



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

GUÍA METODOLÓGICA PARA EL CONTROL DE VULNERABILIDADES INFORMÁTICAS EN DISPOSITIVOS IOT (INTERNET OF THE THINGS) PARA REDES HAN (HOME AREA NETWORK).

DAVID RODRIGO MENA GALARZA

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

Riobamba - Ecuador

Marzo- 2021

©2021, DAVID RODRIGO MENA GALARZA Se autoriza la reproducción total o parcial, con fines académicos por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.



CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado “Guía metodológica para el control de vulnerabilidades informáticas en dispositivos IOT (Internet of the Things) para redes HAN (Home Area Network)”, de responsabilidad del señor David Rodrigo Mena Galarza, ha sido minuciosamente revisado y se autoriza su presentación.

FIRMA

Ph.D. Luis Eduardo Hidalgo Almeida

DIRECTOR DE LA IPEC

Ing. Hugo Oswaldo Moreno Avilés PhD

DIRECTOR DE TESIS

Ing. Edwin Vinicio Altamirano
Santillán MsC

MIEMBRO DEL TRIBUNAL

Ing. Andrés Santiago Cisneros Barahona MsC.

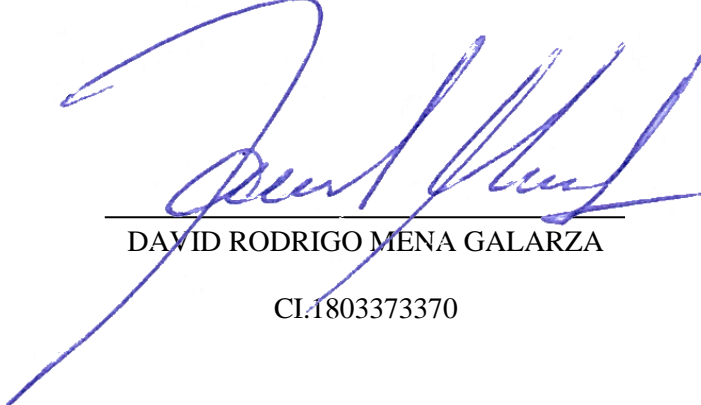
MIEMBRO DEL TRIBUNAL

EDWIN VINICIO ALTAMIRANO SANTILLAN
Firmado digitalmente por
EDWIN VINICIO
ALTAMIRANO SANTILLAN
Fecha: 2021.04.23 11:22:41
-05'00'

Riobamba, Abril 2021

DERECHOS INTELECTUALES

Yo, DAVID RODRIGO MENA GALARZA, declaro que soy responsable de las ideas y resultados expuestos en la presente Trabajo de Investigación, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.



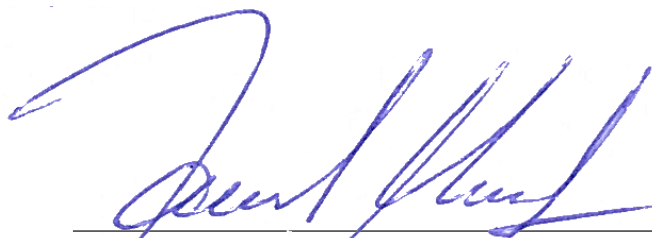
DAVID RODRIGO MENA GALARZA

CI.1803373370

Yo, DAVID RODRIGO MENA GALARZA, declaro que el presente Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, 22 de marzo del 2021



DAVID RODRIGO MENA GALARZA

180337337-0

DEDICATORIA

El esfuerzo del presente trabajo, se lo dedico a mi familia, por ser el apoyo incondicional para mi superación.

David

AGRADECIMIENTO

Mi agradecimiento a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, FACULTAD DE INFORMÁTICA Y ELECTRÓNICA, por darme la oportunidad de especializarme como un profesional de calidad.

También agradezco al Ing. Hugo Moreno. PHD, por su invaluable apoyo a la culminación del presente trabajo.

David

TABLA DE CONTENIDOS

RESUMEN	xviii
SUMMARY.....	xix

CAPÍTULO I

INTRODUCCIÓN	1
1. PROBLEMA DE INVESTIGACIÓN.....	1
1.1. Planteamiento del problema	1
1.2. Formulación del problema.....	4
1.3. Sistematización del problema	4
1.4. Justificación de la investigación	5
1.5. Objetivos de la investigación.....	6
1.5.1. <i>Objetivo general</i>	6
1.5.2. <i>Objetivos específicos</i>	7
1.6. Hipótesis	7

CAPÍTULO II

2. MARCO DE REFERENCIAL	8
2.1. Antecedentes del problema	8
2.2. Bases teóricas	9
2.2.1. <i>Seguridad informática</i>	9
2.2.2. <i>Objetivos de la seguridad informática</i>	9
2.2.3. <i>Vulnerabilidad</i>	9
2.2.3.1. <i>Impacto de la vulnerabilidad</i>	9
2.2.4. <i>Riesgo asociado con las aplicaciones web</i>	10
2.2.4.1. <i>Vulnerabilidades más comunes</i>	11
2.2.5. <i>Forma de ataque (vector)</i>	12
2.2.5.1. <i>Otros vectores de ataque</i>	12
2.2.6. <i>CVE (Common Vulnerabilities and Exposures)</i>	13
2.2.6.1. <i>CVE-2011-1234</i>	13
2.2.6.2. <i>CVSS (Common Vulnerability Scoring System)</i>	14
2.2.6.3. <i>Puntuación de una vulnerabilidad</i>	14
2.2.6.4. <i>CVRF (Common Vulnerability Reporting Framework)</i>	15

2.2.6.5.	<i>Parches y actualizaciones</i>	15
2.2.6.6.	<i>Internet de las cosas (IOT)</i>	16
2.2.7.	Vulnerabilidades en el Internet de las cosas	19
2.2.7.1.	<i>Interfaces web inseguras</i>	19
2.2.7.2.	<i>Autenticación/autorización insuficiente</i>	19
2.2.7.3.	<i>Servicios de red inseguros</i>	20
2.2.7.4.	<i>Carencia de cifrado de transporte</i>	20
2.2.7.5.	<i>Preocupación por la privacidad</i>	20
2.2.7.6.	<i>Interfaz en la nube insegura</i>	21
2.2.7.7.	<i>Interfaz móvil insegura</i>	22
2.2.7.8.	<i>Insuficiente configuración de seguridad</i>	22
2.2.7.9.	<i>Software/Firmware inseguro</i>	23
2.2.7.10.	<i>Pobre seguridad física</i>	23
2.2.8.	Gestión de la información	25
2.2.8.1.	<i>Impacto del IOT sobre las personas</i>	25
2.3.	Optimización	26
2.3.1.	<i>Elección de estándares</i>	26
2.3.2.	<i>Una visión de IOT</i>	26
2.3.2.1.	<i>Discusión de la IOT</i>	27
2.3.2.2.	<i>La tecnología IOT</i>	28
2.4.	Tendencias tecnológicas	28
2.4.1.	<i>Aplicaciones de IOT</i>	28
2.4.2.	<i>Entidades inteligentes</i>	29
2.4.2.1.	<i>Habilitadores de tecnología en iot</i>	30
2.5.	Tecnologías semánticas e IOT	31
2.5.1.	<i>Aplicaciones de la IOT</i>	32
2.5.1.1.	<i>Modelado y diseño</i>	33
2.5.1.2.	<i>Validación e interoperabilidad</i>	33
2.5.1.3.	<i>Estándares</i>	33
2.6.	OSSTMM, Manual de la metodología abierta de testeo de seguridad	34
2.6.1.	<i>Estructura</i>	34
2.6.1.1.	<i>Seguridad de la información</i>	35
2.6.1.2.	<i>Seguridad de los procesos</i>	35
2.6.1.3.	<i>Seguridad de las tecnologías de Internet</i>	35
2.6.1.4.	<i>Seguridad en las comunicaciones</i>	36
2.6.1.5.	<i>Seguridad inalámbrica</i>	36

2.6.1.6.	<i>Seguridad física</i>	36
----------	-------------------------------	----

CAPÍTULO III

3.	METODOLOGÍA DE LA INVESTIGACIÓN	37
3.1.	Tipo y diseño del estudio	37
3.1.1.	<i>Investigación teórica</i>	37
3.1.2.	<i>Investigación experimental</i>	37
3.1.3.	<i>Investigación tecnológica</i>	38
3.2.	Método de investigación	38
3.2.1.	<i>Investigación correlacional</i>	39
3.2.1.1.	<i>Operacionalización de variables</i>	40
3.3.	Pruebas de vulnerabilidad Bluetooth	42
3.3.1.	<i>Elementos de laboratorio</i>	42
3.3.1.1.	<i>Equipo y dispositivos de pruebas</i>	42
3.3.1.2.	<i>Dispositivos IoT de prueba</i>	43
3.3.2.	<i>Raspberry pi</i>	45
3.3.2.1.	<i>Raspberry Pi 2 Model B</i>	45
3.3.2.2.	<i>Ubetooth one</i>	46
3.3.3.	<i>Implementación del equipamiento para pruebas de laboratorio</i>	48
3.3.3.1.	<i>Preparación del Raspberry Pi y Ubetooth one</i>	48
3.3.3.2.	<i>Sniffer cc2540</i>	48
3.3.3.3.	<i>SmartRF packet sniffer</i>	49
3.3.3.4.	<i>Bluehydra</i>	50
3.3.3.5.	<i>Btscanner</i>	51
3.3.3.6.	<i>Crackle</i>	52
3.4.	Pruebas de vulnerabilidad radiofrecuencia (RF)	52
3.4.1.	<i>Elementos de laboratorio de pruebas</i>	54
3.4.1.1.	<i>Equipos y dispositivos de pruebas</i>	54
3.4.1.2.	<i>Detección de dispositivos RF en el hogar</i>	55
3.4.1.3.	<i>Uso del Rtl-sdr software</i>	55
3.4.1.4.	<i>Instalación de Apache y Php</i>	57
3.4.1.5.	<i>Conexión de del módulo TX/RX 433mhz</i>	57
3.4.1.6.	<i>Rfsniffer</i>	59
3.5.	Pruebas de vulnerabilidad Zigbee	59
3.5.1.	<i>Equipos y dispositivos de pruebas</i>	59
3.5.2.	<i>Construcción de un kit de pruebas killerbee</i>	61

3.6.	Alcance de la investigación	65
3.6.1.	<i>Población de estudio</i>	65
3.6.2.	<i>Unidad de análisis</i>	66
3.6.3.	<i>Encuesta</i>	67
3.6.4.	<i>Observación</i>	67
3.6.5.	<i>Instrumentos de recolección de datos</i>	68
3.6.6.	<i>Instrumento para procesar datos recopilados</i>	68
3.6.7.	<i>Validación de la información</i>	68
3.6.8.	<i>Frecuencias observadas</i>	90

CAPÍTULO IV

4.	RESULTADOS Y DISCUSIÓN	95
4.1.	Elementos de prueba para controlar la vulnerabilidad	95
4.1.1.	<i>Reconocimiento de dispositivos bluetooth clásico</i>	95
4.1.1.1.	<i>Hcitol</i>	95
4.1.1.2.	<i>Btscanner</i>	97
4.1.2.	Descubrimiento pasivo	100
4.1.2.1.	<i>Ubetooth</i>	100
4.1.2.2.	<i>Reconocimiento de dispositivos Bluetooth Low Energy</i>	103
4.1.2.3.	<i>Blue Hydra</i>	104
4.1.2.4.	<i>Análisis de Trafico Bluetooth (Eavesdropping)</i>	105
4.1.3.	<i>Eavesdroppinge en Bluetooth Low Energy</i>	107
4.1.3.1.	<i>Captura de datos con Ubetooth one</i>	108
4.1.4.	<i>Análisis mediante Wireshark</i>	110
4.1.5.	<i>Análisis mediante SmartRF</i>	111
4.1.6.	<i>Ataques Bluetooth</i>	112
4.1.7.	<i>Bluetooth Low Level</i>	113
4.1.7.1.	<i>Crackle</i>	113
4.1.8.	<i>Ataque de Re-Emparejamiento</i>	115
4.1.8.1.	<i>Bdaddr</i>	115
4.2.	Reconocimiento de dispositivos RF	118
4.2.1.	<i>Ataque mediante el uso de Rfsniffer</i>	119
4.3.	Reconocimiento de redes Zigbee	122
4.3.1.	<i>Ataque Zigbee</i>	124

CAPÍTULO V

5.	Guía metodológica para el control de vulnerabilidades de dispositivos IoT en redes	
	HAN	126
5.1	<i>¿Qué es el Internet de las cosas (IoT)?</i>	126
5.1.1.	<i>Aseguramiento de las cosas en Internet</i>	127
5.1.2.	<i>Recomendaciones de seguridad para dispositivos IoT en el hogar</i>	128
5.1.2.1.	<i>Conocer que dispositivos poseo en el hogar</i>	128
5.1.2.2.	<i>Utilización de interfaces web y aplicaciones seguras</i>	128
5.1.2.3.	<i>Cambiar las contraseñas por defecto</i>	129
5.1.2.4.	<i>Aplicar configuraciones de seguridad</i>	130
5.1.2.5.	<i>Mantener los dispositivos IoT actualizados</i>	131
5.1.2.6.	<i>Proteger físicamente los dispositivos IoT</i>	132
5.1.2.7.	<i>Utilizar dispositivos y software de seguridad</i>	132
5.1.2.8.	<i>Asegurar las redes de comunicación de los dispositivos IoT</i>	133
5.1.3.	<i>Cuadro resumen de resultados</i>	150
	CONCLUSIONES	151
	RECOMENDACIONES	154
	BIBLIOGRAFÍA	
	ANEXOS	

ÍNDICE DE TABLAS

Tabla 1-2:	Aplicaciones IoT	17
Tabla 2-2:	Habilitadores IoT	30
Tabla 1-3:	Variable Independiente – Vulnerabilidades	40
Tabla 2-3:	Variable Dependiente – Seguridad en Dispositivos IoT	41
Tabla 3-3:	Calculo Muestra	67
Tabla 4-3:	Cyber Ataques.....	69
Tabla 5-3:	Conocimiento de riesgos.....	70
Tabla 6-3:	Enfrentamiento del peligro.....	71
Tabla 7-3:	Minimizar vulnerabilidades	72
Tabla 8-3:	Riesgos de no tener protección	73
Tabla 9-3:	Enfrentado el peligro.....	74
Tabla 10-3:	Elemento para existencia de control.....	75
Tabla 11-3:	Conocimiento de no tener protección.....	76
Tabla 12-3:	Manera de enfrentar el riesgo.....	77
Tabla 13-3:	Protección en el sistema informático	78
Tabla 14-3:	Cuenta con una protección.....	79
Tabla 15-3:	Acceder al control de la vulnerabilidad.....	80
Tabla 16-3:	Como implementar controles de seguridad.....	81
Tabla 17-3:	Conoce acerca de IoT.....	82
Tabla 18-3:	Dispositivos IOT	83
Tabla 19-3:	Dispositivos seguros.....	84
Tabla 20-3:	Información personal	85
Tabla 21-3:	Datos seguros	86
Tabla 22-3:	IOT comportamiento.....	87
Tabla 23-3:	Medidas de seguridad.....	88
Tabla 24-3:	Factor para establecer seguridades.....	89
Tabla 25-3:	Pregunta Variable Independiente	90
Tabla 26-3:	Pregunta Variable Dependiente.....	90
Tabla 27-3:	Grados de libertad	92
Tabla 28-3:	Frecuencias Esperadas	92
Tabla 29-3:	Tabla de contingencia	93
Tabla 30-3:	Datos Decisión	93
Tabla 1-4:	Resultados Hcitol.....	102
Tabla 1-5:	Cuadro resumen de resultados	150

ÍNDICE DE FIGURAS

Figura 1-1:	Cambio Tecnológico.....	2
Figura 2-1:	Redes y Ciudades Inteligentes	3
Figura 3-1:	Condiciones para su uso.....	3
Figura 4-1:	Estimación de crecimiento IoT	5
Figura 1-2:	Modelo IoT	16
Figura 2-2:	Velocidad de adopción del Internet de las Cosas en las distintas industrias	18
Figura 3-2:	Crecimiento IoT	18
Figura 4-2:	Vulnerabilidades IoT	24
Figura 5-2:	Tecnología IoT.....	28
Figura 6-2:	Aplicaciones de IoT	29
Figura 7-2:	Tecnologías semánticas e IoT	32
Figura 8-2:	Modelo OSSTMM	34
Figura 1-3:	SmartWatch U8.....	43
Figura 2-3:	Xiaomi Mi Band 2.....	43
Figura 3-3:	Smartphone Samsung S6 Edge +	44
Figura 4-3:	Dknight Magic Box II.....	44
Figura 5-3:	Raspberry Pi 2.....	45
Figura 6-3:	Ubertooth One.....	46
Figura 7-3:	Arquitectura Ubertooth One	47
Figura 8-3:	USB Dongle CC2540.....	49
Figura 9-3:	Packet Sniffer.....	50
Figura 10-3:	Crackle	52
Figura 11-3:	Hub Hook.....	53
Figura 12-3:	Switch RF.....	53
Figura 13-3:	Kit Etekcitcity	54
Figura 14-3:	RTL-SDR.....	55
Figura 15-3:	Escaneo frecuencia 433 Mhz	56
Figura 16-3:	Instalación GPIO.....	57
Figura 17-3:	Transmisor y Receptor 433 Mhz.....	58
Figura 18-3:	Conexión transmisor receptor a Raspberry Pi.....	58
Figura 19-3:	Hub Smarththings	60
Figura 20-3:	Sensor de movimiento y temperatura Smarththings	60
Figura 21-3:	Bombilla Inteligente GE Link.....	61
Figura 22-3:	ATMEL RZ Raven USB.....	62
Figura 23-3:	ATMEL AVR Dragon On-Chip Programador.....	62

Figura 24-3: Instalación libusb-win32.....	63
Figura 25-3: KIT ATMEL RZ Raven USB.....	64
Figura 26-3: Instalación Firmware Killerbee.....	64
Figura 27-3: Finalización Instalación Killerbee	65
Figura 28-3: Formula Muestra.....	66
Figura 1-4: Resultados hcitool.....	96
Figura 2-4: Resultados hcitool con usuario root.....	96
Figura 3-4: Btscanner	98
Figura 4-4: Resultados Btscanner Magicbox II	99
Figura 5-4: Resultados Btscanner Smartwatch U8.....	99
Figura 6-4: Resultados Btscanner Smartphone Samsung Galaxy S6 edge	100
Figura 7-4: Escaneo Ubertooth 1	101
Figura 8-4: Escaneo Ubertooth 2.....	101
Figura 9-4: Resultados Ubertooth Scan.....	102
Figura 10-4: Resultados Hcitool BLE.....	103
Figura 11-4: Resultados Blue Hydra.....	105
Figura 12-4: Monitoreo de tráfico BLE.....	106
Figura 13-4: Patrón de saltos BLE (Canales)	108
Figura 14-4: Captura de Trafico BLE 1.....	109
Figura 15-4: Captura de Trafico BLE 2.....	109
Figura 16-4: Wireshark BLE	111
Figura 17-4: Captura de Trafico BLE 1.....	111
Figura 18-4: Ejemplo Captura con BTCrack	112
Figura 19-4: Captura Xiaomi Mi Band.....	113
Figura 20-4: Resultados crackle Xiaomi Mi Band.....	114
Figura 21-4: Captura Moto 360	114
Figura 22-4: Resultados crackle Moto 360.....	115
Figura 23-4: Ejecución y resultados Bdaddr.....	116
Figura 24-4: Cambio de MAC mediante Bdaddr.....	116
Figura 25-4: Ataque Re-emparejamiento.....	117
Figura 26-4: Ataque Re-emparejamiento fallido	118
Figura 27-4: Lectura dispositivo RF.....	119
Figura 28-4: Lectura de códigos de control	120
Figura 29-4: Toogle.php	121
Figura 30-4: Reconocimiento de redes Zigbee	122
Figura 31-4: Reconocimiento Zigbee a un archivo.....	123
Figura 32-4: Pruebas Zbdump	123

Figura 33-4: Lectura en Wireshark paquetes Zigbee	124
Figura 34-4: Ejemplo descubrimiento clave de red Zigbee	125
Figura 1-5: Guía metodológica para el control de vulnerabilidades de dispositivos IoT en redes HAN.....	126
Figura 2-5: The Internet of your things Microsoft´s Vision for IoT (Tuzovic).....	127
Figura 3-5: Dispositivos IoT en el hogar	128
Figura 4-5: Asegurar aplicaciones móviles.....	129
Figura 5-5: Contraseñas seguras	130
Figura 6-5: Configuraciones de Seguridad	131
Figura 7-5: Actualizar dispositivos IoT	131
Figura 8-5: Seguridad Física IoT	132
Figura 9-5: WIFI.....	134
Figura 10-5: Dispositivos IoT en el Hogar	135
Figura 11-5: Ataque Hombre en el medio	136
Figura 12-5: Bluetooth.....	138
Figura 13- 5: Computadores.....	138
Figura 14-5: Teléfonos Inteligentes.....	139
Figura 15-5: Relojes Inteligentes	139
Figura 16-5: Tablets.....	140
Figura 17-5: Bandas Inteligentes	140
Figura 18-5: Monitores de Salud	141
Figura 19-5: Dispositivos IoT RF en el hogar	143
Figura 20-5: Sistemas de Alarma	143
Figura 21-5: Boquillas de Luz	144
Figura 22-5: Tomacorrientes RF.....	144
Figura 23-5: Puertas de Garaje	145
Figura 24-5: Zigbee	147
Figura 25-5: Aplicaciones Zigbee.....	148

ÍNDICE DE GRÁFICOS

Gráfico 1-3: Cyber Ataques.....	69
Gráfico 2-3: Conocimiento de riesgos.....	70
Gráfico 3-3: Enfrentamiento del peligro.....	71
Gráfico 4-3: Minimizar vulnerabilidades	72
Gráfico 5-3: Riesgos de no tener protección	73
Gráfico 6-3: Enfrentado el peligro.....	74
Gráfico 7-3: Elemento para existencia de control.....	75
Gráfico 8-3: Conocimiento de no tener protección.....	76
Gráfico 9-3: Manera de enfrentar el riesgo.....	77
Gráfico 10-3: Protección en el sistema informático	78
Gráfico 11-3: Cuenta con una protección	79
Gráfico 12-3: Acceder al control de la vulnerabilidad.....	80
Gráfico 13-3: Como implementar controles de seguridad?.....	81
Gráfico 14-3: Conoce de IoT	82
Gráfico 15-3: Conoce de IOT	83
Gráfico 16-3: Dispositivos seguros.....	84
Gráfico 17-3: Información personal.....	85
Gráfico 18-3: Datos seguros	86
Gráfico 19-3: IOT comportamiento	87
Gráfico 20-3: Medidas de seguridad.....	88
Gráfico 21-3: Factor para establecer seguridades	89
Gráfico 22-3: Aceptación Hipótesis.....	94

ÍNDICE DE ANEXOS

- ANEXO A:** INSTALACIÓN DE UBERTOOTH EN RASPBIAN
- ANEXO B:** FORMULARIO DE ENCUESTAS DIRECCIONADO A LAS PERSONAS QUE UTILIZAN LAS NUEVAS TECNOLOGÍAS
- ANEXO C:** MATRIZ DE VALIDACIÓN DE CONTENIDO DE LA ENCUESTA
- ANEXO D:** TABLA DE DISTRIBUCIÓN

RESUMEN

El objetivo de la presente investigación fue generar un documento técnico e informativo enmarcado en la educación en seguridad informática que sirva como guía a las personas en general para promover el uso correcto y seguro de las tecnologías denominadas IoT "Internet de las Cosas" presentes en su vida cotidiana y en el hogar, de esta manera mediante este marco de orientación donde a través de un análisis de seguridad a las principales tecnologías inalámbricas presentes en el hogar se ha podido generar información de recomendaciones y buenas prácticas para desarrollar en ellos una cultura de concientización sobre los riesgos informáticos presentes en el uso de estos dispositivos y la forma adecuada y segura de implementarlos, configurarlos y utilizarlos.

Para el desarrollo de este estudio se aplicaron varias metodologías de investigación donde se recabaron datos referentes al funcionamiento y vulnerabilidades de las tecnologías inalámbricas más presentes en el hogar así también se realizaron pruebas de concepto y experimentación para evidenciar la existencia de estas vulnerabilidades y la forma adecuada de mitigarlas. Mediante la formulación de una encuesta dirigida al personal administrativo de una entidad pública se determinó que un porcentaje importante de los mismos desconocían aspectos básicos de seguridad informática de sus dispositivos IoT y la forma adecuada de manejarlos para un uso seguro dentro de su hogar. Con los resultados obtenidos se pudo validar la importancia de contar con este tipo de información a través de una guía que permitirá a las personas a tener un mejor conocimiento de seguridad y manejar de sus dispositivos IoT cuando accedan desde su red casera a redes externas como Internet y evitar que su información sensible y privada esté al alcance de los ciberdelincuentes.

Palabras claves: DISPOSITIVOS IoT, VULNERABILIDADES, SEGURIDAD INFORMÁTICA, CIBERDELINCUENTES, INFORMACIÓN PRIVADA.

LUIS ALBERTO
CAMINOS
VARGAS

Firmado digitalmente por LUIS
ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN):
c=EC, l=ROBAMBA,
serialNumber=0602766974,
cn=LUIS ALBERTO CAMINOS
VARGAS
Fecha: 2021.03.26 14:46:03 -05'00'



0034-DBRAI-UPT-IPEC-2021

SUMMARY

The aim of this research was to generate a technical and informative document enclosed in safety computer education that assists as a guide for people in general to promote the correct and safe use of the technologies called IoT "Internet of Things" present in their daily life and at home. Thus, through this guidance framework where, through a security analysis of the main wireless technologies at home, it has been possible to generate information on recommendations and good practices to develop a culture of awareness on the computer risks present in the use of these devices and the appropriate and safe way to implement, configure, and use them.

For the development of this study, several research methodologies were applied where data regarding to the operation and vulnerabilities of the wireless technology most present at home were collected, as well as tests of concept and experimentation to demonstrate the existence of these vulnerabilities and the appropriate way to mitigate them. Through the formulation of a survey directed to the administrative personnel of a public entity, it was determined that a significant percentage of them were unaware of basic computer safety aspects of their IoT devices and the appropriate way to handle them for safety use at home. With the results obtained, the importance of having this type of information could be validated through a guide that will allow people to have a better knowledge of security and manage their IoT devices when they access external networks such as the Internet from their home network and prevent your sensitive and private information from being accessible to cybercriminals.

Keywords: IoT DEVICES, VULNERABILITIES, COMPUTER SAFETY, CYBER CRIMINALS, PRIVATE INFORMATION.

CAPÍTULO I

INTRODUCCIÓN

En el mundo actual existe una creciente demanda de la información y la tecnología, esto debido principalmente a la aparición de Internet que ha orientado a las personas a la necesidad de obtener inmediatez y automatización en sus tareas cotidianas, como las relacionadas a la educación, ocio, comunicación entre algunas.

Esta tendencia ha sido observada por las principales empresas fabricantes de tecnología las cuales han desarrollado funcionalidades especiales como inteligencia y capacidades adicionales de comunicación a los dispositivos electrónicos tradicionales y a otro tipo de objetos que implícitamente no lo poseían con la intención de satisfacer las expectativas del consumidor de lograr interactuar con ellos de una forma rápida, remota y dinámica.

En el proceso de fabricación de estos dispositivos se han observado falencias como la falta de aplicación de normas técnicas enfocadas a brindar seguridad en la información a los datos generados por los usuarios cuando estos utilicen estos dispositivos, en muchos casos los productos inteligentes dentro del concepto del Internet de las Cosas que están siendo ofrecidos en el mercado mundial adolecen de estas características con el consecuente riesgo de promover la presencia de vulnerabilidades informáticas en los hogares de las personas que los adquieren esto sumado a una falta de cultura de seguridad en la información en el hogar por desconocimiento de sus miembros puede ocasionar que puedan sufrir ataques informáticos poniendo en riesgo su información privada inclusive sus posesiones materiales.

1. PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

En las últimas décadas se ha gestado en una nueva revolución digital, la permanente mejora en las capacidades de transmisión, procesamiento y almacenamiento de la información de las nuevas tecnologías digitales han producido cambios importantes en la economía global e impactado favorablemente en la sociedad.

El desarrollo de la tecnología a nivel mundial ha sido creciente, de esta manera esta constante evolución ha generado la presencia de factores de impacto que conllevan a evaluar la seguridad

informática, ya que es necesario establecer parámetros de protección, y privacidad de la información almacenada en un sistema informático.

En América Latina su expansión se produjo debido a tres factores principales, el fuerte crecimiento económico, la reducción de la pobreza y la disminución del coste de los equipos y de las tarifas de accesos a los servicios, esto permitió que las empresas operadoras pudieran ampliar su cobertura de servicio.

Internet como elemento importante en esta revolución han dado lugar a cambios fundamentales en los métodos de comunicación y acceso a fuentes de información tradicionales, su permanente expansión y la disponibilidad hacia las personas con mayores velocidades han permitido que aparezcan nuevos modelos de negocios y la prestación de nuevos servicios. Tal es su influencia que en la actualidad Internet se ha hecho indispensable para cualquier empresa, sea esta independiente de su tamaño o modelo de negocio, asimismo su presencia en los hogares ha llevado a sus miembros al acceso de varias experiencias enfocadas a la diversión como es el uso de redes sociales, streaming de video o juegos en línea hasta otras relacionadas a la educación, domótica, etc. muchas de estas actividades mediante el uso de un sinnúmero de dispositivos electrónicos pertenecientes al concepto de Internet de las Cosas (IoT). (CEPAL, 2015)

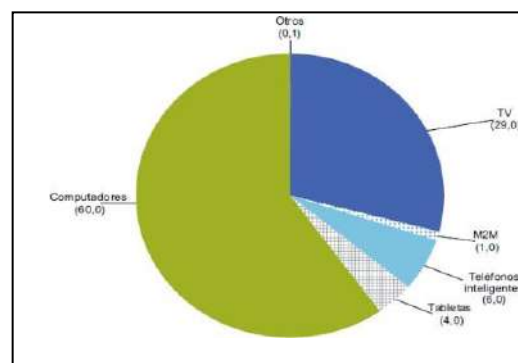


Figura 1-1: Cambio Tecnológico

Fuente: (CEPAL, 2015)

Las nuevas tecnologías digitales están llevando a la masificación de servicios que son considerados parte del internet del futuro como son: la computación en la nube, la analítica de grandes datos y áreas cruciales de la Internet de las Cosas tales como Domótica, Redes y Ciudades Inteligentes y la manufactura digital.

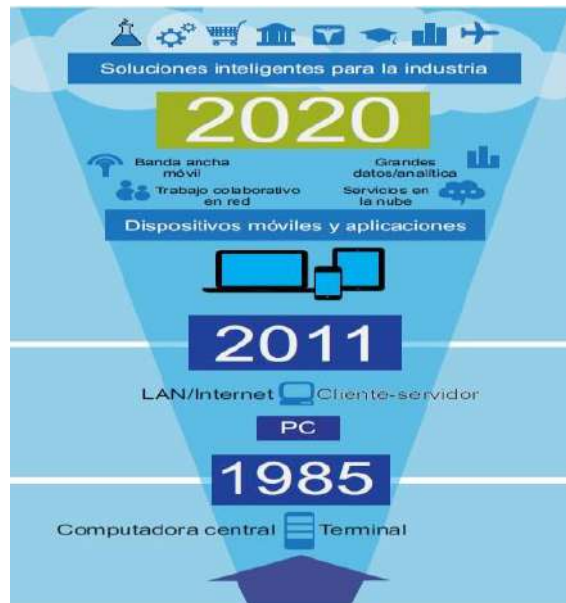


Figura 2-1: Redes y Ciudades Inteligentes

Fuente: (International Data Corporation, 2014)

Para aprovechar estas nuevas tecnologías se requiere mejorar considerablemente las condiciones para su uso tanto en velocidad como en latencia, a continuación, se detalla una tabla con el ancho de banda previsto por aplicación.

Proyectos Mozilla Ignite y US Ignite	Ancho de banda requerido
Manufactura avanzada	Entre 38 y 74
Preparación para emergencias y seguridad	Entre 6 y 18
Educación y capacitación	Entre 38 y 74
Tecnologías de la salud	Entre 38 y 74
Redes limpias de energía y transporte	Entre 2 y 3
Monitoreo de clima y aviones	Entre 38 y 74
Uso de video interactivo en 3D	Entre 77 y 148

Figura 3-1: Condiciones para su uso

Fuente: (CEPAL, 2015)

Frente a esto indica (Corletti, 2011). Que, la persona con gran habilidad para acceder a tecnología informática, protocolos de comunicación y que puede causar daños o perjuicios por el acceso no autorizado a un computador mediante un usuario remoto, se conoce como “intruso informático.

De esta manera se presentan problemas de seguridad y se genera vulnerabilidad, lo cual conlleva a ataques en los sistemas, para ello (Alvarez, 2009), aquellas personas que atacan sistemas informáticos con el fin de ganar notoriedad y/o divulgar la debilidad de sus sistemas de seguridad, se los conoce como hackers. Por tanto, las grandes vulnerabilidades que se presentan en los sistemas informáticos se pueden encontrar en una gran variedad desde virus, spam y malware entre otras.

El phishing, constituye un mecanismo de ataque basado en la ingeniería social en donde un atacante envía mensajes de correo electrónico a su objetivo aparentado provenir de fuentes confiables como entidades bancarias, organismos de gobierno, empresas reconocidas, etc. con la finalidad de intentar de obtener información confidencial como datos personales, contraseñas, información detallada de tarjetas de crédito, información bancaria, etc.

Se determina entonces que para la explotación de una vulnerabilidad para en el servicio de nombres de dominio (Domain Name System, DNS) de software de servidor que permite a un hacker para redirigir el tráfico de este sitio web. Los servidores DNS son las computadoras encargadas de encontrar los nombres de Internet en sus direcciones IP y se utilizan cada vez que un usuario escribe el nombre de un sitio web en su navegador e intenta acceder a él (Philco, 2014).

Por tanto, los clientes y consumidores de servicios en línea no cuentan con la máxima seguridad de sus transacciones, sean estas comerciales, financieras, pues la información que se genera es susceptible de ser interceptadas debido a su alto nivel de vulnerabilidad.

(Philco, 2014), lo cual permite evidenciar que no existe la infraestructura para generar una seguridad informática eficiente que minimice la vulnerabilidad del fraude informático.

1.2. Formulación del problema

¿La falta de una guía metodológica para el control de vulnerabilidades informáticas en redes caseras afecta al control de riesgos de seguridad informática en dispositivos IoT (INTERNET OF THE THINGS)??

1.3. Sistematización del problema

¿Qué tipo de vulnerabilidades han sido identificadas actualmente en los dispositivos IoT?

¿Cuáles son los medios de comunicación más comúnmente utilizados en hogares para la implementación de dispositivos IoT en redes HAN?

¿Cuáles son las técnicas y metodologías más idóneas para controlar el riesgo causado por las vulnerabilidades identificadas?

¿Cuál es el método más adecuado para alertar al usuario de dispositivos IoT ante la presencia de vulnerabilidades en los mismos?

¿Cómo ayudará la oportuna alerta al usuario de la presencia de vulnerabilidades en dispositivos IoT presentes en su hogar?

1.4. Justificación de la investigación

La presente investigación es importante por cuanto pretende generar un cambio de modelo de trabajo en el tratamiento de vulnerabilidades en el ámbito de la seguridad informática, de esta manera indica (INEC, 2010, p.3). El impacto es lo que puede conseguir un atacante que aprovechase la vulnerabilidad. Por ejemplo, si existe un desbordamiento de memoria intermedia, es posible que el atacante pueda conseguir ejecutar código. Si la consecuencia de la vulnerabilidad es que el programa comienza a consumir recursos, es posible que el atacante pueda llegar a conseguir una denegación de servicio (hacer que el programa deje de responder). Si no se han comprobado bien los permisos del programa (causa) puede que se produzca un salto de restricciones (consecuencia) y que el atacante consiga elevar privilegios en el sistema (impacto). De esta manera se determina que la vulnerabilidad informática puede generar un ataque a la información, ya que no existen estándares sólidos de protocolos sólidos de seguridad.

En los últimos años el uso de dispositivos IoT se ha venido incrementando debido principalmente al impacto que ha tenido el Internet en la vida de las personas, permitiéndoles alcanzar la inmediatez y la automatización de sus actividades cotidianas, tal como la comunicación, educación, negocios, compras, etc. Se estima que hasta el 2020 existan al menos 50 millones de dispositivos conectados al Internet, según la fig.1-1 (CSIRT-CV, 2015).

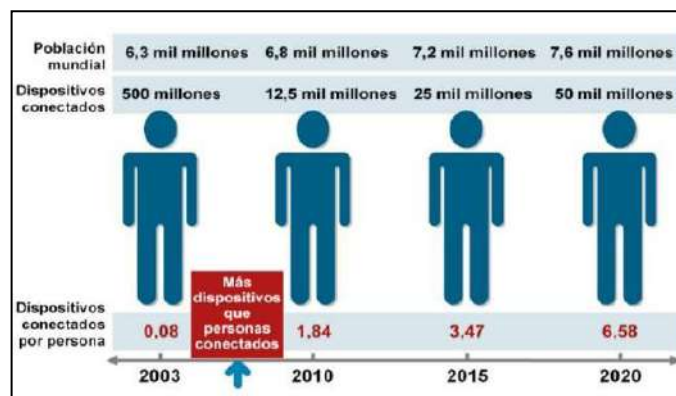


Figura 4-1: Estimación de crecimiento IoT

Fuente: (CISCO IBSG, 2011)

Debido a que la presencia de estos dispositivos es cada vez mayor en los hogares, es necesario realizar un análisis de su funcionamiento específicamente en el ámbito de la seguridad informática a fin de que los mismos no constituyan por sí solos de un elemento vulnerable en el hogar, desde donde un atacante o intruso pueda obtener de información confidencial de sus habitantes. Según informe de HP FORTIFY de fecha Julio de 2014, el 80% de los dispositivos IoT presentan fallas en las formas de autenticación y 6 de cada 10 dispositivos tienen interfaces de usuario vulnerables. (Smith & Miessler, 2014).

La guía metodológica resultado de la investigación propone identificar las principales vulnerabilidades informáticas que se encuentran en los dispositivos IoT y como resultado de su análisis proporcionar una base de conocimientos que permita a cualquier persona interesada en conocer sobre los riesgos a los que es expuesto su hogar e información privada al no considerar ciertos aspectos importantes de seguridad informática al utilizar estos dispositivos. Por tanto, se pretende generar una guía metodológica que permita a las personas a controlar adecuadamente los dispositivos IoT en su hogar de manera que se pueda minimizar el riesgo presente ante las vulnerabilidades informáticas.

1.5. Objetivos de la investigación

1.5.1. Objetivo general

- Elaborar una guía metodológica para el control de vulnerabilidades informáticas en dispositivos IoT presentes en redes HAN.

1.5.2. *Objetivos específicos*

- Revisar la literatura para identificar los problemas de vulnerabilidad más comunes en los dispositivos IoT.
- Determinar cuáles son las tecnologías presentes comúnmente en el hogar para el funcionamiento de los dispositivos IoT.
- Investigar las diferentes metodologías y herramientas para el análisis de vulnerabilidades informáticas aplicables a los dispositivos IoT.
- Realizar las pruebas necesarias para comprobar la presencia de las vulnerabilidades informáticas en los dispositivos IoT.
- Establecer en base a los resultados obtenidos el método más idóneo para identificar las vulnerabilidades en los dispositivos IoT que se encuentran comúnmente en el hogar como también la manera de controlarlos.

1.6. *Hipótesis*

La propuesta de una guía metodológica para el control de vulnerabilidades informáticas en dispositivos IoT para redes HAN servirá como una herramienta de conocimiento para controlar los niveles de riesgos de seguridad informática presentes en el hogar al adoptar este tipo de dispositivos.

CAPÍTULO II

2. MARCO DE REFERENCIAL

En el desarrollo del presente capítulo se determina el análisis sistemático de las variables de estudio, de manera que se conceptualiza a las vulnerabilidades informáticas en dispositivos IoT (internet of the things) para redes HAN (home área network), para posteriormente establecer la guía metodológica.

2.1. Antecedentes del problema

En marco de desarrollo de la investigación se estableció las siguientes investigaciones:

De (Espinosa, 2010), quien concluye:

- Los servicios internos y externos que manipula el usuario final por medio de la red LAN siempre se encuentran acechados por múltiples riesgos de seguridad informática, el nivel de criticidad identificado por cada uno de los riesgos fue determinado en base a la continuidad del negocio más no en un servicio específico, también en la experiencia de las personas que están al contacto de los usuarios finales y por la probabilidad de ocurrencia de los riesgos.
- De tal forma que la red cableada como la red inalámbrica puede ser interceptada las comunicaciones, sin embargo, la red inalámbrica es más propensa ya que algunos Puntos de Acceso están abiertos, considerar las mismas políticas de utilización y administración para estos dos tipos de redes que son utilizados por los usuarios.
- El conjunto de técnicas, procesos y herramientas utilizadas fue lo más importante para realizar las pruebas de ethical hacking, ayudando a recopilar información y obtención de resultados. La mayoría del software es gratuito y está disponible ampliamente en el internet, siendo una amenaza para la seguridad.

2.2. Bases teóricas

2.2.1. Seguridad informática

La seguridad informática, es un área de la informática que se encarga de proteger los recursos de un sistema computacional, esto incluye su infraestructura y principalmente sus datos, por tanto su principal función es minimizar los riesgos que se presenten y que conlleven a un daño o robo de la infraestructura y los datos que esta maneje en todas sus formas. (Pérez Porto & Merino, 2008a)

2.2.2. Objetivos de la seguridad informática

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos para una organización, tales como la información, el hardware o el software. Para esto emplea un conjunto de medidas que permitan prevenir, detectar y actuar frente a posibles cyber ataques, estos esfuerzos siempre dirigidos a preservar la confidencialidad, integridad y disponibilidad de estos recursos. (Pérez Porto & Merino, 2008b)

2.2.3. Vulnerabilidad

Las vulnerabilidades son debilidades internas de un sistema de información las cuales, si son explotadas, podrían causar un daño significativo. La existencia de una vulnerabilidad no causa por sí misma un daño, es necesario que se presente una amenaza para detonarla. (Caschile, 2009a: p. 1).

De esta manera, la vulnerabilidad es una deficiencia en el diseño, implementación, operación o los controles internos en un proceso, que podría utilizarse para violar la seguridad de un sistema. Ahora bien, una vulnerabilidad que no tiene su correspondiente amenaza, puede que no requiera la implantación de un control, pero aun así debe ser reconocida y monitoreada para cambiarla. (Caschile, 2009b: p. 1).

2.2.3.1. Impacto de la vulnerabilidad

El impacto es lo que puede conseguir un atacante que aprovechase la vulnerabilidad. Por ejemplo, si existe un desbordamiento de memoria intermedia, es posible que el atacante pueda conseguir ejecutar código. Si la consecuencia de la vulnerabilidad es que el programa comienza a consumir recursos, es posible que el atacante pueda llegar a conseguir una denegación de servicio (hacer que el programa deje de responder). Si no se han comprobado bien los permisos que otorga el

programa (causa) puede que se produzca un salto de restricciones (consecuencia) y que el atacante consiga elevar privilegios en el sistema (impacto). (INEC, 2010a: p.3).

El impacto define en gran medida la gravedad de la vulnerabilidad. La ejecución de código arbitrario supone la mayor gravedad puesto que significa que el atacante podrá ejecutar cualquier programa en el sistema de su víctima. Por tanto, podría realizar cualquier acción. En estos casos, se dice que el sistema queda "comprometido" porque ha quedado en manos de la voluntad de un tercero. (INEC, 2010b: p.3).

