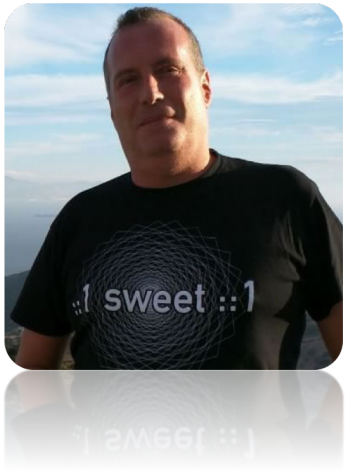
28 de febrero 2020 | SICUR-Mundo Hacker Day (Madrid, España)

Explotación práctica de vulnerabilidades en IoT

Tipo de documento: Presentación
Autor del documento: CS³ Group (Pedro C. aka s4ur0n)
Código del Documento: MHD_2020.pdf
Versión: 1.1

Categoría: Público
Fecha de elaboración: 25/02/2020
Nº de Páginas: 61

Whoami




```
class PedroC:
    def __init__(self):
        self.name =      'Pedro Candel'
        self.email =     's4ur0n@s4ur0n.com'
        self.web =       'https://www.s4ur0n.com'
        self.nick =      '@NN2ed_s4ur0n'
        self.company =   'CS³ Group'
        self.role =      'Security Researcher'
        self.work =      [ 'Reversing', 'Malware', 'Offensive
                           Security', '…' ]
        self.groups =    [ 'mlw.re', 'OWASP', 'NetXploit', '...' ]
```

mlw.re

OWASP Open Web Application Security Project

CS³ SECURITY SERVICES https://cs3group.com

sicur MUNDO HACKER

CS³ Group

Formación en Seguridad
Cursos presenciales a medida impartidos en las instalaciones del cliente o las concertadas con prácticas reales desde el primer momento

Hacking Ético
Auditorías de caja negra, gris o blanca para aplicaciones web, sistemas y redes de comunicaciones

Análisis de Malware
Análisis de Malware automatizados y manuales con completos informes de comportamiento e indicadores de compromiso (IOC)

Ingeniería Inversa
Ingeniería Inversa para binarios de sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits, ARM y firmwares

Exploiting
Desarrollo y adaptación de exploits para sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits y Android

Desarrollo Seguro
Auditoría SAST, DAST, IAST y RASP para análisis de vulnerabilidades en el código de proyectos en Java, .Net, PHP, C/C++ y Cobol

Hardware Hacking
Análisis de vulnerabilidades en dispositivos hardware, sistemas embebidos y firmware con técnicas de ingeniería inversa

Seguridad en dispositivos móviles
Análisis estático, dinámico e instrumentación dinámica de aplicaciones Android (APK), iOS (IPA) y Windows Mobile (APPX)

Respuesta ante incidentes
Investigación remota de incidentes de seguridad, análisis de las situaciones y respuesta inmediata ante las amenazas

Forense
Adquisición y elaboración de informes periciales con garantía de imparcialidad y objetividad para todo tipo de sistemas de información

DevSecOps
Desarrollo, Seguridad y Operaciones en CSI (Continuous Security Integration) con pruebas automatizadas de seguridad para CI/CD

Intelligence
Recopilación, análisis y explotación de datos a gran escala con fuentes OSINT, SIGINT, HUMINT, Deep Web, redes P2P, etc.

SIGINT
Inteligencia de comunicaciones, análisis y auditoría de seguridad en señales y protocolos de radiofrecuencia (RF)

T.S.C.M.
Technical Surveillance Counter-Measures: Contramedidas electrónicas para detección y localización de dispositivos de escucha

Telecom
Análisis y auditoría GSM/3G/4G, implementación de servicios de operadores móviles virtuales (HLR, VLR, GGSN, Roaming voz y datos)

ATM
Análisis de vulnerabilidades, auditoría, forense, skimming, shimming y pruebas de blackbox para NCR, Hyosung, WRG, Diebold Nixdorf e Hitachi

PoS/TPV
Auditoría y cumplimiento de controles en terminales Verifone e Ingenico. Monitorización y transaccionabilidad completa según ISO 8583

LOPD/GPDR/Cumplimiento
LOPD, adaptación GPDR, ISO 27000, SGSI, análisis y gestión de riesgos, Políticas de seguridad, continuidad de negocio, ITIL, PCI DSS

CS³ SECURITY SERVICES https://cs3group.com

sicur MUNDO HACKER

sicur
MUNDO HACKER

Agenda

Descubrimiento y explotación práctica de vulnerabilidades en dispositivos IoT

CS³ SECURITY SERVICES
https://cs3group.com

Agenda

Descubrimiento y explotación práctica de vulnerabilidades en dispositivos IoT

1. Introducción
2. Áreas y superficie de ataques en IoT
3. Proyecto OWASP IoT Top 10
4. Pentesting IoT 101
5. Conclusiones

sicur
MUNDO HACKER

1. Introducción

Descubrimiento y explotación práctica de vulnerabilidades en dispositivos IoT

CS³ SECURITY SERVICES
https://cs3group.com

Organización OWASP

owasp.org

Save the Date: Global AppSec Dublin is June 15-19th. CfP & CfT are now open.

OWASP

PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org

Donate Join

Who is the OWASP Foundation?

