Charla de Seguridad Digital para el Mundo Maker

"Entender los riesgos para protegerse sin paranoia"

[DrYouu]

Contents

1 Introducción: Tecnología y Seguridad en el Mundo Maker

Vivimos en la era dorada del acceso a la tecnología. La comunidad maker puede hoy fabricar, programar, automatizar y construir sistemas con herramientas que antes sólo poseían gobiernos o grandes corporaciones. Pero esa accesibilidad también tiene una contrapartida: el riesgo.

La seguridad digital ya no es algo exclusivo del mundo informático. Muchas amenazas digitales tienen consecuencias directas en el mundo físico: puertas que se abren, alarmas que se desactivan, dispositivos que actúan sin nuestra intervención.

El objetivo de esta charla es:

- Mostrar de forma práctica cómo se explotan vulnerabilidades físicas y digitales.
- Enseñar cómo protegerse de forma realista, evitando la paranoia.
- Reflexionar sobre la ética del uso de herramientas de pentesting.

2 El Flipper Zero: El Cuchillo Suizo del Pentesting Personal

2.1 ¿Qué es el Flipper Zero?

Un dispositivo multifunción portátil, diseñado para investigación de seguridad pero popularizado masivamente.

- Compacto, con interfaz intuitiva.
- Permite interactuar con protocolos muy utilizados en el día a día.

2.2 Funciones principales

- **Sub-GHz (300-928 MHz):** captura, análisis y retransmisión de señales de mandos de garaje, persianas, alarmas.
- **RFID (125 KHz y 13.56 MHz):** lectura, clonación y emulación de tarjetas de acceso.
- **Infrared (IR):** replicación de controles remotos.
- **USB HID:** simulación de teclado para ataques tipo BadUSB.
- **GPIO:** control de hardware externo.
- **Bluetooth BLE:** escaneo e interacción con dispositivos cercanos.

2.3 Add-ons y expansión

- Wi-Fi Devboard (exploración de redes Wi-Fi)
- Antenas externas (amplificación Sub-GHz)
- Firmwares modificados (RogueMaster, Unleashed, etc.)

3 Desde el punto de vista de la víctima

- **Acceso físico no autorizado:** clonación de tarjetas de hotel, oficinas, gimnasios.
- **Interferencia remota:** apertura de garajes, desactivación de alarmas.
- **Ataques BadUSB:** ejecución de comandos automatizados en segundos.
- **Explotación BLE:** análisis de dispositivos cercanos.

4 Amenazas Digitales con Impacto en el Mundo Físico

- Cerraduras electrónicas vulnerables.
- Portones y barreras sin rolling-code.
- Sistemas DIY caseros sin protección básica.
- Dispositivos IOT sin cifrado.

5 Hackeo Social: Atacar a la Persona

5.1 Ingeniería social aplicada al mundo maker

- Ganar confianza mediante conocimiento técnico aparente.
- Observar rutinas y hábitos.
- Manipular al usuario para obtener claves o acceso físico.

5.2 Ataques combinados

- Evil Twin Wi-Fi en eventos makers.
- USB drop attacks (dejar dispositivos USB preparados para ser recogidos).
- Escucha pasiva de frecuencias abiertas.

6 Cómo Protegerse sin Paranoia

6.1 Prácticas físicas

- Fundas Faraday para tarjetas.
- Bloqueadores físicos de señales.
- Desactivación de llaves digitales cuando no se usan.

6.2 Prácticas digitales

- Actualización constante de firmware.
- Contraseñas robustas y autenticación múltiple.
- No conectar dispositivos USB de origen dudoso.

7 Ética Hacker y Cultura del Pentesting

- Un hacker no es un criminal.
- Divulgación responsable: reportar vulnerabilidades.
- No explotar debilidades fuera de entornos controlados o con víctimas no consentidas.