2.2.4. Riesgo asociado con las aplicaciones web

La seguridad de la web debe ser prioritaria para aquellas organizaciones que usan internet como elemento primordial de comunicación con sus clientes o ciudadanos. Asegurarse de una adecuada protección contra aquellos accesos no autorizados a los recursos de información, es esencial para la viabilidad de cada organización. (Caschile, 2009c: p. 1).

Lo anterior debe ser incluido en la parte más alta de la lista de riesgos a los que hay que hacer frente, lo cual puede requerir de capacitación especializada para los auditores, profesionales de la seguridad y equipo de desarrollo. Lo más importante, es que estos grupos sean conscientes de todas las vulnerabilidades de las aplicaciones web, que incluyen la conocida y recientemente descubierta debilidad que puede ser explotada por los atacantes de internet. (Caschile, 2009d: p. 1).

Hay tres reglas generales que deben ser continuamente reforzadas para minimizar los riesgos asociados a la utilización de la web para negocios y el uso privado:

1. Control de acceso a la información sensible: Desarrolladores de aplicaciones web no deben colocar información predecible o sensible en cualquier página web de acceso libre, dentro de un registro de Internet.
2. Establecer fuertes controles sobre la entrada: La regla más importante es nunca confiar en las transmisiones de datos entre el browser, el servidor web y los dispositivos de red. Siempre debe existir validación y revalidación en los controles de entrada (Caschile, 2009e: p. 1).
3. Establecer pruebas de vulnerabilidad en el ciclo de vida del desarrollo de sistemas: La mayoría de las empresas de auditoría y consultoría de Tecnologías de la Información proveen económicas pruebas para testear la vulnerabilidad de las aplicaciones web. Estas pruebas permiten identificar debilidades en seguridad que pueden permitir el acceso a

intrusos a la aplicación web y a las bases de datos. La incapacidad de identificar las vulnerabilidades en la Web a través de un testing estandarizado puede generar un impacto significativo en el proceso de solicitud del cliente. (Caschile, 2009f: p. 2).

2.2.4.1. Vulnerabilidades más comunes

Para entender mejor las vulnerabilidades de las aplicaciones Web, exponemos los siguientes ejemplos de conocidos casos de seguridad, la cual continúa siendo quebrantada por atacantes desde la Internet ya sea para su propia diversión o beneficio ilícito. (Caschile, 2009g: p. 2).

- **Cross-site scripting:** Esto ocurre cuando la aplicación web toma los datos suministrados por el usuario y los envía al browser sin una validación o codificación previa del contenido. En consecuencia, las vulnerabilidades XSS* permiten a los atacantes ejecutar un programa script en el browser de la víctima. Además, este riesgo es considerado como TOP TEN dentro de las debilidades de las aplicaciones web.
- **Inyección SQL:** Esta vulnerabilidad ampliamente publicitada, ocurre al nivel de la base de datos de una aplicación. Es un ataque vía web, que aprovecha errores en la filtración de datos introducidos por el usuario y que permiten a un atacante tener el control de cierta aplicación.
- **Insecure Direct Object Reference:** Una referencia directa a un objeto ocurre cuando un desarrollador expone una reseña a un objeto de implementación interno como un archivo, directorio, registro de una base de datos, clave como una URL o un parámetro formal. Los atacantes pueden manipular estas referencias para acceder a otros objetos sin autorización.
- **Cross-site request forgery (Falsificación en sitios cruzados):** CSRF o también conocido como XSRF es una clase de ataque que afecta a las aplicaciones web con una estructura de invocación predecible. Existen aplicaciones que usan cookies, autenticación de navegador o certificados de cliente. La idea básica de XSRF es un simple atacante que engaña de alguna manera al usuario para que realice una acción determinada en la aplicación objetivo / vulnerable sin que el usuario tenga conocimiento de los hechos que están ocurriendo realmente. (Caschile, 2009h: p. 2).
- **Manejo incorrecto de errores:** Algunas aplicaciones pueden filtrar involuntariamente información sobre su configuración y funcionamiento. De esta manera, las aplicaciones web a menudo otorgan datos acerca de su estado interno por medio de mensajes de error detallados o de depuración. Muchas veces esta información puede ser aprovechada para poner en marcha o incluso automatizar los ataques más poderosos.
- **Error para restringir un acceso URL:** El método de ataque para explotar una vulnerabilidad puede ser muy simplista. Este incluye enlaces y el uso de técnicas de fuerza

bruta para encontrar páginas desprotegidas. Vulnerabilidades específicas incluyen acceso y explotación de la información sensible, URLs ocultos y especiales, artículos y códigos de seguridad que evalúan los privilegios en el cliente. Como resultado, los atacantes pueden obtener acceso a información confidencial, de control de seguridad en el cliente para que el navegador y las aplicaciones eludan los controles integrados en el código que se envía a browser. (Caschile, 2009i: p. 3).

2.2.5. Forma de ataque (vector)

A la forma que tiene el atacante de aprovechar la vulnerabilidad se le conoce como “vector de ataque”. Un vector de ataque común es el envío de información especialmente manipulada a un puerto concreto del sistema. Otra forma de conseguir aprovechar una vulnerabilidad es creando un fichero manipulado que será procesado por ese programa. Por ejemplo, si se encuentra una vulnerabilidad en Word, es muy probable que el vector de ataque sea un archivo en formato .doc. Que aproveche la vulnerabilidad. Si la víctima lo procesa con un Word vulnerable, el atacante conseguirá el impacto deseado. (INEC, 2010c: p.3).

2.2.5.1. Otros vectores de ataque

Otros vectores de ataque pueden ser muy sencillos de llevar a cabo: cómo hacer que la víctima visite un enlace. Por ejemplo, muchas de las vulnerabilidades encontradas en los navegadores son aprovechadas por atacante creando una página web adulterada que, al ser visitada con el navegador vulnerable, aprovecha la vulnerabilidad. Por tanto, enviar un enlace a la potencial víctima, sería el vector de ataque en este caso, y el impacto, podría ser la ejecución de código. (INEC, 2010, p.4).

Llegados este punto, pongamos un ejemplo concreto para unir todos estos parámetros que definen una vulnerabilidad. (INEC, 2010d: p.4).

La aplicación de diseño Figura MSPaint necesita conocer el tamaño de la imagen que va a abrir antes de procesarla. Para conseguir esto, mspaint.exe se ayuda de fichero llamado image_size.dll que está especializado en esta función. (INEC, 2010e: p.4).

El programador de la aplicación MSPaint 7 omitió la comprobación correcta de un parámetro que define la longitud que debe tener una imagen, en la función SetImageSize del fichero image_size.dll. Así pues, como no se comprueba que el valor del parámetro coincida con el tamaño real de la imagen, se produce un desbordamiento de memoria. Explicado de forma sencilla: la memoria del ordenador llega a sitios donde no debería. Por tanto, un atacante puede

retocar la cabecera de una imagen para modificar su atributo de tamaño, añadir a esa imagen qué código quiere ejecutar y aprovecharse de la vulnerabilidad. (INEC, 2010f: p.4).

Vamos a extraer la información necesaria que define la vulnerabilidad:

- Producto y versión: MSPaint 7 es la versión afectada.
- Causa / Consecuencia: Se omite la comprobación del parámetro tamaño (causa) y se produce un desbordamiento de memoria intermedia (consecuencia)
- Dónde / Módulo: En la función SetImageSize del componente image_size.dll. Es una librería en la que se apoya mspaint.exe.
- Impacto: Lo que podría conseguir un atacante es ejecutar código arbitrario. O sea, ejecutar cualquier programa que desee: malware, virus, etc.
- Vector: ¿Cómo puede un atacante explotarla? Un atacante debería enviar un archivo de imagen manipulado (con el código que quiere ejecutar incrustado en su interior, y el parámetro incorrecto retocado) a la víctima, y ésta abrirla con la versión de MSPaint vulnerable. En ese momento se ejecutaría el código arbitrario con el que se ha manipulado la imagen y la víctima quedaría comprometida. (INEC, 2010g: p.3).

Gestión de vulnerabilidades

Las vulnerabilidades son difíciles de gestionar. Se descubren decenas día a día, y clasificarlas es una tarea compleja. Para ello, la organización sin fines de lucro MITRE creó un mecanismo imprescindible hoy en día para estandarizar las vulnerabilidades, haciendo más fácil su identificación, detección y corrección, logrando con esto proporcionar a los analistas de seguridad una mejor referencia de las vulnerabilidades que sean descubiertas.

2.2.6. CVE (Common Vulnerabilities and Exposures)

El CVE es un estándar (administrado por MITRE que se encarga de identificar unívocamente a las vulnerabilidades. Se puede decir que es DNI de una vulnerabilidad. Su formato es el siguiente:

2.2.6.1. CVE-2011-1234

CVE, seguido del año en el que se asignó el código a la vulnerabilidad, seguido de un número de cuatro cifras. Los grandes fabricantes normalmente toman lotes de CVE válidos, pero no usados, que MITRE les adjudica. A medida que van encontrado vulnerabilidades, se los van asignando. Con los creadores de software más pequeños, el propio MITRE se encarga de dicha asignación a medida que se descubren vulnerabilidades (INEC, 2010h: p.5).

El CVE ha tenido gran aceptación entre todos los fabricantes porque la mayor parte de las veces es muy compleja saber a qué vulnerabilidad nos estamos refiriendo solo por ciertas características. Es necesario disponer de una especie de número de identidad único para cada fallo, puesto que en ocasiones las vulnerabilidades son tan parecidas entre sí, tan complejas o se ha ofrecido tan poca información sobre ellas que la única forma de diferenciar las vulnerabilidades es por su CVE. (INEC, 2010i: p.5).

2.2.6.2. CVSS (*Common Vulnerability Scoring System*)

El CVSS es también un estándar que gradúa la severidad de manera estricta a través de fórmulas establecidas. De esta forma los administradores o usuarios pueden conocer de manera objetiva (a través de un número) la gravedad de los fallos que afectan a sus sistemas. Esto permite dar prioridad a la hora de parchear. (INEC, 2010j: p.5).

CVSS clasifica la facilidad de aprovechar el fallo y el impacto del problema teniendo en cuenta los tres pilares de la seguridad de la información: qué nivel de compromiso de la confidencialidad, integridad y disponibilidad de los datos se podrían obtener aprovechando la vulnerabilidad. (INEC, 2010, p.6).

2.2.6.3. *Puntuación de una vulnerabilidad*

Para calcular la puntuación base de una vulnerabilidad se toman nueve parámetros, divididos en tres grupos de tres parámetros cada uno. Los tres grupos principales son: Explotabilidad, Impacto y Temporal. (INEC, 2010k: p.6).

- Explotabilidad define cuán complicado puede llegar a ser para un atacante aprovechar el fallo. Cuenta a su vez con tres parámetros, Vector, Complejidad y nivel de Autenticación. Cada uno a su vez con varios valores posibles.
- El grupo Impacto define qué grado de acceso a los datos podría obtener el atacante. Se define a través de tres valores a su vez, confidencialidad: (si el atacante puede leer aquello que no debería). Integridad (si el atacante puede escribir o modificar aquello que no debería) y Disponibilidad (si el servicio o máquina puede seguir funcionando después de ser atacado).
- El grupo Temporal cuenta también con tres parámetros. Mide ciertas propiedades que influyen en cómo se percibe la vulnerabilidad a lo largo del tiempo y por tanto, son susceptibles de cambios. Explotabilidad: Indica si es sencillo aprovechar la vulnerabilidad. Nivel de Remedio: Si existe o no existe una solución y Confianza de la

información: O sea, si la información sobre la vulnerabilidad es oficial o no (INEC, 2010: p.6).

2.2.6.4. *CVRF (Common Vulnerability Reporting Framework)*

Finalmente, el CVRF se trata de un estándar reciente, que pretende dar uniformidad a la forma en la que se avisa de vulnerabilidades de software a un programador o compañía que crea un programa. Con este método se persigue que, cuando un investigador o empresa cree haber encontrado un fallo de seguridad en un programa, se le proporcione al fabricante la información precisa, rigurosa y adecuada para que pueda confirmarlo, entenderlo y sobre todo, parcharlo de forma eficaz. (INEC, 2010m: p.7).

2.2.6.5. *Parches y actualizaciones*

Cuando se descubre una vulnerabilidad, lo más importante desde el punto de vista del usuario es saber cómo defenderse. Evitar una vulnerabilidad conocida puede pasar por varios estadios y requiere de un seguimiento constante:

- **Conocer la vulnerabilidad:** Es importante mantenerse informado en listas de seguridad sobre los nuevos fallos que van apareciendo. Existen listas públicas y gratuitas a las que los usuarios pueden suscribirse, como por ejemplo los boletines de INTECO, Hispasec, etc. En este aspecto, informarse cuanto antes es vital para reducir la ventana de tiempo de riesgo en la que se es vulnerable.
- **Si no existe parche, aplicar contramedidas:** La mayoría de vulnerabilidades se solucionan cuando el programador arregla el error en el programa y lo publica de nuevo. Esto se llama parche o actualización. Pero esto no siempre se consigue a tiempo. Si el fabricante no ha creado todavía un parche o actualización para solucionar el fallo es importante deshabilitar el módulo del programa vulnerable o bien dejarlo de usar hasta que exista parche. Se pueden utilizar programas alternativos que cumplan la misma función, mientras tanto.
- **Si existe parche, aplicarlo:** Si el fabricante crea un parche o una actualización del programa para solucionar el fallo, es importante instalarlo cuanto antes. En entornos críticos (servidores) es importante realizar pruebas previas, puesto que introducir un parche para arreglar un problema puede a su vez introducir otro fallo y volver inestable un servidor.

2.2.6.6. Internet de las cosas (IOT)

¿Qué es el Internet de las cosas?, es un término que hace referencia a la capacidad de interconexión que poseen los objetos tanto virtuales como físicos para interactuar con otros objetos, personas o entidades externas a través de redes heterogéneas y estándares con el objeto de intercambiar y compartir información útil de su entorno para tal efecto adquieren una identidad que les permite ser identificables desde cualquier lugar y accesibles en cualquier momento. (Maroto, 2014)

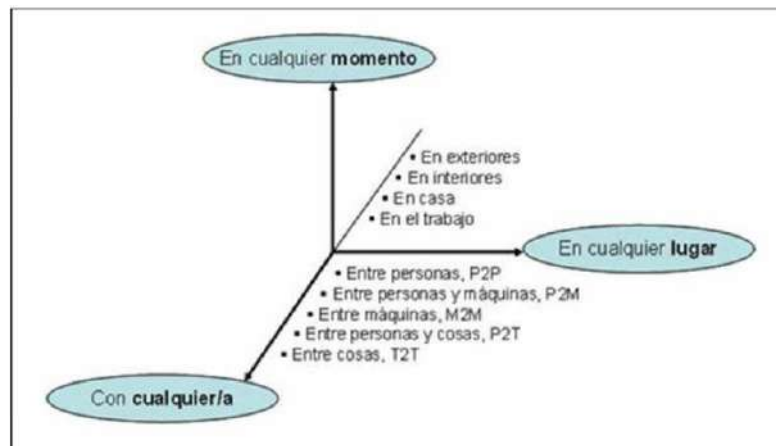


Figura 1-2: Modelo IoT

Fuente: (García Salvatierra, 2012)

Otra definición señala que el Internet de las Cosas es una red de redes que permite la identificación directa y sin ambigüedad de entidades digitales y objetos físicos a través de sistemas electrónicos de identificación estándar y dispositivos inalámbricos móviles haciendo posible la recuperación, almacenamiento, transferencia y procesamiento de información relacionada con estos sin haber discontinuidad entre los mundos físicos y virtuales. (Open Editions Book, 2015)

El Internet de las cosas es una tecnología vigente, y aplicable a un amplio abanico de campos, su uso potencial está presente especialmente en áreas como: smart cities, domótica, control industrial o incluso eHealth para una comunicación médico-paciente más eficaz. (Caldas, 2014)

Algunos ejemplos de su aplicación actual:

Tabla 1-2: Aplicaciones IoT

PERSONAL	Dispositivos ponibles (wearable) para el monitoreo de salud, actividades de deporte, entretenimiento, etc.
VEHICULAR	Dispositivos para el monitoreo, control y rastreo de vehículos o servicios relacionados.
CASAS INTELIGENTES	Automatización de hogares, medidores de servicios, dispositivos de entretenimiento.
EDIFICIOS INTELIGENTES	Automatización de Sistemas e instalaciones eléctricas, climatización, iluminación, control de acceso, etc. para un mejor control y gestión de estos
CIUDADES INTELIGENTES	Manejo eficiente de infraestructura de agua potable, generación eléctrica, tránsito, servicios de emergencia y demás infraestructura y servicios enfocados a mejorar la calidad de vida de sus habitantes
NEGOCIOS INTELIGENTES	Bienes de consumo transformados en objetos inteligentes para captar datos sobre los hábitos y necesidades de los clientes, este involucramiento permitirá mejorar la cadena de producción y distribución de estos
CUIDADOS CRÍTICOS DE SALUD	Monitoreo de signos vitales y dispositivos de soporte de vida

Realizado por: Mena, D. 2017

El RFID, Sensores, las tecnologías inteligentes y las nanotecnologías son la mayor contribución que ha permitido a Internet de las Cosas brindar una amplia variedad de servicios.

Su rápida adopción por parte de las industrias, empresas y hogares se ha incrementado en los últimos años, por lo que se prevé para los próximos años una velocidad de crecimiento en los distintos sectores como se muestra en la figura. Fig.6. (Fundación Barkinter, 2011).

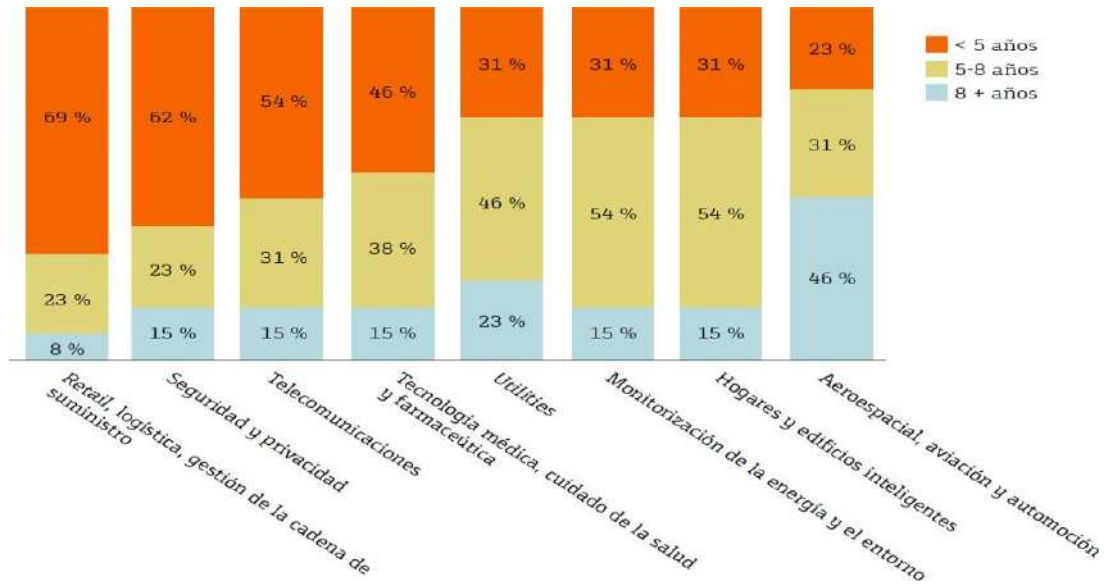


Figura 2-2 : Velocidad de adopción del Internet de las Cosas en las distintas industrias

Fuente: (Fundación Barkinter, 2011)

Hoy en día es habitual que los hogares dispongan de varios dispositivos y equipos electrónicos pertenecientes a la categoría de Internet de las Cosas como son Smartphones, tablets, laptops, Smartwatches, televisores, etc. en muchos de los casos estos se encuentran conectados a Internet o a una red local del hogar.

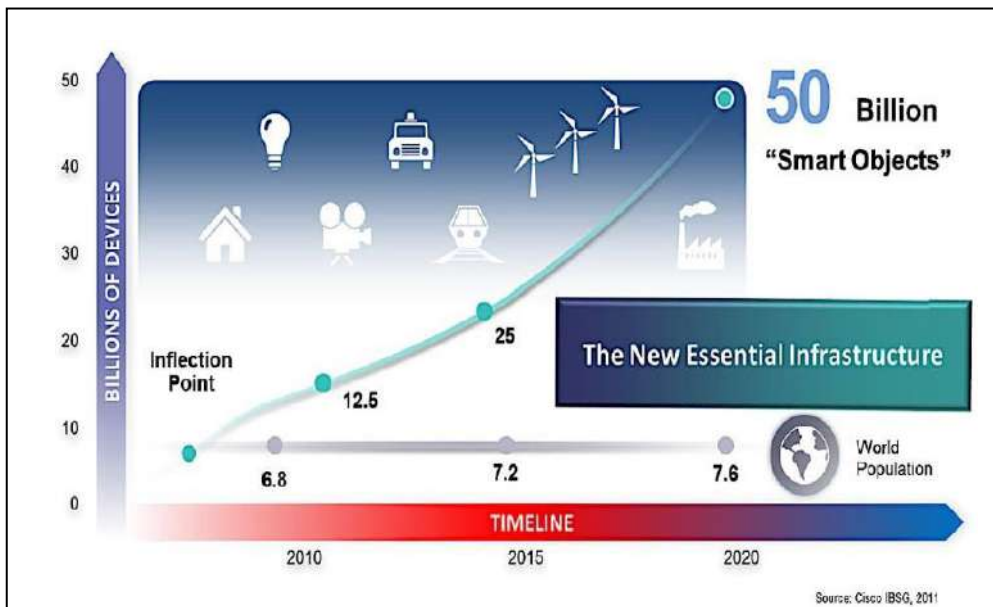


Figura 3-2: Crecimiento IoT

Fuente: (Evans, 2011)

2.2.7. Vulnerabilidades en el Internet de las cosas

La Open Web Application Security Project's (OWASP) conformo un listado de las diez principales vulnerabilidades presentes en la actualidad en los dispositivos IoT según el informe de seguridad del año 2014.

2.2.7.1. Interfaces web inseguras

Considerando que una interfaz web por su razón propia de ser accesible a los usuarios estos pudieren tornarse en una fuente de amenazas, en una organización los ataques informáticos provenientes desde usuarios internos pueden ser de igual o mayor relevancia que los usuarios externos.

Las interfaces web de servicio o administración que poseen ciertos dispositivos IoT permiten el uso de contraseñas inseguras, no poseen mecanismos de bloqueo de cuentas y permiten mantener los usuarios y contraseñas por defecto, asimismo las vulnerabilidades se presentan por la mala configuración y programación de la interfaz web haciéndola susceptible a ataques recurrentes como: XSS (Cross-site scripting), SQLi (SQL injection), CSRF (Cross-site request forgery) o ataques de fuerza bruta.

Todo esto puede llevar a la consecuente pérdida o corrupción de información, fallos en la autenticación y denegación de acceso a usuarios válidos, que pueden llevar a un atacante a tener el control total del dispositivo.

2.2.7.2. Autenticación/autorización insuficiente

Esta vulnerabilidad se enfoca a las falencias en los mecanismos de autenticación de los interfaces web, interfaces móviles o interfaces en la nube, en la que un atacante puede aprovecharse de la misma para acceder al dispositivo.

Se presenta debido a una mala política de contraseñas en la que no se considera parámetros seguros para su generación y aceptación, como también la falta de mecanismos adicionales de validación como es la autenticación de dos o más factores, que solicita información de lo que un usuario autorizado tiene, conoce o es parte. Otras causas también consideradas son la falta de precauciones por parte de un usuario en mantener privada su contraseña y la falta de opciones para caducar una contraseña después de un periodo de tiempo.

Esta vulnerabilidad puede ocasionar que usuarios o atacantes accedan a información y funcionalidades no autorizadas del dispositivo IoT.

2.2.7.3. *Servicios de red inseguros*

Al estar obligados los dispositivos IoT a pertenecer a un entorno de red de comunicación para mantener sus funcionalidades, se presenta esta vulnerabilidad específicamente en los servicios de red que se encuentran accesibles para los usuarios.

Las causas más usuales para que se presente esta vulnerabilidad son:

- Dispositivos que permitan el uso de puertos abiertos sin ser necesarios.
- Utilización de protocolos obsoletos de administración.
- Puertos expuestos a internet mediante UPnP (Universal Plug and Play).
- Vulnerabilidad a ataques de negación de servicio DoS (Denial of Service), afectando la disponibilidad de un recurso.
- No utilización de dispositivos de protección y filtrado como firewalls, ante ataques como fuzzing y buffer overflow.
- Errores de configuración de los dispositivos de red.

La Inseguridad en los servicios de red puede desembocar en la pérdida o corrupción de datos, denegación de servicio o facilitar el ataque a otros dispositivos.

2.2.7.4. *Carencia de cifrado de transporte*

La carencia de cifrado a nivel de capa transporte implica una vulnerabilidad que permitiría a intrusos o usuarios maliciosos a interceptar, modificar, inyectar o redireccionar el tráfico de la comunicación de los dispositivos, ya que la información se mostraría visible debido a que esta recorrería la red en texto plano.

Los dispositivos que poseen esta vulnerabilidad exponen generalmente las siguientes características:

- La información entre dispositivos o hacia Internet es transportada en texto plano.
- No están disponibles en su configuración el uso protocolos de encriptación SSL y TLS.
- Se han aplicado protocolos de encriptación propietarios, que no ofrecen las seguridades debidas.

2.2.7.5. *Preocupación por la privacidad*

Ante la posible presencia en los dispositivos de ciertas vulnerabilidades de seguridad como las anteriormente mencionadas, es poco probable que no exista la preocupación en los usuarios de

que estas puedan comprometen su información personal, de hecho, una encuesta global realizada por Fortinet a hogares indica que existe un porcentaje del 69% de preocupación ante la posibilidad de que los dispositivos IoT pudieren ser una brecha para la fuga de información sensible. (Arroyo, s.f.)

La tendencia de estos dispositivos es la de ofrecer mayores servicios e interactividad con el usuario esto conlleva a que recolecte más información de este que no es debidamente protegida. Existen múltiples casos en la actualidad que evidencian esta vulnerabilidad por ejemplo en el acceso remoto a cámaras de video vigilancia de circuitos cerrados de televisión privados.

Entre las características que indica la presencia esta vulnerabilidad en los dispositivos esta:

- Falta de cifrado de información en especial la considerada sensible tanto en la recepción, almacenamiento y transporte de la misma.
- Términos y políticas de uso por parte del fabricante denotando problemas de privacidad.
- Recolección de información personal innecesaria.
- Presencia de métodos no seguros para el ingreso y resguardo de información crítica.
- No se especifica el destino y alcance que tendrá la información entregada por el usuario final.

2.2.7.6. *Interfaz en la nube insegura*

Un sinnúmero de dispositivos IoT intercambian información con servicios externos alojados en la nube o su vez solicitan a sus usuarios que se conecten a servidores web remotos en donde ingresan información para trabajar con estos, estos interfaces pudieren ser inseguros ya que también son susceptibles a las mismas vulnerabilidades que otros servicios web como XSS, SQLi o CSRF, adicionalmente presentan inconvenientes con relación a ataques de enumeración de usuarios en donde la información de usuarios validos puede ser recolectada, según un estudio de HP el 70 % de los sistemas que hacían uso de interfaces en la nube eran vulnerables a este tipo de ataque.

Esta vulnerabilidad está presente en dispositivos IoT cuando aparecen los siguientes casos:

- Los interfaces en la nube usan mecanismos de autenticación simples.
- Son vulnerables a ataques de enumeración de cuentas.
- Se permite al usuario mantener el usuario y contraseña por defecto en la configuración inicial.
- La interfaz no cuenta con un bloqueo de sesión cuando se ha realizado varios intentos fallidos de autenticación.
- Los métodos para recuperar o resetear las contraseñas no son confiables.
- La interfaz basada en la nube es susceptible a ataques web comunes como XSS, SQLi o CSRF.
- Las credenciales no son correctamente protegidas y pueden ser expuestas a Internet.

2.2.7.7. *Interfaz móvil insegura*

Muchos de los dispositivos IoT presentan un conjunto de funcionalidades a través de aplicaciones móviles que les permiten intercambiar información e interactuar con otros dispositivos, lastimosamente estas funcionalidades no son debidamente protegidas y presentan las mismas deficiencias de seguridad que otros casos, por ejemplo un interfaz móvil estaría vulnerable a ataques como XSS, SQLi, enumeración de cuentas como sucede en las interfaces en la nube inseguras, otro ejemplo, si algún dispositivo posee la capacidad de comunicarse con otro vía inalámbrica este pudiera convertirse en un punto de acceso no deseado e inseguro ya que las medidas de seguridad a aplicarse para asegurar el tráfico y autenticarse no estarían debidamente implementadas o disponibles.

Una interfaz móvil insegura puede resultar en el comprometimiento de la información de los usuarios que usan el dispositivo.

2.2.7.8. *Insuficiente configuración de seguridad*

Esta vulnerabilidad hace referencia a las deficiencias encontradas en la evaluación a la comparativa de las políticas de seguridad requeridas contra las características de seguridad que posee el dispositivo y que pueden ser configuradas. Los dispositivos IoT que permiten el total o parcial configuración de estas funcionalidades habitualmente son accesibles mediante un interfaz de usuario remoto.

Los dispositivos IoT inteligentes generalmente son basados en sistemas operativos tradicionales como Linux o MS Windows por lo que pueden ser blanco de ataques específicos de estos.

Entre las deficiencias de seguridad relacionadas a la configuración de los dispositivos IoT tenemos:

- No existe un manejo de niveles de acceso para los diferentes tipos de usuarios.
- No permite la utilización de protocolos de cifrado para el almacenamiento y transmisión de la información.
- No permite un registro de eventos (logs), ni alertas en caso de requerir evaluar algún incidente.

2.2.7.9. *Software/Firmware inseguro*

Uno de los principales problemas que tienen ciertos dispositivos IoT es su capacidad de mantenerse actualizado mediante una permanente emisión de software/firmware por parte del fabricante, es de conocimiento general que constantemente se generan y descubren nuevas vulnerabilidades informáticas en muchas ocasiones aplicables de manera directa o indirecta a estos dispositivos, por tanto es importante que el dispositivo tenga la funcionalidad de recibir actualizaciones periódicamente para corregir algún fallo de seguridad, existen casos en que los dispositivos dejan de recibir este tipo de soporte por tanto estos se tornan inseguros.

Los métodos de actualización utilizados pueden ser objetivo para los atacantes, ya que, si no existen las medidas de seguridad necesaria como el uso de canales seguros y criptoFiguras que validen la autenticidad e integridad de la actualización, estos pudieren ser alterados para provocar la ejecución de código malicioso que les permita obtener el control total del dispositivo.

2.2.7.10. *Pobre seguridad física*

Esta vulnerabilidad se refiere a la no existencia de medidas adecuadas de seguridad física, que protejan a los dispositivos IoT ante un contacto directo con el atacante.

Al existir esta ventaja el atacante podría acceder fácilmente a puertos, interfaces y controles como también a componentes internos del dispositivo con lo cual pudiera recolectar información mediante diversas técnicas forenses.

Esta vulnerabilidad está presente comúnmente en los dispositivos que poseen las siguientes características:

- Fácil desmontaje del dispositivo y de sus componentes internos que almacenen información.
- Permiten el acceso a datos desde puertos externos, tales como puertos USB, Serial, etc.
- No poseen la capacidad de mantener protegida la información en los medios de almacenamiento.
- Poseen puertos externos que no son estrictamente necesarios para el correcto funcionamiento del dispositivo.

Estudios actuales demuestran que los dispositivos IoT que se encuentran en el mercado presentan varias vulnerabilidades las cuales son una brecha de seguridad para sus usuarios. Según informe de HP FORTIFY de fecha Julio de 2014, el 80% de los dispositivos IoT presentan fallas en las formas de autenticación y 6 de cada 10 dispositivos tienen interfaces de usuario vulnerables. (Craig Smith, 2015).

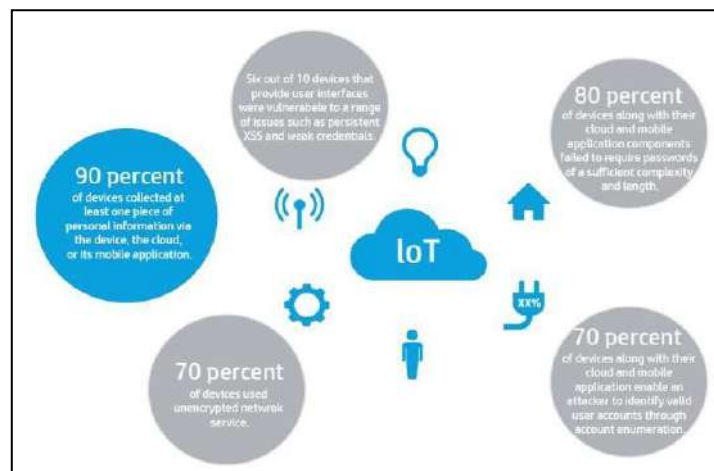


Figura 4-2: Vulnerabilidades IoT

Fuente: (Hewlett Packard, 2014)

La web ha atravesado varias etapas evolutivas diferentes:

- Etapa 1. Primero fue la fase de investigación, cuando la web se denominaba Red de la Agencia de Proyectos de Investigación Avanzados (ARPANET). Durante este período, la web era utilizada principalmente por el área académica para fines de investigación. (Evans, 2011a: p. 5)
- Etapa 2. La segunda fase de la web fue la explosión de los sitios web publicitarios. Esta etapa se caracterizó por la “fiebre del oro” por los nombres de dominio y se concentró en

la necesidad de que casi todas las empresas compartieran información en Internet para que los consumidores pudieran conocer sus productos y servicios. (Evans, 2011b: p. 5)

- Etapa 3. La tercera evolución fue el paso de la web de los datos estáticos a la información transaccional, que permitió la compra y venta de productos y servicios y la prestación de servicios. Durante esta fase, irrumpieron en escena empresas como eBay y Amazon.com. Esta etapa también será injustamente recordada como el auge y la caída de las “punto com”. (Evans, 2011c: p. 5)
- Etapa 4. La cuarta fase, en la que actualmente nos encontramos, es la web “social” o de “experiencia”, en la que las empresas como Facebook, Twitter y Groupon se han hecho inmensamente famosas y rentables (una notoria diferencia respecto de la tercera fase de la web) por permitir a las personas comunicarse, conectarse y compartir información (texto, fotos y video) personal con amigos, parientes y colegas. (Evans, 2011d: p. 5)

2.2.8. *Gestión de la información*

IoT implica que todo objeto puede constituir una fuente de datos. Separar el grano e la paja de toda la información que se genera se vuelve cada vez más complicado. Si se sigue el ritmo actual, para el año 2020 el universo digital será cuarenta y cuatro veces más grande que en el año 2009. Esto está empezando a transformar la forma de hacer negocios, la organización del sector público y el día a día de millones de personas. Por ejemplo, la empresa estadounidense Walmart maneja más de un millón de transacciones... a la hora. Por ello, empresas y emprendedores se encuentran en la carrera por innovar en términos de almacenamiento, velocidad, acceso y métodos de análisis de datos, google cuenta con más de treinta centros de datos, equivalentes a más de un millón de servidores. Para alcanzar este despliegue, su competencia, Microsoft, está invirtiendo miles de millones de dólares en añadir hasta 20.000 servidores al mes. Se espera que en el año 2020, el consumo de estos centros equivalga al consumo actual de electricidad de Alemania, Canadá y Brasil juntos. (ICT, 2013a: p. 9)

2.2.8.1. *Impacto del IOT sobre las personas*

Gracias a la posibilidad de estar permanentemente conectados y localizables, está surgiendo una nueva generación de consumidores en paralelo a la aparición de la banda ancha de móvil. Este segmento espera, o casi exige, que la red facilite todas las actividades que desea llevar a cabo y que les permita permanecer conectados allá donde vayan. Casi dan por sentada la existencia de conexión wifi y cualquier avance técnico que permita la movilidad. En otras palabras, internet de las cosas comprende todo lo que pueda satisfacer sus necesidades. (ICT, 2013b: p. 11).

2.3. Optimización

Actualmente existe, además, una creciente preocupación por el desarrollo sostenible motivada por la escasez de recursos. No es casualidad que la optimización del consumo de recursos sea uno de los campos más prometedores para internet de las cosas. Los sensores y sistemas de control automáticos que quedan integrados en los objetos que encontramos a nuestro alrededor permiten medir distintas variables que puedan llevar al cambio en los patrones de uso de recursos escasos. Hewlett Packard ha construido una plataforma llamada CeNSE (Central Nervous System for the Earth, en español “Sistema Nervioso central para la Tierra”). Se trata de una red mundial de miles de millones de sensores que recaba información sobre variables como localización, temperatura, presión, sonido, Luz, humedad y un largo etc. Toda esta recopilación de información puede resultar fundamental para lograr el objetivo de un uso eficiente y sostenible de los recursos del planeta. (ICT, 2013, p. 12).

2.3.1. Elección de estándares

Los sensores que se colocan en objetos cotidianos para medir variables como la temperatura o el movimiento y enviar esta información a través de Internet, no resultan demasiado rentables a nivel particular o residencial. Si bien es cierto que los sensores son cada vez más baratos, muchas de las herramientas y equipos complementarios para su uso requieren una inversión muy alta. Algo similar ocurre con las etiquetas RFID. Los fabricantes de bienes de consumo susceptibles de llevarlas están esperando a que existan en el mercado suficientes lectores RFID. Y viceversa: los fabricantes de los lectores no quieren aumentar su producción hasta que no haya una masa crítica de productos con etiquetas integradas. Este círculo vicioso tiene su efecto en la acogida de estándares. (ICT, 2013c: p. 12).

2.3.2. Una visión de IOT

La visión de Internet de las Cosas, Internet no es solo para personas, los objetos tienen también cabida en ella. En el Internet de las cosas se espera que objetos (“cosas”) inteligentes sean participantes activos de los procesos sociales, de negocio y de información al ser capaces de interactuar y comunicarse entre ellos mismos y con el entorno mediante el intercambio de datos e información. Estos objetos inteligentes reaccionan de manera autónoma ante los acontecimientos del mundo real que les rodea e influyen en él ejecutando procesos que desencadenan acciones y crean servicios con o sin intervención humana directa. Los servicios generados son a su vez capaces de interactuar con estas "cosas inteligentes" mediante interfaces estándares que proporcionan el vínculo necesario vía Internet, para poder consultar y cambiar su

estado y recuperar toda la información asociada a ellos teniendo en cuenta aspectos como la seguridad y la privacidad. El resultado último de Internet de las Cosas es por tanto el despliegue de servicios y aplicaciones caracterizados por un elevado grado de captura autónoma de datos, transferencia de eventos, conectividad de red e interoperabilidad. (ICT, 2013d: p. 12).

2.3.2.1. *Discusión de la IOT*

Ubiquitous computing: A pesar de que la miniaturización de los dispositivos informáticos y los servicios ubicuos derivados de sus datos son, probablemente, requisitos para IoT, éste no es igual a ubiquitous computing. Ubiquitous computing no implica el uso de los objetos, ni requiere una infraestructura de Internet. Clúster (ICT, 2013e: p. 19)

- El Protocolo de Internet: Internet puede ser utilizado a nivel mundial porque los clientes y servidores utilizan el mismo protocolo para la comunicación: sin embargo, muchos objetos en Internet de las Cosas no serán capaces de ejecutar un protocolo de Internet. Clúster (ICT, 2013f: p. 19)
- Tecnologías de la Comunicación: Como esto sólo representa un requisito funcional parcial en el Internet de las Cosas, similar al papel de la tecnología de la comunicación en Internet, asemejar tecnologías de la comunicación como WiFi, Bluetooth, ZigBee, 6LoWPAN, ISA 100, WirelessHart/802.15.4, 18000-7, LTE con IoT es demasiado simplista. Sin embargo, podemos decir que estas tecnologías, sin duda, podrían ser parte del Internet de las Cosas. Clúster (ICT, 2013g: p. 19)
- Dispositivos integrados: RFID o las Redes de Sensores Inalámbricos (WSN), pueden ser parte importante de Internet de las Cosas, pero como aplicaciones independientes (intranet) pierden las infraestructuras de información de fondo necesarias para crear nuevos servicios. IoT ha llegado a significar mucho más que sistemas RFID puestos en red. Clúster (ICT, 2013h: p. 20)
- Aplicaciones: Tal como Google o Facebook no podían ser utilizados en los años 90 para describir las posibilidades ofrecidas por Internet o la WWW, podría decirse que es el uso de aplicaciones y servicios de Internet para describir la propia Internet es vago, pero es aún más ilógico referirse a pequeñas aplicaciones que no tendrían un impacto real en Internet de las Cosas. (ICT, 2013i: p. 20)

2.3.2.2. *La tecnología IOT*

A nivel conceptual, la tecnología IoT representa el "middleware" entre la aplicación de los "grandes desafíos", tales como el cambio climático, la eficiencia energética, la movilidad, la sociedad digital, la salud a nivel global, etc., y las tecnologías facilitadoras tales como la nanoelectrónica, las comunicaciones, sensores, los teléfonos inteligentes, sistemas embebidos, el cloud computing y las tecnologías de software. Estos desafíos darán lugar a nuevos productos, nuevos servicios, nuevas interfaces y nuevas aplicaciones y a lo que se empieza a denominar smart environments y smart spaces (entornos y/o espacios inteligentes). (ICT, 2013j: p. 20)



Figura 5-2: Tecnología IoT

Fuente: (ICT, 2013)

2.4. Tendencias tecnológicas

Los avances en la tecnología de red inalámbrica y la mayor estandarización de los protocolos de comunicación permiten recoger datos de los sensores y dispositivos inalámbricos identificables en casi cualquier lugar en cualquier momento. Se diseñan miniaturizados chips de silicio con nuevas capacidades, mientras que los costes, siguiendo la Ley de Moore, están cayendo. El aumento masivo de almacenamiento y potencia de cálculo, también disponible a través de cloud computing, hace que los cálculos numéricos a gran escala y en un alto volumen, sean posibles a bajo coste. (Ruiz, 2013a).

2.4.1. *Aplicaciones de IOT*

El principal objetivo de IoT es la creación de entornos inteligentes y cosas conscientes para aplicaciones relacionadas con el clima, la alimentación, la energía, la movilidad, la sociedad digital y la salud (por ejemplo: transporte, productos, ciudades, edificios, zonas rurales, energía, salud, inteligente, etc.). (Ruiz, 2013b).

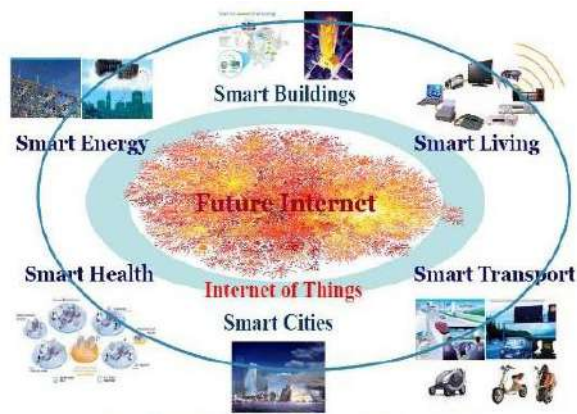


Figura 6-2: Aplicaciones de IoT

Fuente: (Ruiz, 2013)

2.4.2. Entidades inteligentes

Los desarrollos de las “entidades inteligentes” también fomentará el desarrollo de las nuevas tecnologías necesarias para hacer frente a los nuevos retos de la salud pública, el envejecimiento de la población, la protección del medio ambiente y el cambio climático, la conservación de la energía y la escasez de materias primas, mejoras en la seguridad y la continuación y crecimiento de la prosperidad económica. Estos problemas serán abordados de las siguientes maneras:

- Gestión, detección y tecnología de red fiable, inteligente, autoadministrada, sensible al contexto y adaptable.
- Perfeccionamiento de la interacción entre el hardware, software, algoritmos, así como el desarrollo de interfaces inteligentes entre las cosas (máquina a máquina inteligente, interfaces cosas a cosas) y los interfaces inteligentes entre humanos-máquinas y cosas, permitiendo así el software inteligente y móvil.
- Incorporación de la funcionalidad inteligente a través de desarrollos adicionales en el área de la nanoelectrónica, sensores, actuadores, antenas, almacenamiento, fuentes de energía, sistemas integrados y redes de sensores.
- Desarrollos en todas las disciplinas para hacer frente a las comunicaciones multifuncionales y multidominio, las tecnologías de la información y procesamiento de señal, la tecnología de identificación y mejoras en la tecnología de los motores de búsqueda. El desarrollo de nuevas técnicas y conceptos para mejorar la seguridad y la

privacidad de las tecnologías existentes con el fin de adaptarse a los nuevos retos tecnológicos y sociales.

