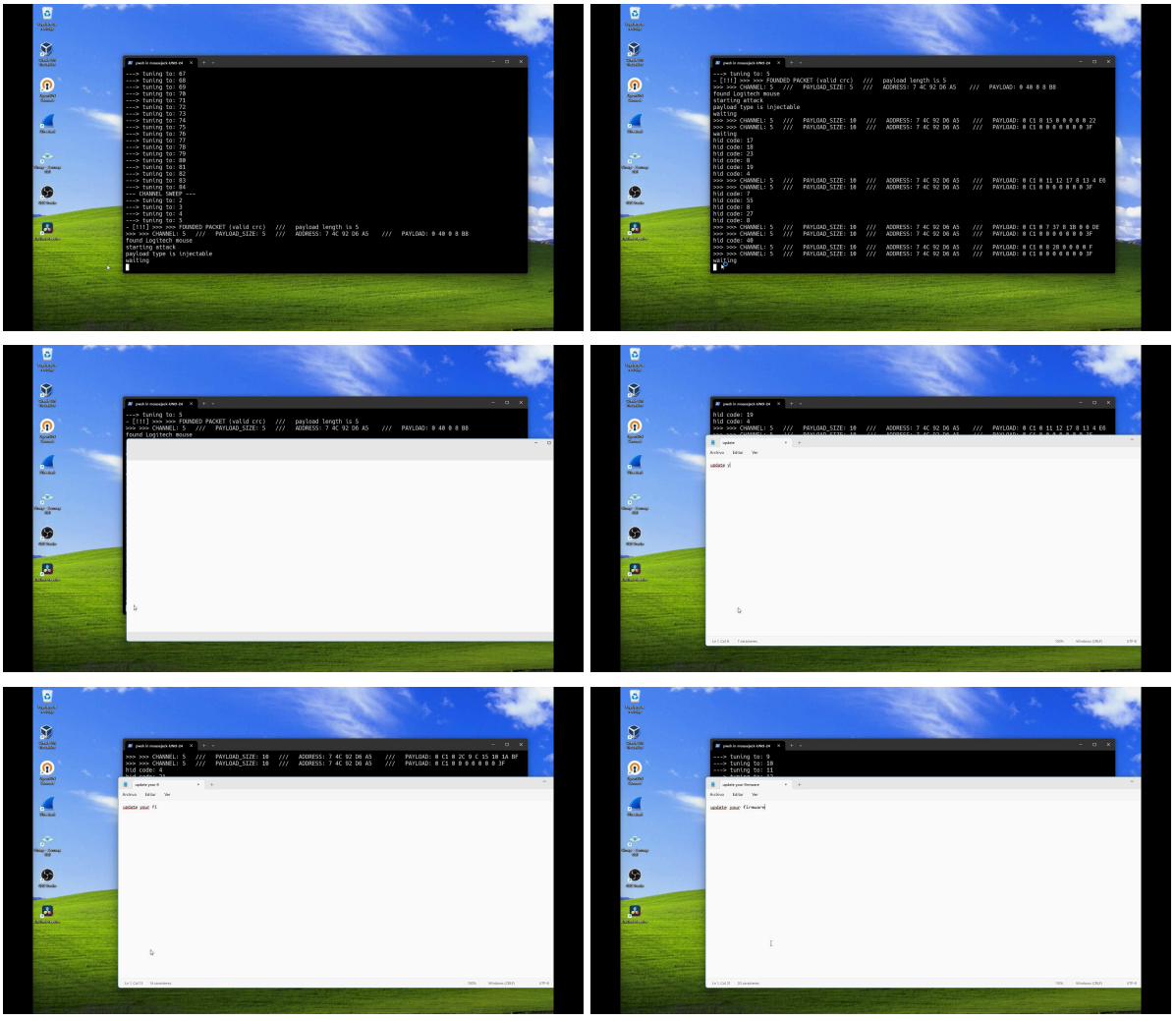
Un sniffer de direcciones que recoge información sobre la dirección o el payload, se podría decodificar para crear un proyecto similar a KeySweeper.

Esto se ha probado con los dispositivos mencionados y en un entorno público para observar la cantidad de dispositivos vulnerables en un entorno convencional.

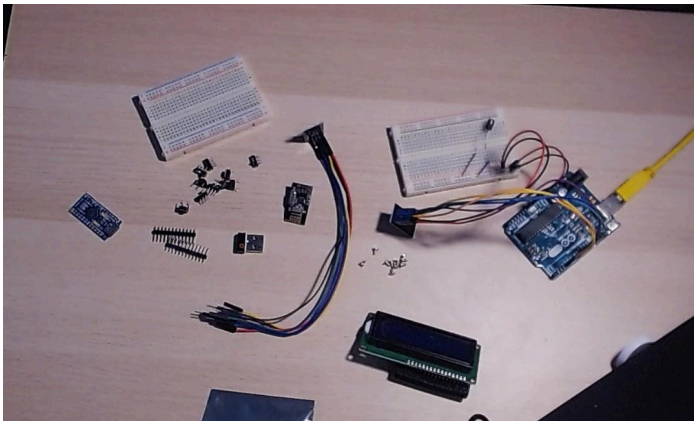
Las conclusiones fueron que 4 de 15 ratones (estimados) eran vulnerables a este tipo de ataques, todos solucionables con una actualización de firmware.

mousejack-UNO-24

Esta herramienta realiza ataques de inyección de paquetes HID sin cifrar en dispositivos Logitech y Microsoft (aunque solo se ha podido probar con Logitech)
Es una adaptación al hardware utilizado de uC_mousejack que en el futuro de este proyecto se mejorará mediante paralelización de recursos mediante una Arduino más potente y más módulos nRF24L01 y una interfaz hardware (teclado y pantalla) para su funcionamiento interactivo y autónomo.



La potencia de la Arduino y la estabilización de la señal para evitar interferencias ha sido un gran reto que se puede solucionar mediante una Arduino Pro Micro, bastante más potente, 3 módulos nRF24L01 para repartir tareas, PCBs personalizadas y algo de trabajo de soldadura, por ello ya se han adquirido para poder trabajar



en la próxima versión tempranamente.

Conclusión de la Investigación

El análisis del protocolo ESB y las implementaciones en dispositivos Logitech y Microsoft revela una alarmante falta de medidas de seguridad. Esto, combinado con la accesibilidad de herramientas como el nRF24L01 y el bajo costo del hardware, hace que los ataques MouseJack sean una amenaza viable.

Todo lo recopilado en este documento evidencia la importancia de mantener actualizado el firmware de nuestros dispositivos HID y el monitoreo de los sistemas.