Keystroke Injection with

MouseJack

Mateus Rocha - 11921BCC027
Vitor Barbosa - 11921BCC035

Introdução

Introdução

- Publicada pela Bastille em 2016.
- Coleção de vulnerabilidades.
- Envolvendo 7 fabricantes e inúmeros dispositivos.
- Permitido injetar comandos no computador da vítima.
- Até 100 metros de distância.

Como funcionam os dongles 2.4Ghz

- Alternativa ao protocolo Bluetooth.
- Transmissão de pacotes para um dongle USB.
- Sem padrão na indústria. Protocolo proprietário.
- Cada fabricante estabelece esquema de segurança.

Como funcionam os dongles 2.4Ghz

- Os dongles esperam por pacotes na frequência de 2.4Ghz.
- Quando recebidos, informam os comandos ao computador.
- Os pacotes trocados entre dongle e teclado são criptografados.
- O dongle sabe a chave para descriptografar o pacote e descobrir a tecla pressionada.

Como funcionam os dongles 2.4Ghz

Como funcionam os dongles 2.4Ghz

- Nenhum mecanismo de criptografia ou autenticação para mouse.
- O dongle não consegue distinguir quem enviou os pacotes para ele.
- Alguém mal intencionado pode transmitir pacotes fingindo ser o mouse.

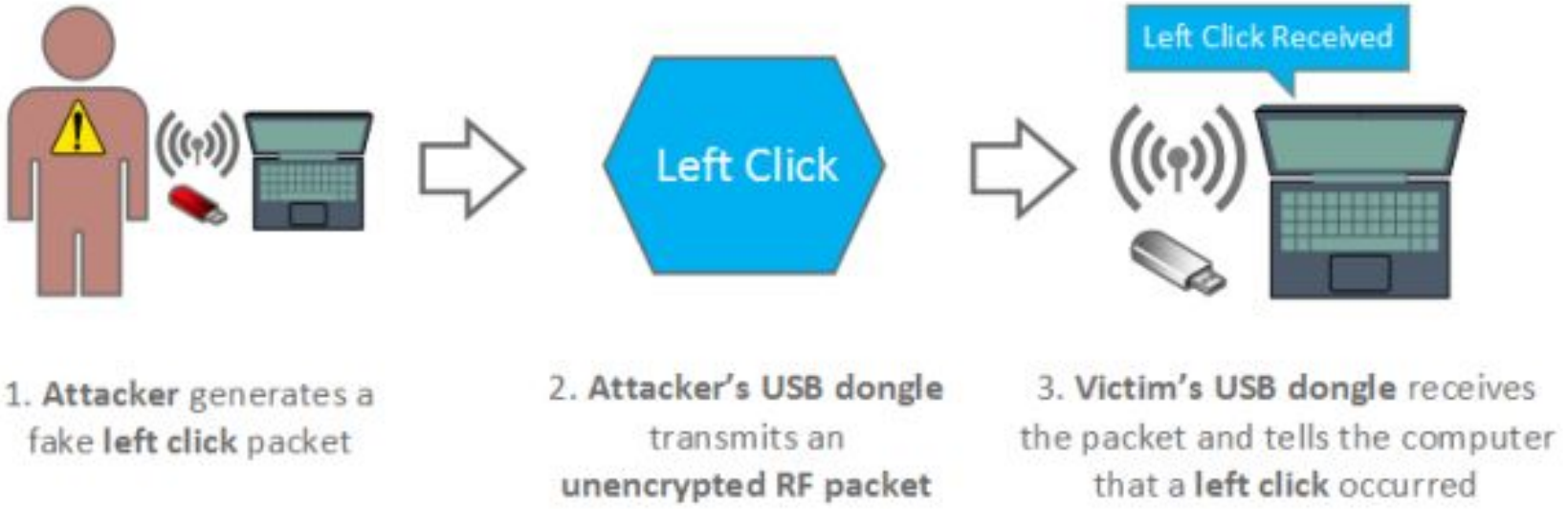
Como funcionam os dongles 2.4Ghz

Como funcionam os dongles 2.4Ghz

"Since the displacements of a mouse would not give any useful information to a hacker, the mouse reports are not encrypted."