- Mejorar la estandarización, la interoperabilidad, la validación y la modularización de las tecnologías y soluciones de IoT.
- Definición de nuevos principios de gobierno que se ocupan de la evolución de la tecnología y permitir el desarrollo de negocios y el acceso libre al conocimiento en línea con las necesidades globales, manteniendo el respeto por la privacidad y la seguridad. (Ruiz, 2013c).

2.4.2.1. *Habilitadores de tecnología en iot*

Las habilidades están determinadas en las siguientes áreas:

Tabla 2-2: Habilitadores IoT

Energía	Las cuestiones energéticas, en todas sus fases, desde la recolección hasta la conservación y el uso, son fundamentales para el desarrollo de IoT. Hay una necesidad de investigar y desarrollar soluciones en este ámbito que tiene como objetivo los dispositivos de ultrabaja potencia, ya que los dispositivos actuales parecen insuficientes teniendo en cuenta la potencia de procesamiento necesaria y las limitaciones energéticas del futuro. El uso de tecnologías que se centran en la integración de sistemas, aumentará la eficiencia de los sistemas actuales y ofrecerá una serie de soluciones para las necesidades futuras.
Inteligencia	Capacidades como la consciencia, la sensibilidad al contexto y el entorno, la comunicación máquina-a-máquina son consideradas de alta prioridad para el IoT. La integración de la memoria y la capacidad de procesamiento y la capacidad de soportar entornos agresivos son también una alta prioridad, así como son las mejoras posibles en las técnicas de seguridad. Más concretamente, proveer de seguridad en la capa física, aprovechando las características de los canales inalámbricos, representa la solución sencilla prevista también haciendo frente a los problemas de escalabilidad que plantean los despliegues a gran escala de las cosas "inteligentes". La densidad de los transistores está destinada a crecer, siguiendo la Ley de Moore, permitiendo por lo tanto una electrónica más "inteligente" con aumentos en la capacidad de procesamiento de los chips y su capacidad de memoria.
Comunicación	Nuevas antenas inteligentes (antenas fractales, antenas adaptativas, antenas receptivas direccionales, antenas de plasma), que se puedan incorporar en los objetos, fabricadas con nuevos materiales, son los medios de comunicación que permitirán el uso de nuevos sistemas de comunicaciones avanzadas en chips, que al combinarse con los nuevos protocolos optimizados a través de las capas física (PHY), de Control de Acceso al

	Medio (MAC) y de Red (NWK) permitirá el desarrollo de diferentes Interfaces de Programación de Aplicaciones (API) que se utilizarán para diferentes usos
Integración	La integración de las tecnologías de identificación inalámbrica (como la identificación por radiofrecuencia - RFID) en envases, o, preferiblemente, en productos, permitirá ahorros de costes significativos, un mayor respeto al medio ambiente de los productos y permitir una nueva dimensión de la auto-consciencia del producto para el beneficio de los consumidores. Esta integración requiere abordar la necesidad de sistemas heterogéneos que tengan capacidad de detección, actuación, comunicación, cognitiva, de procesamiento y adaptabilidad y la inclusión de sensores, actuadores, circuitos nanoelectrónicos, sistemas integrados, algoritmos y software embebido en las cosas y los objetos.
Fiabilidad	La fiabilidad de los sistemas de IoT es de suma importancia, por lo que la infraestructura de red del IoT debe garantizar la fiabilidad de la seguridad y la privacidad mediante el apoyo a la autenticación individual de miles de millones de dispositivos distintos utilizando tecnologías de comunicación heterogéneas a través de diferentes dominios administrativos. Eficientes y confiables protocolos de comunicación también deben ser diseñados para asegurar la fiabilidad.

Fuente: (Cayetano, 2012).

Realizado por: Mena, D. 2017

2.5. Tecnologías semánticas e IOT

IoT requiere dispositivos y aplicaciones que puedan fácilmente conectarse e intercambiar información de manera ad-hoc con otros sistemas. Esto requerirá de dispositivos y servicios que puedan expresar sus necesidades y capacidades de manera formal. Para facilitar la interoperabilidad en el IoT se necesitará investigar más a fondo las tecnologías semánticas. Ejemplos de estos retos pueden ser ontologías distribuidas a gran escala, nuevos enfoques acerca de los servicios web semánticos, motores de reglas y enfoques para el razonamiento híbrido en grandes bases de datos heterogéneas, la detección de dispositivos basada en la semántica y la generación de código semánticamente impulsada para interfaces de dispositivo. (Cayetano, 2012a).

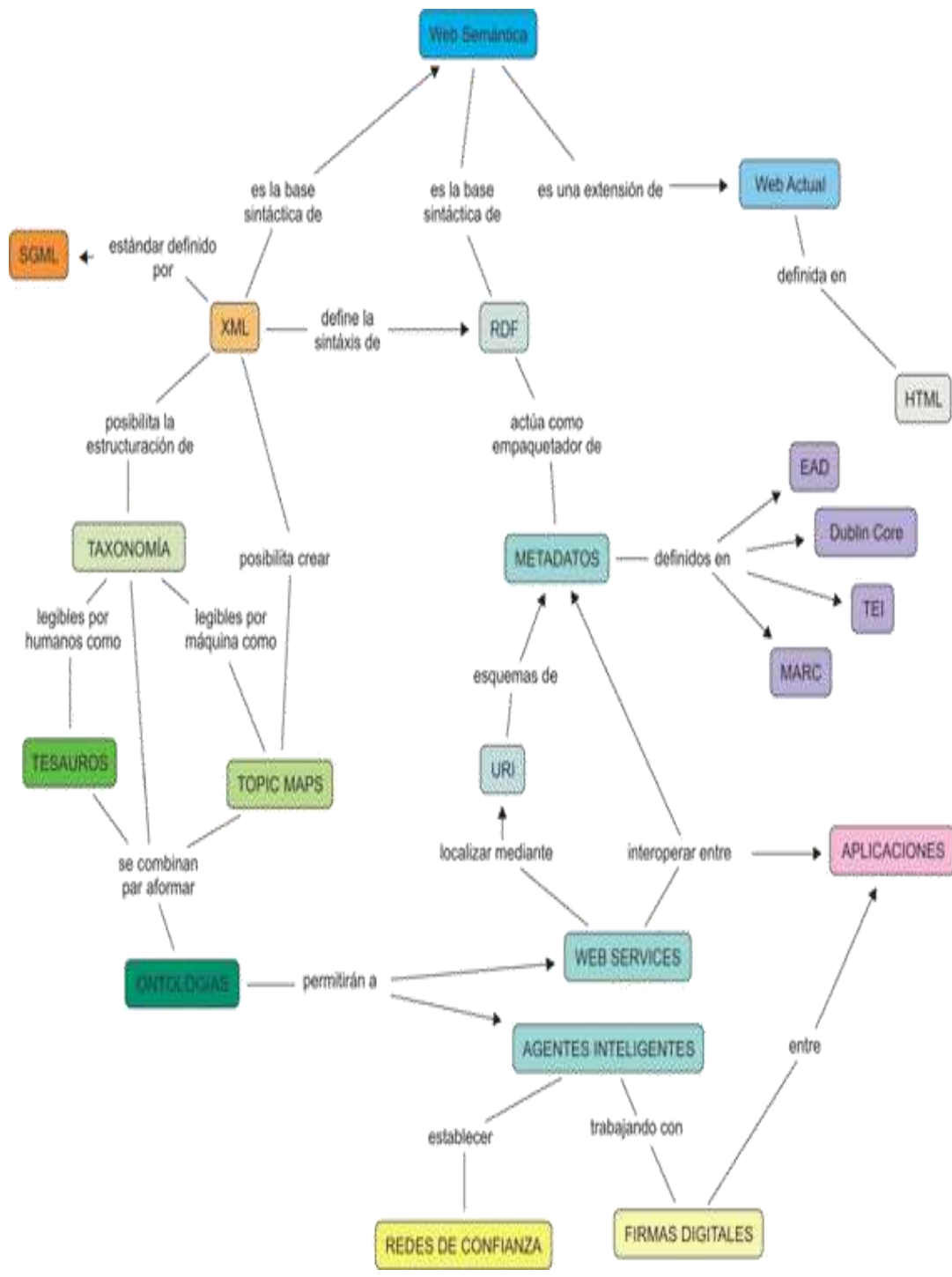


Figura 7-2: Tecnologías semánticas e IoT

Fuente: Mapa conceptual de la Web Semántica. Keilyn Rodríguez Perojo y Rodrigo Ronda León

2.5.1. Aplicaciones de la IOT

IoT implica que incluso el más pequeño dispositivo o sensor puede ser conectado a la red. La investigación en redes de sensores inalámbricos ya ha dado lugar a soluciones prometedoras; herramientas y sistemas operativos que se pueden ejecutar en dispositivos muy pequeños y con

recursos limitados. Estas soluciones deben ser evaluadas en verdaderas aplicaciones industriales a gran escala con el fin de ilustrar posibles escenarios, lo más realistas posible, en negocios asociados IoT. (Cayetano, 2012b).

2.5.1.1. Modelado y diseño

El diseño de sistemas de IoT a gran escala es un reto debido a la gran cantidad de componentes de distinta naturaleza que intervienen y debido a las complejas interacciones entre los dispositivos introducidos por los enfoques cooperativo y distribuido. Para hacer frente a este problema, se requieren modelos innovadores y marcos de diseño; por ejemplo, inspirado en métodos de simulación conjunta para grandes sistemas de sistemas y simulación “hardware-in-the-loop”. (Ronda, 2011a).

2.5.1.2. Validación e interoperabilidad

La estandarización es una necesidad indispensable, pero no es suficiente. Es un hecho conocido que, incluso compartiendo el mismo estándar, dos dispositivos diferentes podrían no ser interoperables. Esto es uno de los principales obstáculos para la adopción generalizada de las tecnologías del IoT. Debido a la naturaleza compleja y diversa de las tecnologías del IoT, quizás una sola solución de interoperabilidad no será posible y por tanto requerirá una integración. (Ronda, 2011b).

Las etiquetas y dispositivos futuros deberán integrar diferentes esquemas de comunicación, permitiendo arquitecturas diferentes, centralizadas o distribuidas, y ser capaces de comunicarse con otras redes. La interoperabilidad de las tecnologías del IoT será siempre un tema complejo que requerirá un esfuerzo de investigación para hacer frente a los nuevos retos planteados. Esto por ejemplo se podría conseguir con la incorporación de una mayor inteligencia y diferentes tecnologías de acceso de radio con capacidades cognitivas. (Ronda, 2011c).

2.5.1.3. Estándares

Claramente, los estándares abiertos son habilitadores claves para el éxito de las tecnologías inalámbricas de comunicación (como RFID o GSM), y, en general, para cualquier tipo de comunicación máquina a máquina (M2M). Sin normas globales reconocidas (como el protocolo TCP / IP o GSM / UMTS / LTE) la expansión de la tecnología RFID y soluciones M2M para el Internet de las Cosas no puede llegar a una escala global. La necesidad de una rápida creación de normas interoperables se ha reconocido como un elemento importante para el despliegue de aplicaciones en IoT. (Cayetano, 2012c).

2.6. OSSTMM, Manual de la metodología abierta de testeo de seguridad

El manual OSSTMM describe una metodología que recoge diversas pruebas y métricas de seguridad, utilizadas por profesionales para la realización de auditorías de seguridad. Se rige al cumplimiento de normas y mejores prácticas como las establecidas en el NIST, ISO 27001-27002 e ITIL entre otras.

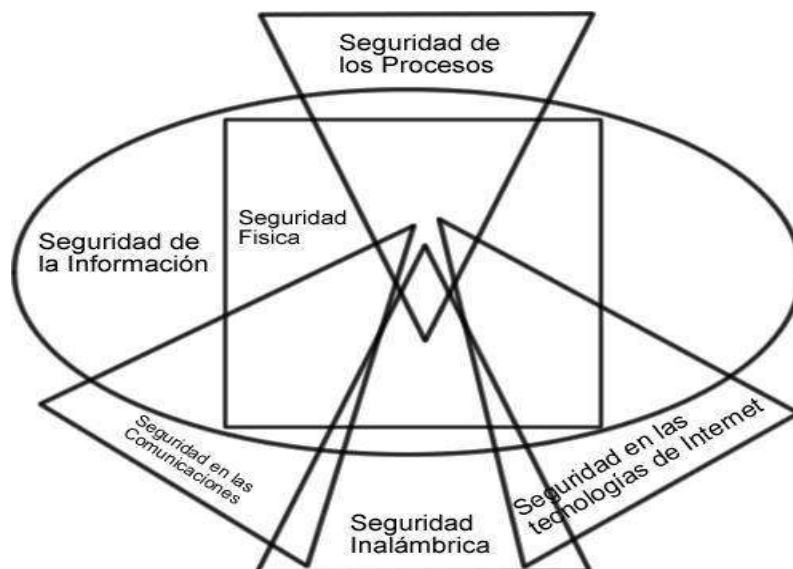
El OSSTMM se centra en detalles técnicos de los elementos que van a ser probados, ¿Qué hacer antes, durante y después de una prueba de seguridad?, y ¿cómo medir los resultados? (García, 2010)

2.6.1. Estructura

Las pruebas de seguridad abarcan seis secciones que componen el manual, en cada sección se hallan módulos donde se señalan las pruebas de seguridad a realizar.

1. Seguridad de la Información
2. Seguridad de los Procesos
3. Seguridad en las tecnologías de Internet
4. Seguridad en las Comunicaciones
5. Seguridad Inalámbrica
6. Seguridad Física

•



•

Figura 8-2: Modelo OSSTMM

Fuente: (Herzog, 2003)

2.6.1.1. Seguridad de la información

En esta sección se trata tres aspectos: la revisión de la inteligencia competitiva, revisión de privacidad y recolección de documentos.

La revisión de la inteligencia competitiva es la recolección de la información obtenida a través de Internet que puede ser analizada con inteligencia de negocio.

Lo concerniente a revisión de privacidad es el punto de vista legal y ético de almacenamiento, transmisión y control de los datos basados en la privacidad del cliente y el empleado. (Herzog, 2003a)

En la recolección de documentos se encarga de obtener la información relevante que posee la organización como: bases de datos, datos web, perfiles de usuarios, personal clave, etc.

2.6.1.2. Seguridad de los procesos

Está compuesta por los siguientes módulos: testeo de solicitud, testeo de seguridad dirigida, testeo de personas confiables.

El testeo de solicitud es un método para obtener privilegios de acceso a una organización mediante técnicas aplicadas al personal que controla el ingreso a esta.

El testeo de sugerencia dirigida está enfocada a identificar los puntos de acceso privilegiado de una organización mediante la invitación de personas a ubicaciones escogidas fuera de la organización a través de canales de comunicación como teléfono o correo electrónicos.

El testeo de personas confiables es valerse de personas de confianza para que induzca a una persona interna de la organización a revelar información acerca de esta.

2.6.1.3. Seguridad de las tecnologías de Internet

El objetivo de esta sección es profundizar en el análisis sobre el funcionamiento de la red de la organización en donde se analiza ciertos aspectos como: la estructura de red, las conexiones hacia el exterior como Internet, dispositivos de seguridad utilizados, su configuración y políticas empleadas, identificar los datos que son transmitidos y recibidos y probar su seguridad, medidas de contingencia, y los servicios que sobre la red se están ejecutando.

2.6.1.4. Seguridad en las comunicaciones

En esta sección se comprobará la seguridad de los dispositivos y tecnologías que permiten establecer las comunicaciones de la organización, como es el caso de centrales telefónicas, buzones de voz, correos electrónicos, equipos de comunicación inalámbricas por radio frecuencia y teléfonos fijos o móviles.

2.6.1.5. Seguridad inalámbrica

Abarca el análisis de todos los dispositivos que emiten radiación electromagnética y entre los cuales se encuentran los que se implementaron para establecer redes de comunicación inalámbrica en la organización. (Herzog, 2003b)

Entre los aspectos a revisar está las configuraciones de seguridad y gestión de acceso de los dispositivos inalámbricos, las actualizaciones de software y firmware y la cobertura de sus señales dentro de la organización.

Otro aspecto importante es la identificación de los datos que estos transmiten a fin de determinar que los mismos no comprometan ante vulnerabilidades a la seguridad e intereses de la organización.

2.6.1.6. Seguridad física

Corresponde a todo lo relacionado a asegurar las instalaciones y bienes de la organización, mediante el aseguramiento del perímetro físico, la ubicación de bienes en sitios seguros, controles de acceso, verificación de los sistemas de vigilancia y personal de seguridad, revisión del entorno ante posibles riesgos externos como desastres naturales.

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

Estos modelos de metodologías de investigación, aunque en esencia incluyen los pasos fundamentales del método científico de investigación, difieren en su aplicación específica según la conceptualización del objeto de estudio. Así, encontramos metodologías de investigación teórica, experimental, tecnológica, documental y otras muchas que son diseñadas ex profeso para las disciplinas de estudio donde se aplican. (Muñoz C. , 2011a).

3.1. Tipo y diseño del estudio

3.1.1. *Investigación teórica.*

Cuando se pretende desarrollar un tema de investigación de carácter teórico conceptual, el objeto de estudios se concentra en el análisis de leyes, teorías, conceptos y conocimientos de una temática específica, ubicada dentro de una disciplina de estudios. El propósito es examinar, bajo un enfoque de carácter científico, la vigencia, utilidad, universalidad, actualización, confiabilidad y todo aquello que permita determinar la correcta aplicabilidad científica de lo que se está estudiando, lo cual será de utilidad para las áreas de estudios donde se ubican esos conocimientos. (Bernal, 2013).

De esta manera se sustenta bibliográficamente las variables de estudio, mediante el análisis de teorías y conocimientos de las vulnerabilidades informáticas en las tecnologías relacionadas a los dispositivos IoT (Internet of the things), principalmente presentes en su comunicación e interacción con otros dispositivos inteligentes y a si establecer un enfoque sistemático para el proceso investigativo.

3.1.2. *Investigación experimental*

Otro de los ejemplos más comunes de investigación es la investigación de carácter experimental, la cual se basa en los principios teórico-empíricos de las ciencias naturales y experimentales, y en la realización de pruebas, ya sea en el laboratorio, en escenarios diseñados ex profeso, o bien, en el ambiente real donde tiene lugar el fenómeno bajo estudio. (Muñoz C. , 2011b).

A fin de comprobar el planteo de hipótesis, se implementaron varios escenarios de laboratorio donde se evaluaron tres tecnologías de comunicación inalámbrica mediante la realización de

pruebas de seguridad a los dispositivos IoT escogidos para el estudio, en donde se observaron las vulnerabilidades presentes en estas tecnologías dependiendo de cada caso con el objetivo de establecer mediante las lecturas obtenidas las posibles medidas para controlarlas.

3.1.3. Investigación tecnológica

Otro método de investigación de la actualidad es la metodología de investigación tecnológica y de desarrollo, la cual se apoya en las teorías y los conocimientos de la ciencia para aplicarlos a la transformación de bienes y servicios útiles a la sociedad; con su aplicación es posible innovar métodos, técnicas y conocimientos para el desarrollo científico y tecnológico de la sociedad, las empresas y la población en general. (Muñoz C. , 2011c).

La sociedad actual viene adoptando en sus hogares una diversidad de dispositivos inteligentes los cuales se denominan del Internet de las cosas sin considerar los riesgos informáticos que estos puedan traer y conlleven a ciberataques para obtener información confidencial.

Por esto la presente investigación está orientada a proponer una guía metodológica a los usuarios en general para que en sus hogares puedan identificar las vulnerabilidades presentes en estos dispositivos y como controlarlos, para lo cual se han utilizado dispositivos especializados para cada tipo de tecnología inalámbrica que fue probada en escenarios que fueron armados de manera específica, el medio de comunicación frecuentemente usado por los dispositivos IoT para la transmisión y recepción de datos es de difícil control si no es correctamente implementada por lo que constituye en una de sus principales vulnerabilidades.

3.2. Método de investigación

El método de investigación será la descriptiva. De acuerdo con este autor, una de las funciones principales de la investigación descriptiva es la capacidad para seleccionar las características fundamentales del objeto de estudio y su descripción detallada de las partes, categorías o clases de dicho objeto. (Bernal, 2013a).

De esta manera se genera la descripción de la situación problemática de las vulnerabilidades informáticas presentes actualmente en los dispositivos IoT que se encuentran en el hogar ante ciberamenazas, los hábitos inseguros, exceso de confianza y las carencias de ciertos conocimientos acerca de seguridad informática en los usuarios pueden promover a el robo de su información sensible ante ciberatacantes, estos factores pueden ser controlados mediante la aplicación de una guía metodológica.

3.2.1. Investigación correlacional

La investigación correlacional tiene como propósito mostrar o examinar la relación entre variables o resultados de variables, uno de los puntos importantes respecto de la investigación correlacional es examinar relaciones entre variables o sus resultados, pero en ningún momento explica que una sea la causa de la otra. En otras palabras, la correlación examina asociaciones, pero no relaciones causales, donde un cambio en un factor influye directamente en un cambio en otro. (Bernal, 2013b).

Por tanto, se pretende generar una relación directa entre la variable independiente: las vulnerabilidades informáticas y su potencial impacto en la variable dependiente los dispositivos IoT (Internet of the things) que se encuentren en redes HAN (Home área network) o redes caseras, y como se asocian en el medio tecnológico.

De esta manera en la metodología se tomó en consideración para el proceso metodológico en el control de la vulnerabilidad los siguientes elementos de acuerdo a la tecnología IoT a probar:

3.2.1.1. Operacionalización de variables

Tabla 1-3: Variable Independiente – Vulnerabilidades

Conceptualización	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Vulnerabilidad es una deficiencia en el diseño, implementación, operación o los controles internos en un proceso, que podría utilizarse para violar la seguridad de un sistema.	<p>Falta de conocimiento sobre seguridad informática</p> <p>Infraestructura de red insegura</p> <p>Falta de medios de protección</p> <p>Deficiencia en controles de seguridad</p>	<p>¿Conoce que son los Cyber Ataques?</p> <p>¿Conoce los riesgos a los que se expone al sufrir un cyber ataque?</p> <p>¿Cómo ha enfrentado el peligro de una vulnerabilidad informática ante un Cyber Ataque?</p> <p>¿Sabe implementar controles para minimizar las vulnerabilidades informáticas?</p> <p>¿Para usted cual es el riesgo que se presenta al momento de no contar con una adecuada protección ante vulnerabilidades informáticas?</p> <p>¿Ha enfrentado el peligro de una vulnerabilidad informática?</p> <p>¿Conoce el riesgo que se presenta al momento de no contar con una protección informática?</p> <p>¿De qué manera enfrenta el riesgo de una vulnerabilidad informática?</p> <p>¿Tiene usted una protección en el sistema informática y de Internet que maneja?</p> <p>¿Cuenta Ud con una protección ante unas vulnerabilidades informáticas en la red de Internet o datos e su hogar?</p> <p>¿Cómo le gustaría acceder al control de vulnerabilidades?</p> <p>¿Cómo desearía implementar controles de seguridad informática para minimizar vulnerabilidades informáticas?</p>	Formulario de encuestas

Realizado por: Mena, D. 2017

Tabla 2-3: Variable Dependiente – Seguridad en Dispositivos IoT

Conceptualización	Indicadores	Ítems Básicos	Técnicas e Instrumentos
<p>IoT es un concepto que hace referencia a una infraestructura de red global que une objetos físicos y virtuales a través de la explotación de la captura de datos y capacidades de comunicación. Esta infraestructura incluye la evolución de Internet y de otras redes existentes implicadas.</p>	<p>Conocimiento acerca de los objetos conectados (IoT)</p> <p>Dispositivos u objetos conectados en el hogar</p> <p>Nivel de protección de la información</p> <p>Factores para establecer seguridad</p>	<p>¿Qué objetos IoT o dispositivos electrónicos tiene usted conectado a las a las redes inalámbricas de su hogar?</p> <p>¿Cree usted que los dispositivos IoT que utiliza en el hogar son seguros?</p> <p>¿Considera usted que ha ingresado información personal en los dispositivos IoT con los cuales interactúa en el hogar?</p> <p>¿Sabe usted si sus datos personales que almacenan, procesan y transmiten los dispositivos IoT de su hogar están seguros?</p> <p>¿La observación el uso diario a los dispositivos IoT de su hogar, servirá para conocer el comportamiento y hábitos de las personas?</p> <p>¿Qué medidas ha tomado para mejorar la seguridad de los dispositivos IoT de su hogar?</p> <p>¿Cuál factor considera más importante para establecer seguridades informáticas en los dispositivos IoT que se encuentran en la red de su hogar?</p>	<p>Formulario de encuestas</p>

Realizado por: Mena, D. 2017

3.3. Pruebas de vulnerabilidad Bluetooth

Para las pruebas de vulnerabilidades en dispositivos IoT que hagan uso de la tecnología Bluetooth, se utilizaron un mini computador Raspberri Pi 2 Modelo B, el cual fue escogido debido a sus características de bajo coste y portabilidad, asimismo se utilizaron dispositivos especializados para el análisis de vulnerabilidades de Bluetooth Clasico y Low Energy como es el dispositivo llamado Ubertooth One y el dongle USB CC2540 ambos operan sin contratiempos bajo el Sistema Operativo GNU Linux a través de un puerto USB.

3.3.1. Elementos de laboratorio

Los dispositivos IoT escogidos para las pruebas con la tecnología Bluetooth se han seleccionado de entretantos conforme a los que habitualmente se encuentran en un hogar y se encuentran vigentes tecnológicamente: relojes inteligentes (Smartwatches), bandas inteligentes, Teléfonos Inteligentes (Smartphones) y Parlantes Bluetooth.

3.3.1.1. Equipo y dispositivos de pruebas

Hardware

- Raspberry Pi 2 Model B
- Ubertooth One
- Dongle USB CC2540
- Dongle Bluetooth BLE USB
- Dispositivos IoT

Software

- Sistema Operativo Raspbian (Raspberry Pi)
- Suite de utilidades Ubertooth
- SmartRF Packet Sniffer
- Blue Hydra
- Crackle
- Btscanner

3.3.1.2. *Dispositivos IoT de prueba*



Figura 1-3: SmartWatch U8

Fuente: (Quetalcompra, 2017)



Figura 2-3: Xiaomi Mi Band 2

Fuente: (CNET, 2017)



Figura 3-3: Smartphone Samsung S6 Edge +

Fuente: (Tecnofullshop, 2017)



Figura 4-3: Dknight Magic Box II

Fuente: (The Tech Insider, 2017)

3.3.2. *Raspberry pi*

La placa Raspberry Pi es un computador que posee la virtud que es de tamaño reducido, fue desarrollado por la Fundación Raspberry Pi que tiene su sede en Reino Unido con el objetivo de fomentar la enseñanza de las ciencias de computación en las escuelas al ser este un producto de bajo coste.

3.3.2.1. *Raspberry Pi 2 Model B*

El Raspberry 2 Model B es la segunda generación de las placas Raspberry Pi y fue puesto a la venta en febrero del 2015 para sustituir el modelo anterior llegando a alcanzar hasta unas seis veces más rápida que esta.



Figura 5-3: Raspberry Pi 2

Fuente: (Wikipedia, 2017)

Características

- Procesador de cuatro núcleos Broadcom BCM2836 ARM Cortex-A7
- GPU VideoCore IV doble núcleo con soporte OpenGL ES 2.0, aceleración por hardware OpenVG, 1080p 30 frames, H.264
- 1 GB LPDDR2 SDRAM
- Salida de vídeo 1080p
- Salida de vídeo compuesto (PAL / NTSC)
- Salida de audio estéreo
- Ethernet 10/100 Base

- HDMI 1.3 y 1.4
- Audio compuesto jack 3,5 mm
- 4 puertos USB 2.0
- MPI CSI-2
- Socket MicroSD
- Conector Serie
- GPIO 40 pines

3.3.2.2. *Ubertooth one*

El proyecto Ubertooth es una plataforma de desarrollo inalámbrica libre para experimentación de la tecnología Bluetooth creado por Michael Ossman, es capaz de capturar paquetes de conexiones BLE (Bluetooth Smart) y ciertos paquetes de BR (Bluetooth Clásico).

El Ubertooth One es la herramienta en el mercado más asequible para realizar pruebas de seguridad de la tecnología Bluetooth BLE ya que su precio se encuentra alrededor de 120USD y tanto su hardware y software son open source.

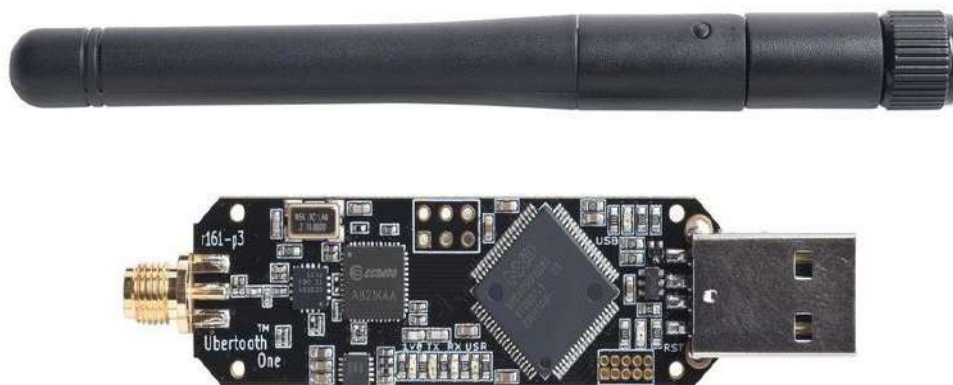


Figura 6-3: Ubertooth One

Fuente: (Project Ubertooth)

Arquitectura

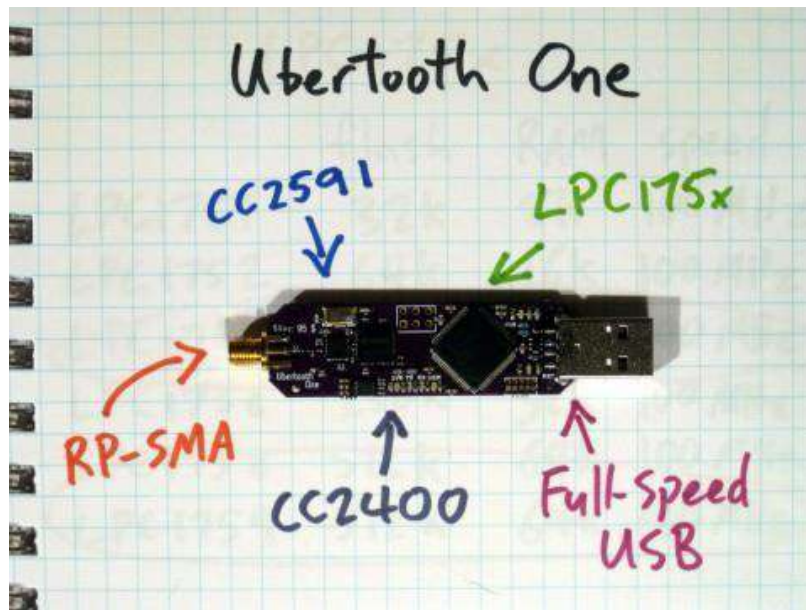


Figura 7-3: Arquitectura Ubertooth One

Fuente: (Project Ubertooth, 2017)

- RP SMA, conector para antenas de Radio Frecuencia RF 2.4 Ghz
- CC2591, Interfaz de RF 2.4 Ghz
- CC2400, Transmisor-Receptor Wireless
- LPC175x, Microcontrolador ARM Cortex-M3 con USB 2.0 Full-speed
- Conector USB

El Ubertooth One está constituido por 3 componentes:

- Dispositivo Hardware Ubertooth One: siendo un dispositivo Bluetooth USB que tanto la sensibilidad de su potencia y recepción es comparable con un dispositivo Bluetooth Clase 1
- Firmware: Software que se ejecuta en el procesador ARM, esta compuesto por un gestor de arranque (bootloader) y el receptor transmisor de Bluetooth (bluetooth_rxtx).
- Software: Es el software que se ejecuta desde un ordenador para controlar el Ubertooth One desde un puerto USB.

3.3.3. Implementación del equipamiento para pruebas de laboratorio

Para las pruebas de vulnerabilidades en dispositivos IoT que utilicen la red Bluetooth para sus comunicaciones

3.3.3.1. Preparación del Raspberry Pi y Ubetooth one

Instalación de Raspbian

El sistema operativo escogido para el Raspberry 2 es el Raspbian, el cual es un GNU Linux basado en Debian Wheezy, debido al gran soporte que posee en las comunidades de Internet. La instalación de Raspbian se detalla paso a paso en el Anexo 1.

3.3.3.2. Sniffer cc2540

El dongle BLE provisto por Texas Instruments es el CC2540 USB kit de evaluación el cual tiene un costo aproximado de \$50 USD, existen en el mercado copias de este con un firmware que permite la captura de paquetes Bluetooth BLE las cuales pueden ser utilizadas con la plataforma SmartRF sin ningún problema.

El dongle USB CC2540 permite incorporar un interfaz Bluetooth Low Energy a cualquier sistema que cuente con un USB host. Su diseño está más orientado a dar soporte a computadores, pero puede integrarse a sistemas como cajas de TV (Set-Top Boxes).

Características

- Conexión fácil que permite agregar BLE a un sistema mediante USB.
- Puede ser usado para depuración y desarrollo en BLE mediante botones y leds incorporados.
- Posee la capacidad de ser usado para capturar paquetes para análisis de protocolos BLE mediante software como SmartRF Packet Sniffer.



Figura 8-3: USB Dongle CC2540

Fuente: (Digi-Key, 2017)

3.3.3.3. *SmartRF packet sniffer*

SmartRF Packet Sniffer es una plataforma creada por Texas Instruments para el diseño, construcción, evaluación y solución a problemas en los circuitos integrados fabricados por esta compañía, entre estos se encuentra el soporte a Bluetooth Low Energy. El link para su descarga desde la página de TI es el siguiente <http://www.ti.com/tool/packet-sniffer>.

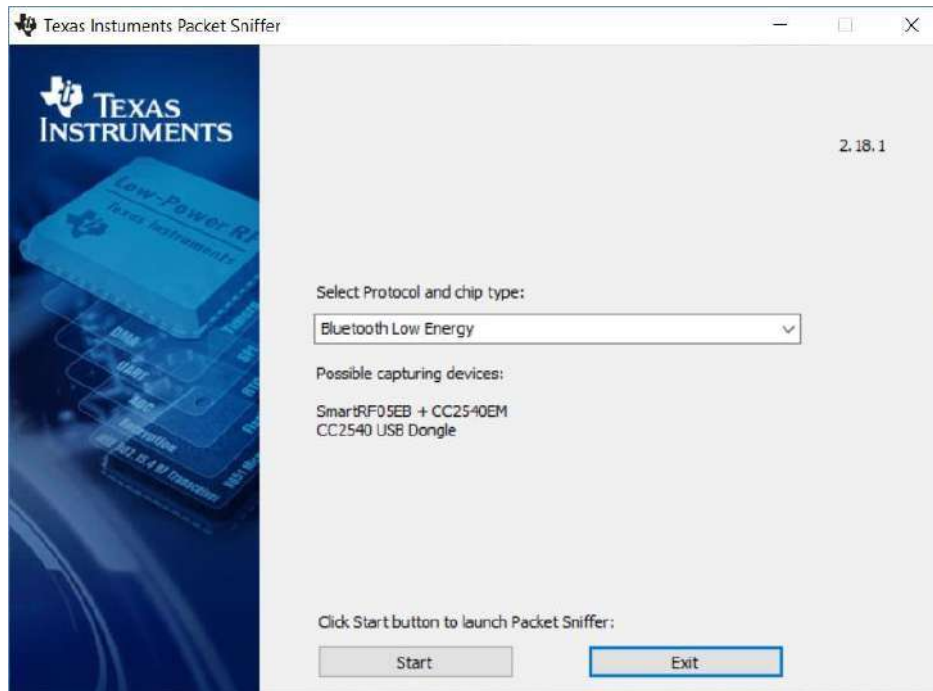


Figura 9-3: Packet Sniffer

Realizado por: Mena, D. 2017

Pantalla inicial, donde permite seleccionar el tipo de tecnología a escanear, en este caso esta seleccionado el soporte al dongle CC2540 USB.

3.3.3.4. *Bluehydra*

Entre las utilidades para reconocimiento de Bluetooth que se encuentran disponibles en los últimos tiempos se encuentra Blue Hydra la cual constituye una herramienta poderosa ya que es capaz de escanear tanto en los dispositivos de Bluetooth clásico como Bluetooth Low Energy mediante el uso de Ubertooth inclusive si estos estuvieran ocultos además puede almacenar los resultados obtenidos en una base de datos para su posterior análisis.

Ciertos dispositivos Bluetooth Low Energy constantemente están emitiendo su estado hacia otros dispositivos cuando su estado se encuentre en reposo esta vulnerabilidad puede ser aprovechada por Blue Hydra ya que puede captar esta información para poder identificar cuales dispositivos están cerca e inclusive mediante el Received Signal Strength Indication (RSSI) estimar la distancia hacia estos.

Instalación de Bluehydra en Raspberry Pi

1. Instalar Ruby

- Instalar ruby con rvm
- `$ curl -L https://get.rvm.io | bash -s stable --ruby`

- Si se muestra un error como el siguiente, se deben seguir las instrucciones indicadas junto al mensaje de error.
- `gpg: Can't check signature: public key not found`

- Constatar la versión de ruby
- `$ rvm current`

- Mediante bundler se instalarán las ruby gems
- `$ sudo gem install bundler`

- Se instalarán las dependencias necesarias
- `$ sudo apt-get install python-bluez python-dbus sqlite3 bluez-tools ruby-dev bluez bluez-test-scripts python-bluez python-dbus libsqlite3-dev ubertooth`

2. Instalar Blue Hydra

```
$ git clone https://github.com/pwnieexpress/blue_hydra.git
```

```
$ cd blue_hydra
```

```
$ bundle install
```

3. Ejecutar Blue Hydra

```
$ sudo ./bin/blue_hydra (Lazaro, s.f.)
```

3.3.3.5. *Btscanner*

La herramienta BTSCANNER disponible para su descarga en <http://www.pentest.co.uk>, o también mediante el gestor de paquetes de Linux apt-get u otras de dependiendo.

El comando para su instalación es el siguiente:

```
$ sudo apt-get install btscanner
```

3.3.3.6. *Crackle*

La herramienta Crackle es una herramienta desarrollada por Mike Ryan que aprovecha una falla en el proceso de emparejamiento de BLE, que puede permitir a un atacante recuperar la clave de emparejamiento o TK (Temporary Key), trabaja con los modos de emparejamiento Just Works y Numeric entry.



Figura 10-3: Crackle

Fuente: (Ryan, 2017)

3.4. Pruebas de vulnerabilidad radiofrecuencia (RF)

En la actualidad han aparecido soluciones para automatizar los hogares dentro de los denominados DIY (Hágalo usted mismo basados en dispositivos RF que operan en las frecuencias de 433 Mhz y 315 Mhz, generalmente estos se conectan a un dispositivo concentrador y permiten la apertura de cerraduras, el control de encendido y apagado de luminarias o de toma corrientes incorporándose la capacidad de ser controlables desde cualquier sitio a través de Internet, muchos hogares los adquieren sin considerar que estos poseen graves vulnerabilidades debido a la tecnología empleada que puede ser aprovechada por un atacante.



Figura 11-3: Hub Hook

Fuente: (Kickstarter, 2016)



Figura 12-3: Switch RF

Fuente: (Ebay, 2017)

3.4.1. Elementos de laboratorio de pruebas

Los elementos escogidos para probar las vulnerabilidades en este tipo de tecnologías son un conjunto de tomacorrientes que operan en la frecuencia de 433 Mhz, los cuales pueden ser integrados a dispositivos IoT como concentradores de automatización de hogar.

3.4.1.1. Equipos y dispositivos de pruebas

Hardware

- RTL – SDR receptor USB 2.0 SDR-DAB-TV - HDTV – FM
- Raspberry Pi 2
- Receptor y transmisor RF 433 Mhz
- Cables y conectores
- Computador portatil

Software

- Sistema Operativo Raspbian (Raspberry Pi)
- Software RTL-SDR bajo el Sistema operativo Windows
- RFSniffer
- Codesend
- Servidor Apache

Dispositivos IoT

- Etekcity Tomacorrientes controlables remotamente mediante RF



Figura 13-3: Kit Etekcity

Fuente: (Tomlinson, 2016)

3.4.1.2. Detección de dispositivos RF en el hogar

A través del uso de dispositivos RTL-SDR (Software Defined Radio), radio definida por software es posible convertir un dongle TV en un analizador de espectros que puede cubrir un rango entre 24 Mhz a 1.766 Ghz, con lo cual para un atacante esta herramienta puede ser útil para mostrar la actividad de los dispositivos RF que operan en el espectro de frecuencias de 433 Mhz o 315 Mhz con lo cual se pudiera establecer si en un hogar existe o no la presencia de estos dispositivos ya que en algunos casos estos controlaran ciertos aspectos del hogar.



Figura 14-3: RTL-SDR

Fuente: (HakShop)

3.4.1.3. Uso del Rtl-sdr software

Para el ataque se utilizó el software RTL-SDR para Windows disponible en la página web <http://www.rtl-sdr.com/big-list-rtl-sdr-supported-software>, existe también soporte para otros sistemas operativos como GNU Linux como para instalarlo en un Raspberri Pi.

Al ejecutarlo luego del proceso de instalación se mostrará una pantalla con varias opciones de configuración se deberá seleccionar como dispositivo origen RTL-SDR USB correspondiente al dongle adquirido y sintonizar a la frecuencia de 433 Mhz debido a que esta es la frecuencia de operación para el encendido y apagado de los tomacorrientes de prueba Eteckcity.

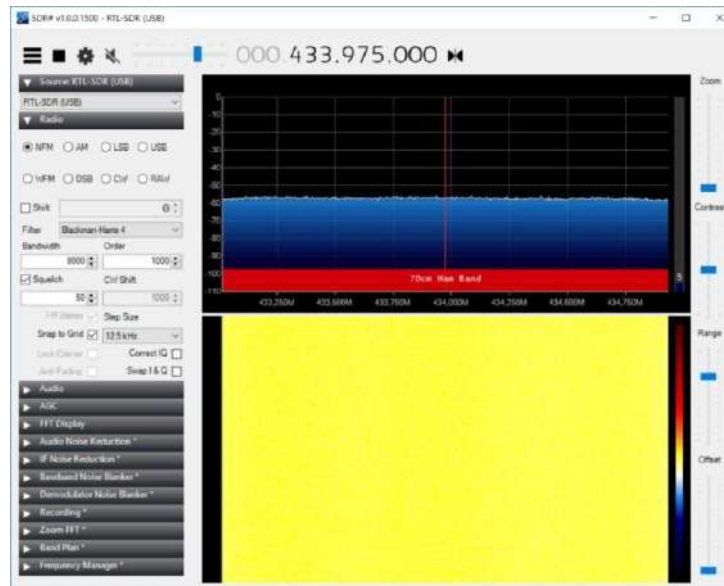


Figura 15-3: Escaneo frecuencia 433 Mhz

Realizado por: Mena, D. 2017

Instalación de Wiring pi

Como se utilizará un Raspberry Pi para la lectura y envío de códigos mediante el transmisor y receptor de 433 Mhz, se instaló Wiring Pi que es necesario para el funcionamiento de RFSniffer y codesend.

