/Rootəd

Hardware hacking sobre IoT

Jesús Muñoz Martínez

MÁLAGA

10 de Diciembre de 2021

DOSSIER DE FORMACIÓN

/Rooted

Día 10 de Diciembre de 2021

Ponencias presentadas por speakers internacionales y expertos técnicos.

E.T.S. de Ingeniería Informática de Málaga
Bulevar Louis Pasteur, 35.
Campus de Teatinos. 29071 Málaga

Presentación

- **Misión**: queremos compartir conocimientos, atraer diferentes culturas, exponer el talento local y marcar la diferencia.
- **Visión**: ser responsables haciendo algo diferente, compartiendo cultura y construyendo una red de conocimiento. Ser un evento honesto, confiable, beneficioso y establecer alianzas y colaboraciones con socios, clientes y competidores.
- **Nuestra cultura ganadora y nuestros valores en vivo:** colaboración, diversidad, talento por todas partes, pasión, calidad y enfoque en los clientes (cada persona que asiste a nuestros congresos).

Objetivos

- Acercar con un enfoque práctico al análisis de seguridad de dispositivos IoT y su arquitectura (Internet of Things)
- Analizar la arquitectura de un dispositivo IoT, desde los circuitos integrados principales hasta los interfaces de comunicación, como UART, SPI y los protocolos de radio, como BLE o ZigBee
- Evaluación física del dispositivo, identificación de CI, acceder a la PCB e identificar sus interfaces
- Realizar un modelado de amenazas de un dispositivo de IoT comercial y evaluar todos los posibles puntos de entrada y vectores de ataque
- Utilizar ingeniería inversa sobre el firmware para identificar problemas de seguridad
- Detectar, capturar y explotar protocolos de comunicación por radio, como WiFi, Bluetooth Low Energy (BLE) y ZigBee.

A quién va dirigido

- Profesionales del sector de la Seguridad de la Información como son pentesters, consultores, auditores, que desean pasar a un rol de seguridad de Internet de las cosas u orientados a la evaluación de producto
- Estudiantes
- Desarrolladores de dispositivos e integradores
- Docentes
- Cualquiera que este interesado en aprender sobre la seguridad IoT y profundizar en el desarrollo de técnicas de hardware hacking

Profesor: Jesús Muñoz Martínez

Jesús Muñoz Martínez es Ingeniero Electrónico, con estudios en Ingeniería Técnica de Telecomunicación especialidad Sistemas electrónicos, graduado en Ingeniería Electrónica Industrial y con el Master de Sistemas Electrónicos para Entornos Inteligentes, estudios que realizó en la Universidad de Málaga.

Jesús ha trabajado durante años en el desarrollo de soluciones basadas en dispositivos electrónicos y diferentes tecnologías de redes. En estos proyectos se encontraba a menudo con la necesidad de utilizar y/o desarrollar técnicas de hacking para activar funciones en determinados productos, como es el caso de conocidos routers donde encontró vulnerabilidades que le permitieron el acceso y control del dispositivo así como creación de herramientas para añadir funcionalidades a sus firmwares, además de securizarlo.

Tras varios años trabajando en proyectos de ingeniería y desarrollando su afición por la ciberseguridad, finalmente entró a trabajar en el departamento de Ciberseguridad de DEKRA Testing and Certification, multinacional del sector TIC (Testing, Inspection and Cetification) especializada en certificación de productos de consumo, industriales, automoción y TIC, así como dispositivos médicos y productos utilizados en atmósferas explosivas a nivel global.

Actualmente, Jesús lidera el laboratorio de Hardware Hacking de Ciberseguridad de DEKRA donde se realizan las evaluaciones de producto y pentesting en los mercados de Automoción, IoT, Industrial, entre otros, además da soporte a otras evaluaciones de ciberseguridad de producto como son las certificaciones: Amazon AVS, CTIA, IoXt, entre otras.

En la parte de I+D+I en este laboratorio, se trabaja en ataques avanzados de hardware como fault injection, side channel attacks, IC decapsulation, chip-off, bypass anti-tamper Mechanisms entre otros.

Requisitos: Conocimientos

Al tratarse de un taller de iniciación no se requieren conocimientos previos, aunque se recomiendan conocimientos básicos de electrónica, redes y saber manejarse con fluidez tanto en entornos de Linux y Windows.

El docente en todo momento dará soporte con explicaciones claras y concisas.

Requisitos: Técnicos

Requisitos técnicos:

- ✓ Se necesita una maquina con el sistema operativo Windows y Linux (recomendamos Kali) para hacer funcionar las herramientas que puedan utilizarse. Se pueden utilizar una máquina virtual para el sistema operativo invitado. Un ordenador con al menos las siguientes características es recomendado
- ✓ CPU DualCore
- ✓ 6 GB de memoria RAM
- ✓ Espacio en disco suficiente como para crear la máquina virtual.
- ✓ Tener instalado VirtualBox o VMWare para correr la máquina virtual.

Contenido

- Introducción.
- Conocimientos necesarios y recomendados.
- Metodología Hardware Hacking.
- Técnicas de reconocimiento de hardware electrónico.
- Identificación de buses e interfaces, depuración y explotación, UART, JTAG, I2C, SPI ...
- Extracción de firmware, memorias, SPI, NAND, eMMC...
- Radio Hacking, Wi-Fi, BLE, Ziigbee, LTE ...
- Otras aplicaciones

Agenda (i)

- 3h. Clase magistral con contenido audiovisual y ejercicios realizados por el profesor sobre dispositivos reales.
- 1h. Práctica guiada. Análisis y extracción de firmware por un interfaz de depuración de un dispositivo IoT.
- Nota: Realizaremos un descanso de 15-30 minutos a mitad del taller.

Costes

- El precio final del Lab será de 95,90€.
- INCLUYE MATERIAL valorado en 30€ .

IMPORTANTE: Se requiere un mínimo de **DOCE (12)** asistentes para que el Lab pueda llevarse a cabo.

FAQ

- Dónde se celebra la formación?
  - Las formaciones se celebran en la E.T.S. de Ingeniería Informática de Málaga Bulevar Louis Pasteur, 35. Campus de Teatinos. 29071 Málaga.
- Qué horario tiene la formación?
  - La formación comienza a las 9:00de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado.
  - Las formaciones acaban a las 18:00h
- Como puedo registrarme?
  - Para el registro, ve directamente al RootedManager. Ahí, una vez registrado podrás seleccionar la formación y pagar directamente. Una vez se imparta la formación podrás solicitar la factura siguiendo los pasos indicados en el Portal.
- El training incluye comida?
  - Los training no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rootəd

Contacto: info@rootedcon.com