Escuela Superior
de Ingeniería y Tecnología
Universidad de La Laguna

# Trabajo de Fin de Grado

Grado en Ingeniería Informática

---

# Seguridad en Cerraduras Inteligentes

*Smart Lock Security*

Joselin Pérez Pérez

---

La Laguna, *8* de *septiembre* de 2021

Dña. **Pino Teresa Caballero Gil,** con N.I.F. 45.534.310-Z Catedrática de Universidad adscrita al Departamento de Ingeniería Informática y de Sistemas de la Universidad de La Laguna, como tutora

D. **Cándido Caballero Gil**, con N.I.F. 42.201.070-A profesor Ayudante Doctor de Universidad adscrito al Departamento de Ingeniería Informática y de Sistemas de la Universidad de La Laguna, como cotutor

**C E R T I F I C A (N)**

Que la presente memoria titulada:

*"Seguridad en Cerraduras Inteligentes"*

ha sido realizada bajo su dirección por Dña. **Joselin Pérez Pérez**, con N.I.F. 42.236.328-W.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firman la presente en La Laguna a 8 de septiembre de 2021

# Agradecimientos

En primer lugar, quiero agradecer a mi tutora Pino y mi cotutor Cándido por toda su ayuda a la hora de realizar este trabajo de fin de grado.

Por otro lado, me gustaría agradecer a mis padres, mi hermana y mis amigos que siempre me han apoyado y confiado en mí.

En especial quiero agradecer a mi padre, que a pesar de que no está conmigo al final de esta etapa siempre me ha apoyado y sé que lo sigue haciendo. Gracias papi.

# Licencia

**Resumen**

*El gran auge de las cerraduras inteligentes ha conllevado a que estas se encuentren presentes en muchos de los hogares de gran cantidad de países. Esto es debido a su gran comodidad de uso y la variedad de opciones que poseen.*

*Sin embargo, por defecto el uso de estas cerraduras no implica que su hogar sea más seguro. Su empleo ha supuesto el uso de nuevas técnicas de robo basadas en ciberataques. Esto implica que este objeto de las cerraduras inteligentes se pueda ver afectado por la desconfianza de la población.*

*El objetivo de este trabajo ha sido la investigación de la seguridad en los dispositivos inalámbricos, centrándonos en la seguridad de las cerraduras inteligentes que funcionan mediante Bluetooth. Por tanto, se han estudiado las ventajas y desventajas de tener una cerradura inteligente y de su modelo de seguridad.*

**Palabras clave:** ciberataque, Bluetooth, cerradura inteligente, seguridad

**Abstract**

*The rise of smart locks has made them present in many homes in a large number of countries. This is due to their user-friendly design and the variety of options they offer.*

*However, by default the use of these smart locks does not make your home more secure. Their use has led to the use of other theft techniques, such as cyber-attacks. This means that this object of smart locks can be affected by public distrust.*

*The aim of this work has been the research of security in wireless devices, focusing on the security of smart locks that work via Bluetooth. Therefore, the advantages and disadvantages of having a smart lock and its security model has been studied.*

**Keywords:** cyber-attack, Bluetooth, smart key, security

# Índice general

# Índice de figuras

# Índice de tablas

# 1. Introducción

## 1.1 Motivación

A pesar de que es un objeto que resulta cotidiano en nuestras vidas, las cerraduras que poseemos hoy en día son una innumerable mejora de cerraduras muy antiguas. Desde los tiempos más remotos, la humanidad tenía la necesidad de protegerse, siendo la primera opción, una piedra que cerrara la caverna. A medida que se evolucionó y las pertenencias personales aumentaron, la invención de nuevas cerraduras comenzó su auge llegando a la creación de las hoy conocidas cerraduras electrónicas inteligentes. La idea principal de poseer una cerradura inteligente es no depender de la utilización de objetos obsoletos como son las llaves. Gracias a las cerraduras inteligentes podemos abrir la puerta con nuestro teléfono móvil, con un mando a distancia o incluso más sencillo, con tu huella dactilar o un código numérico.

En la actual pandemia en la que vivimos, el COVID-19, el uso de estas cerraduras implica mayor seguridad en cuanto a menor uso de dispositivos, que se pueden infectar por tocar manillas que otras personas han tocado también, como es en el caso de los portales. Gracias a las cerraduras que emplean tecnología inalámbrica se puede disminuir el riesgo de contagio.

La cerrajería no brilla en España por su modernidad, la gran mayoría están obsoletas y son vulnerables a las nuevas técnicas de forzamiento, como el impresioning [1] o el bumping [2]. El impresioning es uno de los métodos que utilizan los ladrones para poder acceder a un local, que básicamente consiste en realizar una copia no autorizada de la llave sin que la víctima llegue a advertirlo. El bumping es un método de robo que persigue la apertura de una puerta sin la llave y sin forzar la cerradura. A pesar de que en España se están popularizando estas cerraduras inteligentes, hay otros países como Corea del Sur donde están presentes en prácticamente todos los hogares y empresas. Un hecho está claro y es que las cerraduras inteligentes son el futuro y las cerraduras tradicionales acabarán en desuso.

## 1.2 Objetivos

El objetivo de este trabajo es el estudio de la seguridad en las cerraduras inteligentes, mediante la captura de paquetes con la herramienta Wireshark [3] y un Sniffer Bluetooth [4], mientras se abre o bloquea la puerta donde se encuentre instalada. Posteriormente, con la información capturada, se ha intentado replicar la información de nuevo a la cerradura para comprobar si es posible su hackeo [5]. Durante el desarrollo del proyecto, se han estudiado dos cerraduras inteligentes con funcionamiento a través de Bluetooth y se ha comparado su sistema de seguridad. Finalmente se incluye un estudio de los resultados obtenidos y se ha probado si poseer una cerradura inteligente en nuestros hogares y/o empresas es más seguro que tener una cerradura tradicional.

## 1.3 Estructura de la memoria

La presente memoria se divide en 9 capítulos (ver figura 1) donde se expone la investigación realizada acerca del funcionamiento y seguridad de las cerraduras inteligentes y el trabajo realizado para llegar a una conclusión en cuanto a su nivel de fiabilidad.

El primer capítulo hace referencia a la introducción del proyecto, marcando los objetivos y la motivación, así como el punto actual donde se explica cómo se estructura la memoria.

El segundo capítulo trata acerca de los antecedentes y estado actual de los distintos tipos de cerraduras inteligentes disponibles en el mercado.

El tercer capítulo nos introduce el problema a tratar en el proyecto.

El cuarto capítulo describe las tecnologías y herramientas empleadas para la investigación.

El quinto y sexto capítulos hablan de cada cerradura a analizar. Los temas tratados son una definición de cada cerradura y su funcionamiento, así como la implementación realizada para su hackeo.

El séptimo capítulo trata una comparación entre ambas cerraduras, concretamente las diferencias y/o similitudes en sus modelos de seguridad.

El octavo y noveno capítulos presentan las conclusiones acerca de los resultados obtenidos en la investigación y se proponen líneas futuras de mejoras en el proceso de descifrado de la clave.

Por último, el décimo capítulo establece un presupuesto basado en las tecnologías y herramientas necesarias para la investigación, además del tiempo empleado.

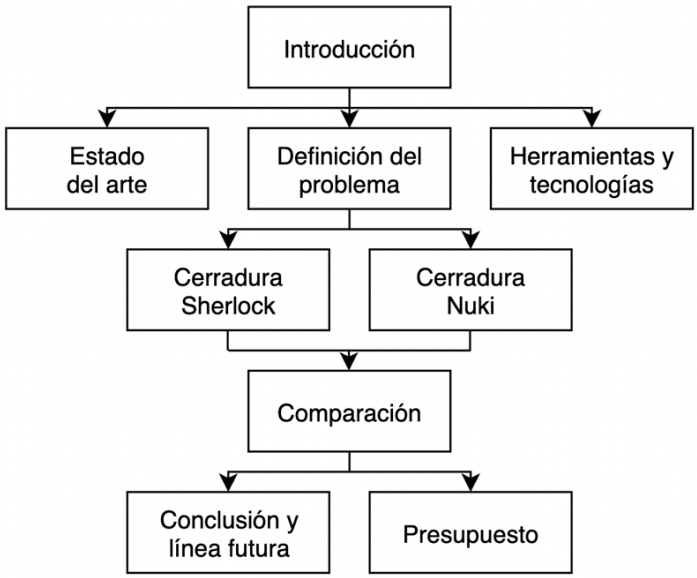


*Figura 1. Estructura de la memoria*

# 2. Estado del arte

Actualmente existen en el mercado una gran variedad de cerraduras inteligentes, entre las cuales se puede elegir según las preferencias. En un mundo en el que cada vez hay más robos, la población está optando por instalar en sus hogares y empresas este tipo de cerraduras. La seguridad depende del sistema de cierre instalado, pero por lo general, este tipo de cerraduras son más seguras que las tradicionales ya que podemos controlar quién accede a estas. Además, tienen la ventaja de que no hay que cambiar la llave si se pierde, pues en su lugar, simplemente debemos cambiar el código si se sospecha que alguien sabe la clave. Este tipo de cerradura aporta mucha comodidad y seguridad, además de que son dispositivos con un funcionamiento sencillo.

