

# Seguridad y robo de información vía periféricos y dispositivos hardware

---

Alberto García Valero  
Manuel Fernández La-Chica



**ETSIIT - Grado en Ingeniería Informática**  
**Periféricos y Dispositivos de Interfaz Humana**



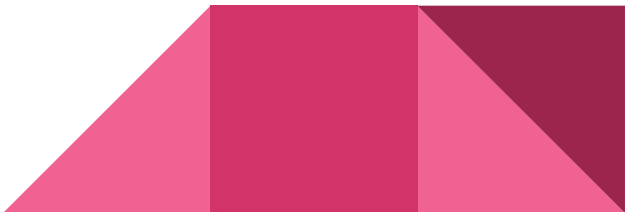
**UNIVERSIDAD  
DE GRANADA**

# Índice

1. Malware y robo de información
  - 1.1. Periféricos
  - 1.2. Hardware
2. Videos de casos prácticos
3. Conclusión



# 1.1 Periféricos

- ❑ Hackear pixeles de un **monitor**
  - ❑ **Ratones y teclados** inalámbricos
  - ❑ Captura de las **pulsaciones del teclado**
  - ❑ Phishing a través de **altavoces inteligentes**
  - ❑ Pendrives **USB**
  - ❑ Cables/interfaz **Thunderbolt**
  - ❑ Acceso a la **webcam y micrófono**
- 

## 1.1.1 Hackear pixeles de un monitor

- Necesario **acceder al firmware** del monitor **via USB o HDMI**.
- Se podría tanto **visualizar el contenido** de la pantalla como **alterar sus pixeles** mostrando imágenes y mensajes para por ejemplo ejercer una extorsión...
- Esta técnica fue presentada en la **Def Con** de Las Vegas por la compañía **Red Balloon Security** tras **2 años de ingeniería inversa** en un Dell U2410.



## 1.1.2 Ratones y teclados inalámbricos

- Necesario acceso físico al teclado o ratón para iniciar el ataque.
- Vulnerabilidad en productos del 2009 hasta el presente que usan **receptores USB** en concreto de la marca **Logitech** bajo el estandar inalámbrico **Unifying**.
- El error permite al atacante **crear una puerta trasera** para inyectar software malicioso o obtener información como por ejemplo las teclas pulsadas.
- Brecha de seguridad descubierta por **Marcus Mengs**.



## 1.1.3 Captura de las pulsaciones del teclado

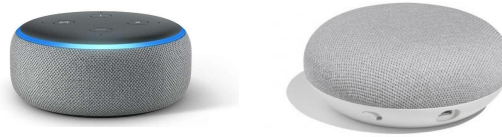
- Se capturan utilizando el **acelerómetro** de nuestro **smartphone** apoyado en la misma mesa que estamos tecleando.



- Investigadores del **MIT** y **Georgia Tech** han podido asignar vibraciones a teclas concretas con un **80% de efectividad**.
- **PRO:** el equipo no necesita estar conectado a ninguna red
- **CONTRA:** no es sencillo y se deben dar muchos factores a la vez

## 1.1.4 Phishing a través de altavoces inteligentes

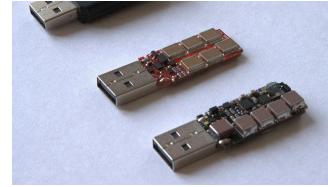
- Un grupo de investigación hacking berlinés ha conseguida poner en jaque a los **altavoces de Amazon y Google.**



- El problema surge cuando **aplicaciones** aprobadas oficialmente **se actualizan** implementando **habilidades nuevas y peligrosas** actuando como espías en la sombra.
- **No solo escuchando** nuestras conversaciones sino **interactuando con el usuario** para el robo de información.

## 1.1.5 Pendrives USB

- Con el fin de **apoderarse del sistema** o acabar con el equipo como por ejemplo con el famoso **USB Killer** que aplica 220 voltios negativos friendo casi cualquier dispositivo en segundos...



- Para el **robo de datos e información** mediante técnicas de Phishing haciéndose pasar por una persona, empresa o servicio.
- Para utilizar tu equipo para el **minado de criptomonedas**.



## 1.1.6 Cables/interfaz Thunderbolt



- Ataque bautizado como **Thunderspy** que permite el **robo de datos** incluso encriptados y con el equipo bloqueado o en suspensión **evitando la pantalla de inicio de sesión**.
- Necesario **acceso físico** y que disponga de **Windows/Linux**. Desde 2019 alguno fabricantes integran **Kernel Direct Memory Access Protection** que protege parcialmente aunque se siguen sacando equipos sin esta protección.
- El **punto fuerte** de la interfaz, una mayor transferencia de datos a dispositivos externos, **es a la vez su punto débil** permitiendo un acceso más directo a memoria.