La instalación a través de git.

```
$ git clone git://git.drogon.net/wiringPi
```

```
$ cd wiringPi
```

```
$ ./build
```

Puede comprobarse la comunicación a través del interfaz GPIO mediante el comando:

```
$ gpio readall
```

```

pi@raspberrypi: /
File Edit Tabs Help
pi@raspberrypi: / $ gpio readall
+-----Pi 2-----+
| BCM | wPi | Name | Mode | V | Physical | V | Mode | Name | wPi | BCM |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 2 | 8 | 3.3v | IN | 1 | 1 | 2 | | | 5v | | |
| 3 | 9 | SDA_1 | IN | 1 | 3 | 4 | | | 5V | | |
| 4 | 7 | SCL_1 | IN | 1 | 5 | 6 | | | 0v | | |
| 4 | 7 | GPIO_7 | IN | 1 | 7 | 8 | 1 | ALT0 | TxD | 15 | 14 |
| | | | | | 9 | 10 | 1 | ALT0 | RxD | 16 | 15 |
| 17 | 0 | GPIO_0 | IN | 0 | 11 | 12 | 0 | IN | GPIO_1 | 1 | 18 |
| 27 | 2 | GPIO_2 | IN | 0 | 13 | 14 | | | 0v | | |
| 22 | 3 | GPIO_3 | IN | 0 | 15 | 16 | 0 | IN | GPIO_4 | 4 | 23 |
| | | | | | 17 | 18 | 0 | IN | GPIO_5 | 5 | 24 |
| 10 | 12 | 3.3v | IN | 0 | 19 | 20 | | | 0v | | |
| 9 | 13 | MOSI | IN | 0 | 21 | 22 | 0 | IN | GPIO_6 | 6 | 25 |
| 11 | 14 | MISO | IN | 0 | 23 | 24 | 1 | IN | CE0 | 10 | 8 |
| | | SCLK | IN | 0 | 25 | 26 | 1 | IN | CE1 | 11 | 7 |
| | | | | | 27 | 28 | 1 | IN | SCL_0 | 31 | 1 |
| 5 | 21 | SDA_0 | IN | 1 | 29 | 30 | | | 0v | | |
| 6 | 22 | GPIO_21 | IN | 1 | 31 | 32 | 0 | IN | GPIO_26 | 26 | 12 |
| 13 | 23 | GPIO_23 | IN | 0 | 33 | 34 | | | 0v | | |
| 19 | 24 | GPIO_24 | IN | 0 | 35 | 36 | 0 | IN | GPIO_27 | 27 | 16 |
| 26 | 25 | GPIO_25 | IN | 0 | 37 | 38 | 0 | IN | GPIO_28 | 28 | 20 |
| | | | | | 39 | 40 | 0 | IN | GPIO_29 | 29 | 21 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| BCM | wPi | Name | Mode | V | Physical | V | Mode | Name | wPi | BCM |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
pi@raspberrypi: / $

```

Figura 16-3: Instalación GPIO

Realizado por: Mena, D. 2017

3.4.1.4. Instalación de Apache y Php

Para mostrar gráficamente los controles de los tomacorrientes que fueron hackeados, se levantará un servidor web mediante Apache donde se desplegará una página web con botones que permitan el encendido y apagado de los tomacorrientes.

A través del comando siguiente se instalará Apache y PHP

```
$ sudo apt-get install apache2 php5 libapache2-mod-php5 -y
```

3.4.1.5. Conexión de del módulo TX/RX 433mhz

Para la conexión del módulo RF 433 Mhz, que permitirá simular el control de los tomacorrientes se utilizará los pines GPIO de Raspberry Pi, las indicaciones de la forma de conexión de pines es el siguiente:

Modulo transmisor

DATA (pin izquierdo) -> GPIO #17

VCC (pin central) -> +5VDC

GND (pin derecho) -> Ground

Modulo receptor

VCC (pin izquierdo) -> +5VDC

DATA (2ndo pin desde la izquierda) -> GPIO 21/27

GND (pin derecho) -> Ground

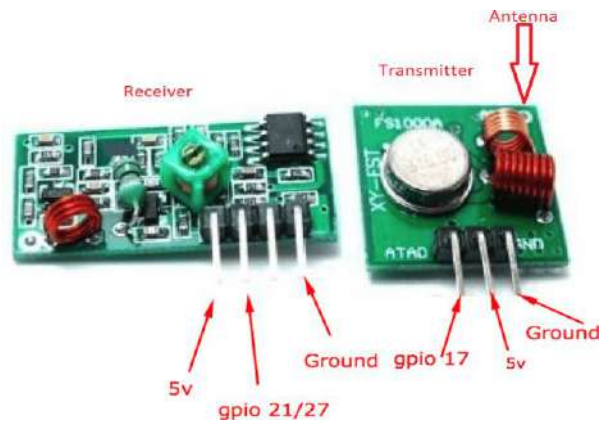


Figura 17-3: Transmisor y Receptor 433 Mhz

Fuente: (Leland, 2014)

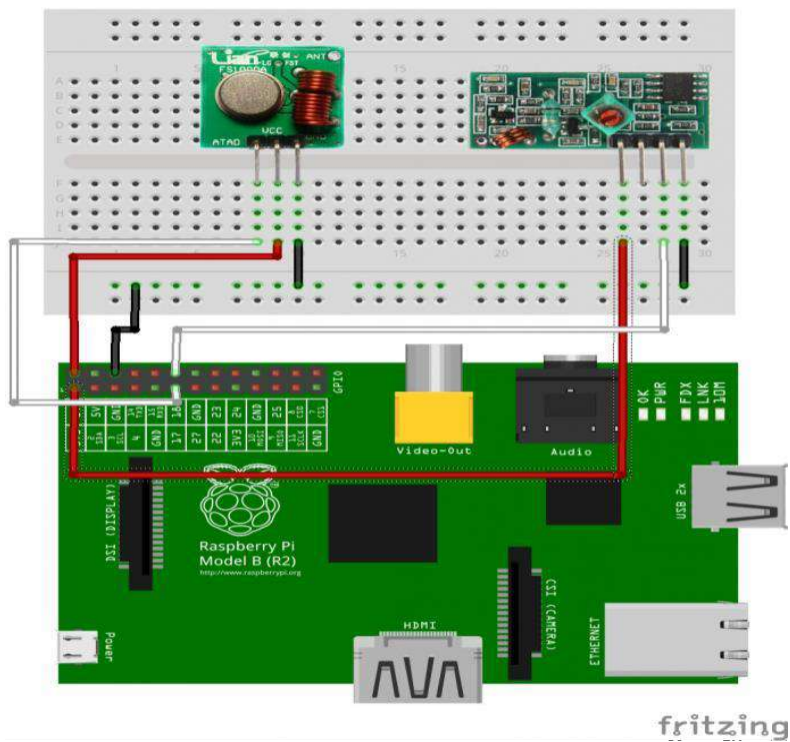


Figura 18-3: Conexión transmisor receptor a Raspberry Pi

Fuente: (Matthinsen, 2015)

3.4.1.6. *Rfsniffer*

En el Raspberry Pi 2, instalaremos la herramienta Rfsniffer escrita por Tim Leland, <https://github.com/timleland/rfoutlet>, la misma que nos permitirá capturar los códigos de encendido y apagado que envía el control remoto a los tomacorrientes Etekcity para luego replicarlos desde un módulo de transmisión 433 Mhz conectado al Raspberry Pi 2.

Instalación De Rfsniffer y asignacion de permisos para codesend

Descarga e instalación mediante GIT

```
$ git clone git://github.com/timleland/rfoutlet.git /var/www/rfoutlet
```

Asignación de permisos para codesend

```
sudo chown root.root /var/www/rfoutlet/codesend
```

```
sudo chmod 4755 /var/www/rfoutlet/codesend
```

3.5. Pruebas de vulnerabilidad Zigbee

Para las pruebas de vulnerabilidades en dispositivos IoT que se comuniquen mediante redes Zigbee, se ha escogido un producto comercial para automatizar hogares llamado Smartthings el cual está compuesto de un dispositivo central que actúa como concentrador, a este se pueden integrar varios elementos de diferentes fabricantes desde bombillas y cerraduras a sensores de varios tipos.

3.5.1. *Equipos y dispositivos de pruebas*

Hardware

- Raspberry Pi 2
- 2 Atmel RZ Raven USB Stick
- Atmel AVR Dragon On-Chip Programmer
- Cables y conectores
-

Software

- Sistema Operativo Raspbian (Raspberry Pi)
- Killerbee

Dispositivos IoT



Figura 19-3: Hub Smarthings

Fuente: (Smarthings)



Figura 20-3: Sensor de movimiento y temperatura Smarthings

Fuente: (Smarthings)



Figura 21-3: Bombilla Inteligente GE Link

Fuente: (GE Link)

3.5.2. *Construcción de un kit de pruebas killerbee*

Para realizar el análisis de vulnerabilidades en las redes Zigbee y 802.15.4 utilizaremos el conjunto de herramientas que provee Killerbee para uso es necesario preparar un hardware específico ya que no todos los dispositivos son soportados.

El Hardware y Software necesario es el siguiente:

- Atmel RZ Raven USB (hardware)
- Atmel AVR Dragon On-Chip Programador (hardware)
- Atmel 100-mm to 50-mm JTAG standoff adaptador (hardware)
- 50-mm male-to-male (hardware)
- Cable 10-pin (2×5) 100-mm female-to-female (hardware)
- AVRDUDE utility (software, gratuito)
- KillerBee firmware for the RZUSBstick (software, gratuito)
- Un computador para programar y cargar Killerbee a los RZ Raven USB.

Atmel RZ Raven USB

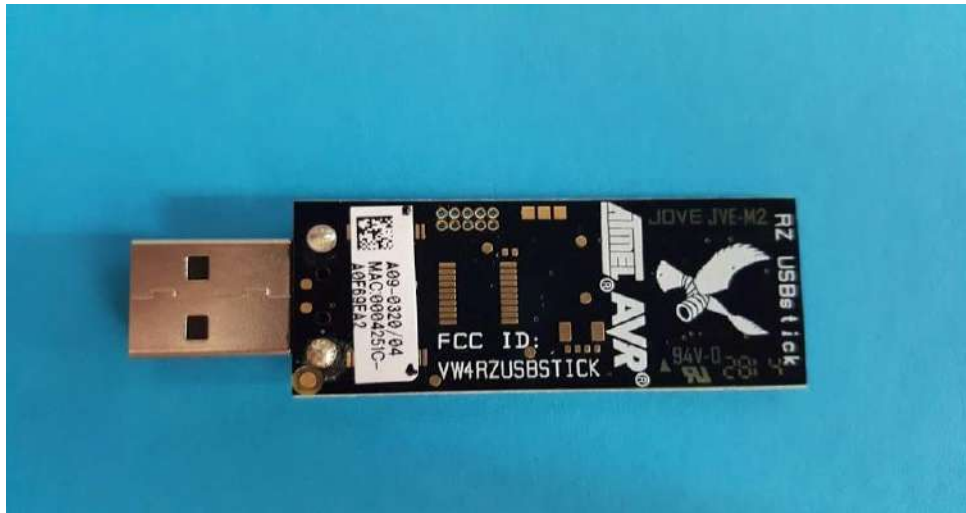


Figura 22-3: ATMEL RZ Raven USB

Realizado por: Mena, D. 2017

Atmel AVR Dragon On-Chip Programador

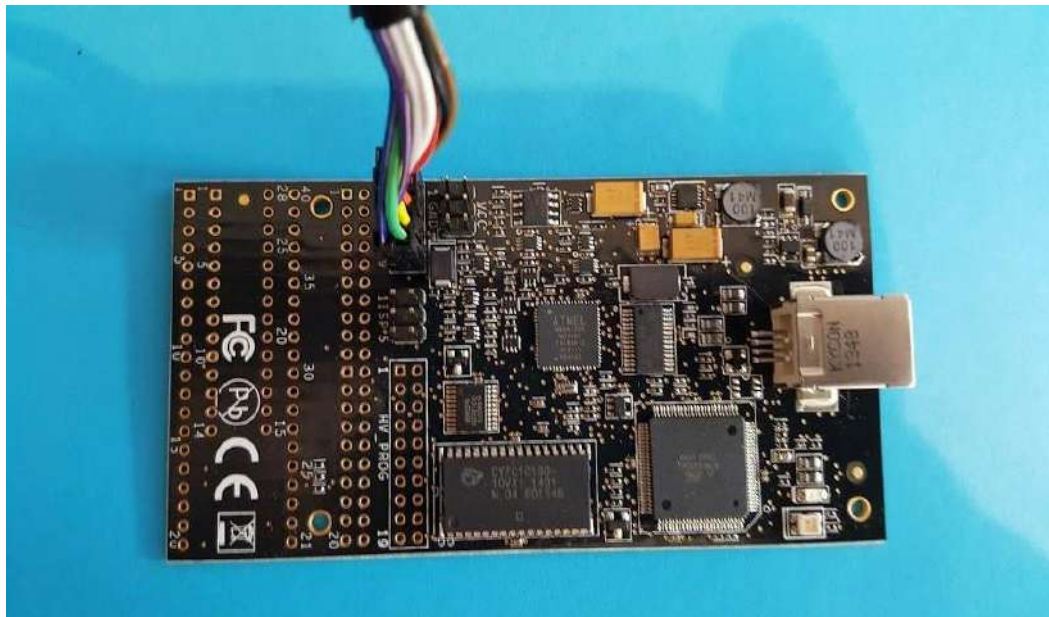


Figura 23-3: ATMEL AVR Dragon On-Chip Programador

Realizado por: Mena, D. 2017

Para poder cargar el firmware de Killerbee en los ATMEL RZ Raven USB, se requiere del siguiente software:

AVR Dude

Es una utilidad por línea de comandos que tiene soporte para varios programadores AVR. Se puede descargar la versión compatible para Windows desde la dirección: <http://winavr.sourceforge.net>.

Firmware Killerbee para ATMEL RZ Raven

El firmware de Killerbee que se cargara a los ATMEL RZ Raven habilitara las funciones de realizar captura de tráfico e inyección de paquetes está disponible de manera gratuita para su descarga desde la dirección: <https://github.com/riverloopsec/killerbee>.

Instalar drivers para Avr Dragon

Para utilizar el programador AVR Dragon en Windows es necesario el driver libusb-win32 que esta disponible en la dirección:

<http://sourceforge.net/projects/libusb-win32>

Una vez realizado se conectara el programador AVR Dragon a un host USB de un computador, y ejecutar la aplicación posteriormente se deben ser los pasos siguientes por defecto hasta que aparezca la opción de aplicar el driver como se muestra en la imagen.



Figura 24-3: Instalación libusb-win32

Realizado por: Mena, D. 2017

Kit armado para programar los ATMEL RZ Raven USB

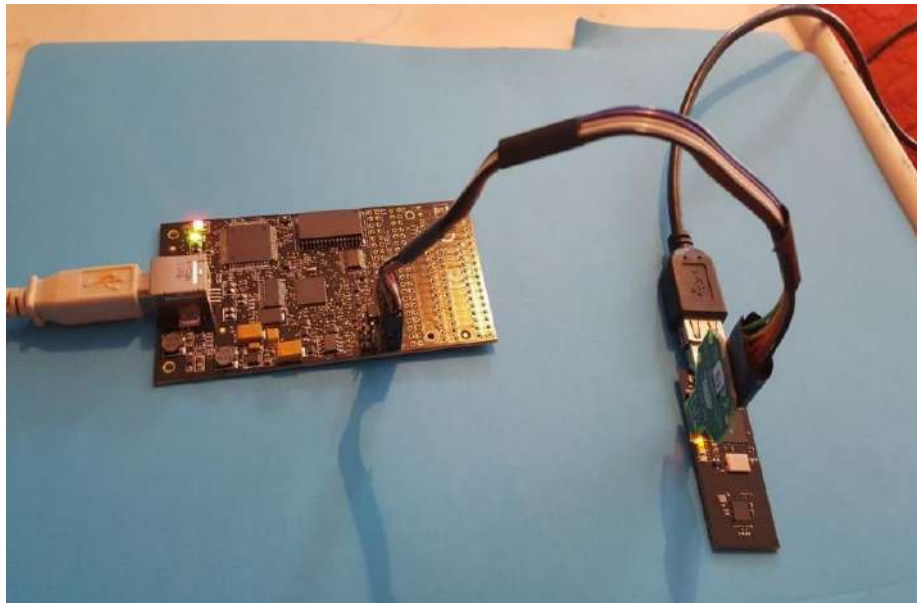
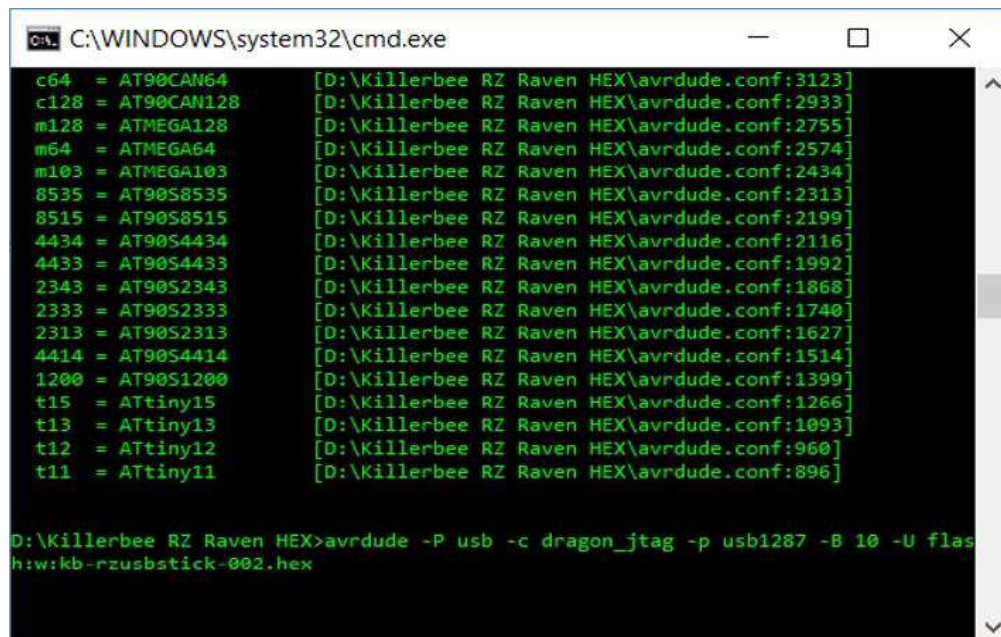


Figura 25-3: KIT ATMEEL RZ Raven USB

Realizado por: Mena, D. 2017

Una vez construido el kit de armado se procederá a cargar el firmware de Killerbee a los ATMEL RZ Raven USB, mediante la herramienta avrdude el comando la aplicar es el siguiente:

```
avrdude -P usb dragon_jtag -p usb1287 -B 10 -U flash:w:kb-rzubstick-002.hex
```



```
C:\WINDOWS\system32\cmd.exe
c64 = AT90CAN64 [D:\Killerbee RZ Raven HEX\avrdude.conf:3123]
c128 = AT90CAN128 [D:\Killerbee RZ Raven HEX\avrdude.conf:2933]
m128 = ATMEGA128 [D:\Killerbee RZ Raven HEX\avrdude.conf:2755]
m64 = ATMEGA64 [D:\Killerbee RZ Raven HEX\avrdude.conf:2574]
m103 = ATMEGA103 [D:\Killerbee RZ Raven HEX\avrdude.conf:2434]
8535 = AT90S8535 [D:\Killerbee RZ Raven HEX\avrdude.conf:2313]
8515 = AT90S8515 [D:\Killerbee RZ Raven HEX\avrdude.conf:2199]
4434 = AT90S4434 [D:\Killerbee RZ Raven HEX\avrdude.conf:2116]
4433 = AT90S4433 [D:\Killerbee RZ Raven HEX\avrdude.conf:1992]
2343 = AT90S2343 [D:\Killerbee RZ Raven HEX\avrdude.conf:1868]
2333 = AT90S2333 [D:\Killerbee RZ Raven HEX\avrdude.conf:1740]
2313 = AT90S2313 [D:\Killerbee RZ Raven HEX\avrdude.conf:1627]
4414 = AT90S4414 [D:\Killerbee RZ Raven HEX\avrdude.conf:1514]
1200 = AT90S1200 [D:\Killerbee RZ Raven HEX\avrdude.conf:1399]
t15 = ATtiny15 [D:\Killerbee RZ Raven HEX\avrdude.conf:1266]
t13 = ATtiny13 [D:\Killerbee RZ Raven HEX\avrdude.conf:1093]
t12 = ATtiny12 [D:\Killerbee RZ Raven HEX\avrdude.conf:960]
t11 = ATtiny11 [D:\Killerbee RZ Raven HEX\avrdude.conf:896]

D:\Killerbee RZ Raven HEX>avrdude -P usb -c dragon_jtag -p usb1287 -B 10 -U flash:w:kb-rzubstick-002.hex
```

Figura 26-3: Instalación Firmware Killerbee

Realizado por: Mena, D. 2017

```
C:\WINDOWS\system32\cmd.exe
O:\Killerbee RZ Raven HEX>avrdude -P usb -c dragon_jtag -p usb1287 -B 10 -U flash:kb-rzusbstick-002.hex
avrdude: jtagmkII_initialize(): warning: OCDEN fuse not programmed, single-byte EEPROM updates not possible
avrdude: AVR device initialized and ready to accept instructions

Reading | ##### | 100% 0.04s

avrdude: Device signature = 0x1e9782
avrdude: NOTE: FLASH memory has been specified, an erase cycle will be performed
        To disable this feature, specify the -D option.
avrdude: erasing chip
avrdude: jtagmkII_initialize(): warning: OCDEN fuse not programmed, single-byte EEPROM updates not possible
avrdude: reading input file "kb-rzusbstick-002.hex"
avrdude: input file kb-rzusbstick-002.hex auto detected as Intel Hex
avrdude: writing flash (26818 bytes):

Writing | ##### | 100% 3.36s

avrdude: 26818 bytes of flash written
avrdude: verifying flash memory against kb-rzusbstick-002.hex:
avrdude: load data flash data from input file kb-rzusbstick-002.hex:
avrdude: input file kb-rzusbstick-002.hex auto detected as Intel Hex
avrdude: input file kb-rzusbstick-002.hex contains 26818 bytes
avrdude: reading on-chip flash data:

Reading | ##### | 100% 3.58s

avrdude: verifying ...
avrdude: 26818 bytes of flash verified

avrdude: safemode: fuses OK

avrdude done. Thank you.

O:\Killerbee RZ Raven HEX>
```

Figura 27-3: Finalización Instalación Killerbee

Realizado por: Mena, D. 2017

3.6. Alcance de la investigación

El alcance de la investigación está sustentado en el momento en que se genere el control del manejo de las vulnerabilidades informáticas a manera de prevención, el cual se da desde la gestión organizacional que se efectúe para poder generar un marco de trabajo de seguridad, de manera que se organicen adecuadamente los recursos y entonces poder establecer un cambio sistemático en dicha gestión, de manera que los datos informáticos se encuentren seguros mediante procedimientos integrales.

3.6.1. Población de estudio

Una vez que se ha definido cuál será la unidad de análisis, se procede a delimitar la población que va a ser estudiada y sobre la cual se pretende generalizar los resultados. Así, una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones. (Hernández, 2013a).

El universo de la población escogido para la investigación corresponde a los 113 funcionarios que laboran en la institución pública SIS ECU911 Ambato, por la variedad de hogares de diversos estratos sociales y económicos reflejados en los dispositivos IoT que posee cada uno.

3.6.2. *Unidad de análisis*

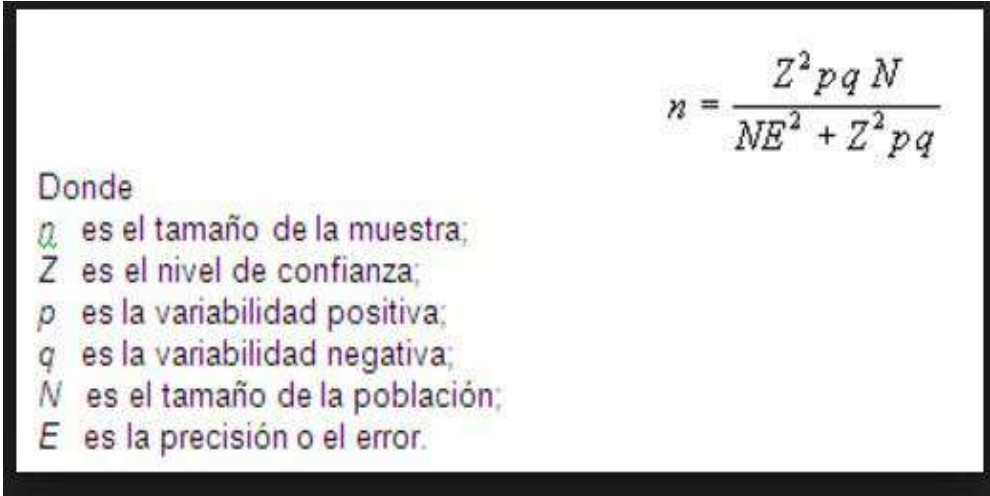
La unidad de análisis está determinada en el proceso investigativo el control de las vulnerabilidades informáticas y su potencial impacto en dispositivos IoT (Internet of the things) para redes HAN (Home área network).

Selección de la muestra

De esta manera se ha establecido la muestra en la investigación de la siguiente manera:

Tamaño de la muestra

Se determina un muestreo probabilístico regulado en el cual la misma población se convierte en una muestra de 80 personas que conforman el universo para nuestra investigación.


$$n = \frac{Z^2 pq N}{NE^2 + Z^2 pq}$$

Donde

- n es el tamaño de la muestra;
- Z es el nivel de confianza;
- p es la variabilidad positiva;
- q es la variabilidad negativa;
- N es el tamaño de la población;
- E es la precisión o el error.

Figura 28-3: Formula Muestra

Fuente: (Diaz Tarascó, s.f.)

Tabla 3-3: Calculo Muestra

CONFIANZA	0,05
Z	1,64
p	0,5
q	0,5
N	113
E	0,05
TAMAÑO MUESTRA	79,7087594

Realizado por: Mena, D. 2017

Técnicas de recolección de la información

Las técnicas de recolección de información permiten recoger datos acerca de la problemática presentada, de esta manera se utilizará lo siguiente:

3.6.3. Encuesta

Indica (Hernández, 2012b). En el desarrollo de la investigación también se generará una recolección de información primaria para lo cual se establecerá un cuestionario direccionado al personal que genera el proceso de control, para conocer sus falencias y necesidades de cambio. El cuestionario se define como una técnica estructurada para recopilar datos, que consiste en una serie de preguntas, escritas y orales, que debe responder un entrevistado.

De esta manera se establece la utilización de una encuesta para recabar información acerca de la necesidad de la guía metodológica del control de las vulnerabilidades informáticas y su potencial impacto en dispositivos IoT (Internet of the things) para redes HAN (Home área network). Las preguntas de la encuesta se encuentran en el Anexo 2.

3.6.4. Observación

Este método de recolección de datos consiste en el registro sistemático, válido y confiable de comportamientos y situaciones observables, a través de un conjunto de categorías y subcategorías. Útil. (Hernández, 2013c).

Se generará la utilización de una ficha de observación para recabar información acerca de la problemática presentada.

3.6.5. Instrumentos de recolección de datos

Para generar la recolección de la información se estableció la utilización de un cuestionario, el mismo que estuvo direccionado a la población en estudio.

3.6.6. Instrumento para procesar datos recopilados

De esta manera para el procesamiento de los datos se lo estableció mediante la utilización del programa estadístico SPSS.

3.6.7. Validación de la información

La validez de la información está determinada por que se presentó el cuestionario a 2 técnicos y expertos en la materia, para su revisión y aprobación la cual se fundamenta en la correlación teórica de las preguntas con cada una de las variables de estudio y así se genera pertenecía, por tanto, la validación y la confiabilidad está sustentada en el proceso investigativo. También en la estructura interna del cuestionario se generó en base a cuatro características específicas como:

- Habilidades operacionales en el desarrollo del producto
- Información suministrada al cliente acerca del producto

Para el proceso de validación se la información se utilizó:

1. Determinar el conocimiento de los encuestados acerca del Internet de las Cosas.
2. Determinar el conocimiento de los encuestados acerca de la presencia de los Dispositivos IoT en el hogar.
3. Determinar el conocimiento de los encuestados acerca de los ataques informáticos o Cyberataques.
4. Determinar los conocimientos de los encuestados acerca de las vulnerabilidades informáticas y los riesgos que conllevan.
5. Determinar los conocimientos de los encuestados sobre las medidas de protección que poseen.

Los informes de validación se encuentran en el Anexo 3.

Pregunta N° 01.- ¿Conoce que son los Cyber Ataques?

Tabla 4-3: Cyber Ataques

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
SI	20	25,0	25,0	25,0
Válidos NO	60	75,0	75,0	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

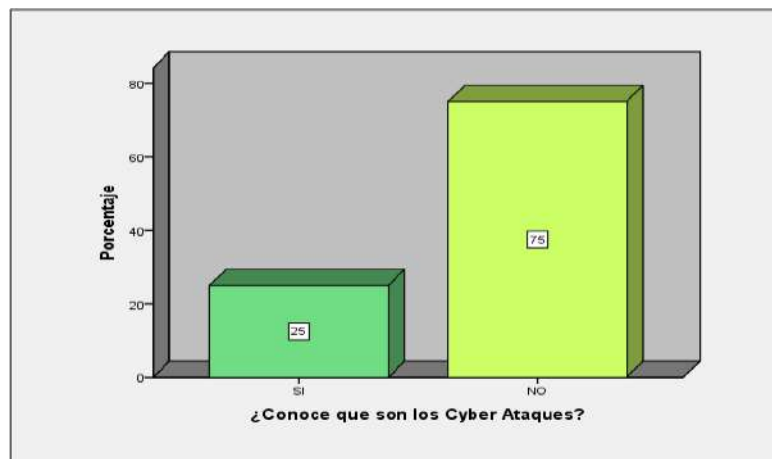


Gráfico 1-3: Cyber Ataques

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un 25% del total de personas afirma conocer lo que son los cyber ataques, en tanto que la mayoría del 75% asegura que no conoce lo que son.

Hay una gran parte de personas que desconocen los cyber ataques y lo que estos conllevan, sin embargo, solo hay pocas personas que si saben lo que son.

Pregunta N° 02.- ¿Conoce los riesgos a los que se expone al sufrir un Cyber Ataque?

Tabla 5-3: Conocimiento de riesgos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	22	27,5	27,5
	NO	58	72,5	100,0
	Total	80	100,0	100,0

Realizado por: Mena, D. 2017

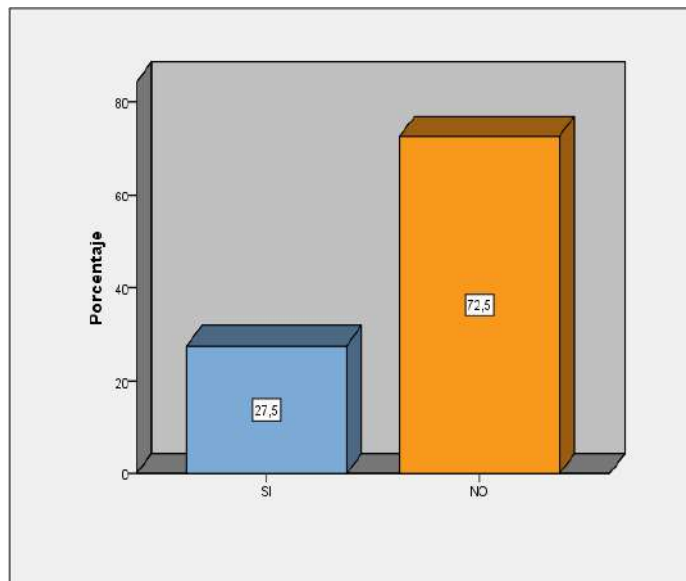


Gráfico 2-3: Conocimiento de riesgos

Realizado por: Mena, D. 2017

Análisis e interpretación:

El primer 27,2% de encuestados asegura saber los riesgos que conlleva los cyber ataques, por otro lado el 72,5% desconoce los riesgos de estos.

La mayoría de personas desconocen sobre los cyber ataques y los riesgos que estos conllevan.

Pregunta N° 03.- ¿Cómo ha enfrentado el peligro de una vulnerabilidad informática ante un Cyber Ataque?

Tabla 6-3: Enfrentamiento del peligro

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Mantenimiento permanente	17	21,3	21,3
	Capacitación personalizada	26	32,5	53,8
	Ninguno	37	46,3	100,0
	Total	80	100,0	100,0

Realizado por: Mena, D. 2017

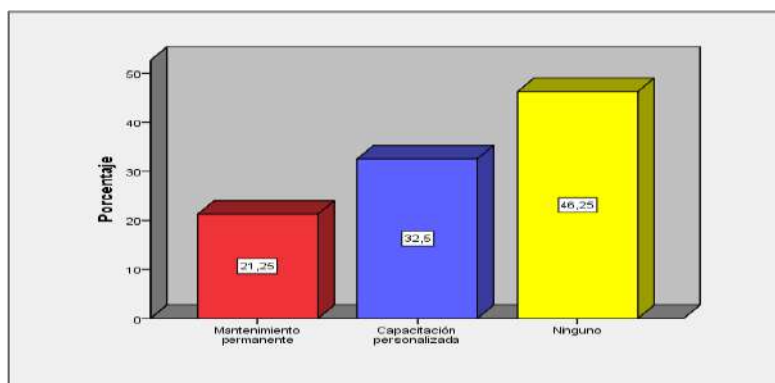


Gráfico 3-3: Enfrentamiento del peligro

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 21,3% de encuestados contestó que enfrenta los cyber ataques con mantenimiento permanente, seguido de un 32,5% afirmando que lo hace con capacitación personalizada, en tanto que el último 46,3% de personas asegura que no lo hace con ninguno.

Pocas personas que conocen de los cyber ataques son las que se enfrentan o previenen de estos, sin embargo, la mayoría no hace nada al respecto.

Pregunta N° 04.- ¿Sabe implementar controles para minimizar las vulnerabilidades informáticas?

Tabla 7-3: Minimizar vulnerabilidades

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	28	35,0	35,0
	NO	52	65,0	100,0
	Total	80	100,0	100,0

Realizado por: Mena, D. 2017

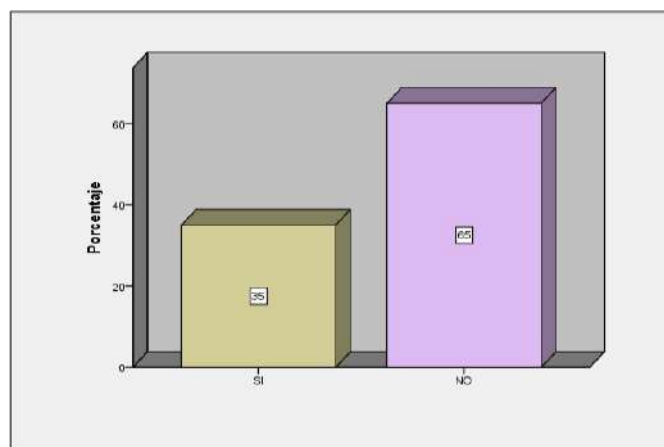


Gráfico 4-3: Minimizar vulnerabilidades

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 35% de personas asegura que si sabe implementar controles para minimizar las vulnerabilidades informáticas, mientras que el restante 65% dice no saber hacerlo.

Pocas personas son capaces de implementar controles para minimizar las vulnerabilidades informáticas, por lo que es recomendable que la mayoría de personas que no pueden hacerlo, aprendan a implementar estos seguros.

Pregunta N° 05.- ¿Para usted cual es el riesgo que se presenta al momento de no contar con una adecuada protección ante vulnerabilidades informáticas?

Tabla 8-3: Riesgos de no tener protección

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos				
Robo de información personal	17	21,3	21,3	21,3
Contagio de virus informáticos	15	18,8	18,8	40,0
Perdida de información importante	12	15,0	15,0	55,0
Acceso a la red de Internet de su casa	14	17,5	17,5	72,5
Mal funcionamiento de dispositivos electrónicos	22	27,5	27,5	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

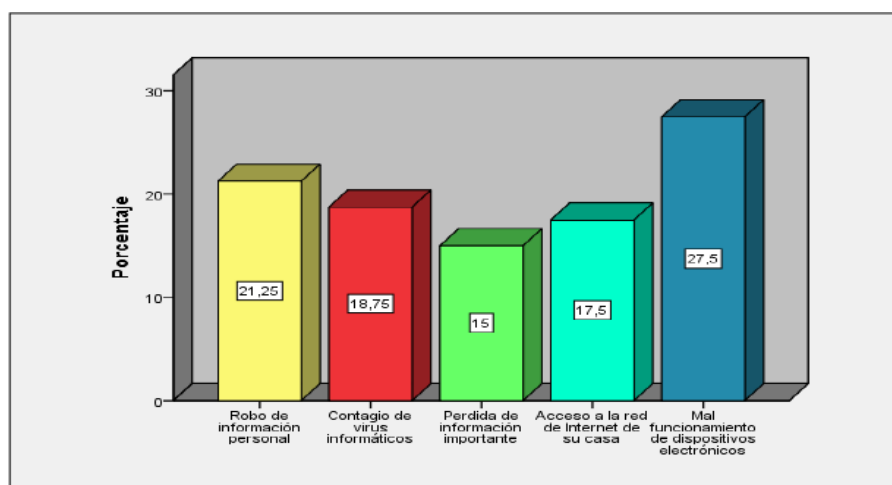


Gráfico 5-3: Riesgos de no tener protección

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 21,3% del total afirma que el robo de información personal es un riesgo de no tener una protección informática seguido de un 18,8% que en cambio dice el riesgo es el contraer virus informáticos, un tercer 15% en cambio asegura que más riesgoso es perder información

importante, por otro lado un 17,5% sostiene que se vulneraría su red de Internet, mientras que el 27,5% defiende que el riesgo sería el mal funcionamiento de equipos electrónicos.

El riesgo más notable de los cyber ataques es el mal funcionamiento de dispositivos electrónicos, el resto tiene conexión entre sí ya que, con virus, estos pueden vulnerar redes y robar información personal.

Pregunta N° 06.- ¿Ha enfrentado el peligro de una vulnerabilidad informática?

Tabla 9-3: Enfrentado el peligro

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos SI	33	41,3	41,3	41,3
NO	47	58,8	58,8	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

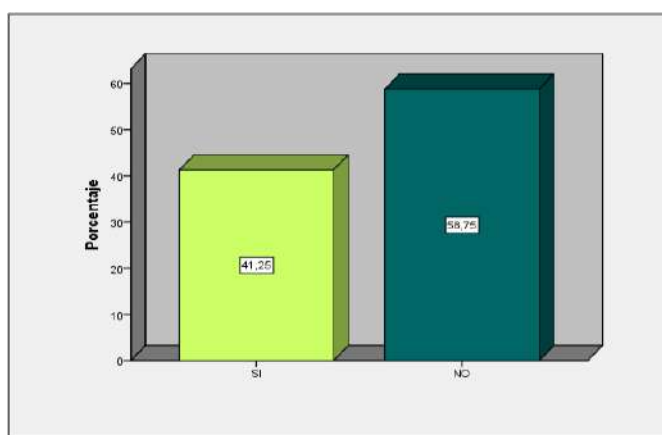


Gráfico 6-3: Enfrentado el peligro

Realizado por: Mena, D. 2015

Análisis e interpretación:

El primer 41,3% de personas asegura si haber enfrentado vulnerabilidades informáticas, seguido del restante 58,8% que afirma no haberlo enfrentado.

Las personas que respondieron que no han enfrentado una vulnerabilidad informática, a lo mejor no reconocieron que sufrieron una.

Pregunta N° 07.- ¿De qué elemento depende para usted la existencia de un control de vulnerabilidad informática?

Tabla 10-3: Elemento para existencia de control

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Desconocimiento de las vulnerabilidades informáticas	20	25,0	25,0
	Inexistencia de herramientas de control	15	18,8	43,8
	Equipos que presentan fallas en su seguridad	13	16,3	60,0
	De las anteriores	32	40,0	100,0
	Total	80	100,0	100,0

Realizado por: Mena, D. 2017

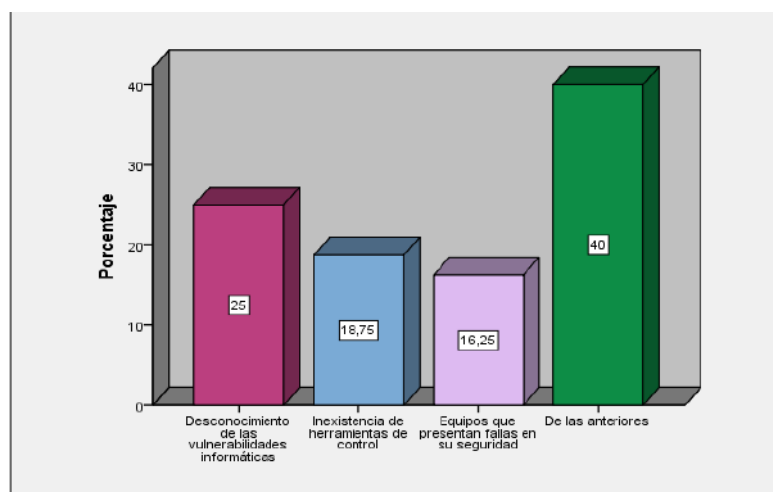


Gráfico 7-3: Elemento para existencia de control

Realizado por: Mena, D. 2017

Análisis e interpretación:

Según un primer 25% el desconocimiento de las vulnerabilidades informáticas es un elemento que depende para la existencia de un control de vulnerabilidad informática, seguido de un 18,8% que cree que este elemento es la inexistencia de herramientas de control, seguido de un 16,3% que afirma que esto depende de los equipos que presentan fallas en su seguridad, en tanto que el restante 40% asegura que depende de todas las respuestas anteriores.

Tanto el desconocimiento de las vulnerabilidades informáticas como la inexistencia de herramientas de control y equipos con fallas en su seguridad son elementos que dependen para la existencia de un control de vulnerabilidad informática.

Pregunta N° 08.- ¿Conoce el riesgo que se presenta al momento de no contar con una protección informática?

Tabla 11-3: Conocimiento de no tener protección

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
SI	23	28,8	28,8	28,8
Válidos NO	57	71,3	71,3	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

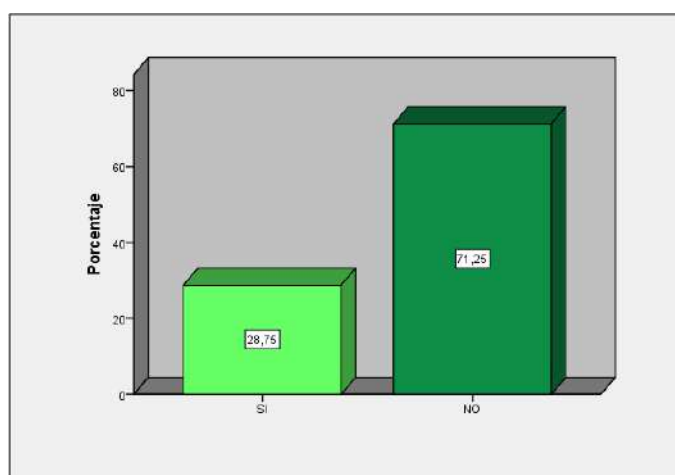


Gráfico 8-3: Conocimiento de no tener protección

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 28,8% de personas afirma conocer los riesgos que se presentan si no se cuenta con una protección informática, seguido de la mayoría del 71,3% que sostiene no conocer estos riesgos.