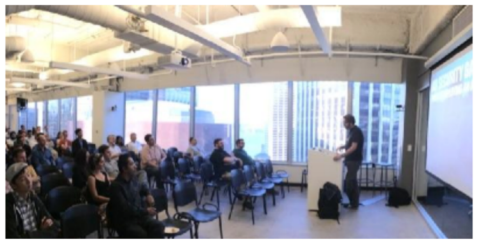
The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

Project Spotlight: Zed Attack Proxy

Featured Chapter: Bay Area



Proyecto OWASP IoT Top 10

https://owasp.org/www-project-internet-of-things/

- OWASP IoT Top 10
- OWASP IoT Top 10 Mapping Project (del 2014 al 2018)
- OWASP Firmware Security Testing Methodology
- OWASP IoTGoat
- ByteSweep

2. Áreas y superficie de ataques en IoT

Descubrimiento y explotación práctica de vulnerabilidades en dispositivos IoT

Áreas y superficie de ataques para IoT

Áreas y superficie de ataques para IoT

Ecosistema (General)

- Estándares de interoperabilidad
- Datos de gobierno
- Fallas en todo el sistema
- Riesgos individuales de los interesados
- Confianza implícita entre componentes
- Seguridad en el registro del dispositivo
- Sistema de desmantelamiento
- Falta de procedimientos de acceso

Áreas y superficie de ataques para IoT

Memoria

- Datos sensibles:

  - ✓ Nombres de usuario de texto claro
  - ✓ Contraseñas de texto sin cifrar
  - ✓ Credenciales de terceros
  - ✓ Claves de cifrado

Áreas y superficie de ataques para IoT

Interfaces físicas

- Extracción de firmware
- CLI de usuario
- CLI de administrador
- Escalada de privilegios
- Reseteo a estado inseguro
- Retirada de medios de almacenamiento
- Resistencia a la manipulación (tampers)
- Puerto de depuración:
  - ✓ UART (serie)
  - ✓ JTAG / SWD
- Identificación del dispositivo (ID)/Exposición del número de serie/Exposición de componentes

Áreas y superficie de ataques para IoT

Interfaces Web

- Conjunto estándar de vulnerabilidades de aplicaciones web (OWASP Top Ten)
- Vulnerabilidades de gestión de credenciales:
  - ✓ Enumeración de nombre de usuario
  - ✓ Contraseñas débiles
  - ✓ Bloqueos de cuentas
  - ✓ Credenciales predeterminadas conocidas
  - ✓ Mecanismos de recuperación de contraseñas inseguros

Áreas y superficie de ataques para IoT

Firmware

- Exposición de datos sensibles:
  - ✓ Cuentas de puertas traseras (backdoors)
  - ✓ Credenciales codificadas
  - ✓ Claves de cifrado
  - ✓ Cifrado (simétrico, asimétrico)
  - ✓ Información sensible
  - ✓ Revelación de URL sensibles
- Visualización de la versión de firmware y/o última fecha de actualización

Áreas y superficie de ataques para IoT

- Servicios vulnerables (web, ssh, tftp, etc):
  - ✓ Verificación de versiones antiguas de software y posibles ataques (Heartbleed, Shellshock, versiones antiguas de PHP, frameworks, etc.)
- Funciones relacionadas con la exposición y seguridad del API
- Posibilidad de rebajar (downgrade) el firmware

Áreas y superficie de ataques para IoT

Servicios de red

- Divulgación de información
- CLI de usuario
- CLI de administración
- Inyección
- Denegación [distribuida] de servicio
- Servicios sin cifrar
- Cifrados mal implementados
- Servicios de prueba/desarrollo
- Desbordamiento de búfer
- UPnP
- Servicios UDP vulnerables

Áreas y superficie de ataques para IoT

- Bloque de actualización del firmware del dispositivo OTA
- Firmware cargado sobre canales inseguros (sin TLS)
- Ataques de repetición
- Falta de verificación del payload
- Falta de verificación de las integridad de mensajes
- Vulnerabilidades de gestión de credenciales:
- Enumeración de nombres de usuarios
- Contraseñas débiles
- Bloqueos de cuentas
- Credenciales predeterminadas conocidas
- Mecanismos de recuperación de contraseñas inseguros

Áreas y superficie de ataques para IoT

Interfaces administrativas

- Conjunto estándar de vulnerabilidades de aplicaciones web
- Vulnerabilidades de gestión de credenciales:
  - ✓ Enumeración de nombres de usuarios
  - ✓ Contraseñas débiles
  - ✓ Bloqueos de cuentas
  - ✓ Credenciales predeterminadas conocidas
  - ✓ Mecanismos de recuperación de contraseñas inseguros
- Opciones de seguridad/cifrado
- Opciones de registro

Áreas y superficie de ataques para IoT

- Autenticación de dos factores
- Referencias inseguras de objetos directos
- Incapacidad para borrar completamente (wipe) el dispositivo

Áreas y superficie de ataques para IoT

Interfaces Web en la nube

- Conjunto estándar de vulnerabilidades de aplicaciones web
- Vulnerabilidades de gestión de credenciales:
  - ✓ Enumeración de nombres de usuarios
  - ✓ Contraseñas débiles
  - ✓ Bloqueos de cuentas
  - ✓ Credenciales predeterminadas conocidas
  - ✓ Mecanismos de recuperación de contraseñas inseguros
- Cifrados en la capa de transporte
- Autenticación de dos factores

Áreas y superficie de ataques para IoT

Almacenamiento local

- Datos sin cifrar
- Datos cifrados con claves débiles, leakeadas, rehusadas...
- Falta de verificaciones de la integridad de datos
- Uso de la misma clave de cifrado estática

Áreas y superficie de ataques para IoT

APIs y Backend de terceras partes

- Acceso a Información Personal Identificable (PII) sin cifrar
- Información Personal Identificable (PII) enviada cifrada y almacenada en claro
- Información del dispositivo filtrada
- Datos de ubicación filtrados

Áreas y superficie de ataques para IoT

APIs y Backend de fabricantes

- Confianza inherente en la nube o aplicaciones móviles
- Autenticaciones débiles
- Controles de acceso débiles
- Ataques de inyección
- Servicios ocultos