En las siguientes secciones se comentan las cerraduras inteligentes más comunes en el mercado.

## 2.1. Cerraduras de teclado digital

Las **cerraduras de teclado digital** [6] sobresalen por su popularidad en el mercado debido a su relación calidad-precio. Su funcionamiento consiste en la inserción de códigos numéricos o alfanuméricos establecidos por el usuario.

Uno de sus principales beneficios es la posibilidad de restablecer la contraseña cuando sea necesario, evitando así el remplazo de toda la instalación en la cerradura tradicional. Además, en cuanto a seguridad, es más difícil obtener el código establecido por el usuario en comparación con técnicas de robo como el impresioning de una llave.

Otros beneficios adicionales en este tipo de cerradura es la posibilidad de restablecer la clave existente, lo que evitaría el gasto innecesario de cambios de cerradura y llave. Además, muchos modelos permiten programar un horario específico para el desbloqueo y bloqueo de usuarios externos.

## 2.2. Cerraduras electrónicas con mando

Las **cerraduras electrónicas con mando** [7] son consideradas la mejores del mercado, gozando de gran aceptación en Europa. Son cómodas, económicas y dan la posibilidad de abrir y cerrar puertas a distancia sin necesidad de permanecer junto a la puerta o manejar gran cantidad de llaves que pueden acabar extraviadas. Proporcionan gran seguridad ya que no pueden ser copiadas (impresioning) y su mecanismo de apertura/cierre impide que sean forzadas (bumping). Además, estas cerraduras aportan un plus de seguridad gracias a aplicaciones que notifican al usuario en tiempo real la apertura de la puerta.

## 2.3. Cerraduras invisibles, Bluetooth o Wifi

Las **cerraduras invisibles** [8] funcionan con tecnología inalámbrica, como el Bluetooth o las ondas Wifi, ejecutadas a través de una Tablet o teléfono móvil. El bloqueo y desbloqueo se realiza a través de una aplicación que dispone de reconocimiento de voz, teclado alfanumérico o lector de huella dactilar que permiten identificar al usuario.

Estas cerraduras son difíciles de forzar con técnicas como bumping. Incluso aunque se produzca el robo del dispositivo móvil, se requiere un identificador para su apertura. La mayoría de estas cerraduras incorporan sistemas de cifrado en sus apps, protegiendo la privacidad de los datos de los usuarios y, además, se pueden renovar sus claves en cualquier momento.

En este proyecto nos centramos en el funcionamiento de este tipo de cerradura y su modelo de seguridad, analizando y comparando dos marcas en profundidad.

## 2.4. Cerraduras electrónicas de huella dactilar

Las **cerraduras de huella dactilar** [9] son las más vulnerables del mercado debido a la falsificación de huellas dactilares. Sin embargo, los fabricantes y proveedores ofrecen otros agregados para aumentar la seguridad, como la combinación de la huella con una contraseña o PIN. No obstante, estas cerraduras ganan en diseño, siendo capaces de resistir a golpes y, además aportando más comodidad y velocidad que una cerradura tradicional.

# 3. Introducción al problema

## 3.1. Definición del problema

El problema al que nos enfrentamos es que, a pesar de que la mayoría de las cerraduras invisibles o Bluetooth incorporan sistemas de cifrado en sus apps, es posible que, si no se adaptan las medidas de seguridad necesarias por parte del fabricante, se puedan descifrar estas claves y de esta forma que la seguridad del hogar o la empresa sea vulnerable.

## 3.2. Conceptualización

Debido a que no existe ningún producto 100% seguro ni infranqueable, las cerraduras inteligentes no son una excepción. A pesar de que las cerraduras electrónicas no se pueden forzar con técnicas como el bumping, vivimos en una era en la que el hackeo está en auge, lo que pone en peligro este tipo de cerraduras.

Por tanto, en este proyecto se ha estudiado un método a través del cual se podría intentar acceder a la clave de la cerradura para comprobar si es posible romper su cifrado y, por consiguiente, desbloquear la puerta.

# 4. Tecnologías y herramientas usadas

## 4.1. Cerradura Sherlock S2

La **cerradura Sherlock S2** [10] (ver figura 2) de Xiaomi es de las más vendidas y con mejor valoración del mercado, y unas de las cerraduras más sencillas de instalar. Esta es la principal cerradura analizada en este proyecto. Veremos una descripción más detallada de su funcionamiento más adelante.


*Figura 2. Cerradura Sherlock S2*

## 4.2. Cerradura Nuki

La **cerradura Nuki Smart Lock** [11] (ver figura 3) ha ido ganando bastante popularidad en los últimos años. Nuki sobresale por su seguridad y su sencilla instalación. Esta es la segunda cerradura analizada en este proyecto, con el fin de poder hacer una comparación entre varias cerraduras inteligentes.


*Figura 3. Cerradura Nuki*

## 4.3. Wireshark

**Wireshark** es el analizador de paquetes más conocido y utilizado en todo el mundo. Gracias a este programa, se puede capturar y analizar en detalle todo el tráfico de red que entra y sale de nuestro PC. Este programa gratuito permite realizar una inspección profunda de cientos de protocolos, ya que soporta protocolos de capa física, de enlace, protocolos de red, capa de transporte y también capa de aplicación.

Esta herramienta nos permite realizar una captura en tiempo real del tráfico en la red y, una vez capturados todos los paquetes, efectuar un análisis en detalle. Wireshark es el programa que se ha empleado en este proyecto para analizar los paquetes enviados entre el dispositivo móvil y ambas cerraduras.

## 4.4. Adafruit bluefruit LE Sniffer

**Adafruit bluefruit LE Sniffer** [12] (ver figura 4) está programado con una imagen de firmware que lo convierte en un sniffer de Bluetooth Low Energy (BLE) [13] fácil de usar. Puede capturar los intercambios de datos entre dos dispositivos BLE, introduciendo los datos en Wireshark donde se puede visualizar la información a nivel de paquete, con descriptores útiles para una lectura más cómoda y sencilla.

Este sniffer Bluetooth es el empleado para capturar los paquetes enviados entre ambos dispositivos.

*Figura 4. Adafruit bluefruit LE Sniffer*

## 4.5. Antena Bluetooth CBT40NANO

El **Nanoadaptador Bluetooth CBT40NANO** [14] (ver figura 5) se emplea para crear una conexión inalámbrica con otros dispositivos Bluetooth. En este proyecto se emplea para crear una conexión a través de una máquina virtual, con el sistema operativo Linux, con la cerradura. De este modo, se puede replicar el tráfico necesario para el desbloqueo de la cerradura.

*Figura 5. Antena Bluetooth CBT40NANO*

## 4.6. Gatttool

**Gatttool** [15] es una herramienta que permite obtener información o manipular atributos de un dispositivo BLE.

```
$gatttool
```

En este proyecto se ha implementado la escritura de claves en las cerraduras gracias a esta herramienta.

## 4.7. Otros

### 4.7.1. nRF Sniffer for Bluetooth LE

**nRF Sniffer for Bluetooth LE** [16] es una herramienta útil para depurar y aprender sobre aplicaciones de Bluetooth Low Energy. Permite visualizar casi en tiempo real los

dispositivos Bluetooth LE cercanos disponibles. Gracias a esta herramienta y con el sniffer conectado, podemos capturar el tráfico en Wireshark enviado desde la cerradura.

### 4.7.2. Hcitool

hcitool [17] es una herramienta que nos permite configurar las conexiones Bluetooth y enviar algunos comandos interesantes a dispositivos Bluetooth.

```
$hcitool
```

En este proyecto, se emplea esta herramienta para poder escanear los dispositivos Bluetooth LE que detecta nuestra máquina virtual.