La mayoría de gente afirma no conocer los riesgos que conlleva el no tener una protección informática adecuada, por lo que tampoco le dan importancia a implementar una.

Pregunta N° 09.- ¿De qué manera enfrenta el riesgo de una vulnerabilidad informática?

Tabla 12-3: Manera de enfrentar el riesgo

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Consulta información relacionada en Internet	17	21,3	21,3	21,3
Permanente actualización del software de protección informática	18	22,5	22,5	43,8
Permanente actualización del firmware de los dispositivos electrónicos	14	17,5	17,5	61,3
Asesoría profesional	16	20,0	20,0	81,3
Ninguna	15	18,8	18,8	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

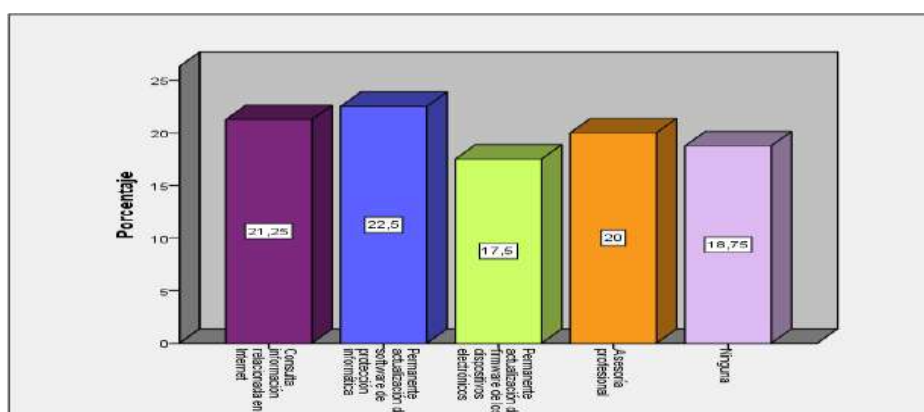


Gráfico 9-3: Manera de enfrentar el riesgo

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 21,3% del total enfrenta una vulnerabilidad informática consultando información relacionada en Internet, un segundo 22,5% en cambio dice que lo enfrenta con la permanente actualización de software de protección, seguido de un tercer grupo del 17,5% que lo hace mediante la permanente actualización de software de los dispositivos electrónicos, un cuarto grupo en cambio del 20% asegura que lo enfrenta con asesoría profesional y el ultimo 18% por otro lado dice que no lo hace de ningún modo.

La opción más recomendable es la actualización de software de protección como antivirus, sin embargo esta no tienen tanta diferencia con el resto de opciones, por lo que también son alternativas viables para implementa, con excepción de no implementar ninguna que es la última opción.

Pregunta N° 10.- ¿Tiene usted una protección en el sistema informático y de Internet que maneja?

Tabla 13-3: Protección en el sistema informático

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
SI	28	35,0	35,0	35,0
Válidos NO	52	65,0	65,0	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

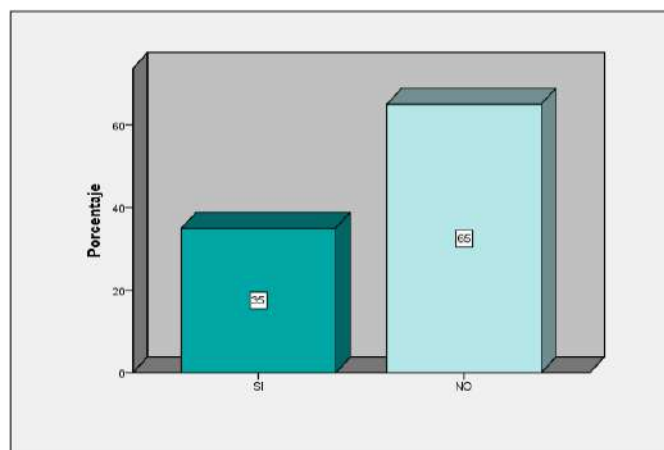


Gráfico 10-3: Protección en el sistema informático

Realizado por: Mena, D. 2017

Análisis e interpretación:

Solo la pequeña parte del 35% de encuestados asegura contar con un sistema de protección informática y de internet, en tanto que la mayoría del 65% dice no contar con ningún software o herramienta de este tipo.

La mayoría de gente no cuenta con sistemas de protección informática y de Internet por lo que es recomendable que implementen algún tipo de protección para evitar ataques relacionados.

Pregunta N° 11.- ¿Cuenta Ud. con una protección ante vulnerabilidades informáticas en la red de Internet o datos de su hogar

Tabla 14-3: Cuenta con una protección

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
SI	25	31,3	31,3	31,3
NO	55	68,8	68,8	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

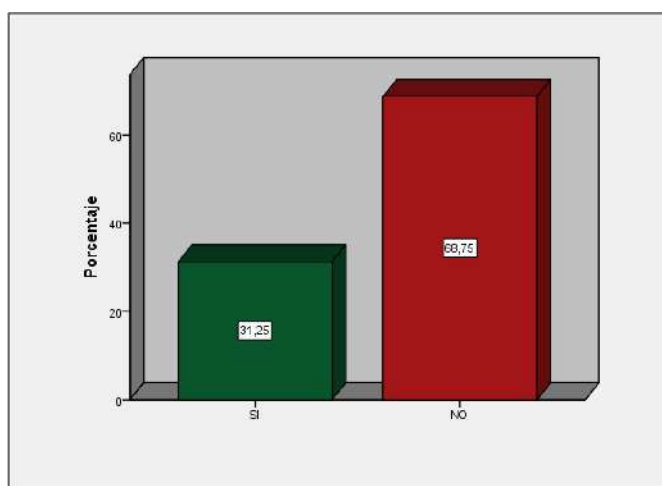


Gráfico 11-3: Cuenta con una protección

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 31,3% de personas asegura contar con un sistema de protección ante vulnerabilidades de red de Internet y de datos, seguido de un 68,8% del total que asegura no tener ningún sistema de protección.

La mayoría de personas no cuenta con ningún sistema de protección ante vulnerabilidades de Internet o datos, por lo que se recomienda que cuenten con una herramienta de este tipo.

Pregunta N° 12.- ¿Cómo le gustaría acceder al control de la vulnerabilidad?

Tabla 15-3: Acceder al control de la vulnerabilidad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Guías especializadas	35	43,8	43,8	43,8
Válidos Acceso por Internet	45	56,3	56,3	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

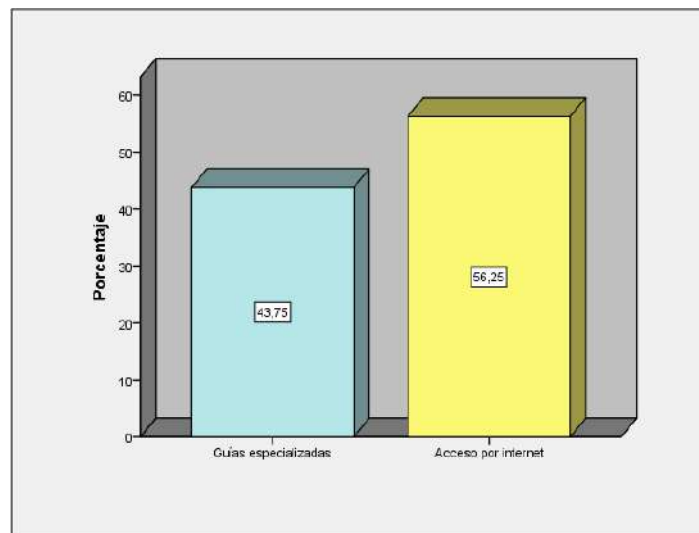


Gráfico 12-3: Acceder al control de la vulnerabilidad

Realizado por: Mena, D. 2017

Análisis e interpretación:

Para un primer 43,8% las guías especializadas serian una forma de acceder al control de vulnerabilidad, por otro lado, un 56,3% asegura que la mejor forma de acceder seria mediante Internet.

Al no haber tanta diferencia entre ambas opciones, es recomendable aplicar las dos formas para acceder al control de vulnerabilidad.

Pregunta N° 13.- ¿Cómo desearía implementar controles de seguridad informática para minimizar las vulnerabilidades informáticas en su hogar?

Tabla 16-3: Como implementar controles de seguridad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Internet	18	22,5	22,5	22,5
Asesorías eventuales	17	21,3	21,3	43,8
Válidos	15	18,8	18,8	62,5
Guía metodológica	30	37,5	37,5	100,0
Capacitación permanente	80	100,0	100,0	
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

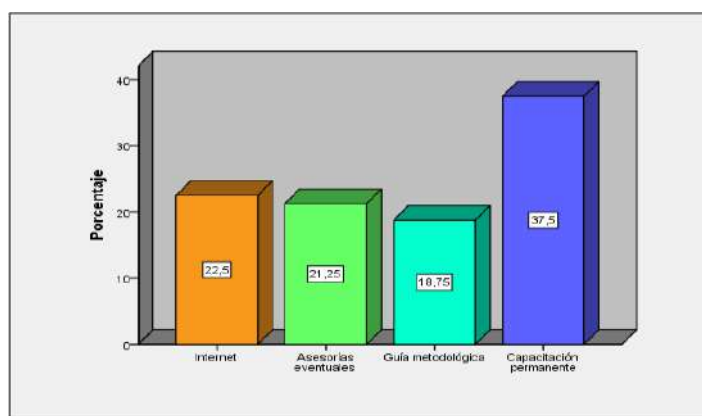


Gráfico 13-3: Como implementar controles de seguridad?

Realizado por: Mena, D. 2017

Análisis e interpretación:

El Internet sería una forma de implementar controles de seguridad informática, eso según un primer 22,5%, a continuación, un 21,3% sostiene que las asesorías eventuales serian una forma de implementar estos controles, seguido de un tercer 18,8% asegurando que se lo haría mejor mediante una guía metodológica, en tanto que el ultimo 37,5% afirma que convendría la capacitación permanente.

Por un amplio margen, la capacitación permanente es la mejor forma de implementar controles de seguridad informática, en caso de que no se aplique esto, también son viables las otras 3 alternativas ya que no existe demasiada diferencia de aceptación entre ellas.

Pregunta N° 14.- ¿Conoce usted que son los dispositivos IoT (Internet de las Cosas)?

Tabla 17-3: Conoce acerca de IoT

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos SI	24	30,0	30,0	30,0
NO	56	70,0	70,0	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

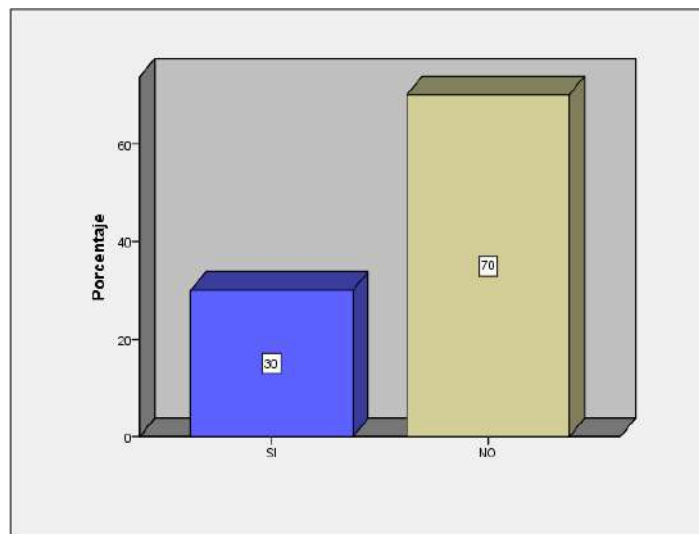


Gráfico 14-3: Conoce de IoT

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 30% del total de encuestados asegura conocer lo que son los dispositivos IOT, seguido de la mayoría del 70% afirmando no conocer sobre estos aparatos.

La mayoría de personas no conoce sobre los dispositivos IOT los cuales son la mayoría de aparatos que usamos hoy en día ya que casi todos están conectados a redes de Internet y datos.

Pregunta N° 15.- ¿Qué objetos IoT o dispositivos electrónicos tiene usted conectado a las redes inalámbricas de su hogar?

Tabla 18-3: Dispositivos IOT

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Teléfonos celulares	11	13,8	13,8	13,8
Tablet	13	16,3	16,3	30,0
Computadores	15	18,8	18,8	48,8
Relojes inteligentes	10	12,5	12,5	61,3
Sistemas de automatización del hogar	13	16,3	16,3	77,5
Modem	11	13,8	13,8	91,3
Router	7	8,8	8,8	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

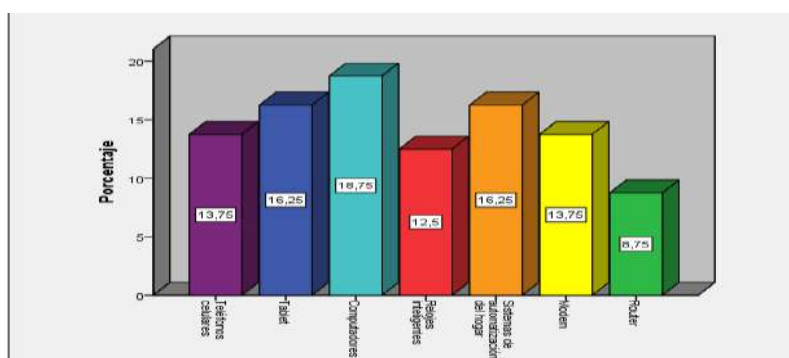


Gráfico 15-3: Conoce de IOT

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 13,8% de personas contestaron que un dispositivo IOT que mantienen conectado a redes de Internet son los teléfonos móviles, seguido de un de tablets con un 16,3% del total, un tercer 18,8% en cambio asegura que estos dispositivos son las computadoras, un cuarto 12,5% en cambio opta por los relojes inteligentes, seguido de un 16,3% que mantiene sistemas de automatización del hogar, por otro lado un 13,8% se inclina por módems y un último 8,8% asegura que estos dispositivos son los routers.

El dispositivo IOT que mantienen más conexión a redes de Internet son obviamente las computadoras, seguido de teléfonos celulares y tablets de nueva generación, sin embargo tanto

los relojes inteligentes como los módems de Internet y sistemas de automatización no se quedan atrás, dejando de último a los routers.

Pregunta N° 16.- ¿Cree usted que los dispositivos electrónicos IoT que utiliza en el hogar son seguros?

Tabla 19-3: Dispositivos seguros

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	47	58,8	58,8	58,8
	NO	33	41,3	41,3	100,0
	Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

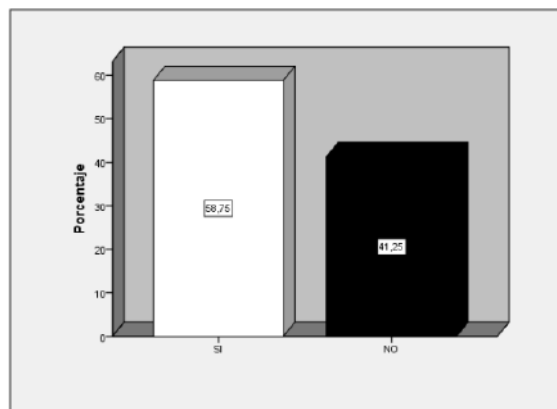


Gráfico 16-3: Dispositivos seguros

Realizado por: Mena, D. 2017

Análisis e interpretación:

La mayoría del 58,8% de personas asegura que los dispositivos IOT que usa en su hogar son seguros, en tanto que el restante 41,3% afirma que no lo son totalmente.

La mayoría de gente asegura que los dispositivos que usa si son seguros, pero el resto de personas que considera que no lo son no está segura de porqué.

Pregunta N° 17.- ¿Considera usted que ha ingresado información personal en los dispositivos IoT con los cuales interactúa en el hogar?

Tabla 20-3: Información personal

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos SI	46	57,5	57,5	57,5
NO	34	42,5	42,5	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

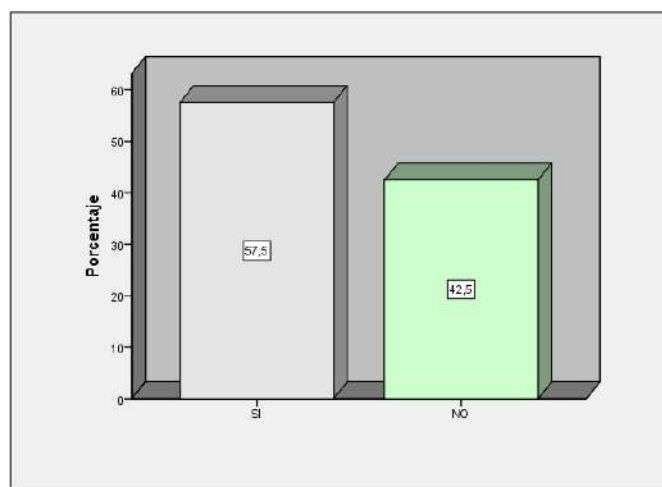


Gráfico 17-3: Información personal

Realizado por: Mena, D. 2017

Análisis e interpretación:

La primera parte del 57,5% del total de encuestados asegura haber ingresado información personal en dispositivos con los que interactúa, seguido de un 42,5% que afirma no haberlo hecho en ningún dispositivo.

Es recomendable saber que tan seguros son los dispositivos con los que interactúa antes de ingresar información personal como correos electrónicos o números de tarjetas de crédito.

Pregunta N° 18.- ¿Sabe usted si sus datos personales que almacena, procesa y transmite los dispositivos IoT de su hogar están seguros?

Tabla 21-3: Datos seguros

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Siempre	16	20,0	20,0	20,0
Casi siempre	18	22,5	22,5	42,5
Válidos Nunca	22	27,5	27,5	70,0
No lo sabe	24	30,0	30,0	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

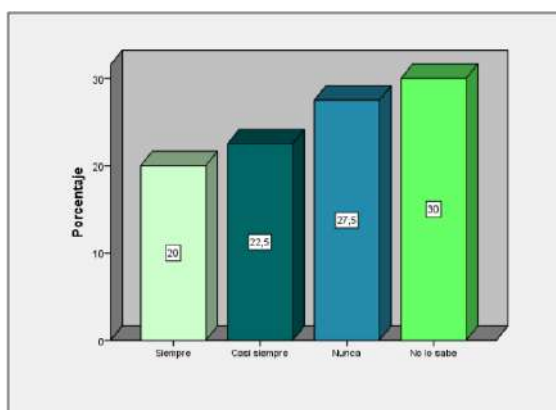


Gráfico 18-3: Datos seguros

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 20% de personas asegura que sus datos ingresados en dispositivos IOT siempre están seguros, un segundo 22,5% sostiene que casi siempre están seguros estos datos, mientras que un 27,5% considera que estos datos nunca están seguros, en tanto que el último 30% no sabe qué tan seguros están estos datos personales.

La mayoría de los datos ingresados por personas en dispositivos IOT están en graves riesgos de vulnerabilidad ya que la mayoría considera que nunca están a salvo o no saben qué tan a salvo están.

Pregunta N° 19.- La observación del uso diario a los dispositivos IoT de su hogar serviría para conocer el comportamiento y hábitos de las personas?

Tabla 22-3: IOT comportamiento

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos SI	35	43,8	43,8	43,8
NO	45	56,3	56,3	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

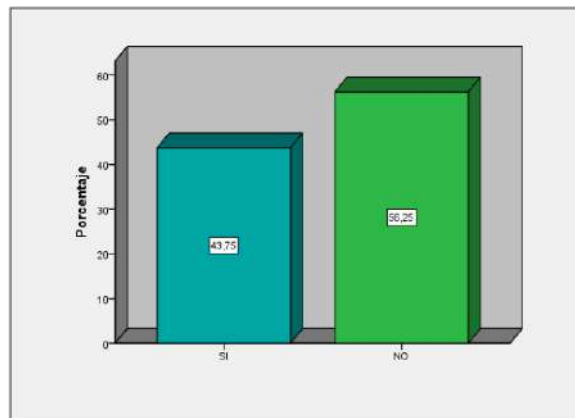


Gráfico 19-3: IOT comportamiento

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 43,8% considera que la observación del uso diario a los dispositivos IoT de su hogar si sirve para mejorar su rendimiento, en tanto que el restante 56,3% considera que esto no sirve para hacerlo.

Hay poca diferencia entre ambas opciones de si sirven para mejorar el rendimiento o si no sirve para hacerlo, por lo que sería necesario establecer más diferencias.

Pregunta N° 20.- ¿Qué medidas ha tomado para mejorar la seguridad de los dispositivos IoT de su hogar?

Tabla 23-3: Medidas de seguridad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos				
Asesoría profesional	19	23,8	23,8	23,8
Configuración y actualización de dispositivos	18	22,5	22,5	46,3
Adquiere marcas de dispositivos reconocidas	15	18,8	18,8	65,0
Coloca los dispositivos de su en lugares seguros	9	11,3	11,3	76,3
Ninguna	19	23,8	23,8	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

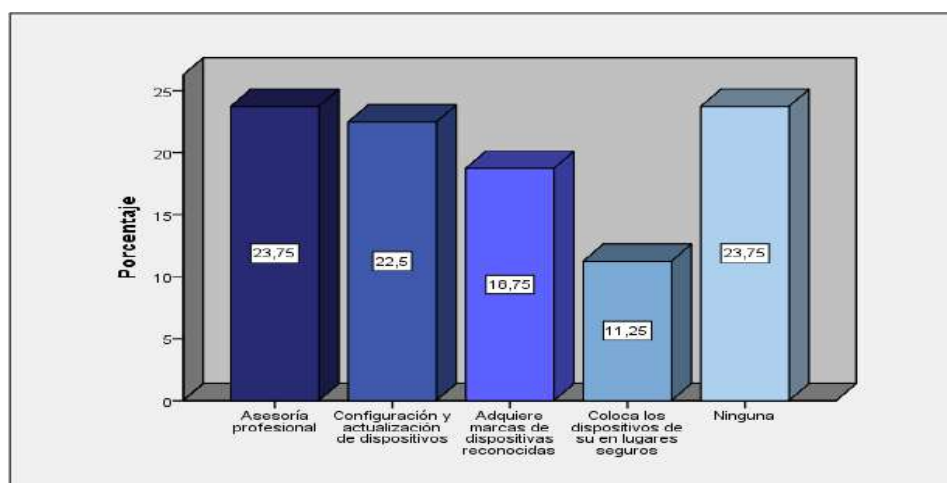


Gráfico 20-3: Medidas de seguridad

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 23,8% de personas asegura que una medida que tomo para aumentar la seguridad en sus dispositivos IOT ha sido la asesoría profesional, seguido de un segundo 22,5% que sostiene que esta medida es la configuración y actualización de dispositivos, un tercer 18,8% en cambio opta por adquirir marcas de dispositivos conocidas, mientras que un 11,3% de personas asegura colocar sus dispositivos en lugares seguros, en tanto que un 23,8% dice no haber tomado ninguna medida de seguridad.

La mayoría de gente no ha aplicado ninguna medida de seguridad, y si lo ha hecho solo ha sido asesoría profesional en este tipo de dispositivos, sin embargo la actualización y configuración de estos también suele ser la opción más recomendable a aplicar como medida de seguridad.

Pregunta N° 21.- ¿Cuál factor considera más importante para establecer seguridades informáticas en los dispositivos IoT que se encuentran en la red de su hogar?

Tabla 24-3: Factor para establecer seguridades

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Factor Humano	22	27,5	27,5
	Factor tecnológico	25	31,3	58,8
	Ambos	33	41,3	100,0
	Total	80	100,0	100,0

Realizado por: Mena, D. 2017

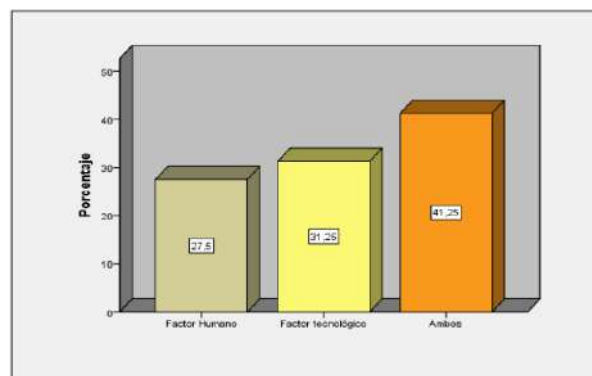


Gráfico 21-3: Factor para establecer seguridades

Realizado por: Mena, D. 2017

Análisis e interpretación:

Un primer 27,5% del total de encuestados considera que el factor humano es importante para establecer seguridades informáticas en los dispositivos IoT que se encuentran en la red de su hogar, seguido del factor tecnológico con un 31,3% del total de respuestas, en tanto que el restante 41,3% sostiene que esto depende de ambos factores.

Ambos factores son esenciales para establecer seguridades informáticas en los dispositivos IoT que se encuentran en la red de su hogar.

Verificación de la hipótesis

En la verificación de la hipótesis se ha desarrollado la aplicación del estadígrafo CH-CUADRADO, para efectuar una relación de las variables de estudio y para lo cual se ha establecido el siguiente proceso:

3.6.8. Frecuencias observadas

Relación de preguntas

Pregunta N° 03.- ¿Cómo ha enfrentado el peligro de una vulnerabilidad informática ante un Cyber Ataque?

Tabla 25-3: Pregunta Variable Independiente

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Mantenimiento permanente	17	21,3	21,3	21,3
Válidos Capacitación personalizada	26	32,5	32,5	53,8
Ninguno	37	46,3	46,3	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

Pregunta N° 21.- ¿Cuál factor considera más importante para establecer seguridades informáticas en los dispositivos IoT que se encuentran en la red de su hogar?

Tabla 26-3: Pregunta Variable Dependiente

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Factor Humano	22	27,5	27,5	27,5
Válidos Factor tecnológico	25	31,3	31,3	58,8
Ambos	33	41,3	41,3	100,0
Total	80	100,0	100,0	

Realizado por: Mena, D. 2017

Para la verificación de la hipótesis se tomo en consideración las preguntas que se efectuaron en la encuesta relacionada a las variables de estudio.

Modelo lógico

Ho = La propuesta de una guía metodológica para el control de vulnerabilidades informáticas en dispositivos IoT para redes HAN, NO servirá como una herramienta de conocimiento para controlar los niveles de riesgos de seguridad informática presentes en el hogar al adoptar este tipo de dispositivos.

H1= La propuesta de una guía metodológica para el control de vulnerabilidades informáticas en dispositivos IoT para redes HAN, SI servirá como una herramienta de conocimiento para controlar los niveles de riesgos de seguridad informática presentes en el hogar al adoptar este tipo de dispositivos.

Nivel de Significación

El nivel de significación con el que se trabaja es del 5%.

$$X^2 = \sum \left[\frac{(O-E)^2}{E} \right]$$

En donde:

X^2 = Chi-cuadrado

\sum = Sumatoria

O = Frecuencia observada

E = Frecuencia esperada o teórica

Nivel de Significación y Regla de Decisión

Grado de Libertad

Para determinar los grados de libertad se utiliza la siguiente fórmula:

Tabla 27-3: Grados de libertad

Grados de Libertad				
$gl = (f - 1) (c - 1)$				
$gl =$	Filas	3	$(3 - 1) =$	2
	Columnas	3	$(3 - 1) =$	2
$gl =$	2	*		2
$gl =$	4			

Realizado por: Mena, D. 2017

Grado de significación

$\alpha = 0.05$

En donde:

O = Frecuencia Observada

E = Frecuencia Esperada

O-E = Frecuencias observada- frecuencias esperadas

O-E² = Resultado de las frecuencias observadas y esperadas al cuadrado

O-E² /E = Resultado de las frecuencias observadas y esperadas al cuadrado dividido para las frecuencias esperadas.

Tabla 28-3: Frecuencias Esperadas

	Factor Humano	Factor Tecnológico	Ambos	TOTAL
Mantenimiento permanente	3	7	12	22
Capacitación personalizada	3	8	14	25
Ninguno	4	11	18	33
TOTAL	10	26	44	80

Realizado por: Mena, D. 2017

Tabla 29-3: Tabla de contingencia

O	E	O-E	(O-E) ²	O-E)/E
3	2,75	0,0	0,00	0
3	7,15	-4,0	16,20	2,27
4	12,10	-8,0	63,60	5,26
7	3,13	4,0	16,20	5,18
8	8,13	0,00	0,00	0,00
11	13,75	-3,0	9,15	0,67
12	4,13	8,0	63,60	15,42
14	10,73	3,0	9,15	0,85
18	18,15	0,0	0,00	0
TOTAL				29,6

Realizado por: Mena, D. 2017

Conclusión

El valor de $X^2 t = 9.49 < X^2 c = 29.6$ de esta manera se acepta la hipótesis alternativa, que indica La propuesta de una guía metodológica para el control de vulnerabilidades informáticas en dispositivos IoT para redes HAN, SI servirá como una herramienta de conocimiento para controlar los niveles de riesgos de seguridad informática presentes en el hogar al adoptar este tipo de dispositivos.

Tabla 30-3: Datos Decisión

Datos para la Decisión	
Nivel de Significación	= 0,025
Valor Crítico	= 9.49
ΣX^2	= 29.6

Realizado por: Mena, D. 2017

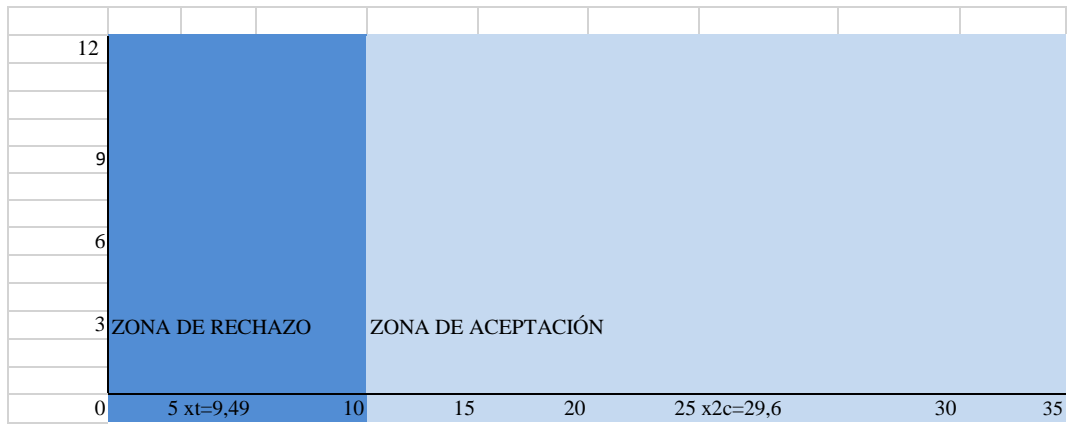


Gráfico 22-3: Aceptación Hipótesis

Realizado por: Mena, D. 2017

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Elementos de prueba para controlar la vulnerabilidad

4.1.1. Reconocimiento de dispositivos bluetooth clásico

Descubrimiento activo

Para descubrir los dispositivos IoT cercanos que hagan uso de Bluetooth clásico en modo activo, se usaran dos herramientas: HCITOOOL y BTSCANNER, la primera es la más fácil de usar ya que mediante el uso de línea de comandos se puede rastrear los dispositivos Bluetooth cercanos, la desventaja de esta herramienta es que no posee la funcionalidad de mantener un escaneo constantemente y solo se muestra actualizaciones cuando encuentre un nuevo dispositivo.

BTSCANNER es una herramienta más completa aparte de tener un interfaz gráfico posee la capacidad de mantener un monitoreo constante para detectar la presencia de nuevos dispositivos Bluetooth, además provee mucha más información acerca de los dispositivos hallados sin la necesidad que este se ya encuentre emparejado con otro.

4.1.1.1. Hcitol

El comando estándar de linux **hcitol** es usado para descubrir la presencia de dispositivos Bluetooth, cuando se lo ejecuta muestra en ese instante los dispositivos Bluetooth cercanos más se limita a esto y no mantiene la búsqueda. Por defecto hcitol solo muestra la dirección BD_ADDR y el nombre del dispositivo, pero puede añadirse otros parámetros para mostrar más información.

En el entorno de pruebas al ejecutar el comando hcitol:

```
$ hcitol scan -all -flush
```

-all Todos los parámetros

--flush Limpiar el cache de resultados

```

pi@raspberrypi: /
File Edit Tabs Help
pi@raspberrypi: / $ hcitool scan --all --flush
Scanning ...

BD Address:      55:F5:0D:49:62:61 [mode 1, clkoffset 0x34b4]
Device name:     Smart watch
Device class:    Phone, Cellular (0x7a0204)

BD Address:      E8:3A:12:45:82:1E [mode 1, clkoffset 0x2811]
Device name:     Galaxy S6 edge+
Device class:    Phone, Smart phone (0x5a020c)

BD Address:      00:02:5B:26:13:AD [mode 1, clkoffset 0x7d99]
OUI company:    Cambridge Silicon Radio (00-02-5B)
Device name:    MagicBox II
Device class:    Audio/Video, Device conforms to the Headset profile (0x240404)

pi@raspberrypi: / $ █

```

Figura 1-4: Resultados hcitool

Realizado por: Mena, D. 2017

Al ejecutarse el comando con privilegios de root, se observa que se despliega más información relacionada a los dispositivos.

\$ sudo hcitool scan --all --flush

```

pi@raspberrypi: /
File Edit Tabs Help
pi@raspberrypi: / $ sudo hcitool scan --all --flush
Scanning ...

BD Address:      00:02:5B:26:13:AD [mode 1, clkoffset 0x7d9a]
OUI company:    Cambridge Silicon Radio (00-02-5B)
Device name:    MagicBox II
Device class:    Audio/Video, Device conforms to the Headset profile (0x240404)
Manufacturer:   Cambridge Silicon Radio (10)
LMP version:    4.0 (0x6) [subver 0x21c8]
LMP features:   0xff 0xff 0x8f 0xfe 0xdb 0xff 0x5b 0x87
                <3-slot packets> <5-slot packets> <encryption> <slot offset>
                <timing accuracy> <role switch> <hold mode> <sniff mode>
                <park state> <RSSI> <channel quality> <SCO link> <HV2 packets>
                <HV3 packets> <u-law log> <A-law log> <CVSD> <paging scheme>
                <power control> <transparent SCO> <broadcast encrypt>
                <EDR ACL 2 Mbps> <EDR ACL 3 Mbps> <enhanced iscan>
                <interlaced iscan> <interlaced pscan> <inquiry with RSSI>
                <extended SCO> <EV4 packets> <EV5 packets> <AFH cap. slave>
                <AFH class. slave> <LE support> <3-slot EDR ACL>
                <5-slot EDR ACL> <sniff subrating> <pause encryption>
                <AFH cap. master> <AFH class. master> <EDR eSCO 2 Mbps>
                <EDR eSCO 3 Mbps> <3-slot EDR eSCO> <extended inquiry>
                <LE and BR/EDR> <simple pairing> <encapsulated PDU>
                <non-flush flag> <LSTO> <inquiry TX power> <EPC>
                <extended features>

```

Figura 2-4: Resultados hcitool con usuario root

Realizado por: Mena, D. 2017

De los resultados obtenidos con los dispositivos IoT de pruebas se pudieron identificar 3 de estos por sus interfaces Bluetooth:

BD Address: 55:F5:0D:49:62:61 [mode 1, clkoffset 0x34b4]

Device name: Smart watch

Device class: Phone, Cellular (0x7a0204)

BD Address: E8:3A:12:45:82:1E [mode 1, clkoffset 0x2811]

Device name: Galaxy S6 edge+

Device class: Phone, Smart phone (0x5a020c)

BD Address: 00:02:5B:26:13:AD [mode 1, clkoffset 0x7d99]

OUI company: Cambridge Silicon Radio (00-02-5B)

Device name: MagicBox II

Device class: Audio/Video, Device conforms to the Headset profile (0x240404)

Como se observa fueron encontrados:

- El reloj inteligente “Smart Watch U8”, con BD ADDRESS 55:F5:0D:49:62:61, el cual NO SE ENCONTRABA EMPARENTADO con algún dispositivo
- El teléfono celular “Samsung Galaxy S6”, con BD ADDRESS E8:3A:12:45:82:1E, el cual fue puesto de manera deliberada en MODO VISIBLE.
- El dispositivo parlante Bluetooth Magic Box II, con BD ADDRESS 00:02:5B:26:13:AD, el cual NO SE ENCONTRABA EMPARENTADO con algún dispositivo

4.1.1.2. *Btscanner*

Para su ejecución desde un terminal se deberá ingresar el comando desde privilegios de root:

```
$ sudo btscanner
```

El cual mostrará un interfaz gráfico la cual es controlable mediante el teclado, mediante teclas rápidas con lo cual puede dar la orden de iniciar y parar el escaneo como también grabar en un archivo los resultados obtenidos.

Los resultados al escanear dispositivos Bluetooth en el entorno de pruebas es el siguiente:

```
pi@raspberrypi: /
File Edit Tabs Help

Time          Address          Clk off        Class          Name
2017/02/11 18:33:37 90:03:B7:95:49:04 0x4c80        0x340408      BT ChevyStar - 682
2017/02/11 18:29:26 00:26:7E:7C:88:74 0x7744        0x340408      (unknown)
2017/02/11 20:21:22 BC:85:1F:D8:C2:58 0x3c39        0x5a0204      C3222
2017/02/11 18:25:18 00:26:7E:AB:E3:FE 0x5f4f        0x340408      (unknown)
2017/02/11 18:19:15 A0:14:3D:75:ED:12 0x60c1        0x340408      (unknown)
2017/02/11 18:09:44 74:5E:1C:6E:E5:00 0x3089        0x340408      (unknown)
2017/02/11 18:04:45 00:26:7E:AB:96:39 0x38c2        0x340408      (unknown)
2017/02/11 18:03:23 00:26:7E:E1:09:61 0x28e6        0x340408      (unknown)
2017/02/11 17:55:19 00:07:80:92:C3:38 0x7b86        0x200408      (unknown)
2017/02/11 17:49:36 90:03:B7:D7:D1:F3 0x3ff5        0x340408      (unknown)
2017/02/11 17:48:57 00:19:B5:04:E3:CE 0x4184        0x240404      (unknown)
2017/02/11 16:19:09 90:03:B7:04:3C:92 0x106e        0x340408      (unknown)
2017/02/11 15:59:52 F0:1C:13:84:04:CE 0x161d        0x5a0204      Wilson
2017/02/11 15:54:20 E8:3A:12:45:82:1E 0x150f        0x5a020c      Galaxy S6 edge+
2017/02/11 21:00:41 55:F5:0D:49:62:61 0x21c0        0x7a0204      Smart watch
2017/02/11 15:54:58 00:02:5B:26:13:AD 0x5455        0x240404      MagicBox II

Found device 55:F5:0D:49:62:61
Found device 55:F5:0D:49:62:61
aborting scan
aborted
```

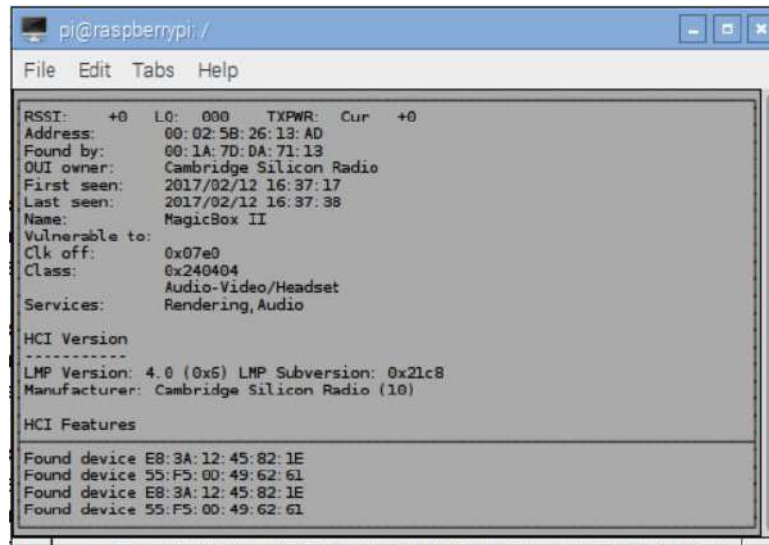
Figura 3-4: Btscanner

Realizado por: Mena, D. 2017

Durante un monitoreo de aproximadamente una hora puede observarse que BTSCANNER constantemente estuvo buscando la presencia de nuevos dispositivos Bluetooth, encontrando durante este ejercicio nuevos dispositivos externos inclusive que no constaban con los escogidos para las pruebas, obteniendo por ende mejores resultados que la herramienta hcitool debido a su monitoreo persistente.

BTSCANNER permite mostrar además más información acerca de los dispositivos descubiertos como: Nombre conocido, BD ADDRESS, clase de dispositivo e información del reloj del sistema.