Áreas y superficie de ataques para IoT

Mecanismos de actualización

- Actualizaciones enviadas sin cifrado
- Actualizaciones no firmadas
- Ubicaciones de actualización con permisos de escritura para cualquier proceso
- Procesos de verificación para las actualizaciones
- Autenticación necesaria para la actualización
- Actualizaciones maliciosas (malware)
- Falta de mecanismos para las actualizaciones
- Sin posibilidad de actualizaciones manuales

Áreas y superficie de ataques para IoT

Aplicaciones de gestión móviles

- Confiables implícitamente por el dispositivo o cloud
- Enumeración de nombres de usuarios
- Bloqueos de cuentas
- Credenciales predeterminadas conocidas
- Contraseñas débiles
- Almacenamiento inseguro de datos
- Cifrado de transporte
- Mecanismo de recuperación de contraseñas inseguros
- Autenticación de dos factores

Áreas y superficie de ataques para IoT

Comunicación del ecosistema

- Controles de "salud"
- Latidos del corazón (heartbeats)
- Comandos del ecosistema
- Desaprovisionamientos
- Actualizaciones push

Áreas y superficie de ataques para IoT

Tráfico de la red

- LAN
- Acceso de la LAN a Internet
- Ondas de corto alcance
- Protocolos inalámbricos (WiFi, Z-wave, XBee, Zigbee, Bluetooth, LoRA)
- Protocolos no estándar
- Fuzzing de protocolos

Áreas y superficie de ataques para IoT

Autenticación y autorización

- Revelación de valores relacionados con la autenticación/autorización (claves de sesión, tokens, cookies, etc.)
- Reutilización de clave de sesión, tokens, etc.
- Autenticación de dispositivo a dispositivo
- Autenticación de dispositivo a aplicación móvil
- Autenticación de dispositivo a sistemas en la nube
- Aplicación móvil para autenticación del sistema en la nube
- Aplicación web para autenticación del sistema en la nube
- Falta de autenticación dinámica

Áreas y superficie de ataques para IoT

Privacidad

- Divulgación de datos del usuario
- Divulgación de ubicación del usuario/dispositivo
- Privacidad diferencial

Áreas y superficie de ataques para IoT

Hardware (sensores y actuadores)

- Manipulación del entorno de detección de los sensores
- Manipulación (física)
- Daños (físicos)

sicur
MUNDO HACKER

3. OWASP IoT 2018

Descubrimiento y explotación práctica de vulnerabilidades en dispositivos IoT

CS³ SECURITY SERVICES
https://cs3group.com

Evolución del Proyecto OWASP Top Ten IoT

OWASP IoT Top 10 2018 (Draft)

2014

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

2018

I1	**Weak, Guessable, or Hardcoded Passwords**	Use of easily bruteforced, hardcoded, publicly available, and/or unchangable passwords in client-side software/firmware that can grant unauthorized access to deployed systems.
I2	**Insecure Network Services / Protocols**	Unneeded and/or insecure listening/active network services—especially those exposed to the internet—that allow sensitive information gathering or unauthorized remote control, e.g., Telnet, WiFi, ZigBee, Bluetooth, FTP, SSH, UPnP, etc.
I3	**Insecure Access Interfaces**	Insecure web, backend API, cloud, or mobile interfaces that allow compromise of the product and/or its ecosystem. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output validation.
I4	**Use of Insecure or Outdated Components**	Use of deprecated and insecure software components/libraries. Insecure customization of operating systems, and use of third-party software or hardware components from compromised supply chain.
I5	**Lack of Secure Update Mechanism**	Lack of ability to securely update the device/ecosystem, lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of roll-back mechanisms.
I6	**Insufficient Privacy Protection**	User's personal information stored insecurely on device, is used insecurely or without permission in logs, is transmitted insecurely over the network or the internet, or the system lacks adequate privacy disclosure before usage.
I7	**Insecure Data Transfer and Storage**	Lack of encryption of sensitive data either at rest or in transit, e.g., weak or lacking cryptography, mismanagement of keys, inefficient platform access controls, insufficient key rotation, absence of secure hardware backed storage, use of known vulnerable hardware.
I8	**Lack of Physical Hardening**	Lack of physical anti-tampering defenses and/or lack of system integrity checking that allows potential attackers to gain sensitive information that can help with a future remote attack.
I9	**Insufficient Security Configurability**	A lack of vendor-provided product features for securing the device, e.g., secure authentication, logging and monitoring, encryption strength management, granular policy management, etc.
I10	**Lack of Device Management**	Lack of security support on existing devices deployed in production, including asset management, update management, and secure decommissioning.

Proyecto OWASP IoT Top 10

- **I1:** Contraseñas débiles, adivinables o codificadas
- **I2:** Servicios de red inseguros
- **I3:** Interfaces inseguras del ecosistema
- **I4:** Falta de mecanismo de actualización segura
- **I5:** Uso de componentes inseguros u obsoletos
- **I6:** Protección de privacidad insuficiente
- **I7:** Transferencia y almacenamiento de datos inseguros
- **I8:** Falta de gestión de dispositivos
- **I9:** Configuración predeterminada insegura
- **I10:** Falta de hardening físico

I1: Contraseñas débiles, adivinables o codificadas

Evaluación de la resistencia de las credenciales en los dispositivos para comprobar el uso de credenciales fácilmente forzadas, disponibles públicamente o que no se pueden cambiar:

- Fácilmente adivinables
- Públicamente disponibles
- Fuerza bruta fácil
- Credenciales sin posibilidad de cambio

Además de los backdoors en el firmware o software que permiten un acceso no autorizado directo...