### 4.7.3. Sniffer Bluetooth CC2540

El **sniffer Bluetooth CC2540** [18] (ver figura 6) permite el rastreo de paquetes BLE. Este sniffer ha sido la primera opción de captura de paquetes para este proyecto. Sin embargo, esta versión tiene una interfaz de interpretación de paquetes ambigua y no se ha podido interpretar los resultados adecuadamente. Además, no se ha reconocido ningún registro de escritura de clave, por tanto, el uso de este sniffer para el desarrollo del proyecto se ha descartado.

*Figura 6. Sniffer Bluetooth CC2540*

# 5. Cerradura Sherlock S2

## 5.1. Definición

La **cerradura Sherlock S2** es una de las cerraduras inteligentes más populares y sencillas del mercado y, es la primera cerradura que se ha estudiado en este proyecto. Primero veremos unos conceptos técnicos sobre ella y su funcionamiento, para posteriormente comentar cómo hemos procedido al estudio de su seguridad.

Sherlock es una cerradura motorizada, es decir, hay un motor que hace girar la llave de manera automática. Su instalación es muy sencilla. Se adapta al bombín que se tenga en la puerta y una de las llaves de las que se disponga para abrir la puerta quedará introducida, mientras se tenga la cerradura instalada, para su correcto funcionamiento. No es necesario desmontar el bloqueo original debido a que se coloca pegada directamente por encima de la que se disponga actualmente y queda adherida a la puerta por un adhesivo 3M muy potente.

Por otro lado, la cerradura Sherlock dispone de múltiples formas de desbloqueo. Mediante la llave original, ***SmartKey*** [19] (un mando que se configura desde la app móvil para accionar la cerradura), desbloqueo por huella digital (deslizando el dedo por un lateral de la cerradura) y, por último, mediante la **aplicación móvil Sherlock** [20]. Este último es el método que se ha empleado para analizar el tráfico en este proyecto.

## 5.2. Funcionamiento

A continuación, se explica el funcionamiento de apertura y bloqueo de la cerradura inteligente mediante el uso de la aplicación móvil. Esta aplicación es muy sencilla e intuitiva, además de que proporciona varios servicios para mejorar la comodidad del propietario.

Permite configurar claves virtuales con diferentes permisos y distribuirlos de forma remota a miembros de la familia, inquilinos, o personal de limpieza. Se puede controlar su tiempo de empleo y eliminar sus derechos de uso. Además, se puede configurar la aplicación para que envíe un mensaje cuando se desbloquee la puerta por parte de otro usuario, llevando así un historial del estado de la cerradura.

El proceso de bloqueo y desbloqueo de la cerradura es muy simple. Debemos ingresar a nuestra app con el usuario que nos hemos registrado anteriormente con nuestro número de teléfono y nos llevará al menú principal de la aplicación, dónde si ya tenemos asociada nuestra cerradura, aparecerá con las opciones para desbloquear, deslizando el dedo hacia la derecha, o bloquear, deslizando el dedo hacia la izquierda. Además, esta aplicación tiene la ventaja de que permite tener varias cerraduras a un mismo usuario y administrarlas según dónde se encuentre.

Y, así de sencillo podemos manipular la apertura y cierre de nuestra cerradura.

## 5.3. Ejemplo ilustrativo

En la figura 7 podemos apreciar como funciona la aplicación móvil para el bloqueo y desbloqueo de la puerta.


*Figura 7. Ejemplo ilustrativo cerradura Sherlock*

## 5.4. Implementación

Una vez explicado el procedimiento de bloqueo y desbloqueo de la cerradura y sus funcionalidades, pasamos a investigar su seguridad. A pesar de que los fabricantes aseguren que un producto es fiable, no implica que no haya algún método para realizar un ciberataque [21].

A continuación, se estudia cómo funciona el envío de información entre la aplicación y la cerradura, siendo el objetivo de este proceso capturar el tráfico cuando la cerradura se conecte con el móvil y le envíe la clave para desbloquear la puerta, para posteriormente intentar replicar ese tráfico.

En primer lugar, debemos tener a nuestra disposición la primera herramienta para realizar la conexión entre nuestro ordenador, la aplicación y la cerradura. En este proyecto se emplea el sniffer **Adafruit bluefruit LE**, el cual permite capturar y analizar los paquetes en tránsito entre los dispositivos.

Para poder analizar el tráfico capturado en la aplicación Wireshark, previamente necesitamos vincular la información recibida por el sniffer. Para ello utilizamos el **programa nRF Sniffer for Bluetooth LE**. Esta herramienta permite ver en tiempo real todos los dispositivos que esta capturando el sniffer para posteriormente filtrar ese contenido en Wireshark y ver la información detalladamente.

Como se puede observar en la figura 8, gracias a esta herramienta se ven todos los dispositivos Bluetooth cercanos disponibles con sus respectivas direcciones MAC [22]. Además, presenta una guía de todos los comandos útiles que podemos usar con esta herramienta.

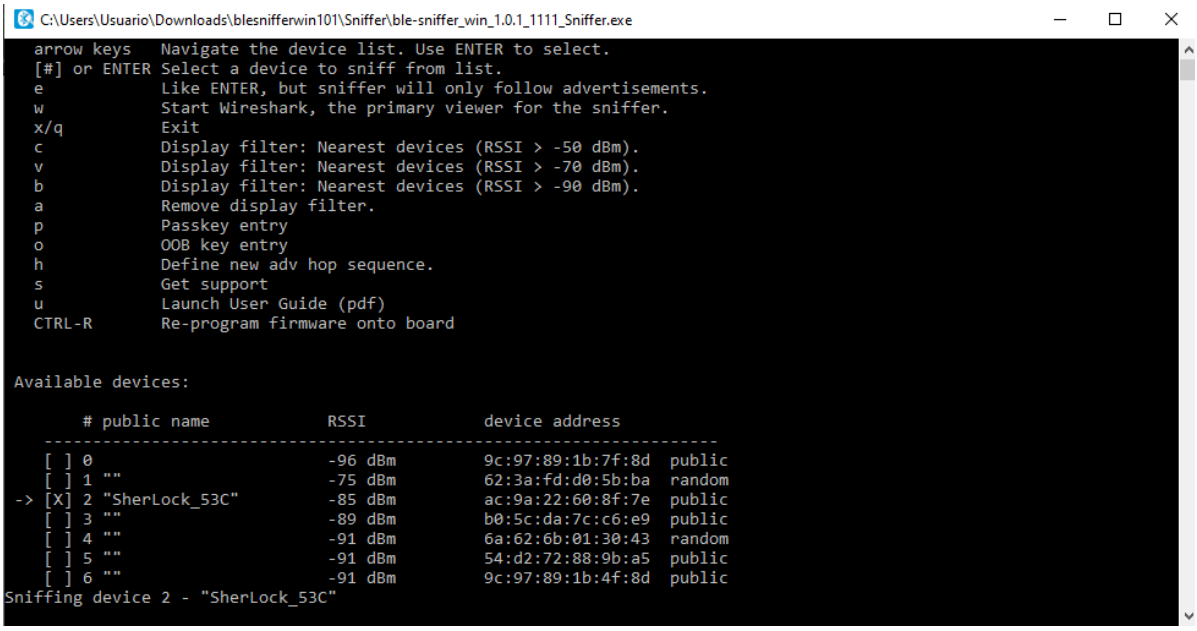


*Figura 8. nRF Sniffer for Bluetooth LE*

En la figura 8 podemos ver que el programa detecta la cerradura Sherlock. Una vez localizado el dispositivo, el siguiente paso es analizar su tráfico en **Wireshark**. Para ello, seleccionamos la cerradura y presionamos la tecla 'w'. De este modo, nos redireccionará directamente a la herramienta Wireshark filtrando únicamente el tráfico de la cerradura seleccionada.

Otro método, para capturar el tráfico entre ambos dispositivos, implementado en principio para el desarrollo del proyecto es a través de la función **HCI snoop log** [23]. Este es un archivo de registro que contiene todas las transmisiones Bluetooth que se han realizado desde un teléfono.

Para poder usar esta funcionalidad se debe activar el modo desarrollador en el dispositivo móvil y, una vez activado:

- Activar el registro de Bluetooth HCI, para habilitar los registros (ver figura 9).
- Y, la depuración por USB, para posteriormente poder extraer los registros a través de USB y verlos en un ordenador.

