TARLOGIC
CYBERSECURITY EXPERTS

BSAM, SEGURIDAD EN BLUETOOTH

2024

TARLOGIC
CYBERSECURITY EXPERTS

BSAM, SEGURIDAD EN BLUETOOTH 2024

TARLOGIC
CYBERSECURITY EXPERTS

$ WHOAMI

Jesús M. Gómez Moreno

Research Engineer @ Tarlogic Security

@zus@masto.es

Jesus.Gomez@Tarlogic.com

TARLOGIC
CYBERSECURITY EXPERTS

$ WHOAMI

Antonio Vázquez Blanco

Research Engineer @ Tarlogic Security

@antoniovazquezblanco@mastodon.social

Antonio.Vazquez@Tarlogic.com

TARLOGIC
CYBERSECURITY EXPERTS

01 SEGURIDAD Y AUDITORÍAS BLUETOOTH

- BLUETOOTH
- AUDITORÍAS BLUETOOTH

BLUETOOTH

- CEPILLOS DE DIENTES
- BÁSCULAS
- ZAPATILLAS
- CINTURONES
- TENEDORES
- CUCHARAS

BLUETOOTH

- TECLADOS Y RATONES
- AURICULARES
- TELÉFONOS
- CERRADURAS
- MARCAPASOS

AUDITORÍAS BLUETOOTH

DOCUMENTACIÓN DEMASIADO COMPLEJA

INFORMACIÓN SOBRE AUDITORÍAS DISPERSA O INCOMPLETA

HERRAMIENTAS POCO MANTENIDAS Y DOCUMENTADAS

IMPLEMENTACIONES SUTILMENTE DISTINTAS

AUDITORÍAS BLUETOOTH

- CRITERIOS DE EVALUACIÓN INCONSISTENTES
- EVALUACIONES INCOMPLETAS
- FALSOS POSITIVOS Y/O FALSOS NEGATIVOS
- RESULTADOS DIFÍCILES DE REPLICAR
- RESULTADOS NO EXTRAPOLABLES A OTROS DISPOSITIVOS O ESCENARIOS

TARLOGIC
CYBERSECURITY EXPERTS

02

BSAM

Bluetooth security assessment methodology

- BSAM
- CONCLUSIONES

BSAM

GUÍA COMPLETA

EJEMPLOS DE USO

ABIERTA Y COLABORATIVA

CONTROLES DE SEGURIDAD

RECURSOS DE APOYO

RESULTADO

- Evaluación integral
- Controles consistentes
- Criterios de evaluación uniformes
- Auditorías comparables y repetibles
- Herramientas y documentación

BSAM

01

RECOPILACIÓN DE INFORMACIÓN

02

DESCUBRIMIENTO

03

EMPAREJAMIENTO

04

AUTENTICACIÓN

05

CIFRADO

06

SERVICIOS

07

APLICACIÓN

BSAM

01 RECOPILACIÓN DE INFORMACIÓN

FASE PREVIA AL ANÁLISIS DEL DISPOSITIVO

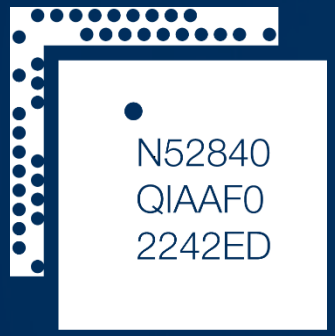
CONSISTE EN:

- Reconocimiento básico
- Búsqueda de información pública
- Búsqueda de vulnerabilidades conocidas

BSAM

01 RECOPILACIÓN DE INFORMACIÓN

01



IDENTIFICACIÓN DEL CONTROLADOR BLUETOOTH

02

Zephyr®

BlueZ

IDENTIFICACIÓN DEL SOFTWARE Y PILA BLUETOOTH

03

Bluetooth® 5.0

IDENTIFICACIÓN DE LA VERSIÓN DEL ESTÁNDAR

BSAM

01 EJEMPLO RECOPILACIÓN DE INFORMACIÓN

MI PORTABLE BLUETOOTH SPEAKER

- **SE ENCUENTRAN TEARDOWNS DEL DISPOSITIVO**
- **SE IDENTIFICA EL SOC:**
  - **FABRICANTE:** ACTIONS TECHNOLOGY
  - **SOC BLUETOOTH:** ATS2819

BSAM

01 EJEMPLO RECOPILACIÓN DE INFORMACIÓN

SOC BLUETOOTH: ATS2819

- SE ENCUENTRAN VARIOS CVE
- ES VULNERABLE A BRAKTOOTH

Name	
CVE-2021-31786	The Bluetooth Classic Audio implemer disconnection and deadlock of the de
CVE-2021-31785	The Bluetooth Classic implementation of the device via crafted LMP packets.