Dknight Magic Box II



```
pi@raspberrypi: /
File Edit Tabs Help
RSSI: +0 LQ: 000 TXPWR: Cur +0
Address: 00:02:5B:26:13:AD
Found by: 00:1A:7D:DA:71:13
OUI owner: Cambridge Silicon Radio
First seen: 2017/02/12 16:37:17
Last seen: 2017/02/12 16:37:38
Name: MagicBox II
Vulnerable to:
Clk off: 0x07e0
Class: 0x240404
Audio-Video/Headset
Services: Rendering, Audio

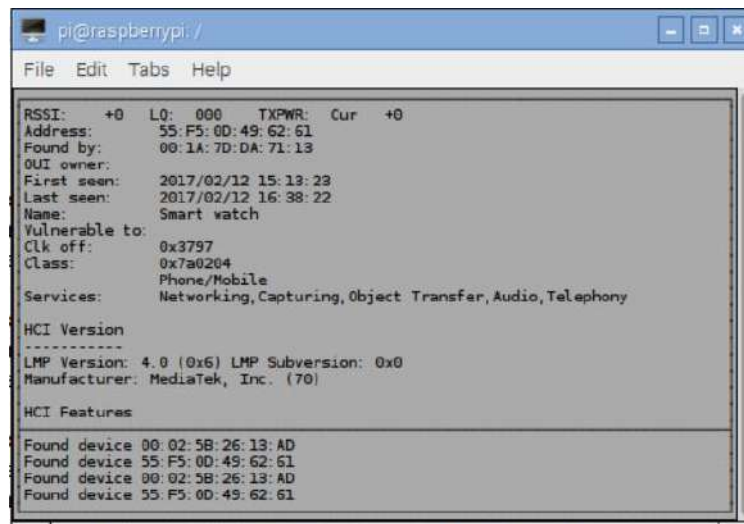
HCI Version
-----
LMP Version: 4.0 (0x5) LMP Subversion: 0x21c8
Manufacturer: Cambridge Silicon Radio (10)

HCI Features
-----
Found device E8:3A:12:45:82:1E
Found device 55:F5:00:49:62:61
Found device E8:3A:12:45:82:1E
Found device 55:F5:00:49:62:61
```

Figura 4-4: Resultados Btscanner Magicbox II

Realizado por: Mena, D. 2017

Smart Watch U8



```
pi@raspberrypi: /
File Edit Tabs Help
RSSI: +0 LQ: 000 TXPWR: Cur +0
Address: 55:F5:00:49:62:61
Found by: 00:1A:7D:DA:71:13
OUI owner:
First seen: 2017/02/12 15:13:23
Last seen: 2017/02/12 16:38:22
Name: Smart watch
Vulnerable to:
Clk off: 0x3797
Class: 0x7a0204
Phone/Mobile
Services: Networking, Capturing, Object Transfer, Audio, Telephony

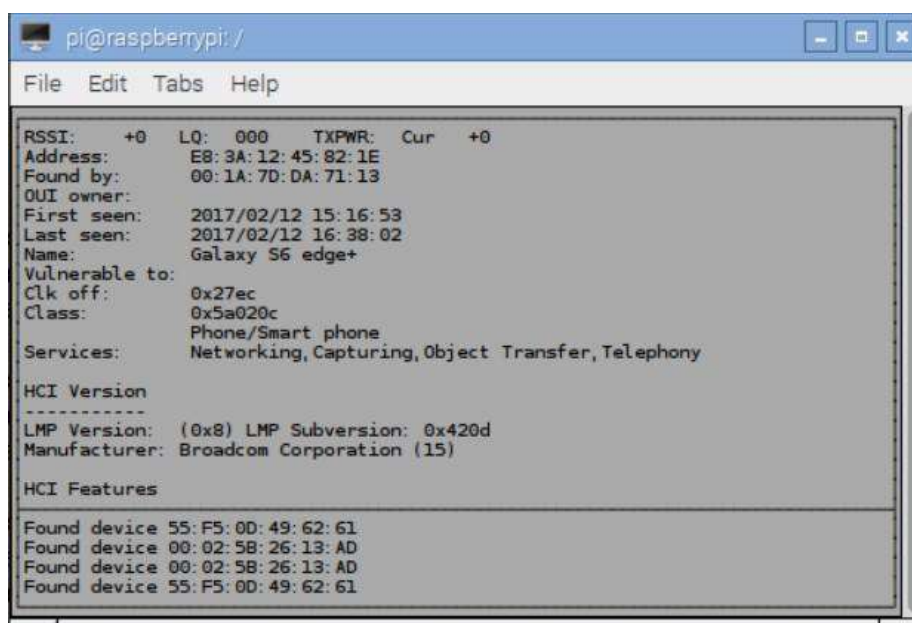
HCI Version
-----
LMP Version: 4.0 (0x6) LMP Subversion: 0x0
Manufacturer: MediaTek, Inc. (70)

HCI Features
-----
Found device 00:02:5B:26:13:AD
Found device 55:F5:00:49:62:61
Found device 00:02:5B:26:13:AD
Found device 55:F5:00:49:62:61
```

Figura 5-4: Resultados Btscanner Smartwatch U8

Realizado por: Mena, D. 2017

Samsung Galaxy S6+



```
pi@raspberrypi: /
File Edit Tabs Help

RSSI: +0 LQ: 000 TXPWR: Cur +0
Address: E8:3A:12:45:82:1E
Found by: 00:1A:7D:DA:71:13
OUI owner:
First seen: 2017/02/12 15:16:53
Last seen: 2017/02/12 16:38:02
Name: Galaxy S6 edge+
Vulnerable to:
Clk off: 0x27ec
Class: 0x5a020c
Phone/Smart phone
Services: Networking, Capturing, Object Transfer, Telephony

HCI Version
-----
LMP Version: (0x8) LMP Subversion: 0x420d
Manufacturer: Broadcom Corporation (15)

HCI Features
-----
Found device 55:F5:0D:49:62:61
Found device 00:02:5B:26:13:AD
Found device 00:02:5B:26:13:AD
Found device 55:F5:0D:49:62:61
```

Figura 6-4: Resultados Btscanner Smartphone Samsung Galaxy S6 edge

Realizado por: Mena, D. 2017

4.1.2. Descubrimiento pasivo

El estándar de Bluetooth no requiere que los dispositivos intenten comunicarse o emparejarse con otros para que revelar la dirección del dispositivo, a través de diferentes técnicas externas es posible identificar la BD_ADDRESS del dispositivo objetivo sin la necesidad de usar herramientas como las indicadas en el descubrimiento activo.

Para realizar el descubrimiento pasivo se usará hardware especializado mediante un sniffer llamado Ubertooth One que es capaz de monitorear el tráfico de dispositivos Bluetooth Clásico (BR) y Bluetooth Low Energy (BLE).

4.1.2.1. Ubertooth

Una vez instalado y configurado correctamente en el Raspbian del Raspberry pi escogido para las pruebas, Ubertooth One tiene la capacidad de capturar paquetes Bluetooth para descubrir dispositivos cercanos incluyendo los que se encuentren en modo no descubrimiento.

Con la utilidad ubertooth-rx se puede descubrir el LAP (Lower Address Part) de la BD_ADDRESS de los transmisores Bluetooth activos que se encuentren cerca al sniffer.

```
$ sudo ubertooth-rx
```



```
pi@raspberrypi: /
File Edit Tabs Help
rf=-59 snr=21
systemtime=1486936181 ch=39 LAP=9e8b33 err=0 clk100ns=3027519713 clk1=484403 s=-39
rf=-65 snr=26
systemtime=1486936181 ch=39 LAP=9e8b33 err=0 clk100ns=3027619700 clk1=484419 s=-40
rf=-70 snr=30
systemtime=1486936181 ch=39 LAP=9e8b33 err=0 clk100ns=3027719677 clk1=484435 s=-40
rf=-71 snr=31
systemtime=1486936182 ch=39 LAP=9e8b33 err=0 clk100ns=3028919486 clk1=484627 s=-40
rf=-76 snr=36
systemtime=1486936182 ch=39 LAP=9e8b33 err=2 clk100ns=3029019527 clk1=484643 s=-40
rf=-78 snr=38
systemtime=1486936182 ch=39 LAP=9e8b33 err=0 clk100ns=3029219467 clk1=484675 s=-36
rf=-79 snr=43
systemtime=1486936182 ch=39 LAP=9e8b33 err=0 clk100ns=3029619385 clk1=484739 s=-32
rf=-66 snr=34
systemtime=1486936206 ch=39 LAP=45821e err=2 clk100ns=947571 clk1=524440 s=-80 rf=-8
l snr=1
systemtime=1486936207 ch=39 LAP=45821e err=0 clk100ns=9996915 clk1=525887 s=-42 rf=-
81 snr=39
systemtime=1486936238 ch=39 LAP=fa2226 err=2 clk100ns=315986235 clk1=574845 s=-69 n
=-84 snr=15
systemtime=1486936247 ch=39 LAP=350471 err=2 clk100ns=408137971 clk1=589590 s=-76 n
=-85 snr=9
systemtime=1486936266 ch=39 LAP=470d92 err=0 clk100ns=592235769 clk1=619046 s=-76 n
```

Figura 7-4: Escaneo Ubertooth 1

Realizado por: Mena, D. 2017

```
pi@raspberrypi: /
File Edit Tabs Help
=-85 snr=9
systemtime=1486936266 ch=39 LAP=470d92 err=0 clk100ns=592235769 clk1=619046 s=-76 n
=-85 snr=9
systemtime=1486936285 ch=39 LAP=470d92 err=0 clk100ns=791735866 clk1=650966 s=-67 n
=-83 snr=16
systemtime=1486936297 ch=39 LAP=470d92 err=0 clk100ns=906449486 clk1=669320 s=-37 n
=-84 snr=47
systemtime=1486936318 ch=39 LAP=94256f err=2 clk100ns=1112664287 clk1=702314 s=-86
rf=-87 snr=1
systemtime=1486936318 ch=39 LAP=45821e err=1 clk100ns=1117377529 clk1=703068 s=-75
rf=-84 snr=9
systemtime=1486936318 ch=39 LAP=45821e err=0 clk100ns=1117477539 clk1=703084 s=-74
rf=-85 snr=11
systemtime=1486936318 ch=39 LAP=45821e err=1 clk100ns=1117877583 clk1=703148 s=-75
rf=-83 snr=8
systemtime=1486936318 ch=39 LAP=2613ad err=0 clk100ns=1119853655 clk1=703464 s=-38
rf=-59 snr=21
systemtime=1486936318 ch=39 LAP=2613ad err=2 clk100ns=1120201801 clk1=703520 s=-35
rf=-70 snr=35
systemtime=1486936319 ch=39 LAP=45821e err=0 clk100ns=1123406625 clk1=704033 s=-64
rf=-74 snr=10
systemtime=1486936322 ch=39 LAP=45821e err=0 clk100ns=1153218693 clk1=708803 s=-43
rf=-82 snr=39
^Cpi@raspberrypi: / $
```

Figura 8-4: Escaneo Ubertooth 2

Realizado por: Mena, D. 2017

De los resultados obtenidos en un periodo corto de monitoreo se puede observar que fueron detectados varios dispositivos incluyendo algunos desconocidos que pudieron haber sido descubiertos a pesar de que pudieron estar en modo de no descubrimiento.

Tabla 1-4: Resultados Hcitol

LAP	POSIBLE DISPOSITIVO
45821e	Samsung S6 Edge+
2613ad	Parlantes MagicBox II
94256f	Desconocido
470d92	Desconocido
9e8b33	DIRECCIÓN RESERVADA POR EL DISPOSITIVO PARA BÚSQUEDA GENERAL
350471	Desconocido

Realizado por: Mena, D. 2017

Así también Ubertooth posee una herramienta que hace uso de los adaptadores o dongles Bluetooth convencionales para identificar el posible NAP (Non-significant Address Part) de los LAP ya identificados, la herramienta se llama ubertooth-scan.

\$ ubertooth-scan

Los resultados fueron parciales a pesar de que se hicieron varios intentos con la herramienta solo se mostraron parte del NAP de un solo dispositivo que se encontraba en modo de no descubrimiento pudiendo identificarse la siguiente información:

?:?:12:45:82:1E Galaxy S6 edge+

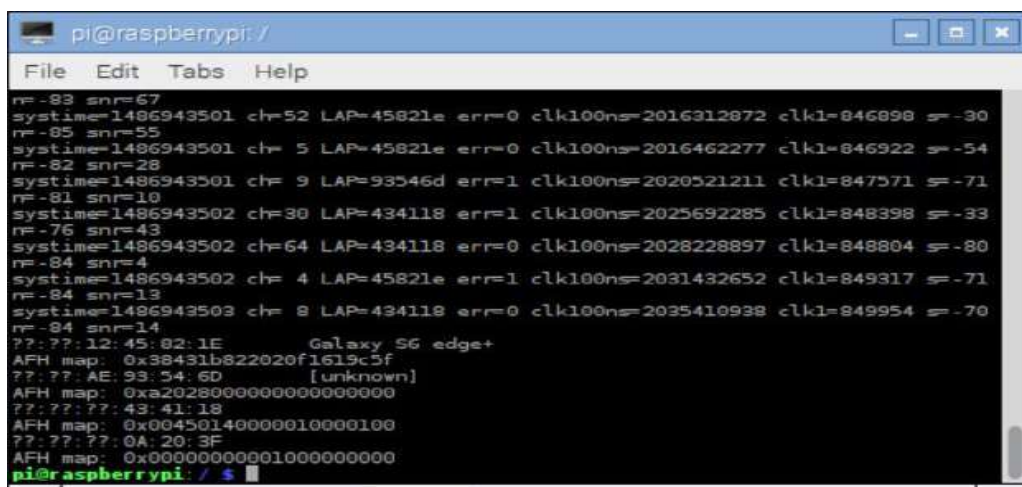


Figura 9-4: Resultados Ubertooth Scan

Realizado por: Mena, D. 2017

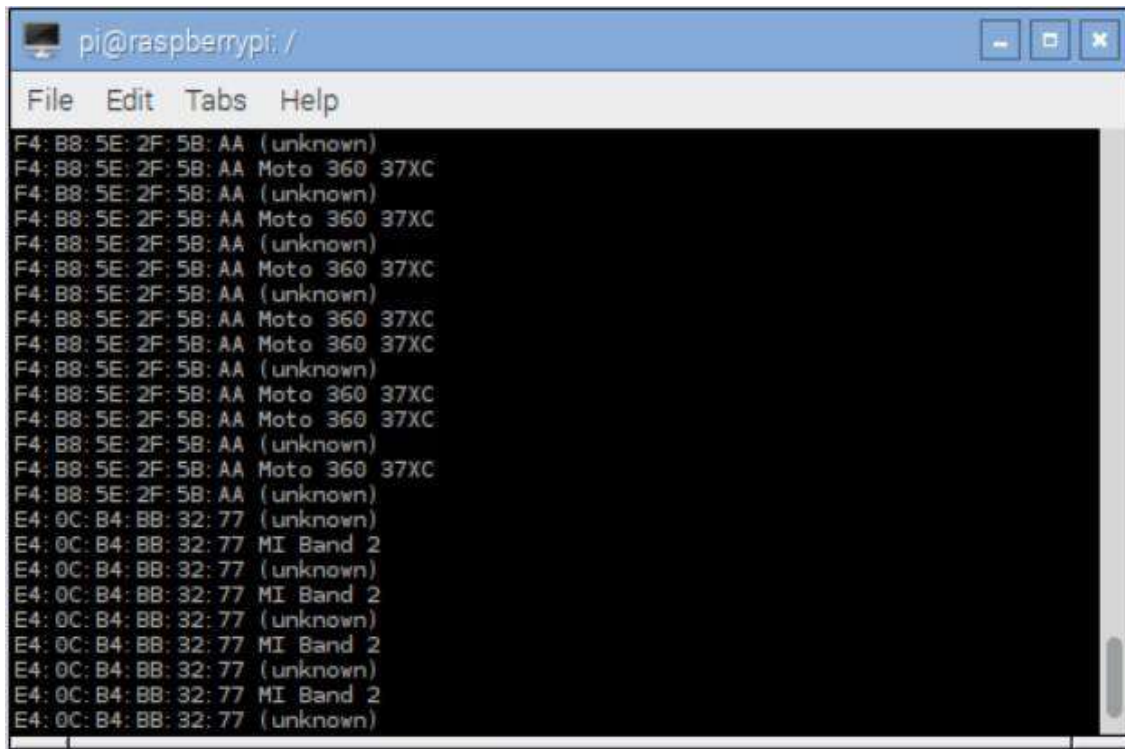
4.1.2.2. Reconocimiento de dispositivos Bluetooth Low Energy

Para el reconocimiento y descubrimiento de dispositivos Bluetooth LE se cuenta con pocas herramientas disponibles en Internet o en otras fuentes, para las pruebas en este tipo de tecnología se utilizó la herramienta hcitool disponible en las distribuciones de Linux, mediante el parametro “lescan” permite escanear los dispositivos Bluetooth Low Energy cercanos.

```
$ sudo hcitool lescan
```

Los resultados obtenidos solo pudieron obtenerse poniendo los dispositivos de prueba en modo descubrimiento cuando no estaban emparejados a otro dispositivo en este caso a un teléfono móvil.

Conclusiones



```
pi@raspberrypi: /
File Edit Tabs Help
F4: B8: 5E: 2F: 5B: AA (unknown)
F4: B8: 5E: 2F: 5B: AA Moto 360 37XC
F4: B8: 5E: 2F: 5B: AA (unknown)
F4: B8: 5E: 2F: 5B: AA Moto 360 37XC
F4: B8: 5E: 2F: 5B: AA (unknown)
F4: B8: 5E: 2F: 5B: AA Moto 360 37XC
F4: B8: 5E: 2F: 5B: AA (unknown)
F4: B8: 5E: 2F: 5B: AA Moto 360 37XC
F4: B8: 5E: 2F: 5B: AA (unknown)
F4: B8: 5E: 2F: 5B: AA Moto 360 37XC
F4: B8: 5E: 2F: 5B: AA (unknown)
F4: B8: 5E: 2F: 5B: AA Moto 360 37XC
F4: B8: 5E: 2F: 5B: AA (unknown)
F4: B8: 5E: 2F: 5B: AA Moto 360 37XC
F4: B8: 5E: 2F: 5B: AA (unknown)
E4: 0C: B4: BB: 32: 77 (unknown)
E4: 0C: B4: BB: 32: 77 MI Band 2
E4: 0C: B4: BB: 32: 77 (unknown)
E4: 0C: B4: BB: 32: 77 MI Band 2
E4: 0C: B4: BB: 32: 77 (unknown)
E4: 0C: B4: BB: 32: 77 MI Band 2
E4: 0C: B4: BB: 32: 77 (unknown)
E4: 0C: B4: BB: 32: 77 MI Band 2
E4: 0C: B4: BB: 32: 77 (unknown)
```

Figura 10-4: Resultados Hcitol BLE

Realizado por: Mena, D. 2017

Los dispositivos encontrados pertenecen a un reloj inteligente (MOTO 360) BD_ADDRESS F4:B8:5E:2F:5B:AA y una banda Fit inteligente (Mi band 2) BD_ADDRESS E4:0C:B4:BB:32:77, estos resultados pudieron obtenerse cuando estos no se encontraban emparejados por tanto pudieron estar en modo descubrimiento.

4.1.2.3. *Blue Hydra*

Entre las utilidades para reconocimiento de Bluetooth más actuales se encuentran Blue Hydra la cual constituye una herramienta poderosa ya que es capaz de escanear tanto los dispositivos de Bluetooth clásico como Bluetooth Low Energy mediante la ayuda de hardware especial como es el Ubertooth One.

Es capaz de detectar dispositivos IoT Bluetooth inclusive si están ocultos además los resultados obtenidos pueden ser almacenados en una base de datos para su posterior análisis.

Ciertos dispositivos Bluetooth Low Energy cuando su estado se encuentre en reposo constantemente están alertando su situación a otros dispositivos cercanos, esto puede ser aprovechada por Blue Hydra ya que puede captar esta información mediante esta vulnerabilidad para identificar cuales dispositivos se encuentren cerca inclusive mediante el Received Signal Strength Indication (RSSI) puede estimarse la distancia de estos hacia el sniffer. (Best Security Search, s.f.)

En las pruebas realizadas Blue hydra pudo identificar a tres dispositivos Bluetooth en este caso fue:

- El teléfono Samsung GalaxyS6 edge+.
- Los parlantes Magic Box II
- El Smart Watch U8

Se logró obtener la BD_ADDR de 2 dispositivos (Smartwatch y teléfono móvil) y parcialmente la de una (Parlantes Bluetooth).

```

pi@raspberrypi: /blue_hydra
File Edit Tabs Help
Blue Hydra : Devices Seen in last 300s
Queue status: result_queue: 0, info_scan_queue: 0, l2ping_queue: 0
Discovery status timers: 5, ubertooth status: 1487305488
SEEN ^ | VERS | ADDRESS | RSSI | NAME | MANUF | TYPE
+4s | CL/BR | 55:F5:00:49:62:61 | -52 | Smart watch | Unknown | Cellular
+18s | CL/BR | 00:02:58:26:13:AD | -54 | MagicBox II | Cambridg | Wearable Headset Device
+112s | CL/BR | E8:3A:12:45:82:1E | -65 | Galaxy S6 edge+ | SamsungE | Smart phone
+156s | CL(0x08) | 00:00:12:45:82:1E | | Galaxy S6 edge+ | Informat |

```

Figura 11-4: Resultados Blue Hydra

Realizado por: Mena, D. 2017

4.1.2.4. Análisis de Tráfico Bluetooth (Eavesdropping)

- Eavesdropping en Bluetooth Clásico

El uso del Bluetooth Clásico es muy popular en un sinnúmero de dispositivos comunes para los usuarios como mouse, teclados, parlantes, etc. sin embargo se puede capturar tráfico Bluetooth de estas piconets pero esta tarea puede ser dificultosa por varias razones:

1. Las seguridad de las redes Piconet del Bluetooth clásico utilizan Saltos de Frecuencia (FHSS) Frequency Hopping Spread Spectrum, donde tanto el transmisor y receptor deben conocer el patrón de frecuencias para intercambiar datos. El patrón de frecuencias se basa en el BD_ADDRESS del dispositivo master y el cambio se lo realiza 1600 veces por segundo en condiciones normales, por tanto es importante conocer este dato.
2. Conocer el BD_ADDRESS del dispositivo maestro no es suficiente ya que es necesario también conocer el CLK o reloj maestro que da la sincronización al patrón de saltos de frecuencia de la Piconet.
3. El estándar Bluetooth clásico no está diseñado para mantener un monitoreo pasivo de su tráfico, se puede utilizar herramientas de Linux como hcidump pero esta no muestra información de actividad ni de las capas inferiores donde se encuentra la información, para poder tener una muestra de la actividad se requiere de que se haya establecido una Piconet.

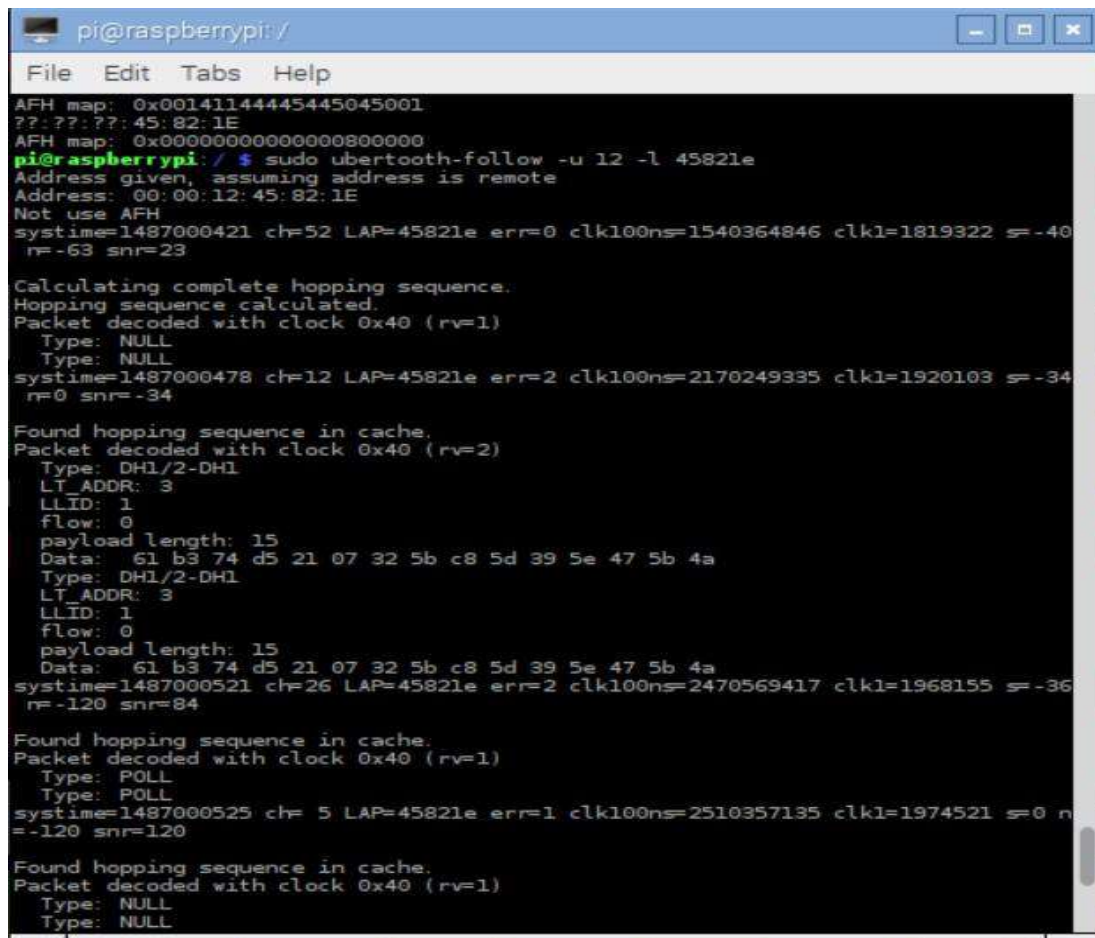
Captura de datos con Ubertooth one

Para capturar los datos de las conexiones de Bluetooth clásico se utilizará el dispositivo Ubertooth One.

Para esto no solo se necesita del Ubertooth One sino también de un dongle Bluetooth estándar, el cual solicitará al dispositivo objetivo el reloj para sincronizar los saltos de canal rápidamente esta información es enviada al Ubertooth One para tratar de enlazarse a la piconet.

Utilizando los resultados obtenidos de la figura 63, en donde se descubrió al dispositivo Bluetooth oculto Galaxy S6 edge+ utilizaremos la herramienta de ubertooth ubertooth-follow donde para su ejecución ingresaremos los datos de la BD_ADDRESS del dispositivo objetivo para monitorear su tráfico

```
$ sudo ubertooth-follow -u 12 -l 45821e
```



```
pi@raspberrypi: /
File Edit Tabs Help
AFH map: 0x00141144445445045001
?:?:?:?: 45: 82: 1E
AFH map: 0x0000000000000000000000
pi@raspberrypi: / $ sudo ubertooth-follow -u 12 -l 45821e
Address given, assuming address is remote
Address: 00:00:12:45:82:1E
Not use AFH
systime=1487000421 ch=52 LAP=45821e err=0 clk100ns=1540364846 clk1=1819322 s=-40
r=-63 snr=23

Calculating complete hopping sequence.
Hopping sequence calculated.
Packet decoded with clock 0x40 (rv=1)
Type: NULL
Type: NULL
systime=1487000478 ch=12 LAP=45821e err=2 clk100ns=2170249335 clk1=1920103 s=-34
r=0 snr=-34

Found hopping sequence in cache.
Packet decoded with clock 0x40 (rv=2)
Type: DH1/2-DH1
LT_ADDR: 3
LLID: 1
flow: 0
payload length: 15
Data: 61 b3 74 d5 21 07 32 5b c8 5d 39 5e 47 5b 4a
Type: DH1/2-DH1
LT_ADDR: 3
LLID: 1
flow: 0
payload length: 15
Data: 61 b3 74 d5 21 07 32 5b c8 5d 39 5e 47 5b 4a
systime=1487000521 ch=26 LAP=45821e err=2 clk100ns=2470569417 clk1=1968155 s=-36
r=-120 snr=84

Found hopping sequence in cache.
Packet decoded with clock 0x40 (rv=1)
Type: POLL
Type: POLL
systime=1487000525 ch= 5 LAP=45821e err=1 clk100ns=2510357135 clk1=1974521 s=0 n
=-120 snr=120

Found hopping sequence in cache.
Packet decoded with clock 0x40 (rv=1)
Type: NULL
Type: NULL
```

Figura 12-4: Monitoreo de tráfico BLE

Realizado por: Mena, D. 2017

Como puede observarse Ubertooth pudo calcular la secuencia de saltos completa de la información por lo que pudo decodificar varios campos de los paquetes capturados

Type NULL: Captura de un NULL-PACKET sin contener datos (payload).

Type DH1/2-DH1: Indica que el paquete lleva información y que no ha sido codificada o modulada usando pi/4-QPSK.

LT_ADDR: Identifica al esclavo en una conexión ACL (Conexión Asincronica) con su master, posee 3 bits y tiene un rango que va de 1 - 7.

LLID: Logical Link Identifier es parte del Logical Link Control and Adaptation Protocol (L2CAP), un valor de 2 indica que es el inicio de un nuevo mensaje y 1 es que la continuación de un mensaje.

Flow: Bit usado para control de flujo

Payload lenght: Indica el tamaño del payload en bytes.

Data: Es la información en sí, Ubertooth no permite decodificar esta información.

POLL: Son solicitudes hechas por el master de la Piconet a sus esclavos.

Mediante el análisis hecho con la herramienta de Ubertooth se pudo capturar paquetes, pero se evidencia además que existen limitaciones todavía para decodificar la información que contienen.

Existe en el mercado soluciones comerciales mucho más sofisticadas y completas para la captura y decodificación de paquetes en el Bluetooth clásico como los equipos Frontline BPA 600 Sniffer o Ellisys Bluetooth Explorer 400, pero estos tienen un costo de alrededor de miles dólares y son utilizados principalmente para fines de análisis del protocolo.

4.1.3. *Eavesdropping en Bluetooth Low Energy*

Bluetooth Low Energy (BLE) al igual que el Bluetooth clásico utiliza para su seguridad FHSS (Frequency Hopping Spread Spectrum) donde tanto el transmisor y receptor usan saltos de frecuencia para su comunicación, pero en el Bluetooth LE a diferencia del Bluetooth clásico utiliza un patrón de saltos menos complejos ya que posee 40 canales en la frecuencia de 2.4 Ghz de los cuales 37 son para transmisión de información y 3 para mensajes de notificación de la red, como se muestra en el gráfico siguiente:

Channel	Frequency (MHz)	Channel Function	Data Channel Index	Advertising Channel Index
0	2402	Advertising	n/a	37
1	2404	Data	0	n/a
2	2406	Data	1	n/a
...	...	Data	...	n/a
12	2426	Advertising	n/a	38
13	2428	Data	11	n/a
14	2430	Data	12	n/a
...	...	Data	...	n/a
39	2480	Advertising	n/a	39

Figura 13-4: Patrón de saltos BLE (Canales)

Fuente: (Wright & Cache)

Cuando está establecida una red Bluetooth BLE, el dispositivo que actúa como maestro utiliza los 3 canales de notificación para enviar a sus esclavos información importante de la red como:

- Dirección de acceso, un valor aleatorio como identificador en la conexión
- Incremento de saltos, la distancia hacia el siguiente canal
- Evento de intervalo de conexión, es el tiempo que debe esperar el transmisor y receptor para cambiar antes del siguiente salto de canal.
- CRC inicial, valor aleatorio utilizado para iniciar el cálculo inicial del CRC

4.1.3.1. Captura de datos con Ubertooth one

Debido a que el funcionamiento de Bluetooth LE es similar al Bluetooth clásico utilizaremos el Ubertooth One para la captura de tráfico mediante la herramienta llamada ubertooth-btle.

```
$ ubertooth-btle -f -c captura.pcap
```

Lo que se pide con este comando es que se haga la captura de paquetes BLE y lo grabe en el archivo captura.pcap (-c) mientras da seguimiento a las solicitudes de conexión (-f)


```

pi@raspberrypi: /
File Edit Tabs Help
CRC: fb 22 5f

system=1487031471 freq=2402 addr=8e89bed6 delta_t=1286.252 ms
40 25 77 32 bb b4 0c e4 02 01 06 1b ff 57 01 00 1c 45 4b 28 55 ea a7 f6 1f c3 20
f4 f0 69 55 b5 01 e4 0c b4 bb 32 77 fb 22 5f
Advertising / AA 8e89bed6 (valid) / 37 bytes
Channel Index: 37
Type: ADV_IND
AdvA: e4:0c:b4:bb:32:77 (random)
AdvData: 02 01 06 1b ff 57 01 00 1c 45 4b 28 55 ea a7 f6 1f c3 20 f4 f0 69 5
5 b5 01 e4 0c b4 bb 32 77
Type 01 (Flags)
00000110
Type ff
57 01 00 1c 45 4b 28 55 ea a7 f6 1f c3 20 f4 f0 69 55 b5 01 e4 0c b4
bb 32 77

Data: 77 32 bb b4 0c e4 02 01 06 1b ff 57 01 00 1c 45 4b 28 55 ea a7 f6 1f
c3 20 f4 f0 69 55 b5 01 e4 0c b4 bb 32 77
CRC: fb 22 5f

system=1487031473 freq=2402 addr=8e89bed6 delta_t=1288.736 ms
40 25 77 32 bb b4 0c e4 02 01 06 1b ff 57 01 00 1c 45 4b 28 55 ea a7 f6 1f c3 20
f4 f0 69 55 b5 01 e4 0c b4 bb 32 77 fb 22 5f
Advertising / AA 8e89bed6 (valid) / 37 bytes
Channel Index: 37
Type: ADV_IND
AdvA: e4:0c:b4:bb:32:77 (random)
AdvData: 02 01 06 1b ff 57 01 00 1c 45 4b 28 55 ea a7 f6 1f c3 20 f4 f0 69 5
5 b5 01 e4 0c b4 bb 32 77
Type 01 (Flags)
00000110
Type ff
57 01 00 1c 45 4b 28 55 ea a7 f6 1f c3 20 f4 f0 69 55 b5 01 e4 0c b4

```

Figura 14-4: Captura de Trafico BLE 1

Realizado por: Mena, D. 2017

```

pi@raspberrypi: /
File Edit Tabs Help
Type 01 (Flags)
00000110
Type ff
57 01 00 1c 45 4b 28 55 ea a7 f6 1f c3 20 f4 f0 69 55 b5 01 e4 0c b4
bb 32 77

Data: 77 32 bb b4 0c e4 02 01 06 1b ff 57 01 00 1c 45 4b 28 55 ea a7 f6 1f
c3 20 f4 f0 69 55 b5 01 e4 0c b4 bb 32 77
CRC: fb 22 5f

system=1487032222 freq=2402 addr=8e89bed6 delta_t=0.495 ms
c5 22 d0 0d 1b 8d c8 43 77 32 bb b4 0c e4 d9 5c 65 50 5f cf 1b 03 1e 00 28 00 00
00 d0 07 ff 0f 00 fe 1e 2e db ef 18
Advertising / AA 8e89bed6 (valid) / 34 bytes
Channel Index: 37
Type: CONNECT_REQ
InitA: 43:c8:8d:1b:0d:d0 (random)
AdvA: e4:0c:b4:bb:32:77 (random)
AA: 50655cd9
CRCInit: 1bcf5f
WinSize: 03 (3)
WinOffset: 001e (30)
Interval: 0028 (40)
Latency: 0000 (0)
Timeout: 07d0 (2000)
ChM: ff 0f 00 fe 1e
Hop: 14
SCA: 1, 151 ppm to 250 ppm

Data: d0 0d 1b 8d c8 43 77 32 bb b4 0c e4 d9 5c 65 50 5f cf 1b 03 1e 00 28
00 00 00 d0 07 ff 0f 00 fe 1e 2e
CRC: db ef 18

^Cpi@raspberrypi: / $

```

Figura 15-4: Captura de Trafico BLE 2

Realizado por: Mena, D. 2017

En la pantalla se muestran capturas de paquetes Bluetooth BLE cuando los dispositivos IoT se encontraban en modo de descubrimiento, de lo que se puede extraer la siguiente información:

Captura 1:

TYPE: ADV_IND

PDU de tipo notificación, por lo que se encuentra en los 3 canales utilizados para este fin

Captura 2:

TYPE: CONNECT_REQ

PDU anunciando un inicio de conexión.

ADVA: e4:0c:b4:bb:32:77

BD ADDRESS del dispositivo anunciador en este caso corresponde a la pulsera Mi FI 2 que anteriormente fue descubierta.

También puede observarse otra información referente a la conexión como el intervalo de salto (14).

El comando ubertooth-btle decodifica parte de la información de los paquetes capturados como los mostrados anteriormente incluyendo los datos o payload, el contenido del payload no puede ser interpretado por esta misma herramienta, pero ventajosamente Wireshark desde su versión 1.12 incluye soporte para decodificar los paquetes Bluetooth LE.

4.1.4. Análisis mediante Wireshark

La información capturada por el comando ubertooth-btle puede ser guardada en un archivo con el parámetro “-c nombre”, el mismo que puede ser abierto desde Wireshark, en las pruebas realizadas se generó el archivo capturable2.pcap mostrando la siguiente información que fue decodificada donde puede observarse la BD ADDRESS del dispositivo Xiaomi Mi Band:

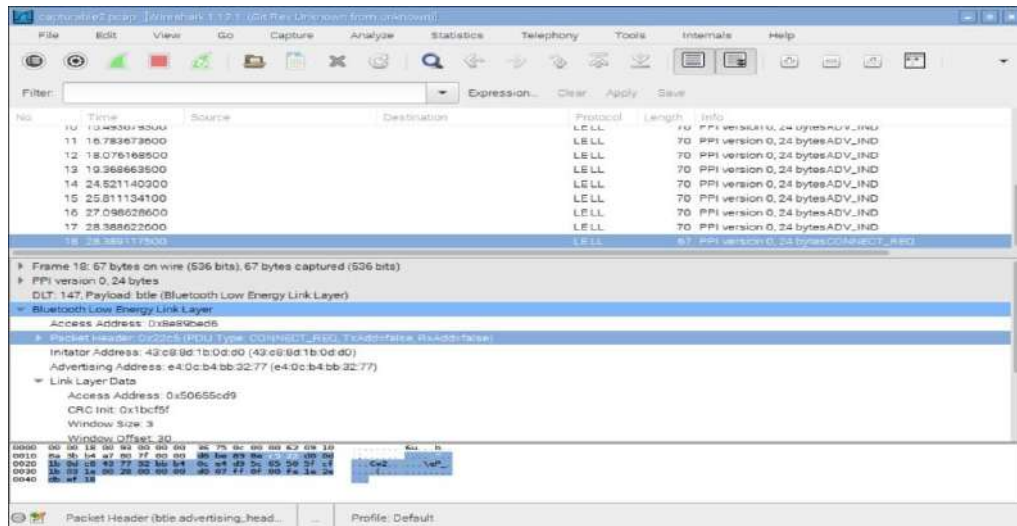


Figura 16-4: Wireshark BLE

Realizado por: Mena, D. 2017

4.1.5. Analisis mediante SmartRF

En la siguiente figura se puede observar como el CC2540USB puede capturar las notificaciones que transmitidas por el canal 37 asimismo se observan existen solicitudes de conexión es capaz de saltar los canales con los dispositivos decodificando cierta información como se muestra en el grafico siguiente:

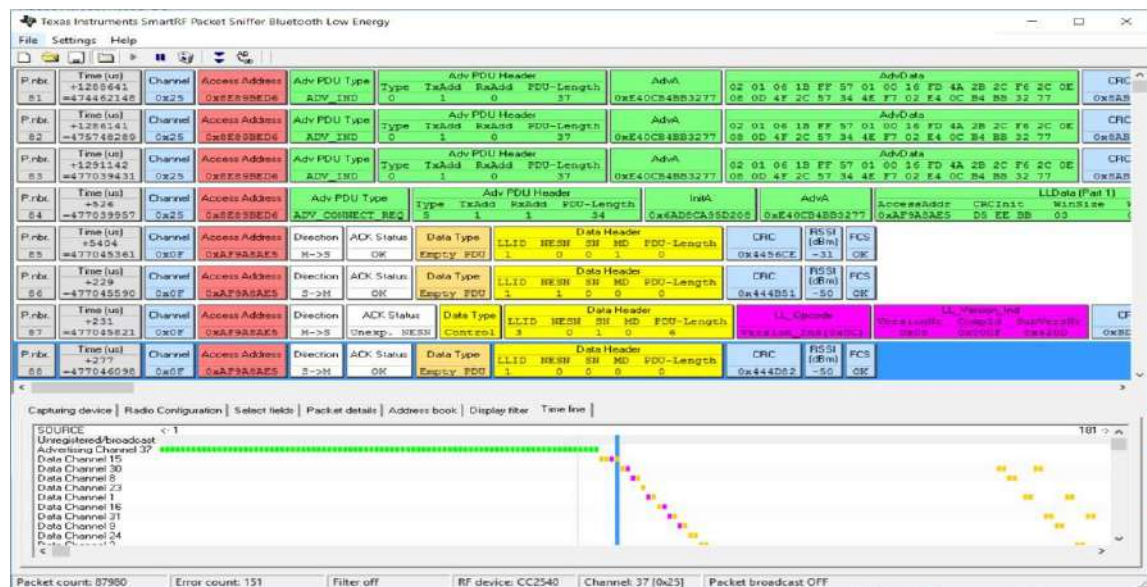


Figura 17-4: Captura de Trafico BLE 1

Realizado por: Mena, D. 2017

En nuestro entorno de pruebas al igual que Ubertooth se puede apreciar las notificaciones para conexión realizadas desde el dispositivo Xiaomi MiFi (BD ADDRESS e40cd4bb3277).

4.1.6. Ataques Bluetooth

BLUETOOTH CLÁSICO

Mediante la aplicación de Windows BTCRACK desarrollada por Thierry Zoller (<http://blog.zoller.lu/2009/02/btcrack-11-final-version-fpgasupport.html>), es posible descubrir la clave PIN de conexión Bluetooth a través del uso de fuerza bruta, para esto esta herramienta requiere de ciertos datos que pueden ser obtenidos a través de equipos comerciales de análisis de protocolos Bluetooth o dispositivos económicos especializados como lo es Ubetooth:

- LMP_IN_RAND
- LMP_COMB_KEY
- LMP_COMB_KEY (Master y esclavo)
- LMP_AU_RAND (Master y esclavo)
- LMP_SRES (Master y esclavo)

En las pruebas realizada no se pudo obtener con Ubetooth y un dongle Bluetooth todos los datos necesarios para ingresar a BTCRACK únicamente se obtuvieron la información de los BD_ADDR master y esclavo. Adjunto una captura como muestra de cómo deberían ser los datos a ingresarse.

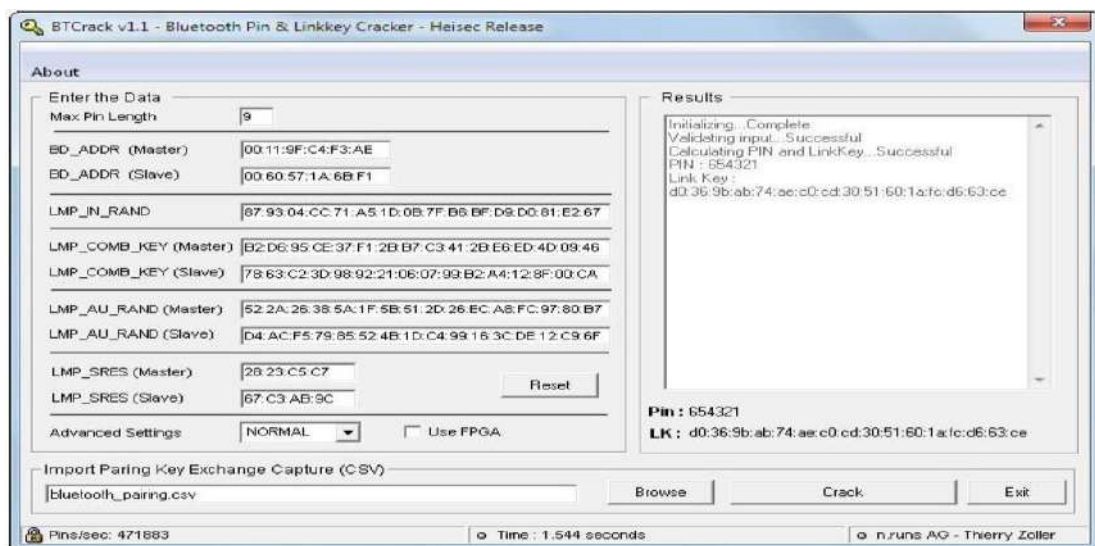


Figura 18-4: Ejemplo Captura con BTCrack

Fuente: (Wright & Cache)

4.1.7. Bluetooth Low Level

4.1.7.1. Crackle

La herramienta Crackle es una herramienta desarrollada por Mike Ryan que aprovecha una falla en el proceso de emparejamiento de BLE, que puede permitir a un atacante recuperar la clave de emparejamiento o TK (Temporary Key), trabaja con los modos de emparejamiento Just Works y Numeric entry.

En las pruebas realizadas con los dispositivos BLE Moto 360 y Xiaomi Mi band 2 no pudieron capturarse paquetes con Ubertooth cuando se realizaba un emparejamiento con el teléfono Samsung S6 edge+, a pesar de que se hicieron varios intentos con la aplicación móvil de cada dispositivo los resultados de crackle fueron similares, sobre esto se puede argumentar que la causa es el método de emparejamiento de estos dispositivos no es vulnerable al ataque de Crackle.