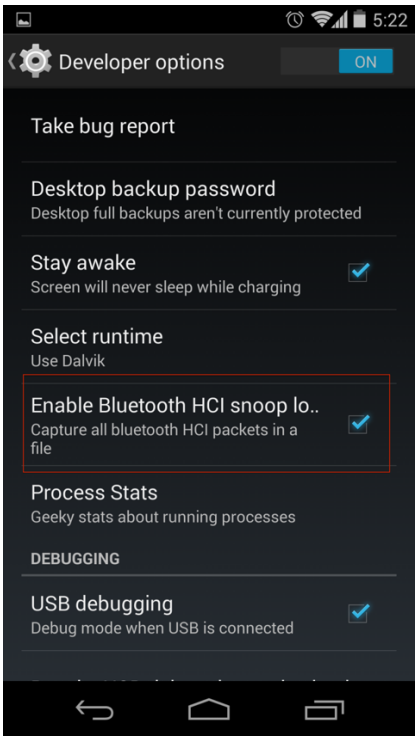


*Figura 9. HCI snoop log*

A continuación, se activa y desactiva Bluetooth para habilitar la recogida de datos. Una vez activado Bluetooth, se puede desbloquear la cerradura para capturar el tráfico.
Para poder analizar los datos recogidos en un ordenador, se pasa el registro a través de una herramienta de línea de comandos **adb** (Android Debug Bridge) [24], que permite la

comunicación con un dispositivo y, finalmente, se genera un archivo .log que se puede analizar en Wireshark.

Este método fue descartado debido a que el uso de un sniffer Bluetooth agiliza el proceso de recogida de datos.

Una vez en Wireshark, ya podemos comenzar el análisis. Para filtrar el tráfico de una manera más efectiva, se emplea el filtro 'btatt' [25]. Este filtro muestra todos los protocolos relacionados con tráfico Bluetooth y, por ello podemos obtener solamente los paquetes que se envían entre la cerradura y la aplicación.

Una vez introducido el filtro, pasamos a capturar el tráfico bloqueando o desbloqueando la cerradura. De esa forma, comenzará a llegar la información al programa, la cual posteriormente utilizaremos para replicar el tráfico y comprobar si es posible su hackeo.

A continuación, se proporciona una breve explicación de los detalles de la lista de paquetes capturados en el proceso.

En la figura 10 podemos apreciar la comunicación entre el Master (La cerradura Sherlock) y el Esclavo (La aplicación móvil), es decir, el recurso que esté enviando o recibiendo la información y el destino de esta.

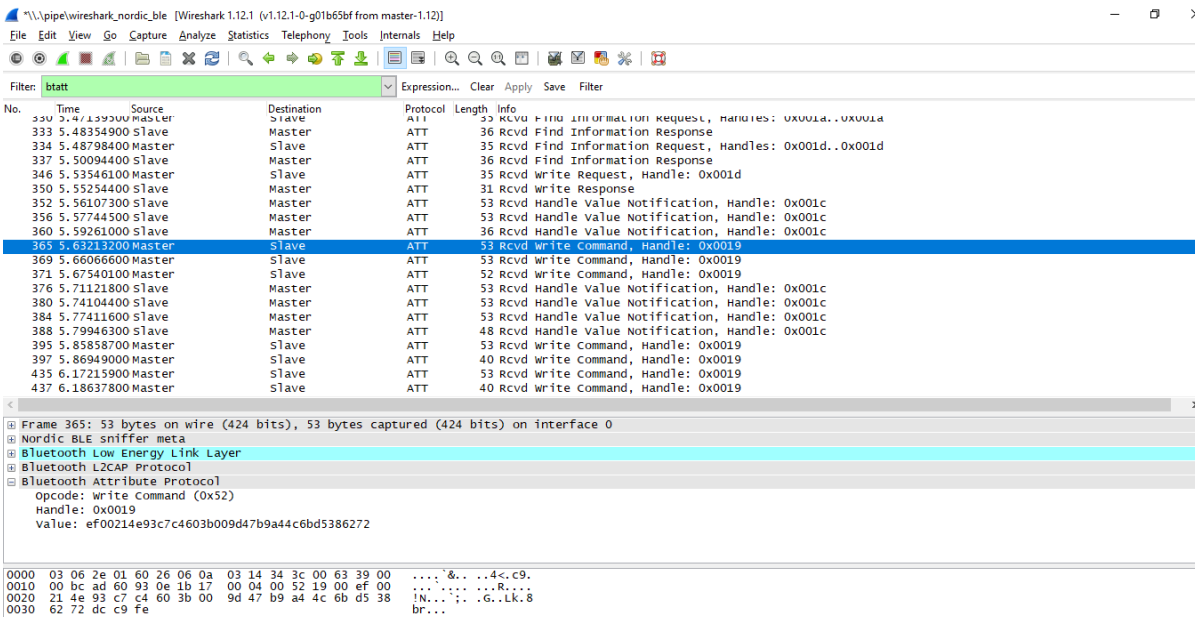


*Figura 10. Tráfico en Wireshark de Sherlock*

El protocolo empleado para la conexión es **ATT** (Atribute Protocol) [26], un protocolo basado en atributos perteneciente a los protocolos de BLE, con arquitectura cliente-servidor [27], que permite el intercambio de información. Este protocolo define cómo se representan los datos y los métodos mediante los cuales esos datos se pueden leer o escribir. En este caso, actúa como un servidor, reteniendo los datos hasta que el teléfono los solicita. Estos datos se almacenan en el servidor BLE como atributos.

La última columna nos notifica la información que se está adquiriendo en cada punto de la conexión. El punto que nos interesa para nuestra investigación es cuando se envía la clave de Maestro a Esclavo:

*Rvcd write command, Handle: 0x0019*

Se trata de un paquete que está haciendo una petición de escritura con un *Handle* 0x0019. Los **Handles** [28] son los componentes que procesan cada uno de los paquetes que pertenecen a las capturas. El *Handle* extrae del paquete la información necesaria, como en este caso el valor que se envía.

Podemos observar que se envían tres peticiones de escritura de claves de la cerradura al móvil. Posteriormente, la aplicación móvil responde a la cerradura enviando una serie de notificaciones informando que se ha recibido el valor. Por último, Sherlock vuelve a enviar cuatro peticiones de escritura de claves al dispositivo. Esto implica que para el desbloqueo de la cerradura se necesita introducir siete claves en total.

El siguiente paso es mirar los valores que se escriben en cada paquete de escritura. Esta información la podemos ver al seleccionar el paquete que deseamos analizar y nos aparecerán una serie de características de dicho paquete. Para ver el valor, nos interesa la información que trae el protocolo ATT.

El protocolo ATT nos aporta los tres puntos más importantes para resolver el problema de nuestro proyecto:

- **Opcode** (Código de operación) [29]. En este caso se trata de una operación de escritura '*Write Command'*

- **Handle** (Puntero). Indica el atributo al que está apuntando la escritura.
- **Value** (Valor). Nos informa del valor de la clave que se está escribiendo.

Cuando obtenemos todas las claves que se envían, podemos pasar a replicar los paquetes. Para ello, necesitamos un sistema operativo Linux [30] o una máquina virtual [31] que lo contenga. En nuestro caso, optamos por la última opción. Debido a ello, se necesita un **adaptador Bluetooth** ya que la máquina virtual no posee conexión Bluetooth.

En primer lugar, comprobamos que se está recibiendo señal de la cerradura. Para ello, empleamos la herramienta **hcitool** para escanear los dispositivos Bluetooth cercanos. Ejecutando el siguiente comando (ver figura 11) podemos ver los dispositivos BLE disponibles con su respectiva dirección MAC y, comprobamos que tenemos conexión con nuestra cerradura mediante:

*$hcitool lescan*

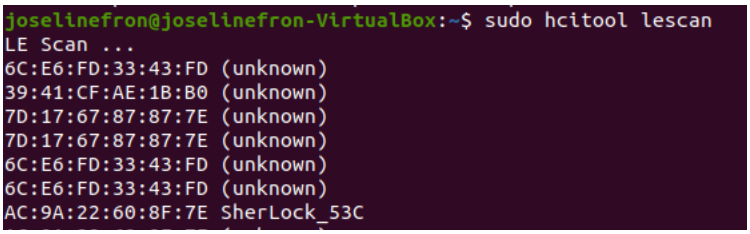


*Figura 11. hcitool*

El siguiente paso es el empleo del comando **hciconfig** (ver figura 12), el cual se utiliza para configurar dispositivos Bluetooth. hciX es el nombre de un dispositivo Bluetooth instalado en el sistema. En nuestro caso, el que tenemos instalado es hci0. Para poder trabajar con los dispositivos Bluetooth necesitamos inicializarlo.