Extracto de cve.mitre.org

Bluetrum Technology	AB5501A	AB32VG1	Default
Zhuhai Jieli Technology	AC6925C	XY-WRBT Module	N.A
Actions Technology	ATS281X	Xiaomi MDZ-36-DB	N.A
Bluetooth 4.2			
Zhuhai Jieli Technology	AC6905X	BT Audio Receiver	N.A
Espressif Systems	ESP32	ESP-WROVER-KIT	bt_spp_acceptor
Bluetooth 4.1			

Extracto del artículo de Braktooth

BSAM

02 DESCUBRIMIENTO

VERIFICA LA SEGURIDAD DE LOS PAQUETES DE ANUNCIO

COMPRUEBA:

- Modos de operación del dispositivo
- Presencia de datos sensibles o inadecuados
- Presencia de datos que permitan el tracking

BSAM

02 EJEMPLO DESCUBRIMIENTO

PHILIPS DREAMSTATION

- DISPOSITIVO PARA USO MÉDICO Y DOMÉSTICO.
- POTENCIA DE TRANSMISIÓN BLUETOOTH MUY ELEVADA, PERMITE CONECTARSE DESDE LARGAS DISTANCIAS (EXTERIOR DE UN HOSPITAL, ETC)

BSAM

02 EJEMPLO DESCUBRIMIENTO

APPLE IPHONE

- ANUNCIA EL NOMBRE DE SU DUEÑO
- INCLUYE INFORMACIÓN DE SERVICIOS NO NECESARIA PARA SU OPERACIÓN Y QUE SON RASTREABLES

BSAM

03 EMPAREJAMIENTO

ANÁLISIS DEL ESTABLECIMIENTO DE LOS SECRETOS BLUETOOTH

COMPRUEBA:

- Emparejamiento entre dispositivos sin interacción del usuario
- Uso de métodos de emparejamiento inseguros
- Dispositivos siempre emparejables
- Eliminación de un enlace legítimo
- Almacenamiento de claves de emparejamiento

BSAM

03 EJEMPLO EMPAREJAMIENTO

XIAOMI MI BAND 5

- CUANDO SE DESCONECTA PASA AUTOMÁTICAMENTE A SER DESCUBRIBLE Y EMPAREJABLE
- ES POSIBLE EMPAREJARSE SIN QUE EL USUARIO SEA NOTIFICADO

BSAM

04 AUTENTICACIÓN

ANÁLISIS DE LA VERIFICACIÓN DE IDENTIDAD EN BLUETOOTH

COMPRUEBA:

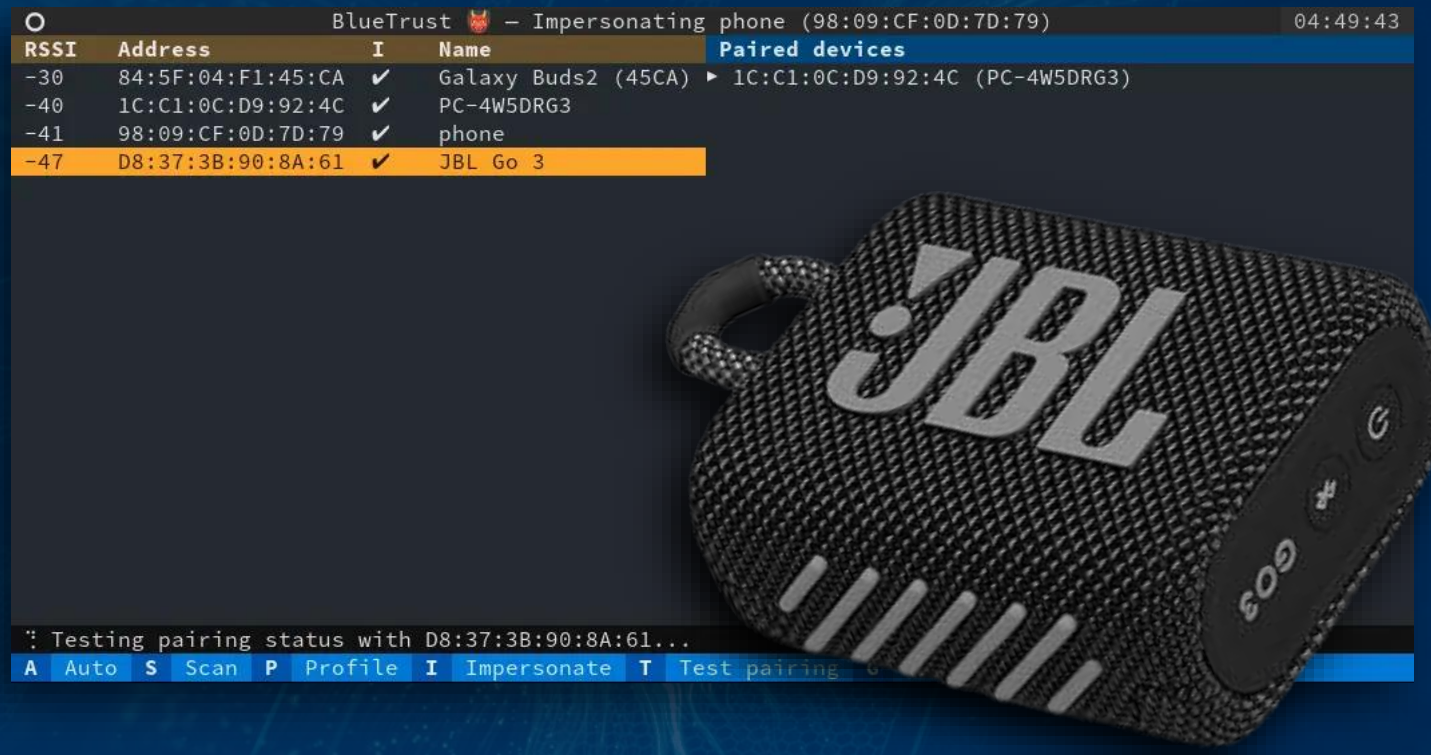
- Modalidades obsoletas o inseguras
- Los cambios de rol durante el proceso
- Uso de autenticación mutua
- Desconexión forzada de dispositivos legítimos

BSAM

04 EJEMPLO AUTENTICACIÓN

JBL GO 3

- USA MÉTODOS DE AUTENTICACIÓN INSEGUROS
- PERMITE EXTRACCIÓN DE INFORMACIÓN CON BLUETRUST



BSAM

05 CIFRADO

SE CENTRA EN EL ESTABLECIMIENTO Y EL MANTENIMIENTO DEL CIFRADO

COMPRUEBA:

- Que las comunicaciones se realizan cifradas
- Que el tamaño de la clave es adecuado
- Que no se permiten cambios de rol

BSAM

05 EJEMPLO CIFRADO

PULSIOXÍMETRO OXYSMART

- NO CIFRA LAS COMUNICACIONES
- ¡SE PUEDE OBTENER DATOS DEL PACIENTE CON UN SNIFFER BLE LOW COST!