8 Comparativa de Dispositivos de Pentesting

Dispositivo	**Precio (€)**	**Dificultad**	**Riesgo ético**
Flipper Zero	150-250	Media	Alto
Rubber Ducky	50-100	Baja	Alto
Wi-Fi Pineapple	200-300	Alta	Alto
LAN Turtle	100-150	Media	Medio
Bash Bunny	120-200	Media	Alto
ESP32 devkits	5-20	Alta	Variable

9 Casos Prácticos y Escenificaciones con Actores

Escenificación 1: El Hotel Comprometido

Personajes: Víctima, Atacante, Narrador.

Narrador: *La víctima desayuna tranquilamente en el hotel. La tarjeta de su habitación está expuesta en la mesa.*

Atacante (pasa disimuladamente cerca): *(Simula escanear la tarjeta con el Flipper Zero)*

Narrador: *La tarjeta ha sido clonada en segundos.*

Mensaje clave: Cuidado con tarjetas RFID LF expuestas; existen fundas protectoras económicas.

Escenificación 2: Apertura de Garaje

Personajes: Propietario, Atacante, Narrador.

Propietario: *(Abre el garaje con su mando habitual.)*

Atacante (a distancia, graba la señal): *(Captura la señal Sub-GHz.)*

Narrador: *El atacante ha grabado la señal fija y ahora puede abrir el garaje sin necesidad de fuerza.*

Mensaje clave: Si el mando no usa rolling-code, es trivial de clonar.

Escenificación 3: El USB Malicioso

Personajes: Víctima, Atacante, Narrador.

Narrador: *Un pendrive encontrado en un taller maker. Curioso, alguien lo conecta a su portátil.*

Víctima: *(Conecta el pendrive.)*

Atacante (por BadUSB): *(El Flipper Zero simula teclado y ejecuta comandos automáticamente.)*

Mensaje clave: No conectar dispositivos USB desconocidos.

Escenificación 4: Evil Twin Wi-Fi

Personajes: Público del evento.

Narrador: *Durante el evento hay un Wi-Fi gratuito disponible: "MakerFest_Free".*

Narrador: *El atacante monta una copia exacta de la red con el mismo nombre y señal más potente.*

Público (algunos se conectan a la red falsa):

Narrador: *El atacante intercepta tráfico y credenciales de quienes cayeron en la trampa.*

Mensaje clave: Usar VPN en redes abiertas; comprobar autenticidad de puntos Wi-Fi.

Escenificación 5: Hackeo Social en evento

Narrador: *Un asistente simpático empieza a conversar con otros participantes. Pregunta sobre los dispositivos que traen, sus credenciales, cómo han configurado sus sistemas...*

Atacante: *(Obtiene datos personales y técnicos valiosos sin necesidad de tecnología, sólo por conversación.)*

Mensaje clave: La ingeniería social es la herramienta más potente. Cuidado con lo que compartimos por simple simpatía.

10 Demostraciones Reales sobre el Público

- Se realizarán demostraciones controladas sobre asistentes previamente avisados.
- Se explicarán los pasos exactos del ataque para que todos puedan aprender.
- El público podrá comprobar en directo los riesgos expuestos.

11 Sorteo de Premios: Hackeados Premiados

- Aquellos que hayan sido "hackeados" durante las pruebas prácticas participarán en un sorteo de premios.
- Premios: fundas Faraday, protectores RFID, dispositivos de aprendizaje maker.

12 Cierre y Reflexión Final

- Todo conocimiento técnico implica responsabilidad.
- Conocer las vulnerabilidades permite protegerse mejor.
- La seguridad es un hábito, no un estado.
- La paranoia es tan inútil como la ignorancia: equilibrio y criterio.

13 Recursos Adicionales y Bibliografía

- *Hacking: The Art of Exploitation* - Jon Erickson
- *The Hacker Playbook* - Peter Kim
- Plataformas: Hack The Box, TryHackMe, Root Me
- Foros: Hackaday, Reddit r/flipperzero, DEFCON, CCC