I1: Contraseñas débiles, adivinables o codificadas

- https://www.routerpasswords.com/
- https://github.com/lcashdol/IoT
- https://github.com/OpCode41/IoTCrusher
- https://www.defpass.com/

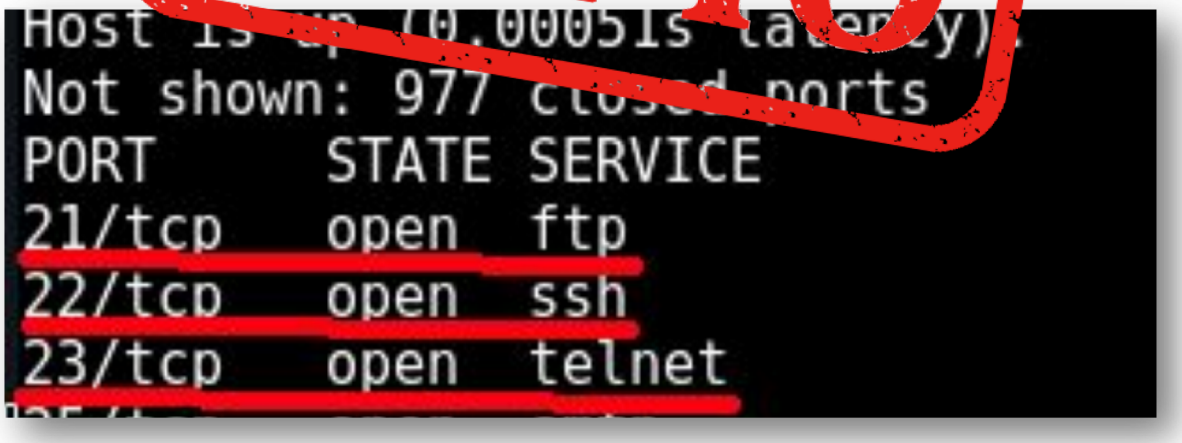
DEMO

I2: Servicios de red inseguros

Servicios de red innecesarios o inseguros que se ejecutan en los dispositivos:

- Los expuestos a Internet
- Cualquiera que comprometa la confidencialidad, integridad / autenticidad o disponibilidad de la información
- Cualquier servicio que permita el control remoto no autorizado

DEMO



I3: Interfaces inseguras del ecosistema

Interfaces inseguras en el ecosistema fuera del dispositivo:

- Web
- API del backend
- Nube
- Móvil

Vulnerabilidades comunes:

- Ausencia de autenticación
- Ausencia de autorización
- Ausencia de cifrado o muy débiles
- Ausencia de filtros de entrada y salida

I4: Falta de mecanismo de actualización segura

Falta de capacidad para **actualizar de forma segura** el dispositivo:

- Ausencia de validación del firmware en el dispositivo
- Ausencia de entrega segura (sin cifrar en tránsito)
- Falta de mecanismos de validación “antirretroceso” de versiones en el firmware o software
- Falta de notificaciones de cambios de seguridad debido a actualizaciones

I4: Falta de mecanismo de actualización segura

I5: Uso de componentes inseguros u obsoletos

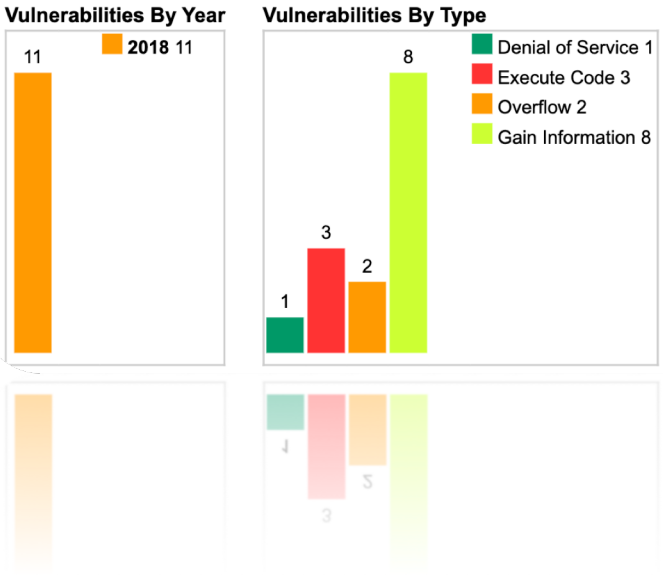
Uso de **componentes / bibliotecas de software obsoletas o inseguras** que permiten que el dispositivo se vea comprometido:

- Personalización insegura de las plataformas del sistema operativo
- Bibliotecas comprometidas en software de terceros y/o fabricantes
- Componentes hardware comprometidos de terceros en la cadena de suministro

I5: Uso de componentes inseguros u obsoletos

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2018	11	1	3	2							8				
Total	11	1	3	2							8				
% Of All		9.1	27.3	18.2	0.0	0.0	0.0	0.0	0.0	0.0	72.7	0.0	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may r
years.)