BSAM

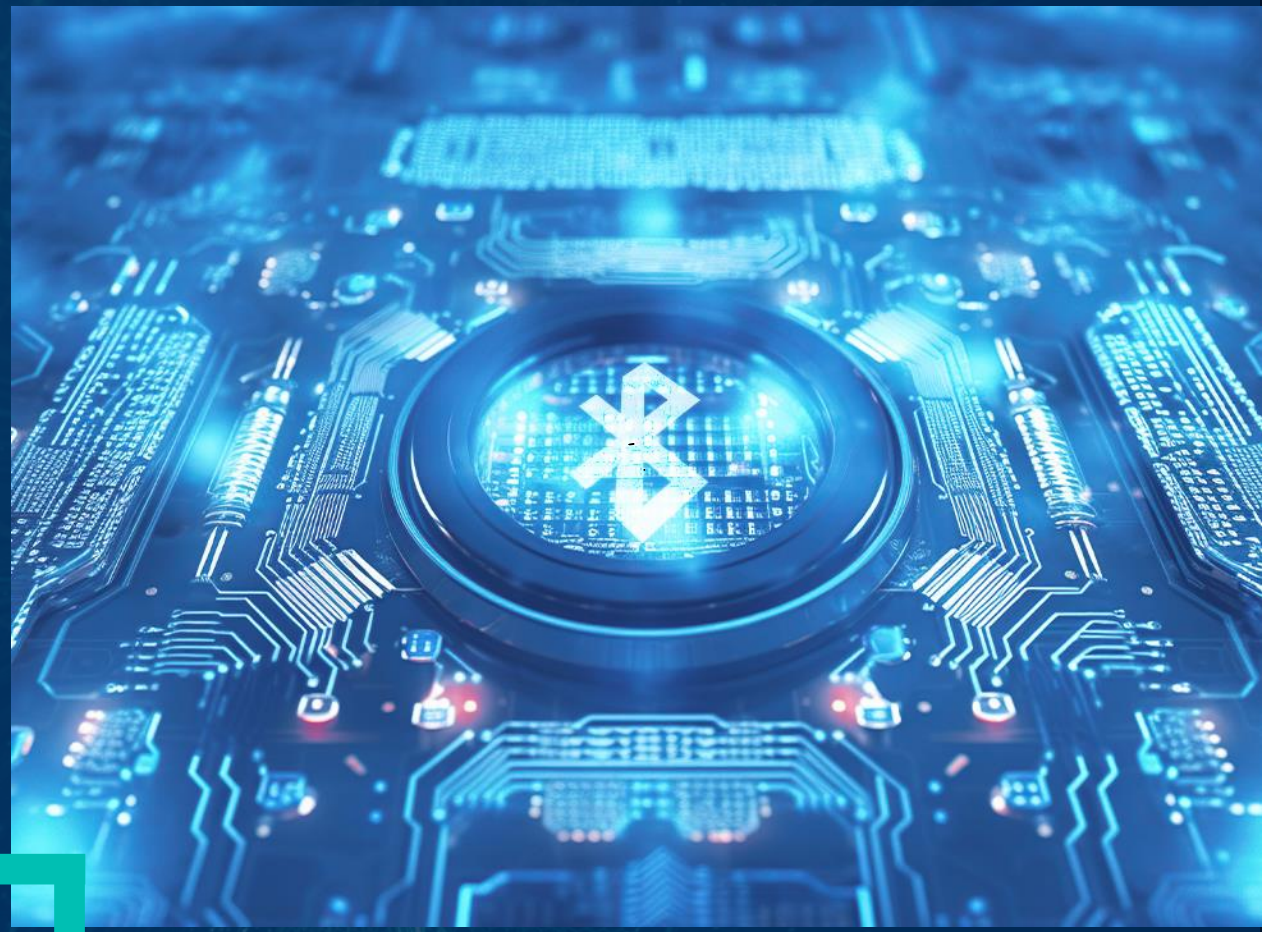
06 SERVICIOS

ANÁLISIS DE LOS SERVICIOS DE UN DISPOSITIVO:

- Classic y LE usan protocolos muy distintos
- Los servicios se pueden “descubrir”

COMPRUEBA:

- Que no existen servicios ocultos
- Que los servicios están debidamente protegidos



BSAM

06 EJEMPLO SERVICIOS

MARSHALL STANMORE II

- **LOS SERVICIOS NO ESTÁN PROTEGIDOS Y PERMITEN TODO TIPO DE INTERACCIÓN**

HANDLE	TYPE	PERM	REQ AUTH	REQ ENC	UUID	
			...			
0x0007	VALUE	R	NO	NO	00002a00-0000-1000-8000-00805f9b34fb	(Device Name)
0x000a	SERVICE	R	NO	NO	0000180a-0000-1000-8000-00805f9b34fb	(Device Information)
0x000c	VALUE	R	NO	NO	00002a24-0000-1000-8000-00805f9b34fb	(Model Number String)
0x000e	VALUE	R	NO	NO	00002a25-0000-1000-8000-00805f9b34fb	(Serial Number String)
0x001e	VALUE	R,W	NO	NO	44fa50b2-d0a3-472e-a939-d80cf17638bb	(Unknown)
0x0021	VALUE	R,W	NO	NO	4446cf5f-12f2-4c1e-afe1-b15797535ba8	(Unknown)
0x0024	VALUE	R,W	NO	NO	95c09f26-95a4-4597-a798-b8e408f5ca66	(Unknown)
0x0027	VALUE	R,W	NO	NO	d5b5e4c2-d2a7-4eec-a2d0-6225033a4caf	(Unknown)
0x002a	VALUE	R,W	NO	NO	fa302d24-d775-4343-b9ed-8cc68ace3284	(Unknown)
0x002d	VALUE	R,W	NO	NO	3ba91c2e-8b08-4c27-9d4e-4936a793fcfb	(Unknown)
			...			