- Logitech (2009)

Como funcionam os dongles 2.4Ghz

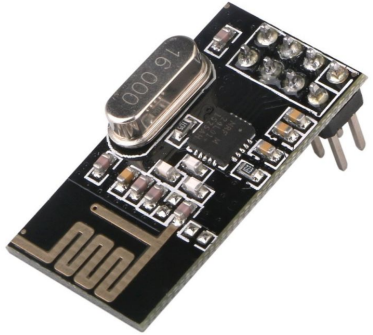


Como funcionam os dongles 2.4Ghz

Problemas relacionados a como o dongle processa o pacotes permitem que alguém mal intencionado transmita pacotes que simulam pressionar de teclas em vez de movimentos de mouse.

Transceivers

Nordic Semiconductor nRF24L



- Transceiver de propósito geral
- Cinco variações diferentes produzidas
- Algumas dão suporte a atualizações de firmware, outras não.
- Muitos dos dispositivos afetados não puderam ter suas vulnerabilidades corrigidas

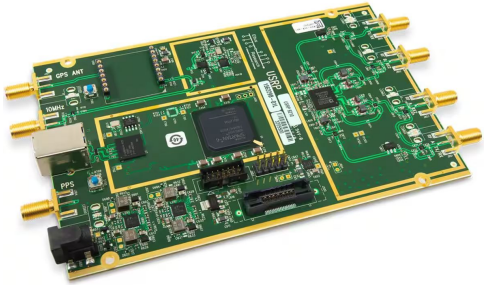
Outros transceivers afetados

- Texas Instruments CC254X
- MOSART Semiconductor
- Signia SGN6210
- GE Mystery Transceiver

Processo de pesquisa

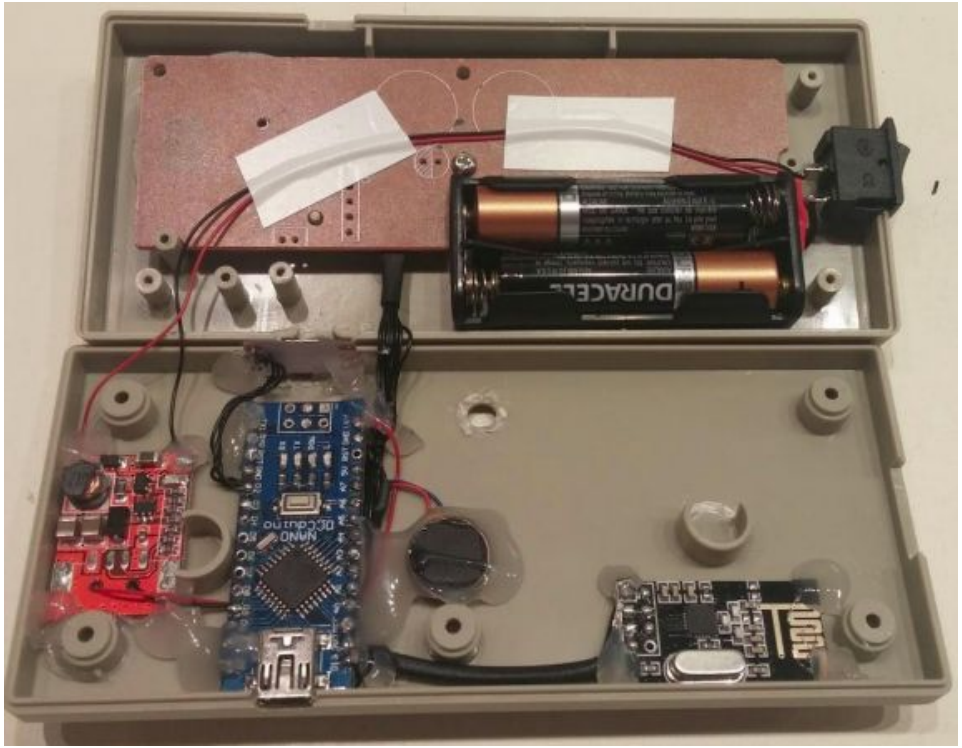
Processo de pesquisa

- Objetivo inicial: engenharia reversa do **mouse M510** da Logitech (**nRF24L**)
- Tentativa: **USRP B210 software defined radio** para receber e decodificar pacotes
  - compatível com vários protocolos de rádio
  - analisar o comportamento (channel hopping, ACKs, crypto, etc)
  - analisar o formato dos pacotes
  - não consegue mudar de canais rapidamente
  - não consegue observar todos os pacotes transmitidos



Processo de pesquisa

- Ferramentas de pesquisa:
  - Controle NES modificado
  - CrazyRadio PA dongle
- Utilizados para comunicação, sniffing e fuzzing
- Programados para transmitir pacotes reconhecidos pelo transceiver da Logitech, controle NES consegue simular um mouse



