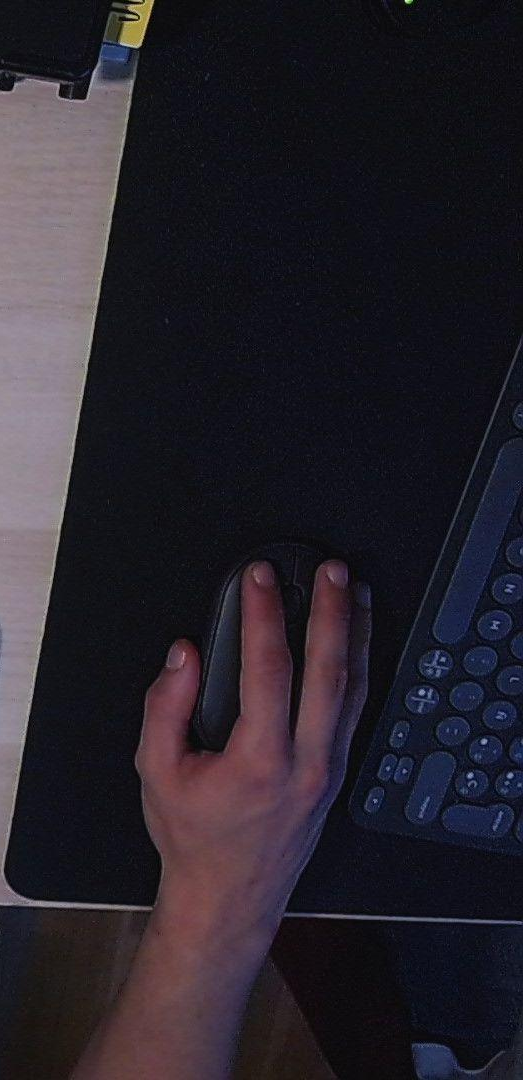
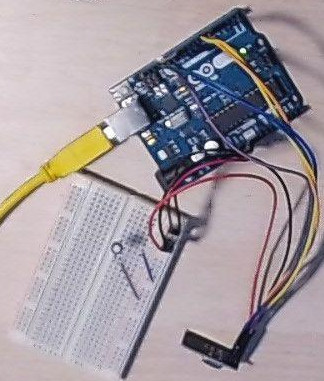


# Seguridad Inalámbrica en Dispositivos HID

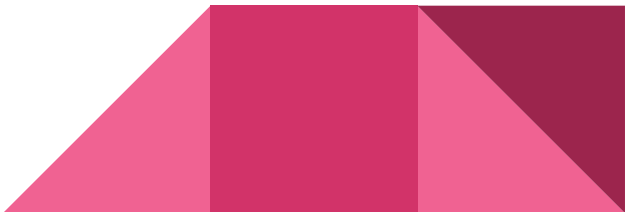
Un Estudio sobre el Protocolo ESB y el Ataque MouseJack



# ¿Qué investigamos?

- La inseguridad de dispositivos HID inalámbricos en la banda ISM de 2.4 GHz.
- Vulnerabilidades del protocolo ESB y sus implementaciones en dispositivos como Logitech y Microsoft.

## Inspiración:

- Trabajos de Marc Newlin (MouseJack, DEFCON 24).
  - Herramientas previas como jackit y KeySweeper.
- 

# Objetivos

## Técnicos:

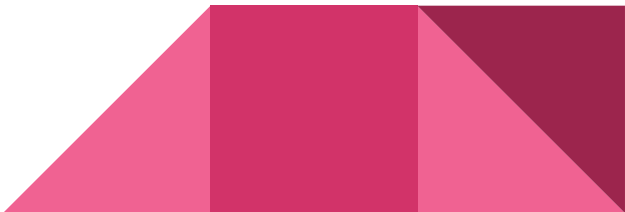
- Implementar comunicación básica entre transceptores nRF24L01.
- Crear un sniffer para identificar dispositivos vulnerables.
- Desarrollar funcionalidad completa de ataques MouseJack.

## Aprendizaje:

- Analizar protocolos inalámbricos y sus limitaciones.
- Mejorar habilidades en hardware embebido y radiofrecuencia.

## Éticos:

- Sensibilizar sobre esta vulnerabilidad.




# Herramientas

## Hardware:

- Arduino UNO, módulos nRF24L01, condensadores de 100uF.