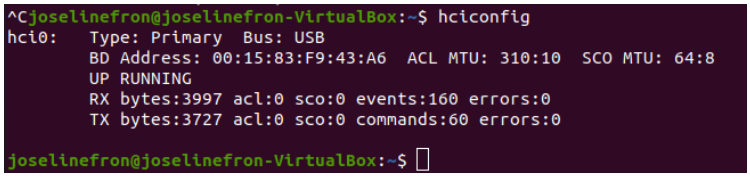


*Figura 12. hciconfig*

*$hciconfig hci0 down*

*$hciconfig hci0 up*

Con los comandos anteriores cerramos el dispositivo HCI en el caso de que estuviera iniciado por un proceso anterior sin terminar y lo volvemos a abrir e iniciar.

La última herramienta que se utiliza y la más importante para nuestra investigación es **Gatttool**. Esta herramienta nos permite conectarnos a dispositivos BLE con la dirección MAC del dispositivo y manipular sus atributos con una serie de comandos disponibles de la herramienta. De tal forma, se podrá replicar los paquetes que hemos capturado previamente.

En el caso de que no se conozca la dirección MAC de la cerradura a analizar, hay dos opciones para su búsqueda. Por un lado, podemos obtener esta información desde la captura de paquetes en Wireshark, la cual muestra las direcciones de los dos dispositivos que se están comunicando. Por otro lado, gracias a la herramienta hcitool, mencionada anteriormente, podemos ver fácilmente los dispositivos BLE que se encuentran y su dirección MAC asociada.

La herramienta Gatttool dispone de varios comandos interesantes para manipular los dispositivos Bluetooth o simplemente para adquirir información relevante de estos. A continuación (ver figura 13) se listan los argumentos que mayor ayuda aportan a nuestro proyecto:

- **-i.** Especifica el nombre del dispositivo Bluetooth instalado en el sistema.
- **-b.** Indica la dirección MAC.
- **--characteristics.** Nos muestra todos los handles asociados y sus propiedades.

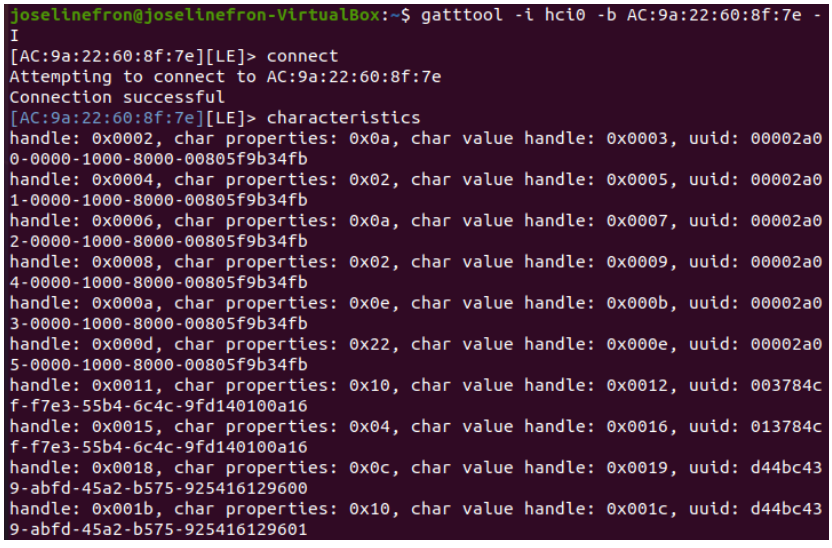


*Figura 13. Gatttool characteristics*

- **--char-read.** Con este comando (ver figura 14) podemos leer las características del dispositivo conectado. Por ejemplo, leer el valor / descriptor de un handle:

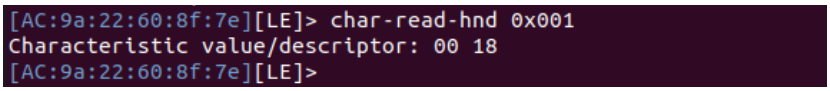


*Figura 14. Argumento --char-read-hnd*

- **--char-write-req.** Este comando se emplea para hacer una petición de escritura en el dispositivo, el cuál se empleará más adelante.
- **-a.** Lee o escribe las características del handle que se especifique.
- **-n.** Contiene el valor que se quiere enviar en la petición de escritura.

Una vez claros los comandos necesarios para poder hacer la réplica de paquetes, nos conectamos a la cerradura y enviamos las claves obtenidas.

En un primer momento, para podernos conectar al dispositivo, se introduce cada clave individualmente de la forma mostrada en la figura 15.

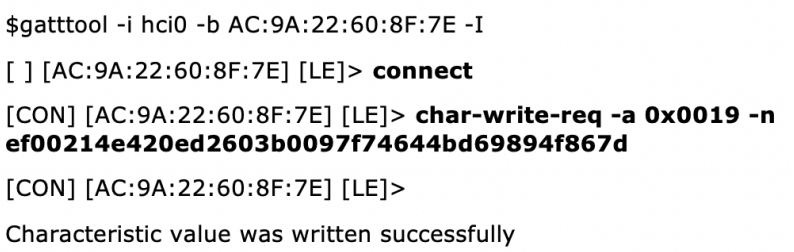


*Figura 15. Conexión con herramienta Gatttool*

Esto llegó a no ser factible debido a que la conexión con la cerradura se perdía a los pocos segundos de inicializarse, y ya que se tenían que introducir 7 claves, resultó ser inviable establecer la conexión por cada clave que se tenía que introducir. Por tanto, se implementó un sencillo **Script de bash** [32] (ver figura 16) que incluye todos los comandos necesarios para la conexión y la escritura, facilitando y agilizando el proceso del envío de paquetes. De este modo, se ejecutan juntos todos los comandos explicados anteriormente (ver figura 17), ahorrando así bastante tiempo a la hora de realizar el hackeo de la cerradura.

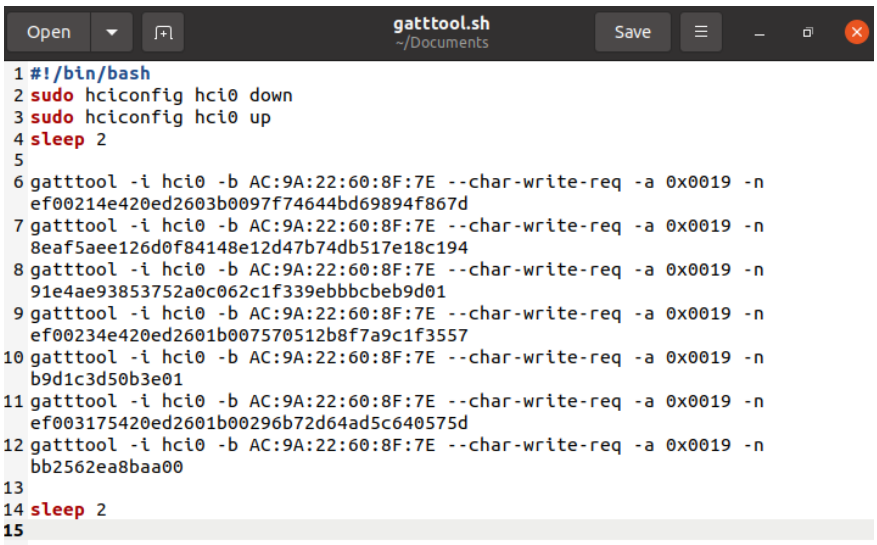


*Figura 16. Script Bash*

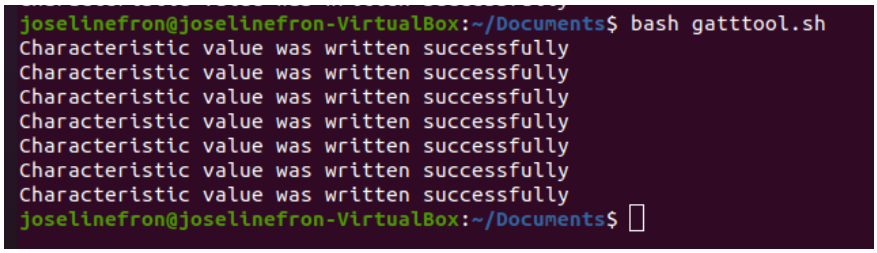


*Figura 17. Ejecución de Script Bash*

Y, finalmente, se desbloquea la cerradura replicando los paquetes. Es un proceso bastante sencillo y que nos plantea dudar acerca de la seguridad de esta marca de cerradura inteligente.