Componentes internos do controle NES modificado, 1ª e 2ª versões

Componentes principais: **Arduino Nano**, transceiver **nRF24L01+**

CrazyRadio PA

- Originalmente utilizado para controlar drones (Crazyflie)
- Utiliza o nRF24L
- Firmware modificado
  - Permite ataques a longa distância, >100m
  - Permite sniffing e injeção
  - Controlado por código Python

Fuzzing

- Envio de dados aleatórios: válidos ou inválidos
- Comportamento é analisado para falhas de segurança ou engenharia reversa

Passo a passo:

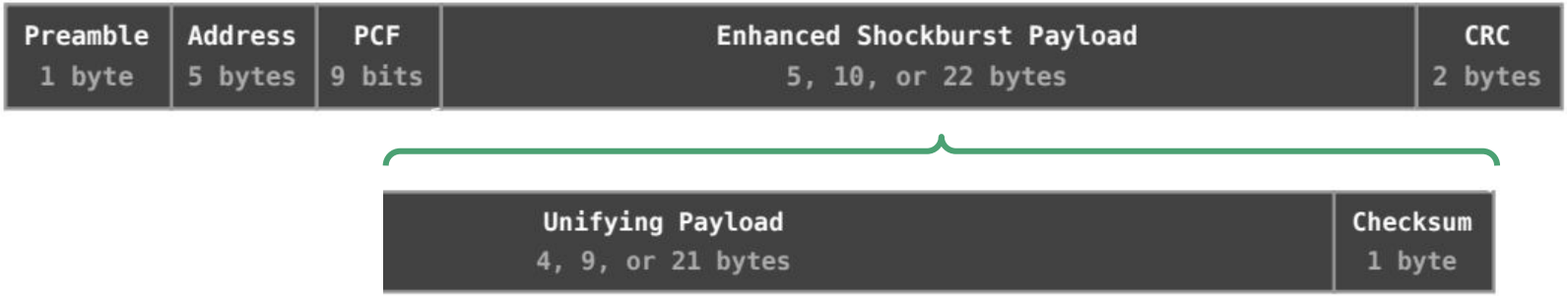
1. CrazyRadio PA envia pacotes aleatórios ao dongle do mouse
2. Dongle envia pacotes USB HID ao sistema operacional
3. Tráfego USB é monitorado (usbmon/wireshark)
4. Entradas válidas são registradas e analisadas (movimento de mouse, teclas pressionadas)

Dispositivos afetados:

Logitech Unifying

Logitech Unifying

- Protocolo utilizado na comunicação wireless de vários dispositivos da Logitech
- Qualquer dispositivo Unifying pode ser conectado a um dongle Unifying



Formato de um pacote do protocolo Logitech Unifying

Logitech Unifying: Segurança

- **Mouse**: pacotes não são criptografados
- **Teclado**: pacotes são criptografados usando AES 128-bit
  - é possível injetar input de teclado não criptografado

Logitech Unifying: Vulnerabilidades

- Forced Pairing (BN-0001)
- **Unencrypted Keystroke Injection (BN-0002)**
- Disguise Keyboard as Mouse (BN-0003)
- Unencrypted Keystroke Injection Fix Bypass (BN-0011)
- Encrypted Keystroke Injection (BN-0013)

Demonstração

Hardware

Logitech Unifying dongle (modelo C-U0007) e mouse Logitech M505 com dongle

Hardware

1. **Attacker** generates a fake **left click** packet

2. **Attacker's USB dongle** transmits an **unencrypted RF packet**

3. **Victim's USB dongle** receives the packet and tells the computer that a **left click** occurred

Spoofed Unencrypted Keyboard Packet

Software

- Github: BastilleResearch/mousejack
  - firmware
  - scanner
  - sniffer
- Github: insecurityofthings/jackit
  - scanner
  - injector
  - duckyscript

Referências

- NEWLIN, Marc. MouseJack, KeySniffer and Beyond: Keystroke Sniffing and Injection Vulnerabilities in 2.4GHz Wireless Mice and Keyboards, 2016. https://github.com/BastilleResearch/mousejack/blob/master/doc/pdf/DEFCON-24-Marc-Newlin-MouseJack-Injecting-Keystrokes-Into-Wireless-Mice.whitepaper.pdf
- Bastille https://www.bastille.net/research/vulnerabilities/mousejack/
- Mousejack https://github.com/BastilleResearch/mousejack
- Jackit https://github.com/insecurityofthings/jackit