Xiaomi Mi Band 2

```
$ ubertooth-btle -f -c test4.cap
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo ubertooth-btle -f -c test4.cap
systemtime=1487450753 freq=2402 addr=8e89bed6 delta_t=283661.131 ms
00 09 aa 5b 2f 5e b8 f4 02 01 18 8e 7a ce
Advertising / AA 8e89bed6 (valid)/ 9 bytes
Channel Index: 37
Type: ADV_IND
AdvA: f4:b8:5e:2f:5b:aa (public)
AdvData: 02 01 18
Type 01 (Flags)
000011000
Data: aa 5b 2f 5e b8 f4 02 01 18
CRC: 8e 7a ce

systemtime=1487450753 freq=2402 addr=8e89bed6 delta_t=35.856 ms
00 1f aa 5b 2f 5e b8 f4 02 01 02 0e 09 4d 6f 74 6f 20 33 36 30 20 33 37 58 43 0
6 ff e0 00 10 50 00 2f bf 28
Advertising / AA 8e89bed6 (valid)/ 31 bytes
Channel Index: 37
Type: ADV_IND
AdvA: f4:b8:5e:2f:5b:aa (public)
AdvData: 02 01 02 0e 09 4d 6f 74 6f 20 33 36 30 20 33 37 58 43 06 ff e0 00
10 50 00 Public scapy-com Templates tesis1 test test1.pcap
Type 01 (Flags)
00000010
Type 09 (Complete Local Name)
Moto 360 37XC
Type ff
test3.cap test4.cap test5.cap tools ubertooth
```

Figura 19-4: Captura Xiaomi Mi Band

Realizado por: Mena, D. 2017

```
$ crackle -I test4.cap -o dtest4.cap
```



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo crackle -i test4.cap -o dtext4.cap
No connect packet found
No pairing request found
No pairing response found
Not enough confirm values found (0, need 2)
Not enough random values found (0, need 2)
No LL_ENC_REQ found
No LL_ENC_RSP found
Giving up due to 7 errors
```

Figura 20-4: Resultados crackle Xiaomi Mi Band

Realizado por: Mena, D. 2017

Moto 360

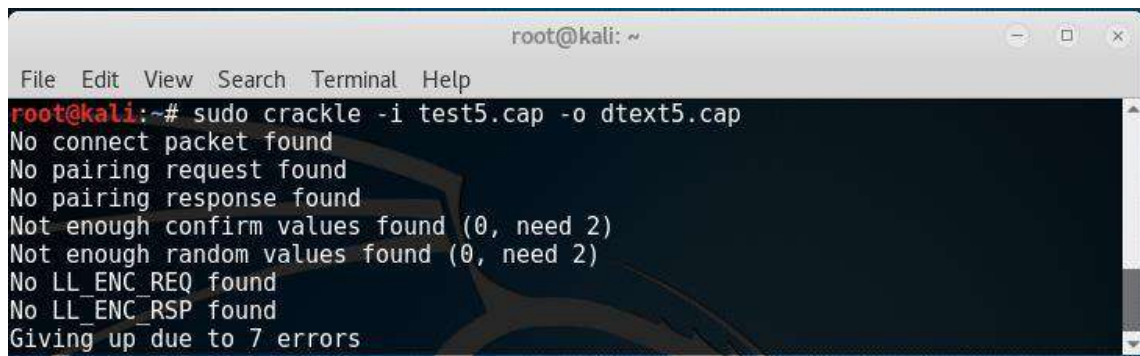
\$ ubertooth-btle -f -c test5.cap

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo ubertooth-btle -f -c test5.cap
systemtime=1487451061 freq=2402 addr=8e89bed6 delta_t=263761.856 ms
40 25 77 32 bb b4 0c e4 02 01 06 1b ff 57 01 00 4e fc 9a 79 c8 a3 ef 74 05 85 b
c 95 2f 62 99 c6 01 e4 0c b4 bb 32 77 85 57 5a
Advertising / AA 8e89bed6 (valid)/ 37 bytes
Channel Index: 37
Type: ADV_IND
AdvA: e4:0c:b4:bb:32:77 (random)
AdvData: 02 01 06 1b ff 57 01 00 4e fc 9a 79 c8 a3 ef 74 05 85 bc 95 2f 62
99 c6 01 e4 0c b4 bb 32 77
Type 01 (Flags)
00000110
Type ff
57 01 00 4e fc 9a 79 c8 a3 ef 74 05 85 bc 95 2f 62 99 c6 01 e4 0c b
4 bb 32 77
Data: 77 32 bb b4 0c e4 02 01 06 1b ff 57 01 00 4e fc 9a 79 c8 a3 ef 74 05
85 bc 95 2f 62 99 c6 01 e4 0c b4 bb 32 77
CRC: 85 57 5a
systemtime=1487451062 freq=2402 addr=8e89bed6 delta_t=1284.993 ms
40 25 77 32 bb b4 0c e4 02 01 06 1b ff 57 01 00 4e fc 9a 79 c8 a3 ef 74 05 85 b
c 95 2f 62 99 c6 01 e4 0c b4 bb 32 77 85 57 5a
Advertising / AA 8e89bed6 (valid)/ 37 bytes
Channel Index: 37
Type: ADV_IND
AdvA: e4:0c:b4:bb:32:77 (random)
AdvData: 02 01 06 1b ff 57 01 00 4e fc 9a 79 c8 a3 ef 74 05 85 bc 95 2f 62
```

Figura 21-4: Captura Moto 360

Realizado por: Mena, D. 2017

\$ crackle -I test5.cap -o dtext5.cap



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo crackle -i test5.cap -o dtext5.cap
No connect packet found
No pairing request found
No pairing response found
Not enough confirm values found (0, need 2)
Not enough random values found (0, need 2)
No LL_ENC_REQ found
No LL_ENC_RSP found
Giving up due to 7 errors
```

Figura 22-4: Resultados crackle Moto 360

Realizado por: Mena, D. 2017

4.1.8. *Ataque de Re-Emparejamiento*

Este ataque consiste en suplantar la BD_ADDR de uno de los dispositivos de la Piconet, con lo cual tratará de conectarse con el dispositivo objetivo esto resultara en una conexión fallida debido a que el atacante no conoce la clave de emparejamiento, como resultado de este intento fallido muchos dispositivos Bluetooth invalidaran la clave anterior haciendo que el dispositivo legitimo no logre conectarse, ocasionando que el usuario deba volver a emparejar los dispositivos, en este momento es cuando un atacante tendrá la oportunidad de monitorear el intento de conexión de los dispositivos para capturar datos importantes del emparejamiento para aplicar otros ataques como los ejemplos vistos anteriormente.

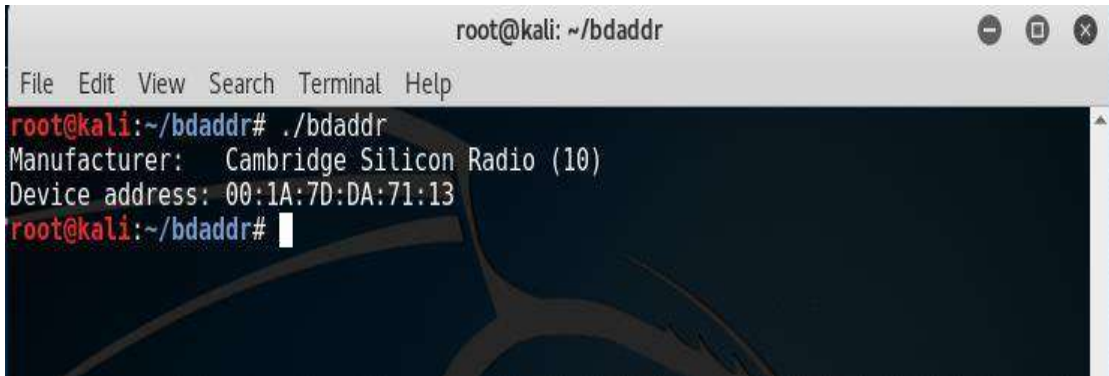
Para lograr un ataque de re-emparejamiento exitoso se necesita los siguientes requerimientos:

- Una interface bluetooth que tenga la capacidad de cambiar su BD_ADDR
- La BD_ADDR del dispositivo master que será cual se tratará de suplantar
- La BD_ADDR de dispositivo victima para forzar su re-emparejamiento
- Capturador de paquetes Bluetooth para cuando vigilar cuando los dispositivos vuelvan a emparejarse
- Proximidad física a los dispositivos a atacar a fin de establecer el intento de conexión necesario para el re-emparejamiento y captura de paquetes.

4.1.8.1. *Bdaddr*

Para lograr cambiar la dirección BD_ADDR de un dispositivo Bluetooth existe la herramienta BD_ADDR escrita por Marcel Holtman.

Para demostrar la vulnerabilidad utilizaremos un dongle Bluetooth como atacante e intentaremos forzar un re-emparejamiento entre el teléfono Samsung Galaxy S6 edge+ y el Smartwatch MOTO 360.



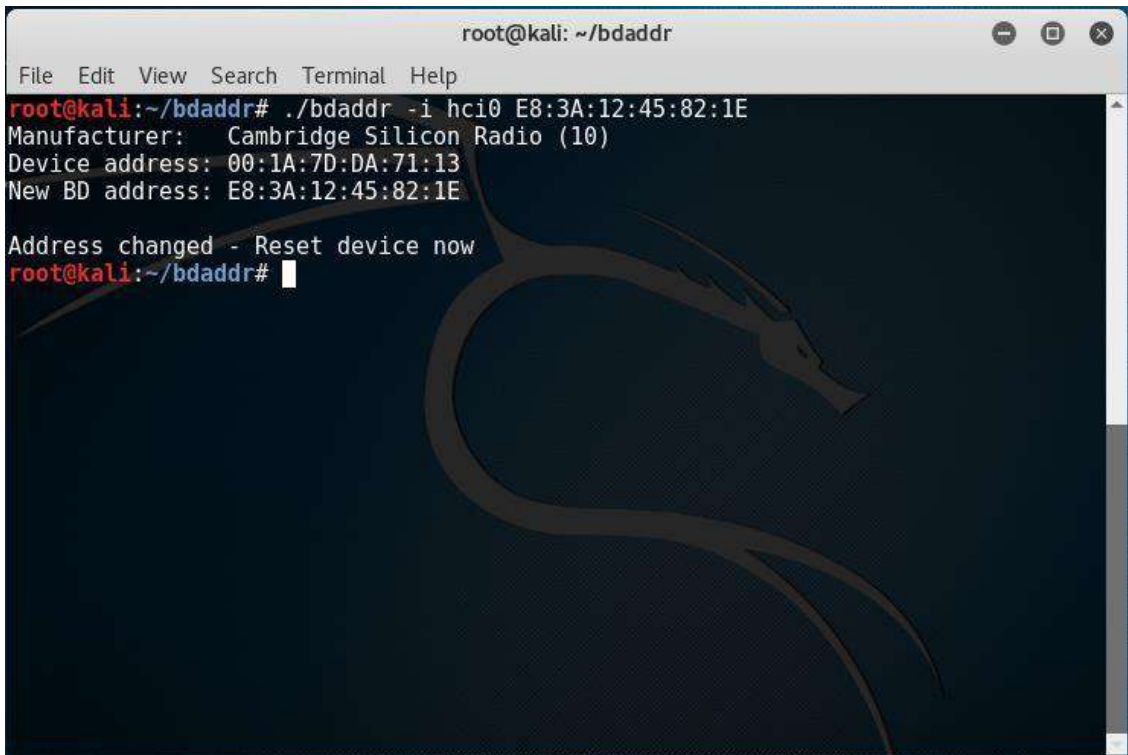
```
root@kali: ~/bdaddr
File Edit View Search Terminal Help
root@kali:~/bdaddr# ./bdaddr
Manufacturer: Cambridge Silicon Radio (10)
Device address: 00:1A:7D:DA:71:13
root@kali:~/bdaddr#
```

Figura 23-4: Ejecución y resultados Bdaddr

Realizado por: Mena, D. 2017

Al conocer en los ataques anteriores la BD_ADDR del Smartphone Galaxy S6 edge+ la clonaremos en el dongle Bluetooth, mediante el comando:

```
# ./bdaddr -i hci0 E8:3A:12:45:82:1E
```



```
root@kali: ~/bdaddr
File Edit View Search Terminal Help
root@kali:~/bdaddr# ./bdaddr -i hci0 E8:3A:12:45:82:1E
Manufacturer: Cambridge Silicon Radio (10)
Device address: 00:1A:7D:DA:71:13
New BD address: E8:3A:12:45:82:1E

Address changed - Reset device now
root@kali:~/bdaddr#
```

Figura 24-4: Cambio de MAC mediante Bdaddr

Realizado por: Mena, D. 2017

Aplicaremos entonces los comandos forzando el emparejamiento intentaremos conectarnos al MOTO 360 con BD_ADDR F4:B8:5E:2F:5B:AA.

```
# sudo hcitool cc F4:B8:5E:2F:5B:AA
```

Luego trataremos negociar el soporte de encriptación con lo cual causara la invalidez de la conexión por clave incorrecta.

```
# sudo hcitool enc F4:B8:5E:2F:5B:AA
```

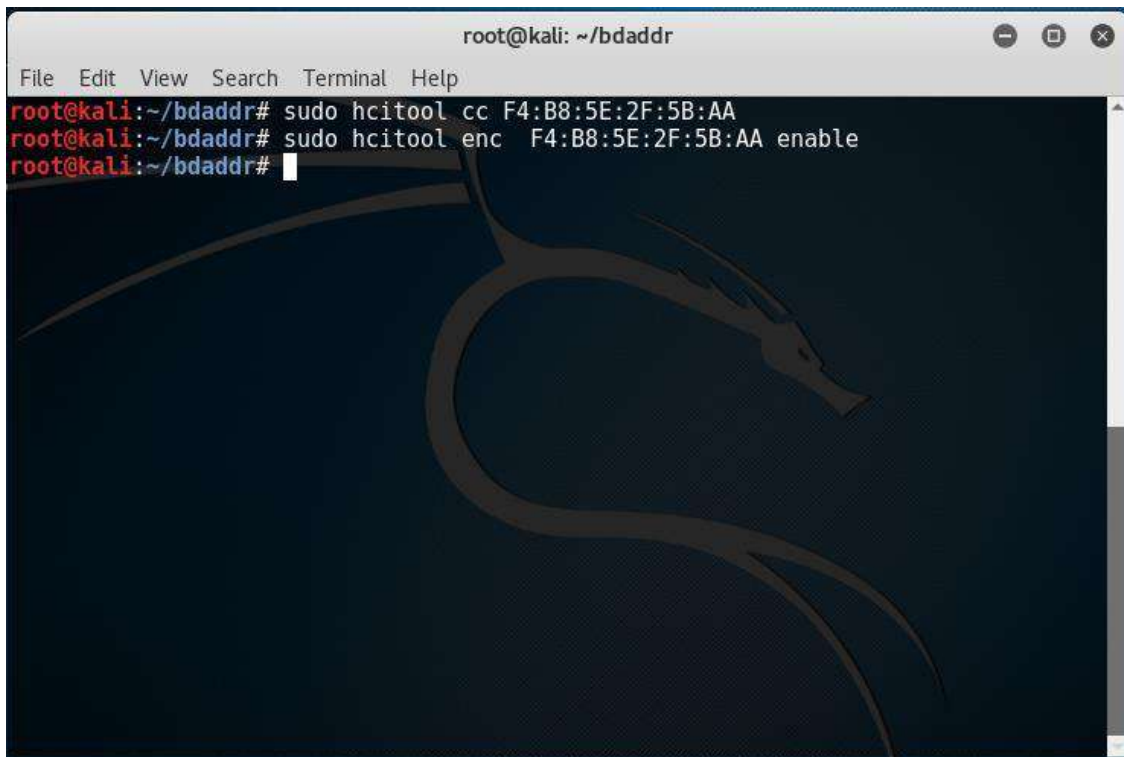
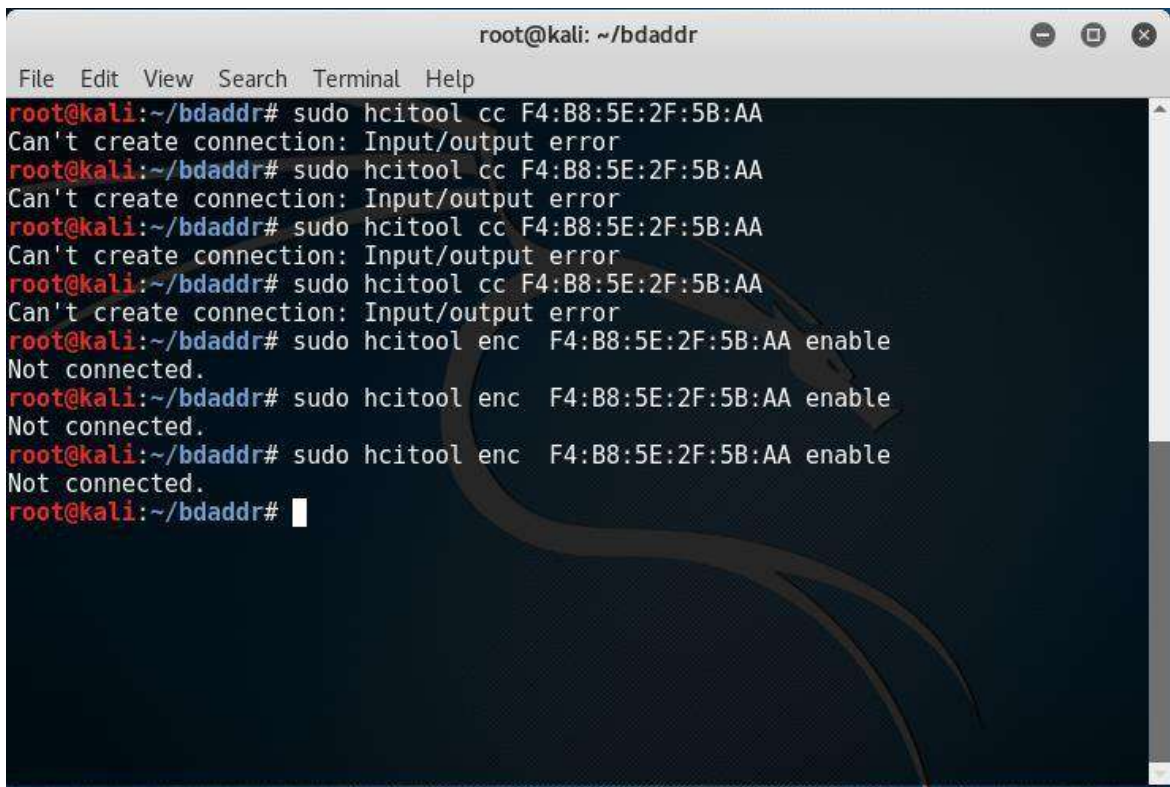


Figura 25-4: Ataque Re-emparejamiento

Realizado por: Mena, D. 2017

Al resultar exitoso este ataque forzará una desconexión de los dispositivos que estaban emparejados para lograr vulnerarlos ante un ataque de captura de tráfico.

Es posible controlar este ataque al manteniendo el Bluetooth apagado mientras no se lo esté utilizando además también depende de la proximidad física entre el dispositivo objetivo y la interface Bluetooth del atacante para que sea exitoso, en las pruebas tambien se pudo evidenciar que el ataque desde una distancia de 15 metros observando que los intentos de conexión resultaron ser fallidos.

A terminal window titled 'root@kali: ~/bdaddr' showing a series of failed commands. The user attempts to connect to a device with MAC address F4:B8:5E:2F:5B:AA using 'hcitool cc'. The first four attempts result in 'Can't create connection: Input/output error'. The next three attempts use 'hcitool enc' with the 'enable' flag, but all result in 'Not connected.' The terminal ends with a prompt 'root@kali:~/bdaddr#'.

```
root@kali:~/bdaddr# sudo hcitool cc F4:B8:5E:2F:5B:AA
Can't create connection: Input/output error
root@kali:~/bdaddr# sudo hcitool cc F4:B8:5E:2F:5B:AA
Can't create connection: Input/output error
root@kali:~/bdaddr# sudo hcitool cc F4:B8:5E:2F:5B:AA
Can't create connection: Input/output error
root@kali:~/bdaddr# sudo hcitool cc F4:B8:5E:2F:5B:AA
Can't create connection: Input/output error
root@kali:~/bdaddr# sudo hcitool enc F4:B8:5E:2F:5B:AA enable
Not connected.
root@kali:~/bdaddr# sudo hcitool enc F4:B8:5E:2F:5B:AA enable
Not connected.
root@kali:~/bdaddr# sudo hcitool enc F4:B8:5E:2F:5B:AA enable
Not connected.
root@kali:~/bdaddr#
```

Figura 26-4: Ataque Re-emparejamiento fallido

Realizado por: Mena, D. 2017

Conclusiones

Los dispositivos Bluetooth Clásico y Bluetooth LE son vulnerables a herramientas de reconocimiento principalmente cuando estos están en modo descubierto como pudo comprobarse en las pruebas al obtener información importante como los BD_ADDR de los dispositivos de la Piconet, un atacante puede aprovechar esta información para realizar varios ataques además existen en el mercado equipos de análisis de protocolos que pueden capturar y analizar las redes Bluetooth con lo cual se pudiera obtener y descifrar los datos capturados.

4.2. Reconocimiento de dispositivos RF

Mediante el uso del RTL-SDR configuraremos nuestro sensor en las frecuencias deseadas, en este caso se escogió 433 Mhz para detectar la posible actividad de los dispositivos usados para las pruebas.

Al encender y apagar varias veces uno de los tomacorrientes se pudo obtener el siguiente resultado como se aprecia en el grafico siguiente:

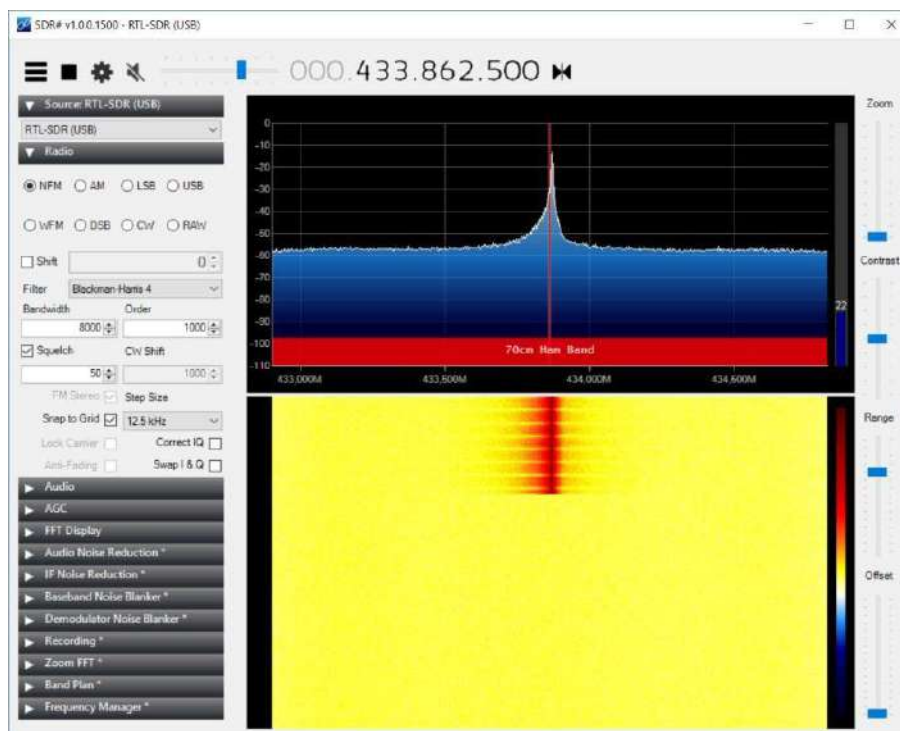


Figura 27-4: Lectura dispositivo RF

Realizado por: Mena, D. 2017

Se puede observar actividad alrededor de la frecuencia 433.862 Mhz evidenciando a un atacante que en el hogar objetivo existe la posible utilización de un dispositivo RF.

Existen soluciones comerciales más potentes para realizar esta prueba con las cual se puede realizarla desde una distancia superior al equipo de pruebas.

4.2.1. Ataque mediante el uso de Rfsniffer

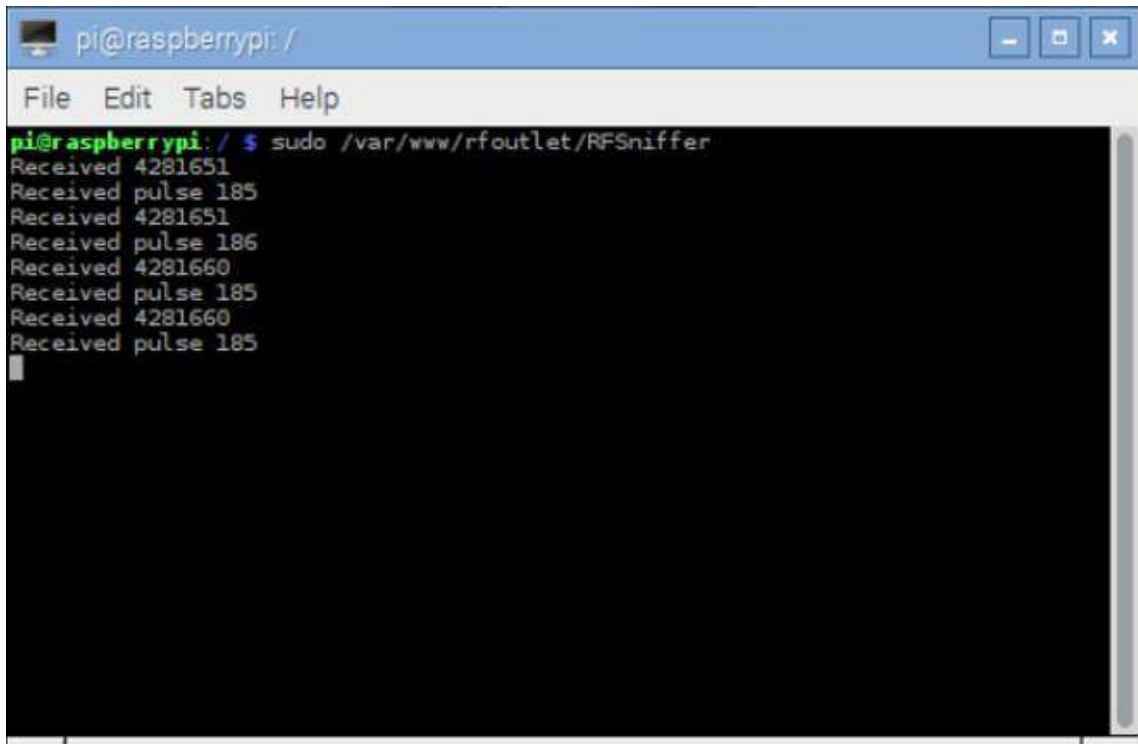
En el Raspberry Pi, instalaremos la herramienta Rfsniffer escrita por Tim Leland, <https://github.com/timleland/rfoutlet>, la misma que nos permitirá capturar los códigos de encendido y apagado que envía el control remoto al tomacorriente de prueba Etekcitty para luego replicarlos desde un módulo de transmisión 433 Mhz conectado al Raspberry pi.

Para capturar los códigos ejecutaremos Rfsniffer

```
$ sudo /var/www/rfoutlet/RFSniffer
```

Podremos observar que cuando se pulsa un botón nos muestra dos códigos el que interesa es el código más largo, los valores capturados son:

1. 4281651 (Encendido)
2. 4281660 (Apagado)

A terminal window titled 'pi@raspberrypi: /' with a menu bar containing 'File', 'Edit', 'Tabs', and 'Help'. The terminal output shows the command 'sudo /var/www/rfoutlet/RFSniffer' and its output: 'Received 4281651', 'Received pulse 185', 'Received 4281651', 'Received pulse 186', 'Received 4281660', 'Received pulse 185', 'Received 4281660', and 'Received pulse 185'.

```
pi@raspberrypi: / $ sudo /var/www/rfoutlet/RFSniffer
Received 4281651
Received pulse 185
Received 4281651
Received pulse 186
Received 4281660
Received pulse 185
Received 4281660
Received pulse 185
```

Figura 28-4: Lectura de códigos de control

Realizado por: Mena, D. 2017

Ingresaremos los códigos capturados en la plantilla web que viene incluida en RFSniffer el archivo a editar es `toggle.php`.

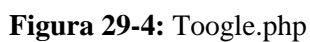


Figura 29-4: Toogle.php

Realizado por: Mena, D. 2017

Ingresaremos servidor web activo en el Raspberry pi para comprobar la posibilidad de controlar los tomacorrientes desde el interfaz web sin la necesidad de contar con el control remoto original, los botones mostrados en la página web poseen los códigos capturados del control remoto estos son enviados por RFSniffer al módulo de transmisión y recepción RF de 433 Mhz instalado en el Raspberry Pi.

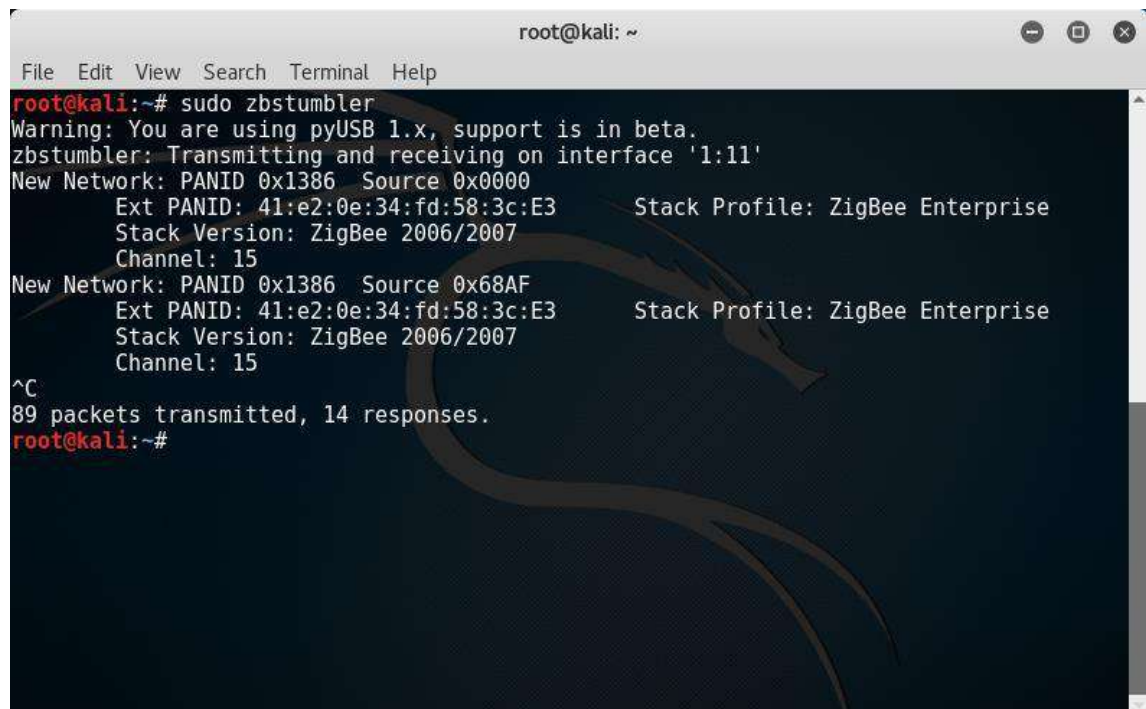
Conclusiones

Como puede observarse los dispositivos RF de prueba no presentaron inconvenientes para detectar y leer los códigos de control, por tanto en este tipo de productos genéricos existe una vulnerabilidad relevante ya que se encuentran disponibles herramientas para atacarlos como en este caso en el encendido y apagado de luces o tomacorrientes, un atacante con la información adecuada pudiera replicar este escenario y tomar control de estos dispositivos RF de un hogar sin la necesidad de poseer el control remoto o aplicación móvil.

4.3. Reconocimiento de redes Zigbee

Mediante el uso del Armel RZ Raven con el firmware Killerbee con la herramienta zbstumbler de Killerbee nos permite descubrir las redes activas Zigbee y 812.15.4 que se encuentren cercanas, en el grafico se muestra las redes que se detectaron de los dispositivos prueba que componen el kit de automatización de hogar utilizado.

```
$ sudo zbstumbler
```



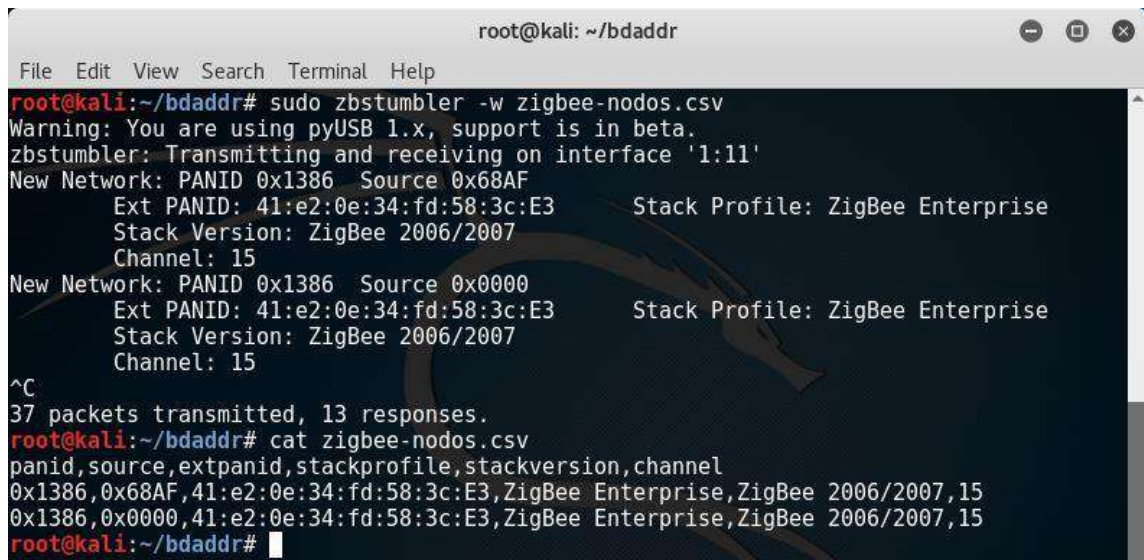
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sudo zbstumbler  
Warning: You are using pyUSB 1.x, support is in beta.  
zbstumbler: Transmitting and receiving on interface '1:11'  
New Network: PANID 0x1386 Source 0x0000  
Ext PANID: 41:e2:0e:34:fd:58:3c:E3 Stack Profile: ZigBee Enterprise  
Stack Version: ZigBee 2006/2007  
Channel: 15  
New Network: PANID 0x1386 Source 0x68AF  
Ext PANID: 41:e2:0e:34:fd:58:3c:E3 Stack Profile: ZigBee Enterprise  
Stack Version: ZigBee 2006/2007  
Channel: 15  
^C  
89 packets transmitted, 14 responses.  
root@kali:~#
```

Figura 30-4: Reconocimiento de redes Zigbee

Realizado por: Mena, D. 2017

Para un mejor descubrimiento de las redes es posible mantener un escaneo permanente y constante y que los resultados sean almacenados en un archivo para su análisis posterior.

```
$ sudo zbstumbler -w nombrearchivo
```

```
root@kali: ~/bdaddr
File Edit View Search Terminal Help
root@kali:~/bdaddr# sudo zbstumbler -w zigbee-nodos.csv
Warning: You are using pyUSB 1.x, support is in beta.
zbstumbler: Transmitting and receiving on interface '1:11'
New Network: PANID 0x1386 Source 0x68AF
Ext PANID: 41:e2:0e:34:fd:58:3c:E3 Stack Profile: ZigBee Enterprise
Stack Version: ZigBee 2006/2007
Channel: 15
New Network: PANID 0x1386 Source 0x0000
Ext PANID: 41:e2:0e:34:fd:58:3c:E3 Stack Profile: ZigBee Enterprise
Stack Version: ZigBee 2006/2007
Channel: 15
^C
37 packets transmitted, 13 responses.
root@kali:~/bdaddr# cat zigbee-nodos.csv
panid,source,extpanid,stackprofile,stackversion,channel
0x1386,0x68AF,41:e2:0e:34:fd:58:3c:E3,ZigBee Enterprise,ZigBee 2006/2007,15
0x1386,0x0000,41:e2:0e:34:fd:58:3c:E3,ZigBee Enterprise,ZigBee 2006/2007,15
root@kali:~/bdaddr#
```

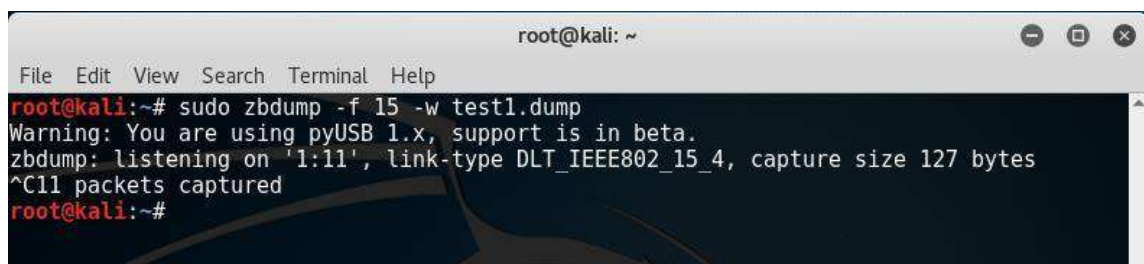
Figura 31-4: Reconocimiento Zigbee a un archivo

Realizado por: Mena, D. 2017

El Atmel RZ Raven USB nos permite monitorear el tráfico de Zigbee de la red cercana y con herramientas complementarias almacenar la captura en un archivo con lo cual mediante herramientas complementarias se pudiera descryptar la información e inclusive obtener las claves de comunicación de las redes Zigbee.

La herramienta zbdump de Killerbee permite hacer lo indicado, en este ejemplo se muestra una captura de las redes Zigbee presentes que se encuentran transmitiendo en el canal 15 como así fueron descubiertas anteriormente con la herramienta zbstumbler.

```
# sudo zbdump -f 15 -w test1.dump
```



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sudo zbdump -f 15 -w test1.dump
Warning: You are using pyUSB 1.x, support is in beta.
zbdump: listening on '1:11', link-type DLT_IEEE802_15_4, capture size 127 bytes
^C11 packets captured
root@kali:~#
```

Figura 32-4: Pruebas Zbdump

Realizado por: Mena, D. 2017

El archivo resultado de la captura (test1.dump), puede ser reconocido por la herramienta sniffer Wireshark en la gráfica se observa que puede mostrarse los datos encriptados de los paquetes capturados.

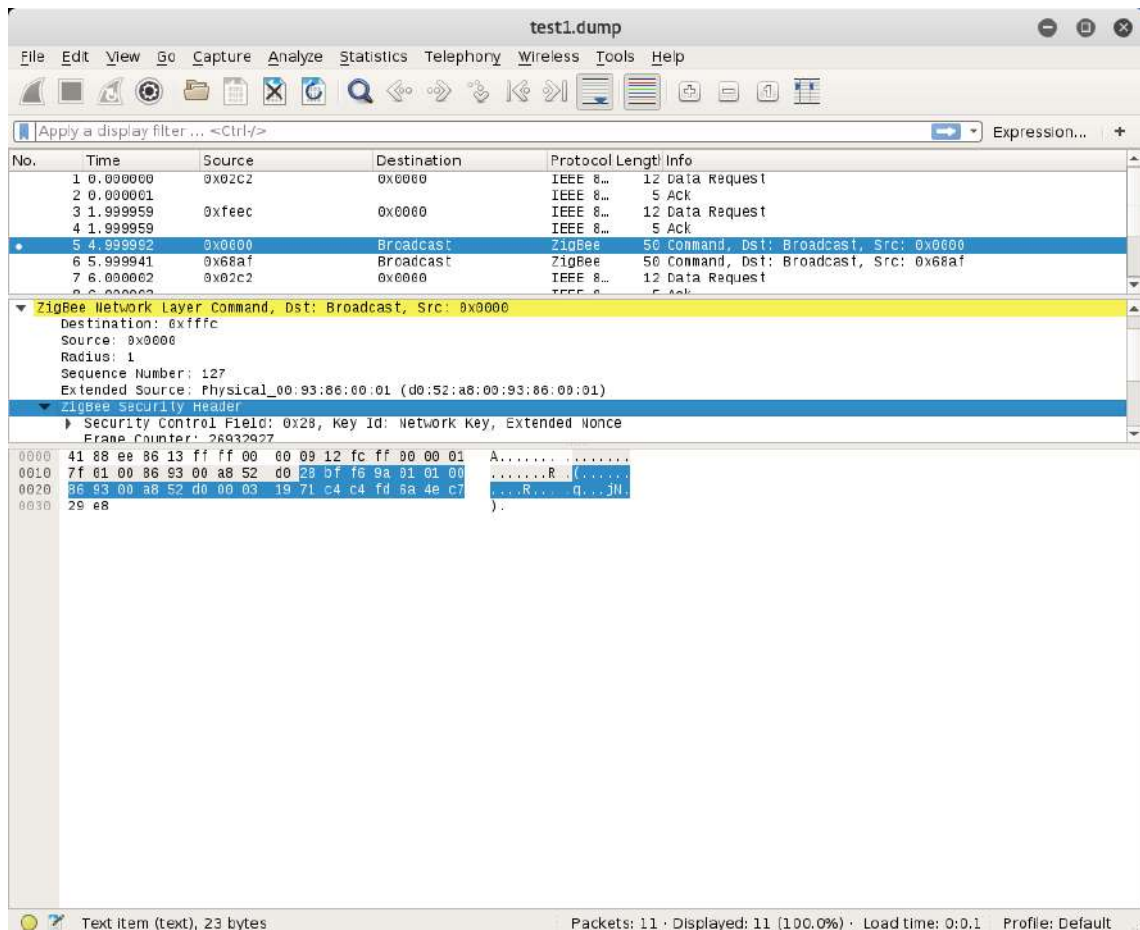


Figura 33-4: Lectura en Wireshark paquetes Zigbee

Realizado por: Mena, D. 2017

4.3.1. Ataque Zigbee

Killerbee posee varias herramientas para realizar ciertos ataques conforme los datos recolectados en el reconocimiento y captura de las redes Zigbee. La herramienta zbdsniff permite descubrir las claves de la red Zigbee desde un archivo que contenga la captura de tráfico con los datos necesarios para revelar las claves.

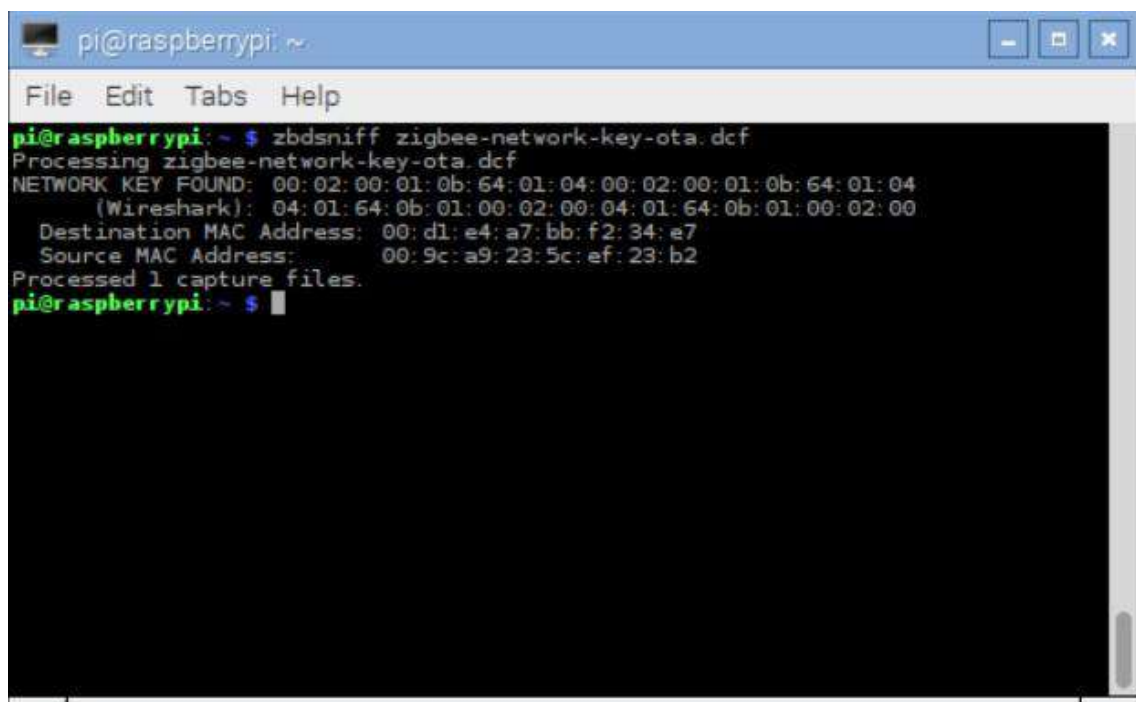
```
#sudo zbdsniff *.dump
```

Conclusiones

En las pruebas de laboratorio realizadas se utilizó las capturas de tráfico de los dispositivos del kit de automatización de hogar simulando un entorno similar al que puede hallarse en un hogar. Después de varios intentos en capturar el tráfico para descubrir las claves no pudieron obtenerse las claves de red de la comunicación de estos dispositivos, probablemente esta limitación fue

debido a los parámetros de seguridad que posee el kit de automatización de hogar utilizado (Smartthings), adicionalmente se pudo notar en las pruebas que el dispositivo Atmel RZ Raven USB presentó cierta inestabilidad en varias herramientas ya que se tuvieron cierres de la aplicación inesperados mientras se estaban ejecutando.

Para demostrar que es posible descubrir las claves de red mediante el uso de Killerbee se utilizó un archivo de ejemplo disponible en el directorio de la aplicación, al aplicar la herramienta zbdsniff a este archivo se pudo obtener la clave de red como se muestra en el siguiente gráfico.