Sin embargo, a pesar de que es sencillo y rápido su hackeo, Sherlock dispone de alguna medida de seguridad, como por ejemplo el cambio de las claves cuando han pasado varios minutos desde que se ha abierto la puerta. No obstante, sigue existiendo un amplio margen de tiempo para realizar la réplica de paquetes. Además, en el futuro se podría implementar un programa u optimizar el script realizado para que la recogida de datos sea más efectiva y rápida, logrando así desbloquear la cerradura en cuestión de segundos.

# 6. Cerradura Nuki

## 6.1. Definición

La **cerradura Nuki** es la primera cerradura inteligente en Europa que abre las puertas con la ayuda de un Smartphone. Además, es la primera cerradura más flexible, es decir, se puede instalar en casi todas las cerraduras europeas existentes. Esta es la segunda cerradura que se ha estudiado en este proyecto. A continuación, veremos unos conceptos técnicos sobre ella y su funcionamiento, para posteriormente proceder a el análisis de su seguridad.

Nuki abre la puerta de manera automática cuando llegas a casa mediante Bluetooth y, además, vuelve a bloquearla cuando te vas. Por ello, Nuki es bastante famosa en el mercado europeo, ya que aporta una gran comodidad al usuario y sencillez.

La instalación es muy simple y rápida. La ventaja es que no se necesita retirar el bombín de la puerta, ya que se debe dejar la llave puesta en la cerradura y colocar Nuki sobre ella. Para ello, Nuki ofrece dos piezas metálicas, que dependiendo del tipo de cerradura que dispongas en tu hogar, se ajustan a la puerta. Posteriormente se encaja la carcasa de la cerradura y, por último, configuramos la app de Nuki [33] en nuestro dispositivo móvil para enlazar la cerradura.

Nuki es compatible con otros métodos de apertura, además del Smartphone, que se pueden comprar aparte. La cerradura dispone de un mando a distancia, un teclado numérico y también se podría utilizar la llave si la puerta tiene un cilindro de doble embrague.

Es especialmente destacable que la cerradura Nuki funciona con un nivel de cifrado de seguridad máxima, ya que utiliza **AES** [34] con claves de 256 bits. AES es lo que se conoce como un cifrado simétrico por bloques, lo que significa que cifra y descifra los datos en bloques de 128 bits cada uno. Para ello, utiliza una clave criptográfica específica, que es efectivamente un conjunto de protocolos para manipular información. Esta clave puede ser de 128, 192 o 256 bits de tamaño.

AES-256, la versión de clave de 256 bits de AES, es el estándar de cifrado utilizado por LE VPN. Es la forma más avanzada del cifrado y consiste en 14 rondas de sustitución, transposición y mezcla para un nivel de seguridad excepcionalmente alto. Su tamaño de clave

mayor hace que sea esencialmente irrompible, lo que significa que, incluso siendo hackeados, los datos serían imposibles de descifrar.

## 6.2. Funcionamiento

A continuación, se explica el funcionamiento de apertura y bloqueo de la cerradura inteligente mediante el uso de la aplicación móvil. La cerradura Nuki proporciona una gran comodidad a la hora de su uso ya que se puede abrir la puerta desde un teléfono móvil, smartwatch o Tablet. Además, se puede dar acceso temporal o permanente a otras personas, como familiares, amigos o servicios de limpieza para un horario determinado. Por otro lado, si se trata de una empresa o un alojamiento turístico, se puede proporcionar un código temporal a los usuarios para evitar la pérdida y copia de llaves.

El proceso de bloqueo y desbloqueo de la cerradura es muy sencillo y tiene varias opciones según las necesidades del inquilino. En primer lugar, debemos hacer una configuración de la cerradura en la app móvil Nuki. Es un proceso largo pero simple. Una vez asociada nuestra cerradura, tendremos las opciones de abrir la puerta o bloquearla. Además, gracias a su sistema de manos libres la puerta se abrirá cuando detecte el móvil, aportando gran comodidad al usuario cuando viene cargado o, simplemente, para mayor rapidez. Esta cerradura también permite tener varios usuarios registrados a la vez, enviándoles un código de invitación, el cual se podrá retirar en cuanto se desee.

Estas son las funcionalidades más básicas que ofrece Nuki dentro de su amplia gama de posibilidades.

## 6.3. Ejemplo ilustrativo

La figura 18 muestra como funciona la aplicación móvil para el bloqueo y desbloqueo de la puerta.


*Figura 18. Ejemplo ilustrativo cerradura Nuki*

## 6.4. Implementación

Una vez explicado el procedimiento de bloqueo y desbloqueo de la cerradura y sus funcionalidades, pasamos a investigar su seguridad. La cerradura Nuki sobresale en Europa por sus buenas críticas en cuanto a su seguridad, por tanto, se ha analizado si con el mismo método de réplica de paquetes realizado anteriormente con la cerradura Sherlock es también posible su hackeo.

En un primer momento se pensaba analizar solamente la cerradura Sherlock en este proyecto, pero debido a la facilidad para romper su cifrado, se decidió comparar con otra marca de cerradura inteligente para tener una referencia de cómo funciona la seguridad en varias cerraduras y sus diferencias. En el capítulo 7 se hará una comparación detallada entre ambas cerraduras y podremos analizar que medidas de seguridad implementa cada una.

Los pasos a seguir son prácticamente los mismos que los implementados con la cerradura Sherlock, por lo que no se explicará en profundidad cada paso implementado.

Con nuestro sniffer **Adafruit bluefruit LE** y su programa **nRF Sniffer for Bluetooth** para detectar los dispositivos BLE cercanos, nos conectamos a la cerradura Nuki para analizar posteriormente los paquetes enviados y recibidos en Wireshark.

Una vez iniciado Wireshark e introducido el filtro ‘btatt’ para adquirir solamente el tráfico Bluetooth, podemos desbloquear la cerradura y comprobar qué información nos está llegando y si será posible su hackeo.

En la figura 19 podemos apreciar la comunicación entre la cerradura Nuki y nuestro dispositivo móvil Samsung.

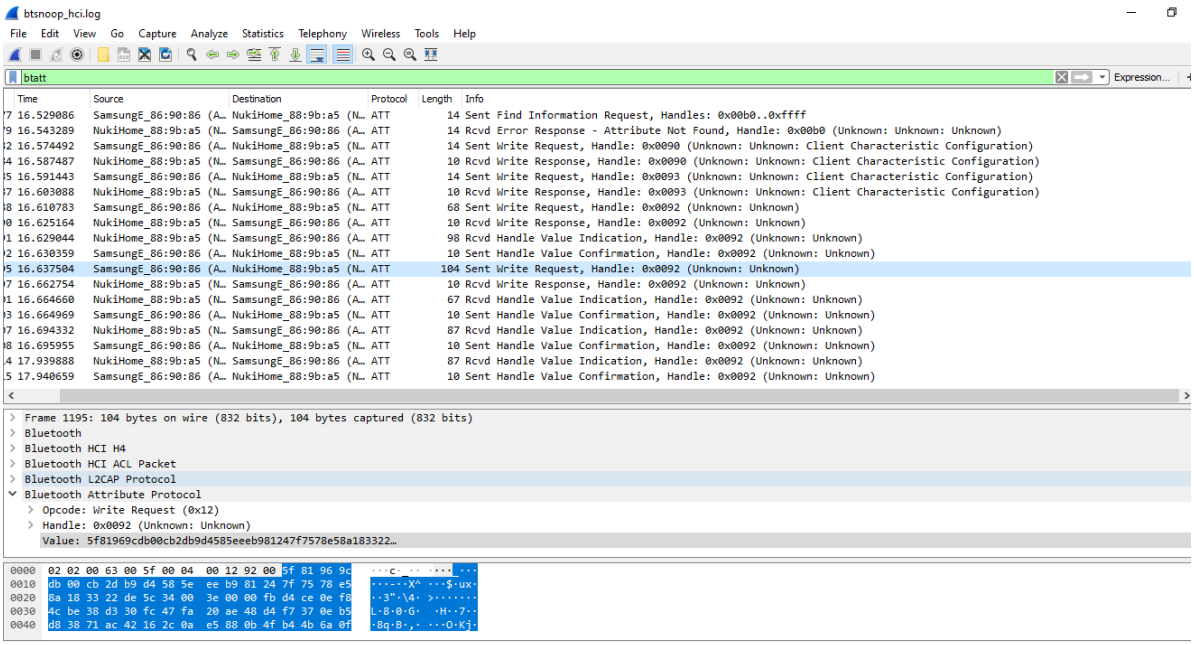


*Figura 19. Tráfico en Wireshark de Nuki*

El protocolo empleado para la conexión es igualmente ATT dónde se almacenan los atributos enviados, pero en la columna que indica la información de los paquetes, se puede observar ligeros cambios de formato que se comentarán más adelante.