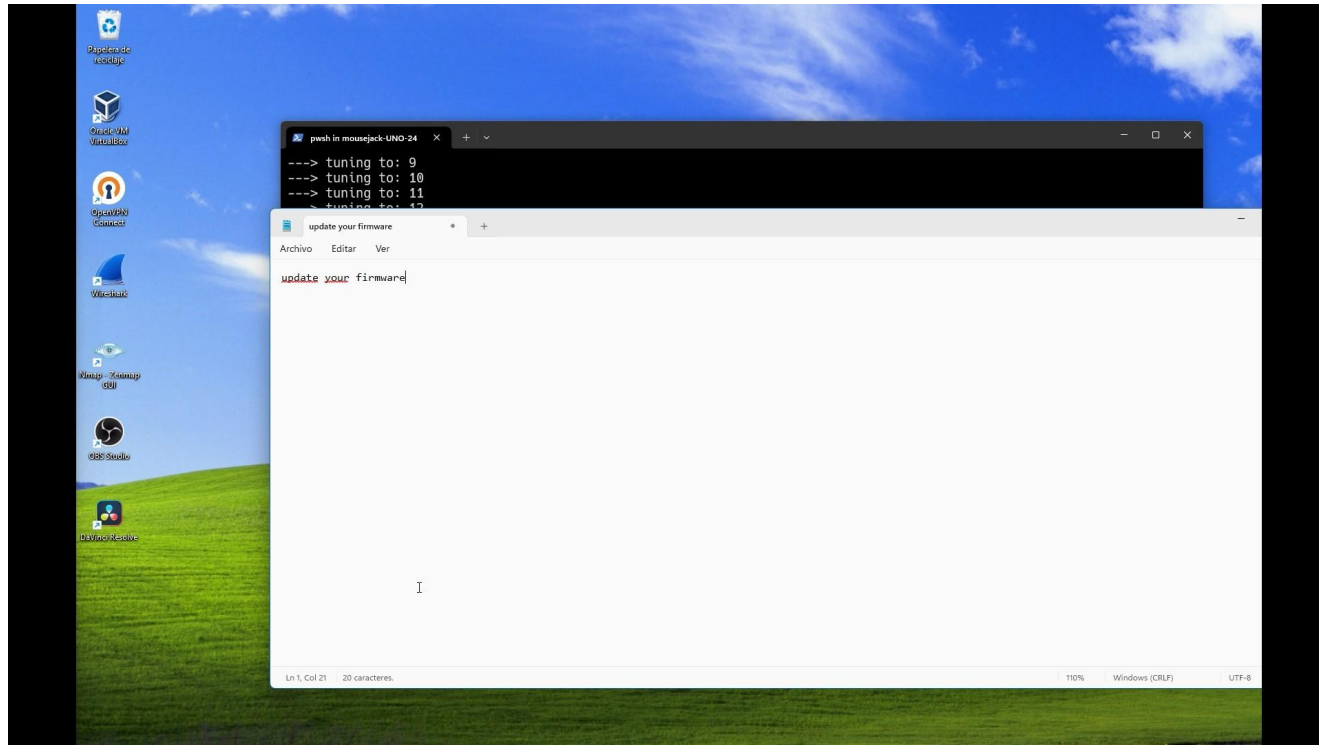
## Software:

- sniffer-UNO-24: Identificación de dispositivos vulnerables.
  - mousejack-UNO-24: Ataques de inyección de paquetes HID.
  - attack\_gen.py: Generador de paquetes HID en base a Ducky Scripts desarrollado en python
- 

# sniffer-UNO-24

```
--> tuning to: 37
--> tuning to: 38
--> tuning to: 39
--> tuning to: 40
--> tuning to: 41
- [!!!] >>> >>> FOUNDED PACKET (valid crc)   ///   payload is empty.
- [!!!] >>> >>> FOUNDED PACKET (valid crc)   ///   payload length is 5
>>> >>> CHANNEL: 41   ///   PAYLOAD_SIZE: 5   ///   ADDRESS: 7 4C 02 D6 A5   ///   PAYLOAD: 0 40 0 8 B8
** Resetting...
- Starting scan...
--> tuning to: 42
--> tuning to: 43
--> tuning to: 44
--> tuning to: 45
--> tuning to: 46
--> tuning to: 47
--> tuning to: 48
--> tuning to: 49
--> tuning to: 50
--> tuning to: 51
--> tuning to: 52
--> tuning to: 53
--> tuning to: 54
--> tuning to: 55
--> tuning to: 56
--> tuning to: 57
--> tuning to: 58
--> tuning to: 59
--> tuning to: 60
--> tuning to: 61
--> tuning to: 62
--> tuning to: 63
--> tuning to: 64
--> tuning to: 65
--> tuning to: 66
--> tuning to: 67
--> tuning to: 68
--> tuning to: 69
--> tuning to: 70
--> tuning to: 71
- [!!!] >>> >>> FOUNDED PACKET (valid crc)   ///   payload length is 10
>>> >>> CHANNEL: 71   ///   PAYLOAD_SIZE: 10   ///   ADDRESS: 7 A8 FB 67 39   ///   PAYLOAD: 0 4F 0 0 6E 0 0 0 0 43
** Resetting...
** Scanning...
- Starting scan...
--> tuning to: 72
--> tuning to: 73
```