## 1.1.7 Acceso a la webcam y micrófono

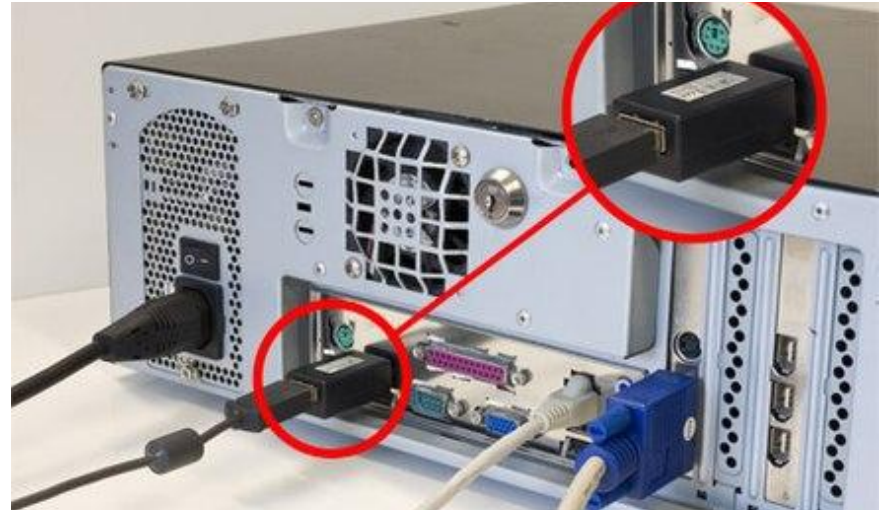
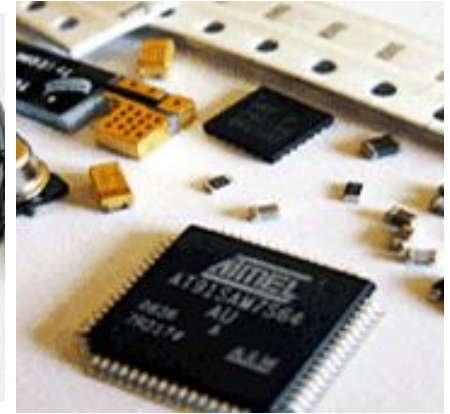


- Hay cientos de **malware** cuyo fin es el **acceso** a la **webcam o micrófono** de tu equipo.
- Los ciberdelincuentes se aprovechan de estas brechas de seguridad normalmente para el **robo de información** y la **extorsión económica**.
- En relación a la **webcam** hay **métodos para deshabilitarla** en el sistema y que no se reconozca, **como si no existiese**, aunque el poner un stick encima de ella no deja de ser el método más fiable hoy día...

# Keyloggers

El keylogger por hardware es una solución perfecta que sirve para seguir la actividad del usuario de ordenador con escaso riesgo de su detección.

Es un dispositivo 100% electrónico así que no requiere acceso al sistema operativo, no deja huellas y los programas no son capaces de detectar este tipo de dispositivo.