En este caso, podemos ver que se realizan varias peticiones de escritura a la cerradura para el envío de las claves con el Handle 0x0092.

*Sent Write Request, Handle 0x0092*

Por tanto, debemos recoger todos los valores que se envían para posteriormente realizar su réplica. Para poder ver estos valores, nos interesa ver la información que trae el protocolo ATT. Una vez poseemos todas las claves que se envían, podemos pasar a replicar de nuevo el tráfico desde nuestra máquina virtual.

En primer lugar, comprobamos que estamos recibiendo conexión de la cerradura Nuki con la herramienta **hcitool** y, desde que obtengamos señal, podemos ejecutar nuestro Script de bash, anteriormente modificado con los valores encontrados en Wireshark.

Sin embargo, a pesar de que los valores se escriben correctamente en la cerradura, no se logra su desbloqueo. Esto es debido a que, al desbloquear la puerta, instantáneamente Nuki cambia de clave para la siguiente apertura, siendo inviable hackear la cerradura con este método, ya que las claves recogidas anteriormente quedarían automáticamente obsoletas.

A continuación, se va a explicar detalladamente como funciona el cifrado en la cerradura Nuki [35]. Esta cerradura emplea el principio de cifrado de extremo a extremo [36], es decir, aplica un cifrado a la clave de tal forma que solo el dispositivo receptor pueda descifrarlo.

Para establecer la comunicación entre la app de Nuki y el Smart Lock se utiliza una clave propia que solamente conocen ambos dispositivos. Como protección ante los atacantes, los datos se cifran antes de que el emisor los trasmita (la app Nuki). Esto se realiza mediante el proceso NaCl (Networking and Cryptography library) [37]. En este proceso se utilizan combinaciones de números y letras únicas y solo una vez. Estos datos se transfieren por Bluetooth y vuelven a descodificarse cuando los recibe el receptor (Nuki Smart Lock).

En la figura 20 se puede ver detalladamente como se realiza el desbloqueo de la cerradura Nuki:

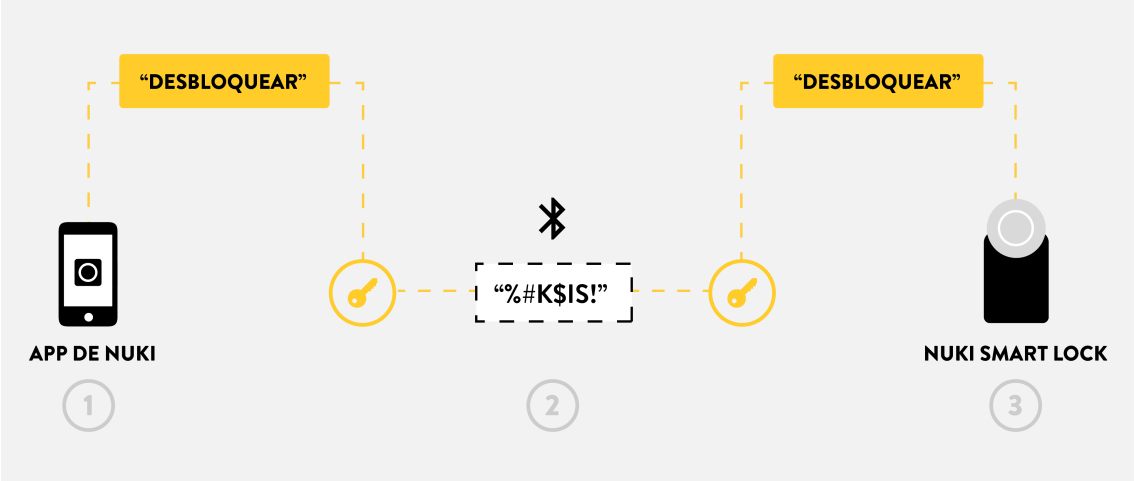


*Figura 20. Ejemplo desbloqueo Nuki[35]*

1. La app de Nuki envía la instrucción “desbloquear” y lo cifra de tal modo que solo la app y Nuki Smart Lock conozcan la clave.

2. La app de Nuki transfiere el mensaje codificado por Bluetooth a la cerradura.

3. Nuki Smart Lock conoce la clave, y por tanto puede descifrar el mensaje contenido y ejecutar la orden “desbloquear”.

4. En el proceso de desbloqueo, la app de Nuki recibe un número aleatorio. La instrucción “desbloquear” solo se podrá enviar a la cerradura cuando este contenga obligatoriamente el número aleatorio idéntico. Si posteriormente se envía otra instrucción de desbloqueo con el mismo número aleatorio a la cerradura de la puerta, Nuki Smart Lock rechaza la instrucción.

Este análisis nos demuestra que el nivel de seguridad de Nuki es elevado, tal y como comunican los fabricantes y que en general es una cerradura de la cual actualmente se puede fiar el mercado. No obstante, dado que el método de réplica de paquetes empleado en este proyecto es solo una de las opciones para realizar el hackeo, esta investigación no implica que no pueda existir otro procedimiento para desbloquear la cerradura y que esta cerradura acabe siendo vulnerable a ataques.

# 7. Cerradura Sherlock vs Cerradura Nuki

Una vez analizado el funcionamiento de ambas cerraduras y visto cómo se envían los paquetes entre ambos dispositivos, podemos hacer un análisis de las diferencias que se han encontrado durante el procedimiento de hackeo para ambas cerraduras. Ante todo, se ha podido comprobar que la cerradura Nuki tiene mayor seguridad que la cerradura Sherlock, pues durante la investigación se ha logrado desbloquear Sherlock, pero no Nuki. Además, existe más información en abierto sobre el cifrado usado en la cerradura Nuki que en el caso de la Sherlock, y de hecho se sabe que en la cerradura Nuki se usa AES con claves de 256 bits.

En conclusión, a continuación, se exponen una serie de puntos que muestran las principales diferencias entre ambas cerraduras y por qué una es más vulnerable que otra.

- **Formato de escritura de paquetes.** A pesar de que en ambas conexiones se realizan peticiones de escritura y se guardan las claves en el protocolo ATT, la petición no se envía con el mismo formato. En la cerradura Sherlock se emplea "Rvcd write command" que significa que ha recibido el comando de escritura con el valor de la clave y en la cerradura Nuki se utiliza "Sent Write Request" que implica que se ha enviado la escritura solicitada con dicho valor. Además, en el primer caso, es la cerradura quien envía el valor y en el segundo caso es la aplicación móvil quién realiza el envío. Con esta información se puede suponer que se logra desbloquear la cerradura Sherlock porque estamos atacando a la cerradura, sin embargo, no logramos hackear la cerradura Nuki porque atacamos al dispositivo móvil, el cuál no estaría presente en el momento del ciberataque.

- **Tiempo de cambio de clave.** Como se comentaba anteriormente, Sherlock mantiene la misma clave durante unos minutos desde que se desbloquea la puerta, permitiendo así, atacar sin problemas su seguridad. Sin embargo, Nuki controla el tiempo de forma mucho más segura. Esta cerradura cambia de clave al instante que se desbloquea la puerta. De esta forma, no da margen de tiempo para el robo. Este es el punto más importante y fuerte de Nuki en cuanto a su seguridad y el que la hace destacar notablemente sobre Sherlock.

Estas son las principales diferencias encontradas en este proyecto entre ambas cerraduras inteligentes en cuanto al funcionamiento de su seguridad.

# 8. Conclusiones y líneas futuras

Este proyecto ha consistido en la investigación de la seguridad en las cerraduras inteligentes, las cuales se están popularizando en todo el mundo. Actualmente, es muy común ver hogares y empresas que emplean este tipo de tecnologías. Dado su gran auge en el mercado, se ha llevado a cabo una investigación de cómo de seguras son estas cerraduras y si verdaderamente vale la pena cambiar la cerradura tradicional por este nuevo tipo de tecnología.

Se ha investigado detalladamente cómo es el proceso de apertura de la puerta y qué información se envía a través de los dispositivos implicados. Además, se ha probado la réplica de paquetes obtenidos con la intención de desbloquear la cerradura desde nuestro ordenador.