# mousejack-UNO-24

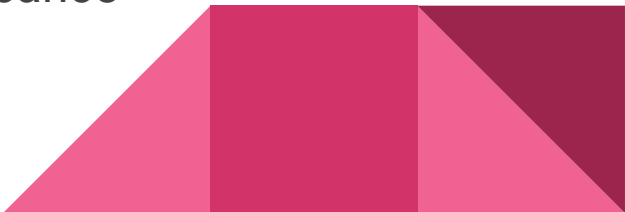


# Protocolo ESB y nRF24L01

## **ESB: características técnicas:**

- Banda: 2.4 GHz, con 126 canales.
- Auto-ACK, Auto-Retransmit.

## **Transreceptor nRF24L01:**

- Muy utilizado por su bajo costo
  - Modo Pseudo-promiscuo
  - GSKF, 250kbps - 2Mbps, entre 30 y 100 metros de alcance
- 



# Problemas encontrados

- **Hardware limitado:** procesamiento limitado en Arduino UNO
- **Interferencias:** ruido en la banda 2.4GHz
- **Soluciones:** mejorar hardware y adaptar el software para paralelizar tareas entre más módulos nRF24L01




# Conclusiones

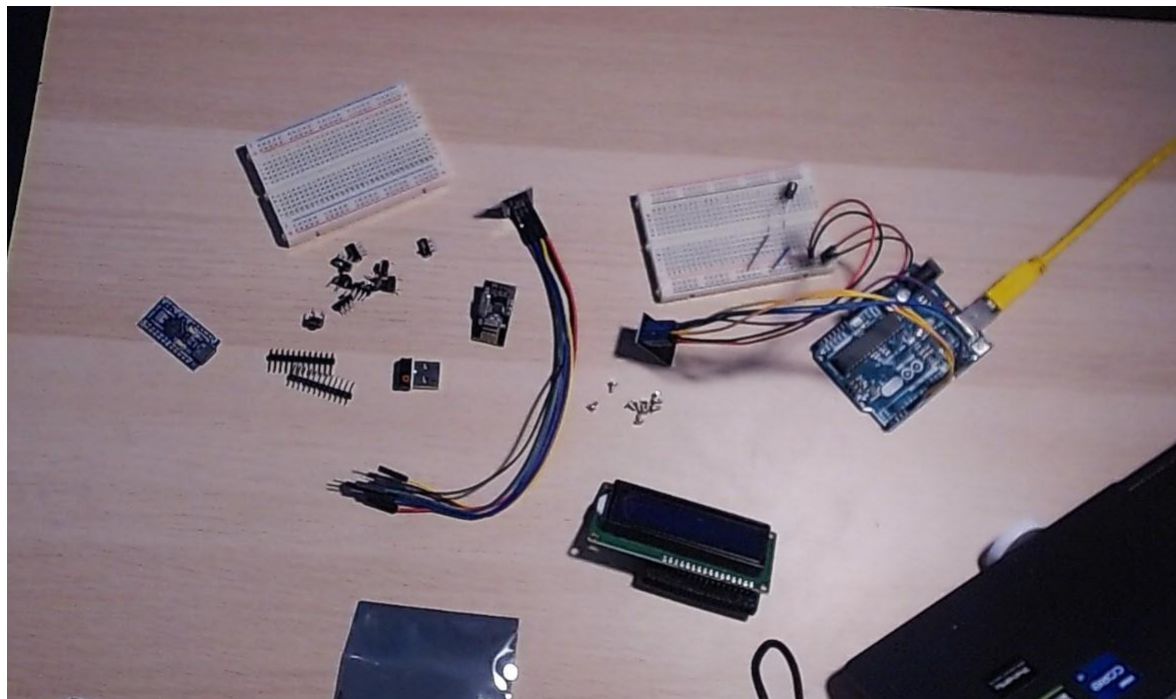
## Impacto:

- Se encontraron bastantes dispositivos con el firmware aún vulnerable.
- El impacto de este tipo de ataques puede ser altísimo si no se toman medidas de seguridad adecuadas.

## Recomendaciones:

- Mantener el firmware actualizado
  - Monitorear sistemas para detectar comportamientos anómalos
  - Bloquear el ordenador **SIEMPRE**.
- 

# Futuro de esta Investigación



# Referencias

- DEFCON-24: Marc Newlin MouseJack: Injecting Keystrokes Into Wireless Mice
- Samy Kamkar: KeySweeper