AWS FreeRTOS

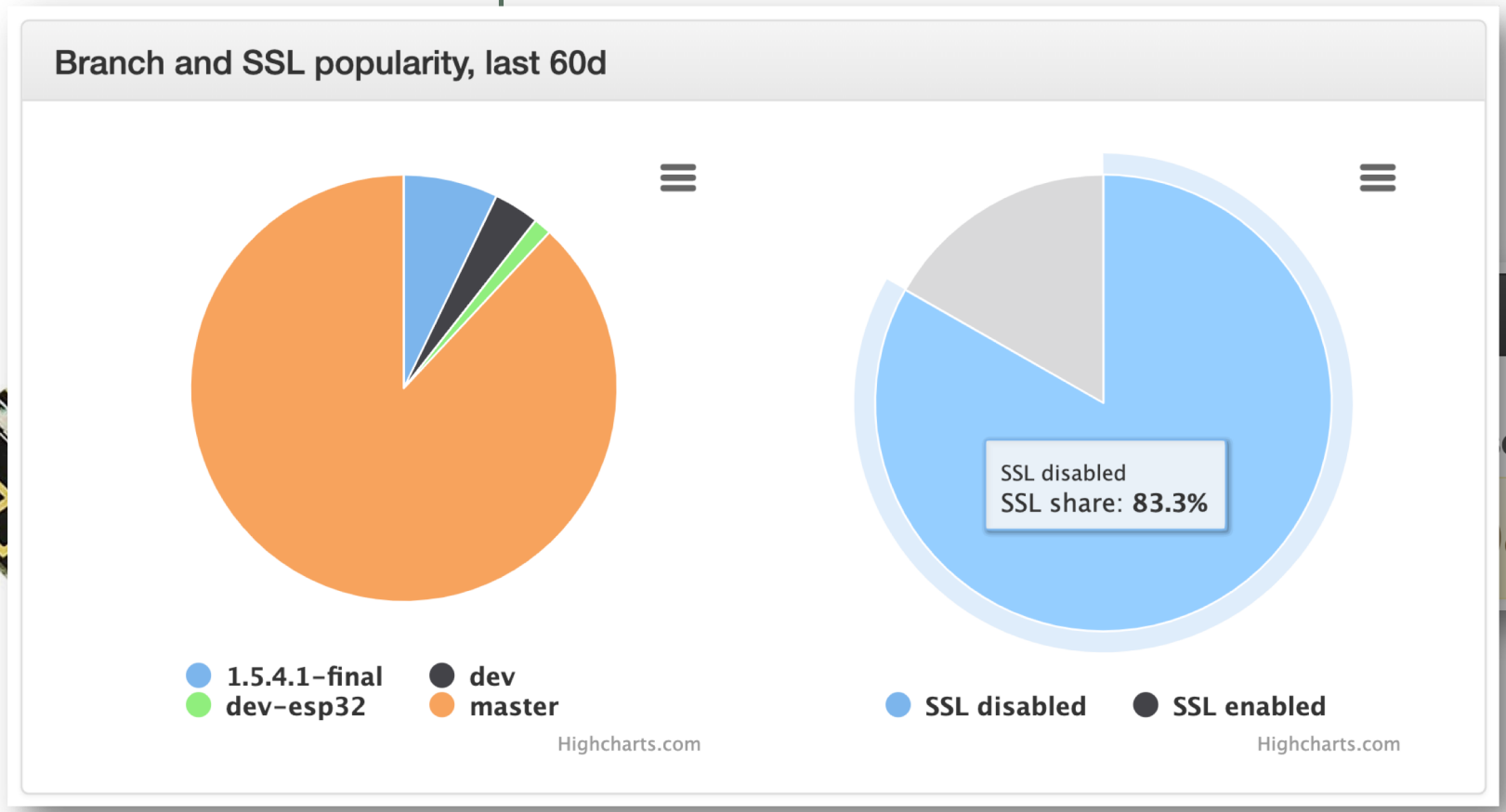
I6: Protección de privacidad insuficiente

La **información personal del usuario se almacena** en el dispositivo o en el ecosistema y **se usa de forma insegura**, inadecuada o sin su permiso y/o consentimiento.

I6: Protección de privacidad insuficiente

I7: Transferencia y almacenamiento de datos inseguros

Ausencia de cifrado o **control de acceso** en datos confidenciales dentro de cualquier parte del ecosistema, incluso en reposo, en tránsito o mientras son procesados.



I8: Falta de gestión de dispositivos

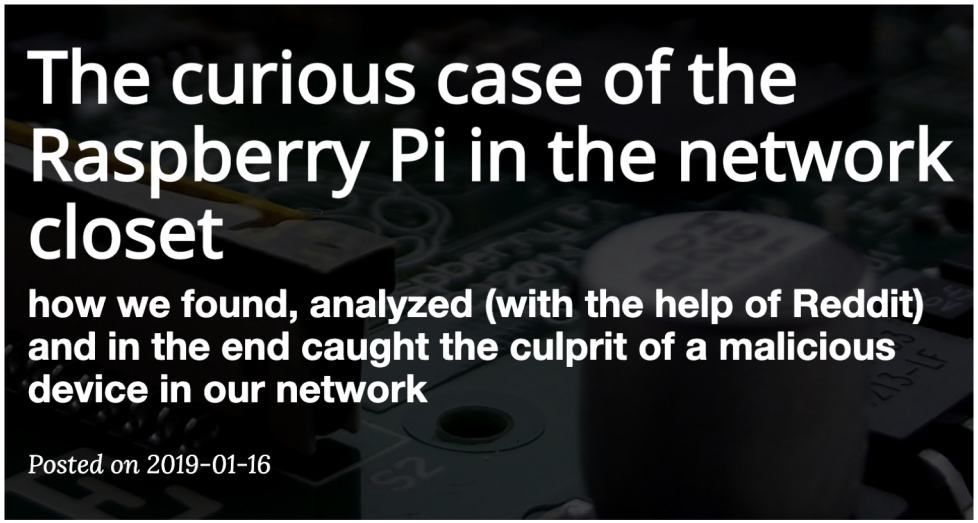
Falta de soporte de seguridad en dispositivos implementados en producción, incluyendo la **gestión de activos**, gestión de actualizaciones, desmantelamiento seguro, monitoreo de sistemas y capacidades de respuesta ante incidentes.