BSAM

07 APLICACIÓN

UNA APLICACIÓN DEBE IMPLEMENTAR ADECUADAMENTE BLUETOOTH

COMPRUEBA:

- Seguridad de las actualizaciones
- Protección contra ataques de replay
- Protección contra la manipulación de paquetes
- Validación de datos de entrada
- Implementaciones seguras

BSAM

07 EJEMPLO APLICACIÓN

LECTOR DE TARJETAS RFID

- **APLICACIÓN VULNERABLE A INYECCIÓN DE COMANDOS**
  - **TX:** “ 1>/dev/null;id #
  - **RX:** uid=0(root) gid=0(root) groups=0(root)

https://www.tarlogic.com/es/blog/analizando-un-escaner-rfid/

CONTRIBUCIONES

DURANTE EL DESARROLLO DE BSAM SE HA CONTRIBUIDO EN:

01

WIRESHARK

BUGFIXES EN “HCI_USB”
IMPLEMENTACIÓN DE PAQUETES “VENDOR_HCI”

02

SCAPY

IMPLEMENTACIÓN DE PAQUETES DEL ESTÁNDAR Y SOCKETS BLUETOOTH

03

NUEVAS HERRAMIENTAS Y PRUEBAS DE CONCEPTO

CONCLUSIONES

- BSAM ES LIBRE, OPEN SOURCE Y COLABORATIVA,
- NOS PROPORCIONA:

01

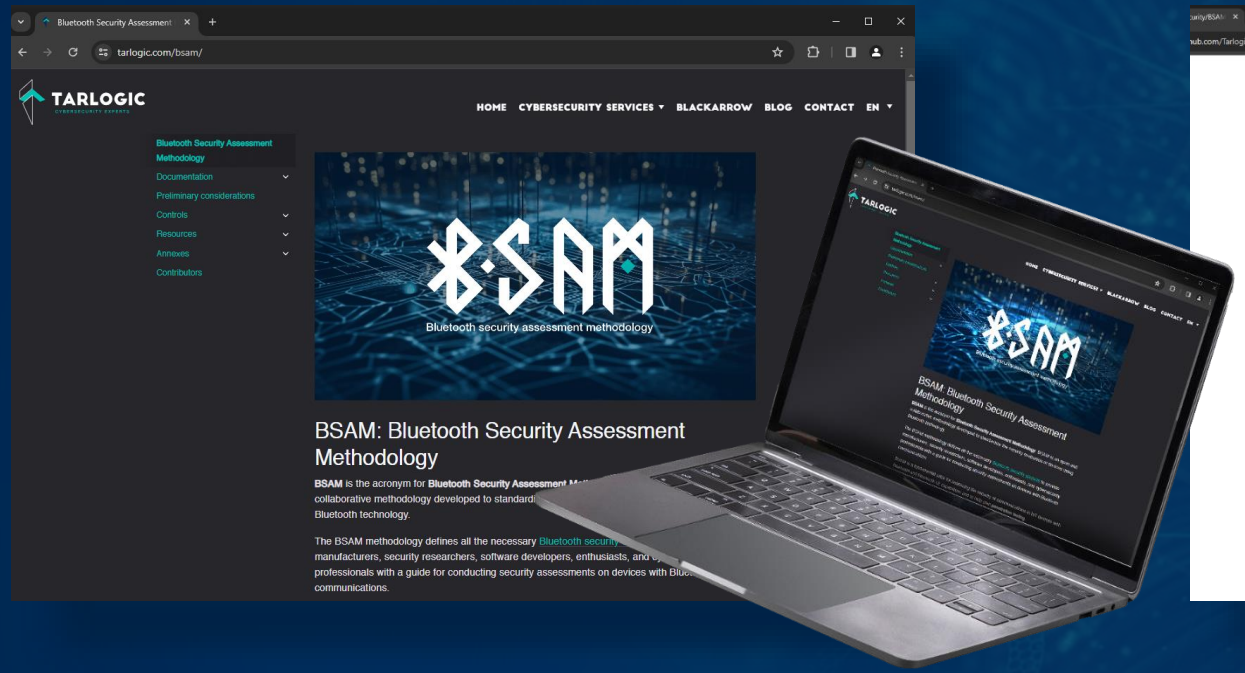
UNA GUÍA DE CONTROLES A SEGUIR DURANTE UNA AUDITORÍA

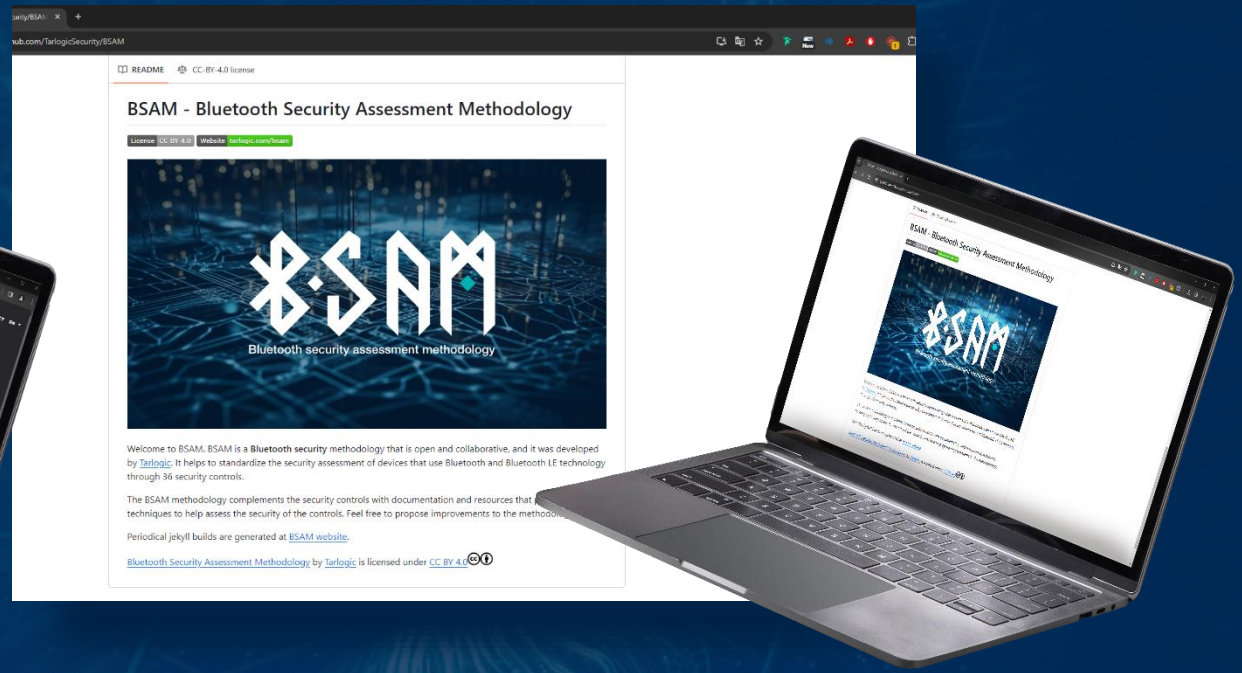
02

UN CRITERIO UNIFICADO PARA EVALUAR LA SEGURIDAD EN BLUETOOTH

03

RECURSOS DE APOYO PARA LA REALIZACIÓN DE PRUEBAS Y VALIDACIONES





https://www.tarlogic.com/bsam/

https://github.com/TarlogicSecurity/BSAM

TARLOGIC
CYBERSECURITY EXPERTS

03 | DEMO

```
dummy@arch ~/code/rooted2024_poc (git)-[master] %
```

TARLOGIC
CYBERSECURITY EXPERTS

¡GRACIAS POR TU ATENCIÓN!

contacto@tarlogic.com

www.tarlogic.com
+34 912 919 319