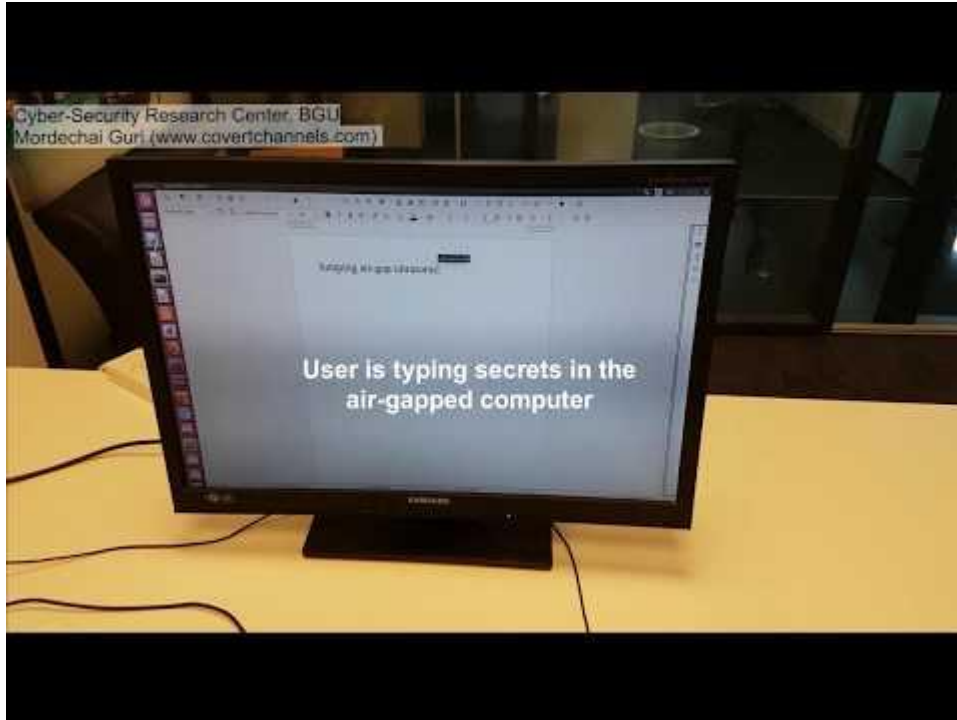


# 1.2 Hardware

- ❑ **Fuente de alimentación** como altavoz de ultrasonidos
- ❑ **Ventiladores** para la transmisión de información en código morse
- ❑ Modificación registros **RAM** para concesión de permisos y robo de información
- ❑ Daño irreparable del **disco duro** alterando su firmware
- ❑ Robo de información de los **HDD** mediante señales acústicas
- ❑ Acceso al código fuente del ROM chip de la **BIOS/UEFI**

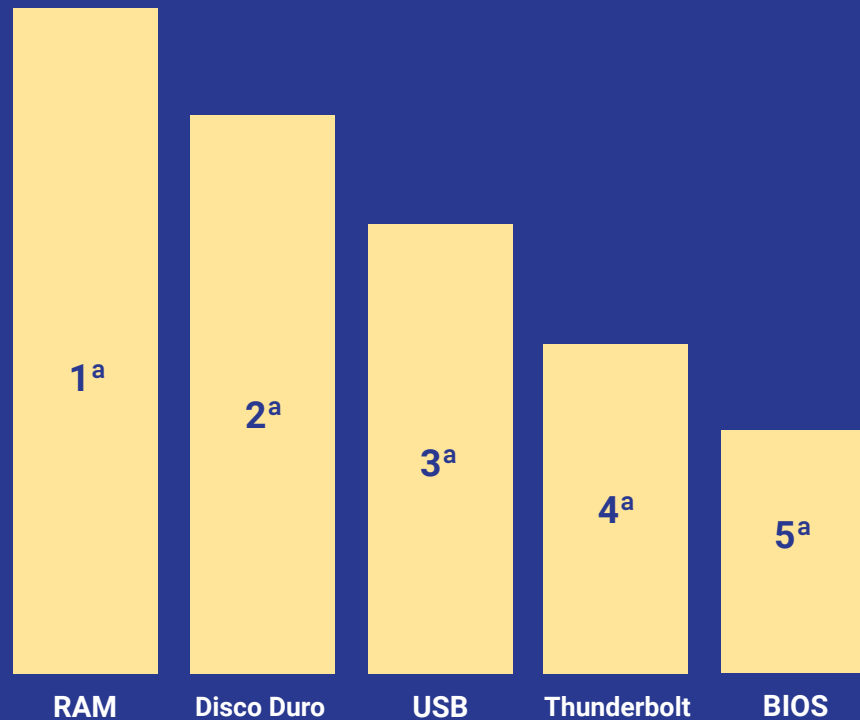


# Power Supplay



# Ranking de vulnerabilidades hardware

Estas son debidas por el aumento en la complejidad de los nuevos firmwares encargados para gestionar sus distintos componentes.



# Bit-flipping en Memoria RAM

Es el fenómeno que ocurre cuando un bit cambia su valor sin que lo haya hecho el sistema. Es evidente que cambiar el valor de un bit arbitrariamente puede tener consecuencias catastróficas en un sistema, normalmente se pueden hacer haciendo que el usuario ejecute un código casi sin darse cuenta, como JavascRipt al abrir una página web.



# RAM

Principal amenaza, problema con los elementos del hardware soldados en el chip.

# BIOS

Cuando el código fuente se convierte en algún común, encontramos un problema.

# Disco Duro

El firmware que controla los discos contiene elementos que pueden piratearlos.





### 3. Vídeos



### 3. Vídeos




# Conclusión

Aunque se ha avanzado mucho los investigadores y ciberdelincuentes a día de hoy **acaban consiguiendo dar con alguna brecha de seguridad.**

Con los conocimientos y habilidades necesarias y utilizando diferentes técnicas como puede ser la ingeniería inversa entre otras muchas prácticamente **no hay sistema infranqueable...**

La **ciberseguridad** se posiciona como uno de los **campos más importantes** dentro de la informática con vistas a un futuro en el que nuestra **privacidad** cada vez está **más expuesta.**



# Fuentes de información

- ❏ [genbeta.com](http://genbeta.com)
- ❏ [computerhoy.com](http://computerhoy.com)
- ❏ [hipertextual.com](http://hipertextual.com)
- ❏ [adslzone.net](http://adslzone.net)
- ❏ [muycomputerpro.com](http://muycomputerpro.com)
- ❏ [globbsecurity.com](http://globbsecurity.com)
- ❏ [xataka.com](http://xataka.com)
- ❏ [keelog.com](http://keelog.com)