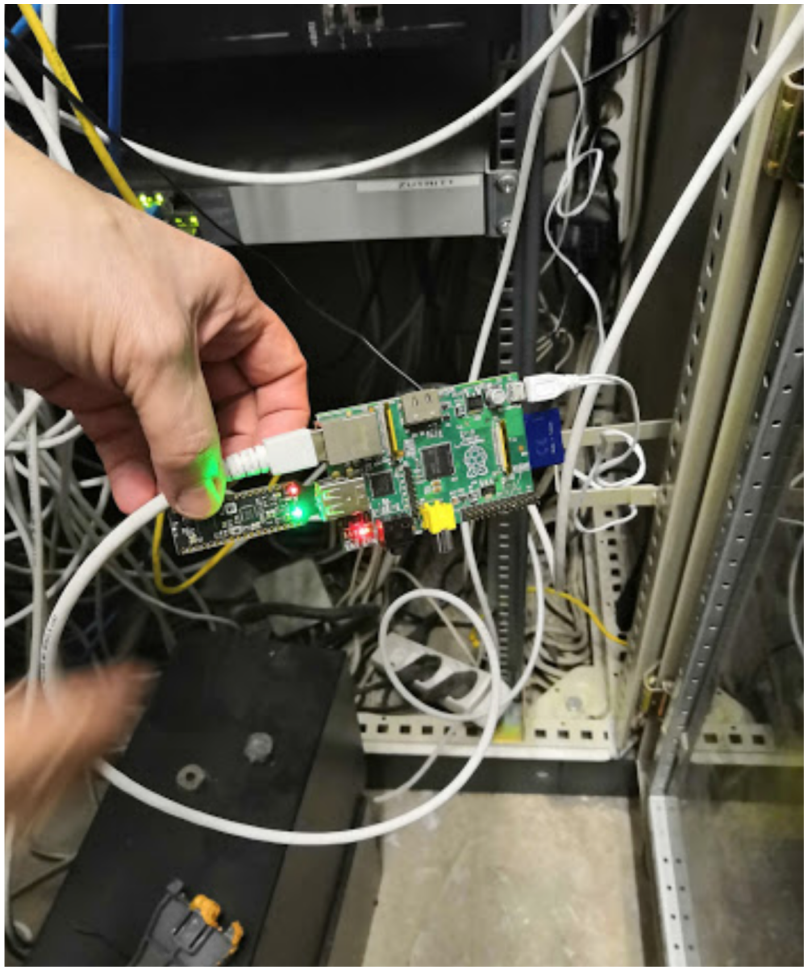
I8: Falta de gestión de dispositivos

The Thing, also known as the **Great Seal bug**, was one of the first covert listening devices (or "bugs") to use passive techniques to transmit an audio signal. It was concealed inside a gift given by the Soviet Union to W. Averell Harriman, the United States Ambassador to the Soviet Union, on August 4, 1945. Because it was passive, needing electromagnetic energy from an outside source to become energized and activate, it is considered a ***predecessor of Radio-Frequency Identification (RFID) technology***

Source: https://en.wikipedia.org/wiki/The_Thing_(listening_device)

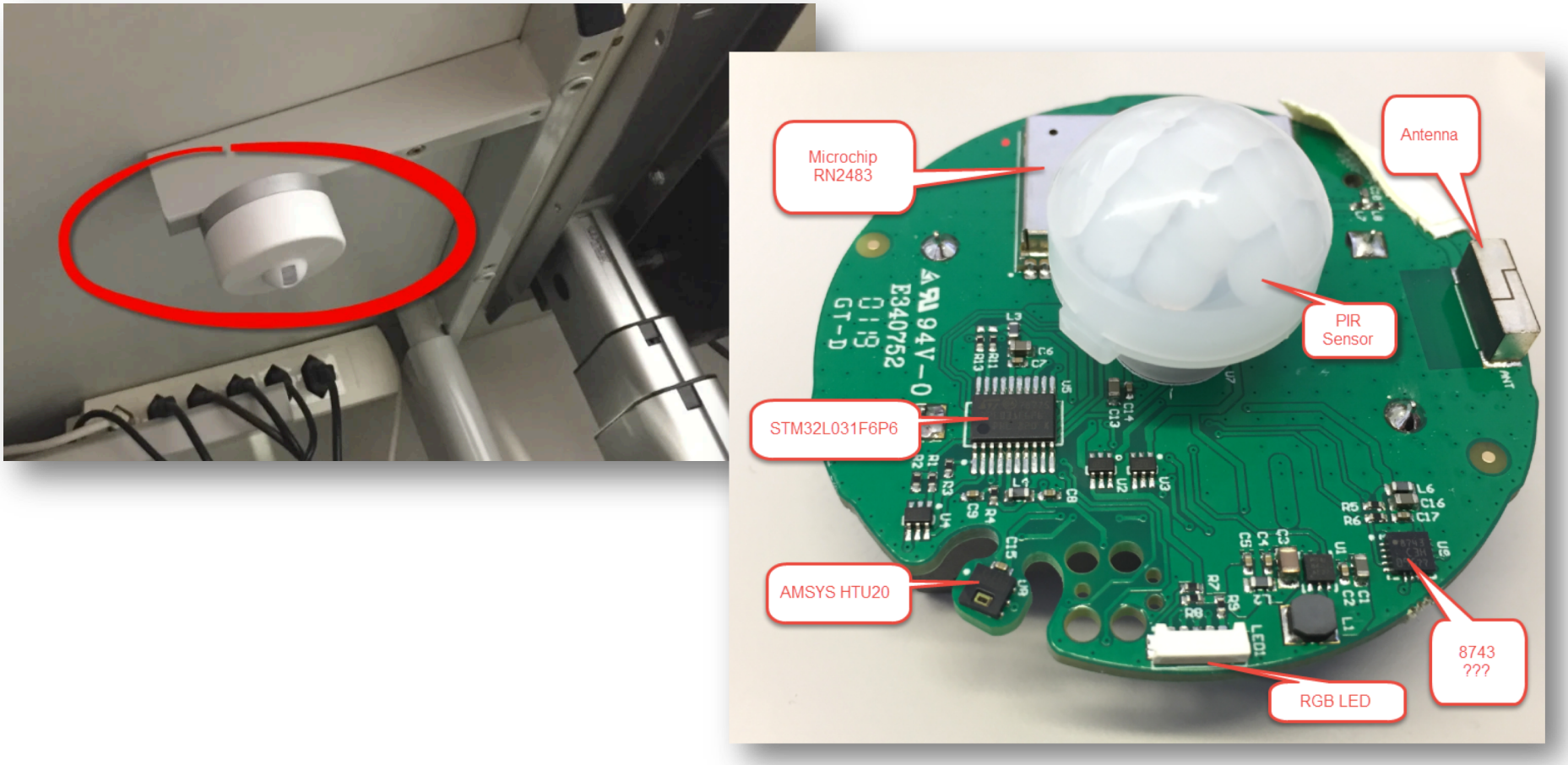
I8: Falta de gestión de dispositivos





Source: https://blog.haschek.at/2018/the-curious-case-of-the-RasPi-in-our-network.html