A lo largo de la investigación se ha logrado verificar que no todas las cerraduras inteligentes tienen el nivel de seguridad que indican los fabricantes a los compradores. A través de un método bastante simple se ha hackeado la cerradura Sherlock S2 y, además, el atacante puede conseguir las herramientas necesarias para el hackeo fácilmente. Quizá esa sea la razón por la que Xiaomi ha sacado otras cerraduras más seguras. Por otro lado, se ha comprobado que otras cerraduras incluyen un nivel de seguridad más elevado, como es el caso de Nuki, la cual no ha sido posible realizar su hackeo. Sin embargo, se podrían encontrar nuevos métodos para realizar el ataque y es posible que se pueda llegar a romper la seguridad de la cerradura Nuki.

El proyecto actual es bastante flexible y se podría expandir mucho más su investigación en un futuro. 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. Por otro lado, en este proyecto 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.

Considerando el avance de la tecnología y la competencia del mercado, los fabricantes reforzarán la seguridad de sus cerraduras inteligentes en los próximos lanzamientos. Aun así, hay una gran variedad de marcas en el mercado que pueden ser analizadas para comprobar su vulnerabilidad y decantar a la población por la opción más segura para su hogar. El mundo de las cerraduras inteligentes sólo acaba de empezar.

# 9. Summary and conclusions

This project has involved research into the security of smart locks, which are becoming popular around the world. Nowadays, it is very common to see homes and businesses using this type of technology. Due to their huge boom in the market, research has been carried out into how secure these locks are and whether it is really worth exchanging the traditional lock for this new type of technology.

Detailed research has been carried out into how the door opening process works and what information is sent through the devices involved. Besides, the replication of packets obtained with the intention of unlocking the lock from our computer has been tested.

In the course of the study, it has been verified that not all smart locks have the security level that the producers indicate to the customers. The Sherlock S2 lock has been hacked by a quite simple method and, moreover, the intruder can easily get the necessary tools for the hack. Perhaps that is the reason why Xiaomi has released other more secure smart locks. On the other hand, other locks have been found to have a higher level of security, such as Nuki, which could not be hacked. However, new methods of attack could be found and it is possible that the encryption of the Nuki lock could be broken.

The current project is quite flexible and could be expanded much further in the future. It is possible to optimize the current script or even create a new program that automatically picks up the sent keys, saving a lot of time in the attack. On the other hand, only one method to unlock the lock is considered in this project, however, many more procedures can be created to unlock the lock from other information or by attacking another point of the connection.

Considering the advancement of technology and competition in the market, producers will increase the security of their smart locks in upcoming releases. Still, there is a wide variety of brands on the market that can be tested for vulnerability and people can choose the most secure option for their home. The world of smart locks is only beginning.

# 10. Presupuesto

El presupuesto para la elaboración y desarrollo de este proyecto se ha deducido del precio en los puntos más comunes de compra de estas cerraduras, Aliexpress y Amazon, así como del resto de herramientas necesarias para la investigación.

También se tiene en cuenta en el presupuesto, las horas dedicadas a la investigación y el tiempo de desarrollo en el proyecto. A continuación, se presenta un desglose con las herramientas, investigación y desarrollo empleado y su presupuesto calculado con las horas invertidas.

| **Concepto** | **Horas** | **Precio** |
|---|---|---|
| Sherlock S2 | -- | 90,25€ |
| Nuki | -- | 161,00€ |
| Adafruit bluefruit LE Sniffer | -- | 21,13€ |
| Nanoadaptador Bluetooth CBT40NANO | -- | 14,00€ |
| Investigación previa | 10 horas | 30€/hora |
| Análisis de requisitos | 8 horas | 30€/hora |
| Pruebas | 240 horas | 30€/hora |
| Análisis de resultados | 10 horas | 30€/hora |
| Informe de resultados | 8 horas | 30€/hora |

*Tabla 1. Desglose de precios*

| **Presupuesto** | 8.566,38€ |
|---|---|

*Tabla 2. Presupuesto*

# 11. Apéndice. Script de automatización

## 11.1. Script

```
/*****************************************************************************
*
* gatttool.sh
*
*****************************************************************************
*
* JOSELIN PÉREZ PÉREZ
*
*
* 25/07/2021
*
*
* Script de bash para establecer la conexión con la cerradura. De esto modo se enviarán los valores de la contraseña para intentar desbloquear la cerradura.
*
*
*****************************************************************************/

#!/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
```

# Bibliografía


[1] Impresioning: https://cerrajerosbarcelona.co/impresioning/

[2] Bumping: https://es.wikipedia.org/wiki/Llave_bumping

[3] Wireshark: https://www.wireshark.org/

[4] Sniffer Bluetooth: https://es.slideshare.net/JosephBentez/sniffer-para-bluetooth-10136116

[5] Hackeo: https://es.malwarebytes.com/hacker/

[6] Cerraduras de teclado digital: https://www.modregohogar.com/blog/tipos-de-cerraduras-electronicas - Cerradura_de_teclado_digital

[7] Cerraduras electrónicas con mando: https://www.modregohogar.com/blog/tipos-de-cerraduras-electronicas - Cerraduras_electronicas_con_mando

[8] Cerraduras invisibles, bluetooth o Wifi: https://www.modregohogar.com/blog/tipos-de-cerraduras-electronicas - Cerraduras_invisibles_bluetooth_o_Wifi

[9] Cerraduras electrónicas de huella dactilar: https://www.modregohogar.com/blog/tipos-de-cerraduras-electronicas - Cerraduras_electronicas_de_huella_dactilar

[10] Cerradura Sherlock S2: https://es.aliexpress.com/item/32895907342.html

[11] Cerradura Nuki Smart Lock: https://nuki.io/es/

[12] Adafruit bluefruit LE Sniffer: https://www.adafruit.com/product/2269

[13] Bluetooth Low Energy (BLE): https://www.elt.es/ble-bluetooth-low-energy

[14] Nanoadaptador Bluetooth CBT40NANO: https://www.opirata.com/p/adaptador-nano-bluetooth-conceptronic-cbt40nano

[15] Gatttool: http://manpages.ubuntu.com/manpages/cosmic/man1/gatttool.1.html

[16] nRF Sniffer for Bluetooth LE: https://www.nordicsemi.com/Products/Development-tools/nRF-Sniffer-for-Bluetooth-LE/Download

[17] hcitool: https://linux.die.net/man/1/hcitool

[18] Sniffer Bluetooth CC2540: https://www.amazon.es/Bluetooth-CC2540-Protocolo-Análisis-Sniffer/dp/B07GD4X1VZ

[19] SmartKey Sherlock: https://www.fruugo.es/sherlock-smart-lock-key/p-56022834-113924813

[20] App Sherlock: https://m.apkpure.com/es/sherlock-smart/com.aerolite.smartlock

[21] Ciberataque: https://es.wikipedia.org/wiki/Ciberataque

[22] Dirección MAC: https://es.wikipedia.org/wiki/Dirección_MAC

[23] HCI snoop log: https://www.mybluetoothreviews.com/what-is-bluetooth-hci-snoop-log/

[24] adb: https://developer.android.com/studio/command-line/adb?hl=es-419

[25] Filtro btatt: https://www.wireshark.org/docs/dfref/b/btatt.html

[26] Protocolo ATT: https://programmerclick.com/article/68241335665/

[27] Arquitectura cliente-servidor: https://es.wikipedia.org/wiki/Cliente-servidor

[28] Handle: https://es.wikipedia.org/wiki/Handle

[29] Opcode: https://es.wikipedia.org/wiki/Código_de_operación

[30] Linux: https://es.wikipedia.org/wiki/GNU/Linux

[31] Máquina virtual: https://es.wikipedia.org/wiki/Máquina_virtual

[32] Script de bash: https://bioinf.comav.upv.es/courses/unix/scripts_bash.html

[33] App Nuki: https://nuki.io/es/app/

[34] Cifrado AES: https://www.le-vpn.com/es/encriptacion-aes-256/

[35] Cifrado de Nuki: https://nuki.io/es/blog/sientete-seguro/seguridad

[36] Cifrado de extremo a extremo: https://www.kaspersky.es/blog/what-is-end-to-end-encryption/23862/

[37] NaCl: https://en.wikipedia.org/wiki/NaCl_(software)

[38] Repositorio GitHub: https://github.com/alu0101037653/Trabajo-de-Fin-de-Grado