I8: Falta de gestión de dispositivos



Source: https://mcuoneclipse.com/2019/05/26/reverse-engineering-of-a-not-so-secure-iot-device/

I9: Configuración predeterminada insegura

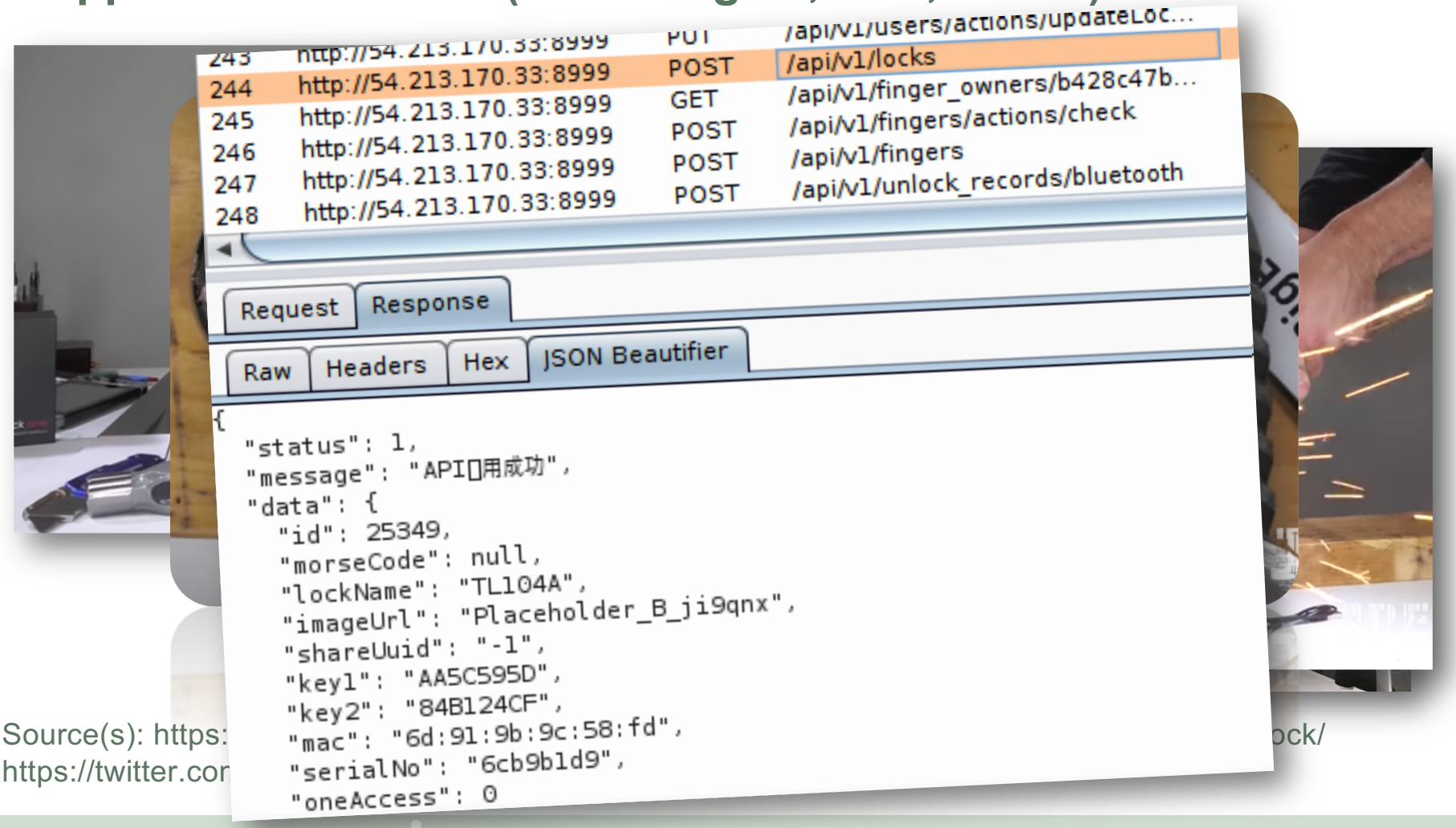
Los dispositivos o sistemas IoT son entregados con **configuraciones predeterminadas inseguras** o carecen de la capacidad de hacer que el sistema sea más seguro restringiendo incluso a los usuarios poder modificar estas configuraciones.

I10: Falta de hardening físico

Falta de medidas de **resistencia física**, lo que permite que potenciales atacantes puedan obtener información confidencial que ayude en un futuro ataque remoto o se pueda llegar a tomar el control local del dispositivo completo.

I10: Falta de hardening físico

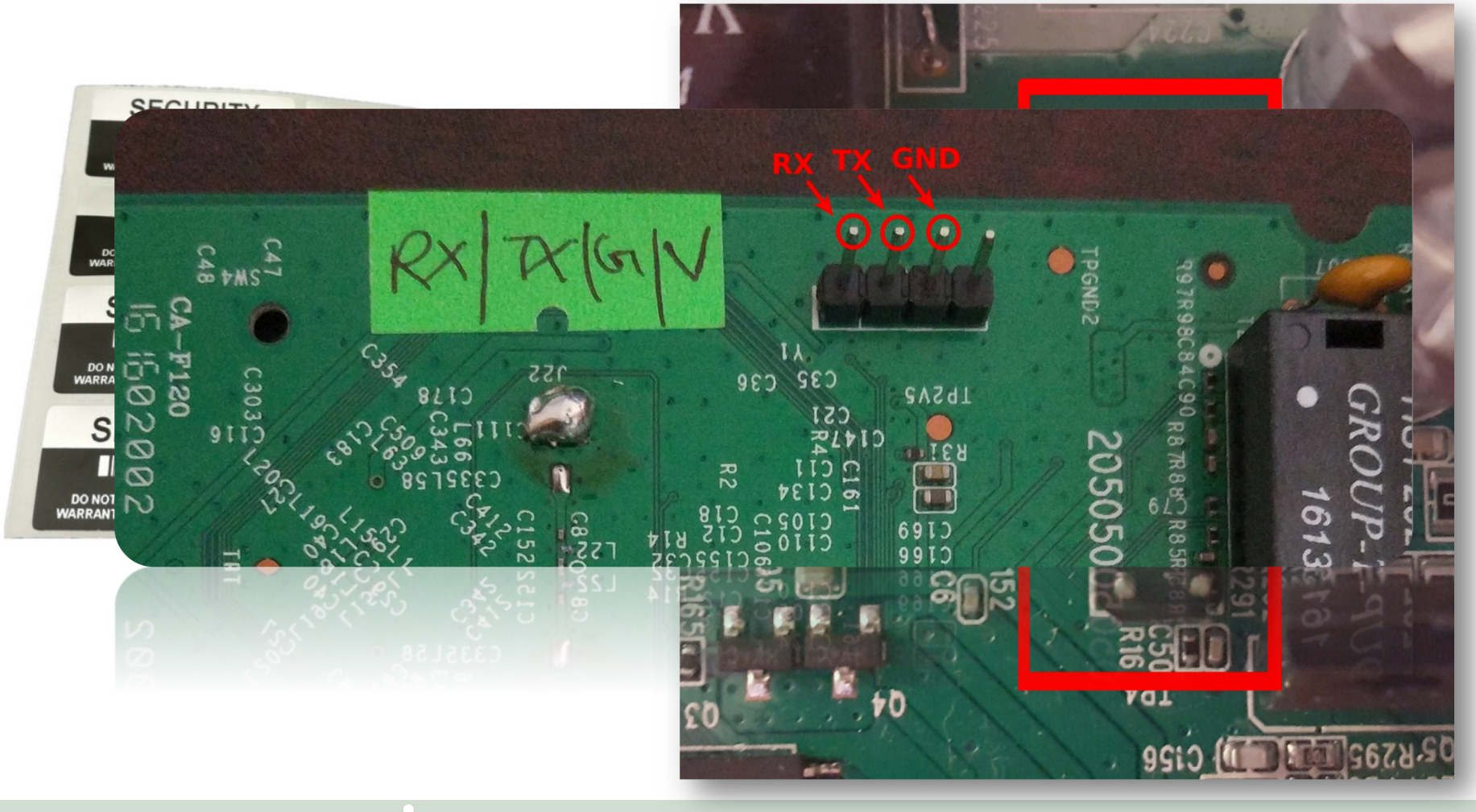
Tapplock Smart Lock (Huella digital, BLE, Morse)



Source(s): https: ock/
https://twitter.com

I10: Falta de hardening físico

Precintos de garantía, pirate bus, puertos de debug...



sicur
MUNDO HACKER

4. Pentesting IoT 101

Descubrimiento y explotación práctica de vulnerabilidades en dispositivos IoT

CS³ SECURITY SERVICES
https://cs3group.com

Pentesting IoT 101

https://www.iotpentestingguide.com/ escrito por Aditya Gupta (@adi1391)

- ~~Hacking~~ Pruebas de 8==Dtración de **Dispositivos Embebidos**
- ~~Hacking~~ Pruebas de 8==Dtración del **Firmware**
- ~~Hacking~~ Pruebas de 8==Dtración de **Comunicaciones**
- ~~Hacking~~ Pruebas de 8==Dtración de **Endpoints y Web**
- ~~Hacking~~ Pruebas de 8==Dtración de **Seguridad en Radiocomunicaciones**

Pentesting IoT 101

https://github.com/fkie-cad/awesome-embedded-and-iot-security

- Herramientas de software:
  - ✓ Marcos de análisis
  - ✓ Herramientas de análisis
  - ✓ Herramientas de extracción
  - ✓ Herramientas de apoyo
  - ✓ Herramientas de hardware
- Libros
- Trabajos de investigación
- Casos de estudio
- Formaciones gratuitas
- Sitios web
- Conferencias

Pentesting IoT 101

https://github.com/nebgnahz/awesome-iot-hacks

- Vulnerabilidades encontradas en dispositivos IoT:

  - ✓ Alarmas, RFID, Automatismos, Timbres, Cafeteras, Accesorios deportivos, Enchufes, Cámaras, Señales de Tráfico, Automóviles, Aeronaves, Básculas, Candados, Bombillas, Termostatos, Frigoríficos, Multimedia y TV, Armas de fuego, Aseos, Juguetes, Drones, etc...

sicur
MUNDO HACKER

5. Conclusiones

Descubrimiento y explotación práctica de vulnerabilidades en dispositivos IoT

CS³ SECURITY SERVICES
https://cs3group.com

Conclusiones

ENISA (https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures)

- **IoT Security Standards Gap Analysis** (https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis)
- **Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures** (https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot)
- **Good Practices for Security of Internet of Things in the context of Smart Manufacturing** (https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot)

Conclusiones

Conoci

- H
  h
  olkit)
- C
  ocolos
  d
  as
  e
- **P**
- **C**
- **Estudiar, leer, documentarse y comprender el proceso**

¡Muchas gracias!