```
pi@raspberrypi: ~  
File Edit Tabs Help  
pi@raspberrypi: ~ $ zbdsniff zigbee-network-key-ota.dcf  
Processing zigbee-network-key-ota.dcf  
NETWORK KEY FOUND: 00:02:00:01:0b:64:01:04:00:02:00:01:0b:64:01:04  
(Wireshark): 04:01:64:0b:01:00:02:00:04:01:64:0b:01:00:02:00  
Destination MAC Address: 00:d1:e4:a7:bb:f2:34:a7  
Source MAC Address: 00:9c:a9:23:5c:ef:23:b2  
Processed 1 capture files.  
pi@raspberrypi: ~ $
```

Figura 34-4: Ejemplo descubrimiento clave de red Zigbee

Realizado por: Mena, D. 2017

CAPÍTULO V

5. Guía metodológica para el control de vulnerabilidades de dispositivos IoT en redes HAN



Figura 1-5: Guía metodológica para el control de vulnerabilidades de dispositivos IoT en redes HAN

Realizado por: Mena, D. 2017

5.1 ¿Qué es el Internet de las cosas (IoT)?

A ciertos dispositivos nuestros a los que podemos conectarlo a Internet ya sea para intercambiar información o para habilitar funciones varias como un acceso remoto a este mediante una aplicación móvil se consideran dispositivos pertenecientes al Internet de las Cosas o IoT.

Entre estos dispositivos comúnmente se encuentran: tablets, computadores, teléfonos inteligentes, aunque se han introducido una variedad de dispositivos o equipos que han incorporado varios métodos para comunicarse con otros para brindar nuevos servicios como por ejemplo un termostato puede tener la capacidad de regular la energía que consumirá para adaptarla a las necesidades o hábitos de un usuario, generando para este un ahorro de dinero.

El hecho que estos dispositivos se comuniquen de manera inteligente sin la intervención humana puede permitir brindar ciertos aspectos de eficiencia en el uso de estos como por ejemplo, un refrigerador puede detectar la falta de un alimento y comunicarlo inmediatamente a un usuario mediante mensajes de texto o correos a través de Internet, inclusive tuviera la capacidad de generar un pedido online a un proveedor.



Figura 2-5: The Internet of your things Microsoft's Vision for IoT (Tuzovic)

Fuente: (Tuzovic, 2015)

5.1.1. Aseguramiento de las cosas en Internet

La materialización de las amenazas de seguridad a las que están expuestos los dispositivos IoT puede afectar al usuario de estos de diferentes maneras que puede ir desde inconvenientes en la accesibilidad del dispositivo, como en falencias a la integridad de la información que contiene o transmiten o a la identidad del usuario autorizado que puede provocar una suplantación de identidad y por consiguiente filtraciones de información confidencial. Para ello se debe generar

una guía que oriente al usuario a minimizar el riesgo de las vulnerabilidades, haciendo énfasis en el tipo de tecnologías inalámbricas más presente en los hogares.

5.1.2. *Recomendaciones de seguridad para dispositivos IoT en el hogar*

Las recomendaciones de la presente guía están basadas en las señaladas por la plataforma OWASP (<https://www.owasp.org/>) que está orientada a ayudar tanto a fabricantes como consumidores en los problemas de seguridad asociados al Internet de las Cosas.

5.1.2.1. *Conocer que dispositivos poseo en el hogar*

El paso principal para asegurar los dispositivos IoT en el hogar es conocer de cuantos dispongo e identificar cuáles son vulnerables a ataques informáticos, entre los más comunes se encuentran computadores, teléfonos inteligentes, tablets, se debe hacer un repaso de todos los dispositivos que puedan estar conectados en el hogar, se debe tomar en cuenta que entre estos también están cámaras de vigilancia, consolas de videojuegos, dispositivos de automatización de hogar, etc. una vez identificados se debe tratar de conocer en cada uno la información a la que tienen acceso y el tipo de tecnología de red utiliza para comunicarse.



Figura 3-5: Dispositivos IoT en el hogar

Fuente: (iStart, 2014)

5.1.2.2. *Utilización de interfaces web y aplicaciones seguras*

Los dispositivos IoT pueden ser vulnerables a cyberataques a través de sus aplicaciones de control o interfaces web, por ejemplo servidores web o aplicaciones móviles (IOS, Android) tienen un rol importante en la seguridad de un dispositivo, ya mediante estas se ejecutan los códigos para su control, aplicaciones maliciosas pueden intentar tratar de comprometer a las aplicaciones válidas para tratar de tomar el control de sus procesos o acciones de manera fraudulenta asimismo

estas aplicaciones intentaran mediante ingeniería inversa tratar de engañar a los usuarios para obtener datos críticos como contraseñas e información personal.

Se recomienda que no se acepte la instalación de aplicaciones móviles de las cuales no se tenga referencia, de igual manera llevar un control periódico de las aplicaciones instaladas en el dispositivo es recomendable la utilización de software de seguridad informática como antivirus.

La utilización de interfaces inseguras por parte de los fabricantes de los dispositivos IoT pueden causar que estas sufran ataques dirigidos a este mediante diversas técnicas para lograr obtener los datos de configuración y acceso al dispositivo se recomienda validar si la interfaz web cuenta con el uso de protocolos de seguridad y si estos pueden ser activados desde su configuración además de políticas de control de contraseña como la limitación de intentos fallidos.



Figura 4-5: Asegurar aplicaciones móviles

Fuente: (CompsMag, 2015)

5.1.2.3. *Cambiar las contraseñas por defecto*

Muchos dispositivos IoT como cámaras de seguridad o routers funcionan de manera independiente, para el proceso de instalación y configuración el fabricante provee de usuarios y contraseñas por defecto los cuales en muchas ocasiones no son cambiados, esto constituye en una grave vulnerabilidad ya que un atacante puede mediante diversas técnicas identificar el dispositivo y realizar la búsqueda de Internet de las claves de acceso, pudiendo alcanzar a obtener el control del dispositivo.

Como medida de seguridad se recomienda cambiar SIEMPRE las claves por defecto del dispositivo, aplicando una contraseña generada mediante una composición segura y compleja de

caracteres especiales, mayúsculas, minúsculas y números de al menos una extensión de 8 caracteres.



Figura 5-5: Contraseñas seguras

Fuente: (International Business Times, 2014)

5.1.2.4. *Aplicar configuraciones de seguridad*

En muchas ocasiones el usuario no toma en cuenta las opciones de seguridad que se encuentran disponibles en los dispositivos IoT, las mismas que generalmente se encuentran indicadas en las guías de uso o manuales.

Es importante revisar si el dispositivo cuenta con las siguientes opciones:

- Cifrado de datos ya sea en el almacenamiento o transmisión a fin de que estos se manipulen de manera segura para proteger la información personal.
- Medidas de Autenticación y Autorización para usuarios autorizados a través de implementar autenticación de dos vías, Acceso granular a la configuración del dispositivo o a los servicios que brinda este, credenciales de acceso y políticas de contraseña.
- Control de puertos de red para evitar que estos sean atacados desde el exterior aprovechado alguna vulnerabilidad existente, se recomienda que los puertos no utilizados o que no influyan en el funcionamiento del dispositivo sean deshabilitados.
- Funciones para control de servicios en algunos dispositivos existe la posibilidad de regular los servicios que proporciona a fin de dar opciones específicas de seguridad a los usuarios como es el ejemplo del control parental para limitar el acceso hacia Internet a ciertos usuarios.



Figura 6-5: Configuraciones de Seguridad

Fuente: (Totality Services, 2016)

5.1.2.5. *Mantener los dispositivos IoT actualizados*

A pesar de que los dispositivos IoT se encuentren correctamente configurados por parte del usuario, a veces el mismo dispositivo está afectado por vulnerabilidades propias de su implementación o fabricación.

Para controlar estas vulnerabilidades se recomienda siempre mantener actualizado el dispositivo con las versiones de software o firmware proporcionadas por el fabricante, en muchas ocasiones el dispositivo tendrá la funcionalidad de descargar automáticamente las actualizaciones de no ser así es necesario que la actualización sea realizada de manera manual además de comprobar periódicamente la existencia de nuevas versiones.

Un aspecto importante es verificar si el fabricante del dispositivo mantiene una constante provisión de actualizaciones a su producto, ya que existen dispositivos que reciben poco o nulo soporte postventa, en este caso se recomienda mantener el dispositivo de manera oculta para su acceso hacia Internet a fin de evitar que pueda ser identificado por un atacante que pueda conocer de sus vulnerabilidades.



Figura 7-5: Actualizar dispositivos IoT

Fuente: (Florian)

5.1.2.6. *Proteger físicamente los dispositivos IoT*

La seguridad física es un aspecto observado pero muy importante al momento de implementar un entorno IoT ya que al existir esta brecha de seguridad un atacante al obtener el acceso físico al dispositivo puede penetrar y explotar ciertos componentes sensibles de este como su memoria, logrando mediante diversas técnicas ganar el acceso a la configuración del dispositivo, contraseñas de usuario autorizados, configuraciones y otros parámetros críticos.

Se recomienda guardar un criterio de seguridad al momento de utilizar los dispositivos IoT y donde estos vana a permanecer a fin de que estos no sean fácilmente accesibles por atacantes, por ejemplo escoger un sitio adecuado y seguro al momento de ubicar un equipo crítico del entorno IoT como es un router ya que a través de su red hacia Internet generalmente se conectarán los dispositivos IoT del hogar.



Figura 8-5: Seguridad Física IoT

Fuente: (Betanews, 2015)

5.1.2.7. *Utilizar dispositivos y software de seguridad*

Para fortalecer la seguridad del entorno IoT del hogar se sugiere la adquisición de dispositivos que actúen como cortafuegos para la red del hogar del exterior, en algunos casos los dispositivos cuentan con algún tipo de protección que actúa de manera similar pero se recomienda adquirir un equipo que ofrezca mayores funcionalidades, cabe indicar que además de adquirir es necesario que el dispositivo de seguridad sea correctamente configurado por un técnico.

El software de seguridad como lo son los antivirus brindarán un nivel más de protección a los dispositivos IoT como los teléfonos móviles ya que aparte verificar la intrusión de software malicioso permitirá el respaldo de información como localización del dispositivo en caso de robo.

5.1.2.8. *Asegurar las redes de comunicación de los dispositivos IoT*

Las redes de comunicación constituyen en una de las principales vulnerabilidades informáticas en el hogar ya que mediante esta los usuarios conectan sus dispositivos IoT hacia Internet u otros dispositivos inteligentes, las redes inalámbricas son las más utilizadas en entornos IoT y específicamente la tecnología WIFI es la más presente en los hogares seguida de Bluetooth, Zigbee, radiofrecuencia, etc. Al usarse tecnología inalámbrica permite que la red casera pueda extenderse sin limitaciones por objetos físicos como paredes o puertas, pero esta ventaja también puede ser contraproducente ya que la red pudiera estar al alcance de un atacante que se encuentra cerca, por tanto, se sugiere que se trate de conectar los dispositivos IoT mediante redes cableadas siempre y cuando no afecte al servicio brindado por el dispositivo y conforme al criterio y comodidad del usuario.

Se recomienda además en crear una red inalámbrica independiente exclusiva para los dispositivos IoT que manejen información personal, muchos routers en el mercado poseen esta funcionalidad a fin de dificultar al atacante a que pueda acceder a estos fácilmente.

Existen otras tecnologías inalámbricas usadas por los dispositivos IoT en el hogar aparte de WIFI como Bluetooth las cuales poseen vulnerabilidades informáticas identificadas propias de su funcionamiento y de su diseño que pueden ser igualmente aprovechadas por atacantes para tomar control del dispositivo y robar información personal. A continuación, se muestra un repaso de las tecnologías IoT presentes en el hogar, sus vulnerabilidades y el método sugerido para controlarlas.

i. Tecnologías de comunicación inalámbricas para dispositivos IoT en el hogar

A. WIFI

WI-FI (Fidelidad inalámbrica) es un término de la WIFI-Alliance para referirse a las tecnologías inalámbricas enmarcadas en el estándar 802.11, fue creada por la necesidad de establecer un mecanismo universal para la comunicación inalámbrica de los dispositivos electrónicos existentes en el mercado por lo que es el más común y utilizado para conectarlos a redes como Internet.

Es soportado por casi la totalidad de dispositivos incluyendo obviamente a los del Internet de las cosas, el mecanismo utilizado para brindarles conexión de red es a través de puntos de acceso o routers inalámbricos.



Figura 9-5: WIFI

Fuente: (Wikipedia)

Estándares WIFI

Los diversos estándares disponibles de acuerdo a sus características y velocidad de transmisión son:

Legacy 802.11

Publicado en 1997

Velocidades de transmisión: 1 y 2 Mbps

3 canales a 2,4Ghz

802.11a

Publicado en 1999

Velocidades de transmisión: 6, 9, 12, 18, 24, 36, 48 y 54Mbps

12 canales a 5 Ghz

802.11b

Publicado en 1999

Velocidades de transmisión: 1, 2, 5'5 y 11 Mbps

3 canales a 2,4Ghz

802.11g

Publicado en 2003

Velocidades de transmisión: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

3 canales a 2,4Ghz

802.11n

Velocidades de transmisión: 1, 2, 5'5, 6, 9, 11, 12, 18, 24, 36, 48 o 54 Mbps

12 canales a 5GHz

Es el más común en dispositivos relativamente modernos.

802.11ac

Publicado en 2014

Velocidades de transmisión: 200, 400, 433, 600, 867 y 1.300 Mbps

24 canales a 5Ghz

Como se había señalado la mayoría de dispositivos IoT que requieren banda ancha tienen soporte a esta tecnología, entre estos tenemos: computadores, teléfonos inteligentes, tablets, televisores inteligentes, video consolas, etc.



Figura 10-5: Dispositivos IoT en el Hogar

Fuente: (Webadictos, 2013)

A.1. Principales amenazas y vulnerabilidades de WIFI

Entre las más importantes vulnerabilidades que posee la tecnología WIFI son las siguientes:

Mac Spoofing

Sucede cuando un atacante descubre una dirección física MAC e intenta suplantarla para aparentar ser un cliente autorizado de la red.

Denegación de Servicio

Un atacante puede afectar la disponibilidad de un servicio o recurso al afectar a la red con tráfico dirigido a explotar las limitaciones de hardware y software de los equipos distribuidores de red como los puntos de acceso, causando que los clientes validos no puedan acceder a la red en un determinado momento.

Access Point Spoofing

Cuando un atacante descubre el nombre de una red autorizada puede tratar de suplantar su identidad creando una red con el mismo nombre para tratar que los clientes validos creen que la red maliciosa a la cual se conectan es la red verdadera.

Hombre en el medio (Man in the Middle)

Esta vulnerabilidad sucede cuando un atacante se encuentra dentro de la red haciendo que el tráfico y datos que circula en esta perteneciente a usuarios validos puedan ser capturada, leída, modificada y transmitida sin que los usuarios noten su presencia, con el aprovechamiento de esta vulnerabilidad.

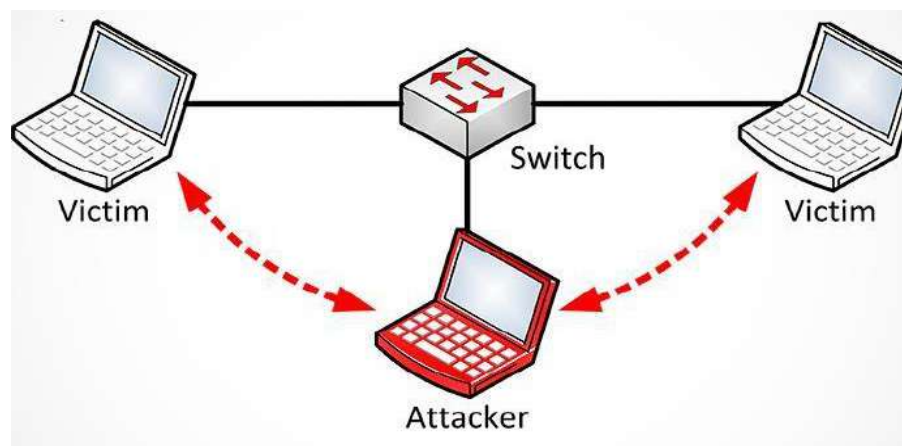


Figura 11-5: Ataque Hombre en el medio

Fuente: (rootear, 2013)

A.2. Como controlar las vulnerabilidades en dispositivos IoT conectados por WIFI

- Evitar el uso de redes abiertas, ya que estas no requieren de autenticación por tanto no cifran la información, al ser de libre acceso o públicos es posible que en la red se

encuentre atacantes dispuestos a escuchar el tráfico o datos que circula por la misma como contraseñas, información personal, datos bancarios, etc.

- Ocultar el nombre de la red WIFI o ESSID con el objeto de evitar que personas maliciosas intenten atacar la red del hogar al conocer la existencia de esta, esta es una medida de prevención algo eficaz ya que existen técnicas para descubrirlas.
- Utilizar métodos fuertes para el cifrado de tráfico de la red WIFI como es el uso de WAP/WPA2, aplicando claves de acceso a la red seguros, se recomienda no utilizar métodos antiguos e inseguros como WEP.
- Utilizar contraseñas robustas para la administración de dispositivo de red como los puntos de acceso, no debe dejarse la clave por defecto del dispositivo ya que es fácilmente descubrible.
- Utilizar el filtrado de MACs en la configuración de los equipos de distribución de red para permitir distinguir que dispositivos son los autorizados para su conexión con la red WIFI del hogar.
- Desactivar la funcionalidad WPS del router, ya que se ha comprobado que método de asociación es vulnerable a ataques de fuerza bruta por tanto se recomienda no utilizarlo.
- Tratar de mantener un criterio al ubicar a los puntos de repetición WIFI en el hogar de manera que la señal inalámbrica abarque únicamente el área del hogar, el alcance aproximado de WIFI es 20 metros, aunque existen dispositivos actuales que superan esta distancia de transmisión.

B. Bluetooth

Bluetooth es un protocolo de comunicaciones inalámbrico de corto alcance y bajo consumo de potencia en la banda ICM de 2,4 GHz que soporta tanto tráfico de datos como de audio.



Figura 12-5: Bluetooth

Fuente: (Amazon)

La tecnología Bluetooth constituye una de las principales tecnologías de comunicación para los dispositivos IoT en el hogar aparte de las conocidas redes WIFI, en la actualidad el estándar Bluetooth Low Energy es el más aceptado y utilizado por los fabricantes debido a sus beneficios, aunque existen dispositivos que aun utilizan el estándar Bluetooth Clásico, entre los dispositivos Bluetooth que comúnmente se encuentran en el hogar están:

Computadores, de escritorio o portátiles son dispositivos que pueden considerarse del IoT debido a que utilizan principalmente una conexión de red cableada o WIFI para conectarse a Internet, entre estos los portátiles o portables cuentan con un interfaz Bluetooth para una conexión con otros dispositivos como teclado o mouse.



Figura 13- 5: Computadores

Fuente: (Ebay)

- Teléfonos inteligentes, desde los teléfonos móviles hasta los más actuales como los denominados Smartwatch, poseen un interfaz Bluetooth generalmente de tipo Clásico con el fin de comunicarse con otros dispositivos para intercambiar información.



Figura 14-5: Teléfonos Inteligentes

Fuente: (HRin Asia, 2015)

- Relojes inteligentes, en los últimos años han parecido estos dispositivos IoT, los cuales se enlazan a teléfonos inteligentes generalmente mediante una conexión de Bluetooth LE.



Figura 15-5: Relojes Inteligentes

Fuente: (Bloomberg, 2013)

- Tablets, o tabletas generalmente cuentan con la mayoría de funcionalidades que los teléfonos inteligentes, es por esto que de igual manera hacen uso de un interfaz Bluetooth para intercambiar datos.



Figura 16-5: Tablets

Fuente: (NEXTPOWERUP, 2014)

Bandas inteligentes, similar a los relojes inteligentes estas bandas hacen uso de la tecnología Bluetooth LE para transferir a un teléfono inteligente información sobre la actividad física y salud de su propietario.



Figura 17-5:Bandas Inteligentes

Fuente: (CNET, 2014)

Monitores de salud, existen otros dispositivos especializados que utilizan la tecnología Bluetooth para enlazar sus datos a un dispositivo inteligente como un teléfono celular.



Figura 18-5: Monitores de Salud

Fuente: (CNBC, 2016)

B.1. Principales amenazas y vulnerabilidades en Bluetooth

Interceptación de paquetes

Con equipamiento específico de captura de paquetes un atacante puede secretamente escuchar las comunicaciones de entre dos dispositivos Bluetooth en tiempo real, sin que estos se dieron cuenta y si la comunicación se la realiza sin encriptación accedería a toda la información confidencial libremente, durante el proceso de emparejamiento se aplican métodos de seguridad para evitar esto pero un atacante también puede capturar paquetes el momento de emparejamiento para descifrar la clave y por ende la información a transmitirse.

Hombre en el medio

Bluetooth LE es principalmente vulnerable a este tipo de ataque que consiste en que un atacante coloca en medio de la comunicación de dos dispositivos Bluetooth emparejados mediante la suplantación de la identidad de ambos, este ataque sucede principalmente por vulnerabilidades presentes en el intercambio de claves de red.

Seguimiento de identidad

Bluetooth LE fue diseñado para que de manera periódica adviertan de su presencia a otros dispositivos, los paquetes de advertencia contienen información importante como la identidad del dispositivo y la proximidad del dispositivo mediante valores de intensidad de señal.

B.2. Como controlar las vulnerabilidades en los dispositivos IoT Bluetooth

Una de las medidas más recomendables para prevenir un ataque informático a nuestro dispositivo IoT es desactivar el modo descubrible de los dispositivos Bluetooth para mantenerlo invisible y dificultar su posible detección o reconocimiento por parte de otros dispositivos maliciosos.

A pesar de que los dispositivos Bluetooth pueden ocultarse, los atacantes pueden descubrir la identidad de estos con nuevas herramientas disponibles libremente por lo que se recomienda desactivar el interfaz Bluetooth mientras no se lo requiera con esta medida podemos evitar que el dispositivo pueda ser descubierto fácilmente.

De ser posible en el dispositivo activar opciones que permitan el cifrado de las comunicaciones.

No aceptar solicitudes de conexión que provengan de dispositivos desconocidos.

En los dispositivos que lo permitan mantener periódicamente un control sobre el listado de dispositivos Bluetooth conocidos a fin de evitar conexiones no deseadas por parte de dispositivos maliciosos.

Asignar un nombre específico al dispositivo Bluetooth a fin de que no revele información acerca de este como modelo o marca ya que esta información puede ser útil a un atacante para establecer un ataque dirigido.

En caso de que exista solicitudes de emparejamiento no deseadas desde un dispositivo Bluetooth conocido validar si el dispositivo solicitante se encuentre a una distancia cercano si existe algún inconveniente con este con el objeto de validar si no existe un intento de suplantación.

Los dispositivos Bluetooth fabricados por marcas reconocidas utilizan métodos de seguridad para asegurar el emparejamiento y conexión entre dispositivos, por tanto, no se recomienda utilizar dispositivos Bluetooth de bajo costo si no se tiene la certeza de las seguridades que brinda.

Asegurarse de que el dispositivo IoT cuente con las últimas actualizaciones de firmware o seguridad disponibles.

Ciertos dispositivos permiten utilizar claves simples para emparejarse por defecto con otros, por ejemplo (clave: 0000), lo que puede ser aprovechado por un atacante al reconocer el modelo y marca del dispositivo mediante técnicas de ataque, por lo que es importante verificar si el dispositivo IoT trae incluida este tipo de vulnerabilidades. (Seguridad Bluetooth Fortalezas y Debilidades, s.f.)

C. RADIOFRECUENCIA



Figura 19-5: Dispositivos IoT RF en el hogar

Fuente: (Amazon)

Desde hace varios años han existido en el mercado una multitud de dispositivos controlables remotamente por radiofrecuencia, tal como alarmas, puertas de garaje, etc. las frecuencias más comunes utilizadas por estos son 433 Mhz y 315 Mhz debido a las características de cada uno tanto en interiores como en exteriores, por su bajo costo estos dispositivos se encuentran en los hogares pudiendo en los últimos años ser controlables por otros medios como dispositivos inteligentes que se conectan a Internet como Smartphones para que puedan ser controlables desde cualquier parte del mundo y bajo parámetros personalizables, constituyéndose por ende en lo denominado como automatización inteligente del hogar que se incluyen en el Internet de las Cosas, entre los dispositivos que pueden encontrarse en el hogar están:

- **Sistemas de Alarma**, los cuales sus sensores, control central e interruptores pueden comunicarse o activados a través de radiofrecuencia.



Figura 20-5: Sistemas de Alarma

Fuente: (Alonso Alarmas)

- **Boquillas de luz**, existen en el mercado boquillas de luz que pueden ser activadas remotamente por radiofrecuencia.



Figura 21-5: Boquillas de Luz

Fuente: (Amazon)

- **Tomacorrientes**, tomacorrientes que permiten controlar el paso de energía de manera remota.



Figura 22-5: Tomacorrientes RF

Fuente: (Amazon)

- **Puertas de garaje**, mediante un control remoto pueden activarse la apertura y cierre de las puertas de garaje.



Figura 23-5: Puertas de Garaje

Fuente: (Erick Security)

C.1. Principales amenazas y vulnerabilidades en los dispositivos controlados por radio frecuencia

Captura de señal

Mediante un analizador de espectros de radiofrecuencia un atacante se puede identificar la presencia de dispositivos RF en el hogar, la frecuencia de operación e inclusive la proximidad de estos.

Seguridad en códigos de operación

En ciertos casos los códigos de operación pueden ser descubiertos sin demasiada complejidad mediante un análisis de las señales que emiten los dispositivos de control remoto, pudiendo con esto donde extraer datos importantes para la construcción de un transmisor que replique los códigos.

Vulnerabilidades en las aplicaciones móviles

Las aplicaciones móviles que permiten controlar los dispositivos RF, generalmente cuentan con un desarrollo ajustado y bajo soporte en actualizaciones de seguridad o de firmware.

Inhibidores de señal

Existen comercialmente equipos inhibidores de señal, los mismos que pudieran afectar el espectro de operación de varios dispositivos RF causando una interrupción en la comunicación de estos.

Replica de dispositivo de control

En dispositivos RF económicos existe la posibilidad de que los controles remotos puedan ser compatibles con otros dispositivos del mismo modelo con lo cual un atacante solamente necesitara conocer el dispositivo que se encuentra en el hogar para adquirir un modelo similar y tomar control de los dispositivos.

C.2. Como controlar las vulnerabilidades en dispositivos controlados por radiofrecuencia

- Los dispositivos RF de bajo coste no cuentan con las seguridades adecuadas para ocultar los códigos de operación, por lo que se sugiere adquirir dispositivos IoT que soporten códigos de generación aleatoria.
- Dependiendo de la frecuencia de operación los dispositivos RF pueden tener un alcance considerable lo que facilitaría a atacantes externo a capturar las señales y realizar ataques desde una distancia segura sin la necesidad de contar con equipamiento altamente sensible.
- Debido a las vulnerabilidades presentes en este tipo de tecnología y si no se está seguro de que el dispositivo escogido brinda las garantías de seguridad se recomienda no utilizarlo para resguardar bienes o alumbrar o encender equipos de alto coste o de importancia.
- Las aplicaciones móviles para controlar los dispositivos RF, pueden sugerir un registro previo por lo que se recomienda utilizar una contraseña segura de al menos 8 caracteres, que incluya letras mayúsculas, números y caracteres especiales, se recomienda utilizar todos estos para formar una contraseña que esté compuesta por una frase fácilmente recordable por el usuario.

D. Zigbee



Figura 24-5: Zigbee

Fuente: (Amazon)

Zigbee es un conjunto de protocolos de comunicaciones inalámbricas creado por la Zigbee Alliance, está basado en estándar IEEE 802.15.4 de redes inalámbricas de área personal (WPAN), su aplicación está orientada a brindar una comunicación segura y fiable a dispositivos que requieran una baja tasa de envío de datos para reducir el consumo y vida útil de sus baterías. La tecnología inalámbrica Zigbee está más orientada a los hogares para aplicaciones de domótica, control inteligente de energía e Internet de las cosas (IoT) como por ejemplo la automatización de los hogares a través de comunicar varios dispositivos o sensores como puertas de garaje, termostatos alarmas, luminarias, etc. La Zigbee Alliance mantienen un listado de productos certificados que puede ser consultado en la página web, <http://www.zigbee.org/>.



Figura 25-5: Aplicaciones Zigbee

Fuente: (Dani, 2011)

D.1. Principales amenazas y vulnerabilidades en dispositivos IoT de redes Zigbee

En los últimos años ha aparecido varias aplicaciones para evaluar las seguridades de Zigbee y las redes 802.15.4, la suite más conocida es KillerBee que incluye varias herramientas que están disponibles de manera gratuita.

Redes descubribles

Los dispositivos Zigbee responden ante solicitudes de otros cuando requieren hacer un descubrimiento de red, esta funcionalidad podría ser aprovechada por un atacante que con el equipo adecuado pueda realizar ataques para conocer las redes Zigbee presentes en un hogar.

Captura de Señal

Muchos dispositivos IoT no emplean encriptación en su comunicación haciéndoles vulnerables para ataques de interceptación para capturar su comunicación, pudiendo obtener información de las redes presentes, su configuración y los dispositivos que están conectados. Existen en el mercado muchos equipos de varios precios dependiendo sus capacidades que pueden capturar el tráfico Zigbee como el Sewio Open Sniffer.

Ataques de Repetición

El concepto de ataques de repetición es observar el tráfico de una comunicación Zigbee y transmitir los paquetes que se capturen pudiendo con esto tener resultados diversos dependiendo de que contengan estos paquetes, por ejemplo puede interceptar el comando que encienda o apague una lámpara con lo cual un atacante puede tomar el control remoto de estos dispositivos.

Ataques por falencia de encriptación

En muchos casos los dispositivos IoT del hogar que se comunican con Zigbee no cuentan con un interfaz para configurar manualmente sus claves, al no poder controlar este aspecto de seguridad es posible que un atacante pueda obtener la clave de red ya que esta pueda ser descubierta aprovechando falencias en el mecanismo de entrega de claves de Zigbee.

D.2. Como controlar las vulnerabilidades en dispositivos IoT de redes Zigbee

- Las redes Zigbee utilizan el mecanismo de descubrimiento para conocer la presencia de otras redes, esta característica es parte del funcionamiento normal de Zigbee por tanto no puede deshabilitarse, para controlar esta vulnerabilidad se sugiere evaluar los dispositivos IoT y su implementación antes de adquirirlos además de identificar qué información obtendrá un atacante si aprovecha esta vulnerabilidad.
- Las redes Zigbee como otras redes caseras pueden ser sujetas a ataques de interceptación y captura de tráfico, por lo que las acciones para controlar este tipo de vulnerabilidades están enfocadas a reducir la información que fluye por nuestras redes de manera insegura, por lo que se recomienda hacer uso de los mecanismos de encriptación disponibles además de la utilización de claves o contraseñas fuertemente constituidas.
- A pesar de que las especificaciones de Zigbee brinda formas para proveer claves encriptadas a los dispositivos IoT desde el momento de su fabricación con el objeto de mitigar un posible riesgo a un ataque los consumidores que los adquieran, es posible que posteriormente se requiera de un correcto manejo de claves cuando se necesite cambiarlas por distintas razones ya que existen ciertas vulnerabilidades en como Zigbee las distribuye que pudieran revelarlas ante atacantes.

5.1.3. Cuadro resumen de resultados

Tabla 1-5: Cuadro resumen de resultados

TECNOLOGIA IOT	VULNERABILIDAD	POSIBLES ATAQUES	CRITERIO DE SEGURIDAD AFECTADO	HERRAMIENTA UTILIZADA	CONTROL DE VULNERABILIDAD RECOMENDADO	VALORACION	DESCRIPCION
BLUETOOTH CLASICO	Descubrimiento Activo	Ataques PIN Interceptacion y captura de tráfico	Confidencialidad Integridad	hcitool btscanner btcrack	- Procurar desactivar modo descubierto - Deshabilitar Bluetooth sino es utilizado - Habilitar las funciones para cifrar la información	Medio	Mediante equipamiento profesional es posible obtener la información necesaria para descubrir la clave PIN
	Descubrimiento Pasivo	Ataque PIN Interceptacion y captura de tráfico	Confidencialidad Integridad	Ubertooth btcrack	- Procurar desactivar modo descubierto - Deshabilitar Bluetooth sino es utilizado - Habilitar las funciones para cifrar la información	Medio	Mediante equipamiento profesional es posible obtener la información necesaria para descubrir la clave PIN
BLUETOOTH LOW ENERGY	Descubrimiento Activo	Ataque PIN Reemparejamiento Interceptacion y captura de tráfico	Confidencialidad Integridad	hcitool Ubertooth crackle	- Procurar desactivar modo descubierto - Deshabilitar Bluetooth sino es utilizado - Habilitar las funciones para cifrar la información	Medio	Deben tomarse medidas para tratar de que los dispositivos Bluetooth se mantengan ocultos
	Descubrimiento Pasivo	Ataque PIN Reemparejamiento Interceptacion y captura de tráfico	Confidencialidad Integridad	Ubertooth Blue Hydra crackle	- Procurar desactivar modo descubierto - Deshabilitar Bluetooth sino es utilizado - Habilitar las funciones para cifrar la información	Medio	Si no fuere suficiente el mantener oculto a un dispositivo se recomienda activar las funciones para cifrar la información a transmitirse
	Desemparejamiento por intento de conexión fallido	Reemparejamiento	Disponibilidad	Bdaddr	- No aceptar solicitudes de conexión de dispositivos desconocidos - Validar desemparejamientos no deseados en condiciones normales de uso	Bajo	A pesar que es un ataque probable hay pocos dispositivos que aun son susceptibles a este tipo de ataques
RADIOFRECUENCIA	Descubrimiento	Inhibir señal	Confidencialidad Disponibilidad	RTL-SDR	- En lo posible colocar los dispositivos RF a una distancia alejada de exteriores para evitar su posible detección y alcance de un atacante	Alto	Al conocerse las frecuencia de operación de un sistema basado en RF, un atacante puede utilizar varias formas de atacarlos como inhibidores de señal específicos
	Poca seguridad codigos de operación	Clonación de codigos de operación	Disponibilidad	RFSniffer codesend	- Se recomienda adquirir dispositivos RF que utilicen codigos aleatorios o de generación segura a fin de que no puedan ser clonados - En lo posible no utilizar estos dispositivos para aplicaciones importantes	Medio	Mediante el uso de equipo especial es posible descubrir los codigos de operación de RF
ZIGBEE	Descubrimiento de redes	Interceptacion y captura de tráfico	Confidencialidad Integridad	killerbee zbstumbler zbdump	- Se recomienda evaluar una posible afectación ante la información que pueda filtrarse por esta vulnerabilidad	Alto	No puede mitigarse esta vulnerabilidad por ser parte del funcionamiento propio de Zigbee
	Distribución claves de red	Ataque claves de red	Confidencialidad Integridad	killerbee zbdsniff	- Controlar la forma en que las claves de red estan implementadas o sean administradas	Medio	Zigbee posee varios mecanismos de seguridad pero puede ser vulnerable por el manejo incorrecto de sus claves

Realizado por: Mena, D. 2017

CONCLUSIONES

- Muchas de las personas que participaron en la encuesta (70%) no conocen el concepto del Internet de las Cosas, pero pudo identificar varios dispositivos comunes conectados que posee en el hogar como computadores, teléfonos inteligentes, routers, etc. De estos la mayoría (58%) creen que son seguros y el 57% considera que ha ingresado información personal y un porcentaje del 24% no sabe si estos datos se manejan de manera segura.
- El 56% de los encuestados indica que mediante la observación del uso de los dispositivos IoT se puede conocer el comportamiento y hábitos de las personas del hogar, entre estos el 19% no ha tomado medidas de las opciones propuestas para asegurarlos y un 33% considera que los factores humanos y tecnológicos inciden en el control de vulnerabilidades informáticas en el hogar.
- Según la investigación realizada existe un gran número de usuarios del hogar que desconocen sobre lo que significa cyber ataques o ataques informáticos (75%) y los riesgos que estos conllevan (72.5%), además un 32% ha enfrentado un cyber ataque mediante el apoyo de una capacitación y el 65% no sabe cómo implementar controles para minimizar las vulnerabilidades informáticas, el trabajo propuesto propone proporcionar una guía metodológica que sirva de ayuda con conocimiento para controlar las vulnerabilidades presentes en el hogar al poseer y hacer uso de los dispositivos IoT que pueden ser aprovechados por atacantes en busca de su beneficio personal.
- La mayoría de las personas encuestadas considera que las vulnerabilidades informáticas afectarían al funcionamiento de los dispositivos IoT del Hogar (22%) y después aspectos como el robo de su información personal (17%) y contagio de virus informáticos (15%), pero más de la mitad (58%) no sabe si ya han enfrentado peligros ante vulnerabilidades informáticas.
- Los elementos como Desconocimiento de las vulnerabilidades informáticas, inexistencia de herramientas de control y equipos que presentan fallas en su seguridad en conjunto son considerados por la mayoría de los encuestados (32%) para el control de las vulnerabilidades.
- El 57% de los encuestados no conocen el riesgo de no contar con una protección informática como un antivirus, asimismo enfrentarían las vulnerabilidades con resultado

similares mediante conocimiento investigado en Internet, actualizaciones de software y de los dispositivos, asesoría profesional o ninguna de las opciones sugeridas.

- A pesar de que existen esfuerzos por parte de los fabricantes para mejorar las características de seguridad en los dispositivos IoT, la tecnología actual que los soporta aún presenta ciertas vulnerabilidades, muchas de las cuales son bien conocidas por los atacantes, se espera que por parte de las entidades encargadas de normalización internacional emitan en los siguientes años nuevos estándares enfocados a mejorar la seguridad en el Internet de las cosas (IoT).
- Se pudo evidenciar que el 65% indica que no cuenta con algún tipo de protección de sus sistemas del hogar y el 56% le gustaría hacerlo de manera remota a través de Internet.
- Según la tabulación de la encuesta realizada se pudo determinar que existe un gran desconocimiento por parte de las personas en identificar correctamente los dispositivos de Internet de las Cosas que tienen en su hogar como también la forma de utilizarlos de manera segura. Lo cual denota un desconocimiento en aspectos de seguridad al momento de adquirirlos y posteriormente utilizarlos.
- En la presente investigación se pudo determinar que los dispositivos IoT más económicos son más susceptibles a que traigan vulnerabilidades de seguridad debido a los estándares de su fabricación a diferencia de los dispositivos IoT más costosos que generalmente aplican mecanismos para suplir las deficiencias de seguridad implícitas en la tecnología que usan.
- El dispositivo Raspberry Pi con los sniffers utilizados para las pruebas de laboratorio puede ser montado en un UAV o dron para realizar acercamientos a viviendas para un reconocimiento de vulnerabilidades con el objeto de detectar la presencia de dispositivos IoT y redes de comunicación, esto es un ejemplo de cómo una persona o atacante puede identificar las vulnerabilidades que posee las viviendas de la zona en estudio sin acercarse este de manera física sino apoyado por otros recursos tecnológicos.
- La guía metodológica propuesta está enfocada a servir a los usuarios de un hogar sin conocimientos de seguridad informática para que estos puedan identificar los dispositivos

IoT que poseen y de esta forma advertirlos sobre los riesgos a los que son expuestos al no usarlos de manera segura.

RECOMENDACIONES

- Es importante que los usuarios finales de los dispositivos IoT en el hogar revisen siempre los manuales de uso que trae el dispositivo cuando son adquiridos los cuales generalmente contienen indicaciones y recomendaciones de seguridad específicas para el dispositivo.
- Las redes caseras son la principal vulnerabilidad en los hogares por ser un elemento fácilmente vulnerable por atacantes si estas no cuentan con las medidas de seguridad apropiadas, por tanto se sugiere la aplicación de controles los cuales están indicados en la presente investigación a fin de reducir el riesgo a que los dispositivos IoT del hogar sufran un cyber ataque.
- Se sugiere que al momento de adquirir un dispositivo IoT se verifique las características de seguridad que este posea especialmente en lo relacionado al soporte para asegurar los datos, como puede ser métodos de encriptación que dificulte a un atacante en descifrar la información que transmiten, almacenan o procesan.
- La ubicación de los dispositivos IoT es muy importante y muy poco considerado en su implementación en el hogar ya que pueden ser susceptibles a ataques si un externo malicioso tiene el acceso físico a componentes críticos de estos como memorias o puertos de datos asimismo los dispositivos IoT se comunican generalmente por redes inalámbricas que pueden sufrir ataques desde el exterior inclusive a cortas distancias, por tanto se sugiere que en lo posible los dispositivos utilizados en el hogar dependiendo de la tecnología que utilicen sean colocados con criterios de seguridad física en el hogar con la finalidad de que las señales que estos propagan sean en lo posible limitadas hacia el exterior de manera que no puedan ser interceptadas o monitoreadas por atacantes.
- Al momento de desechar los dispositivos IoT del hogar se debe considerar la información que contienen en su memoria la cual puede ser de carácter personal, atacantes pueden aprovechar este descuido y recuperar la información de estos dispositivos aplicando técnicas forenses.
- El presente trabajo de investigación proporcionará a los investigadores de una referencia base acerca de las principales vulnerabilidades informáticas presentes en los dispositivos

IoT en el hogar y en sus tecnologías de comunicación como también de los mecanismos de seguridad que pueden aplicarse para reducir el riesgo de sufrir cyber ataques.

- Existen equipamiento comercial más profesional costoso que puede usarse para ahondar en las pruebas de seguridad tratadas en esta investigación principalmente las que corresponden al análisis de los protocolos de comunicación como Bluetooth y Zigbee.

BIBLIOGRAFÍA

- Alarmas, A.** (2017). Kit Inalámbrico N°3 (Kit de Alarma A2K4-NG-RF con DGW-500, DGM-300, TX-500 y sirena MP-100 ST). [En línea]. Argentina. [Consulta: 19 de septiembre 2016]. Recuperado de http://www.alonsohnos.com/Productos/Kits_de_Alarma/Kit-Inalambrico-N13-Kit-de-Alarma-A2K4-NG-RF-con-DGW-500-DGM-300-TX-500-y-sirena-MP-100-ST
- Alvarez, G.** (2009). Como protegernos de los peligros de Internet. [En línea] Madrid: Catarata. [Consulta: 22 de octubre 2016] Recuperado de https://www.catarata.org/libro/como-protegernos-de-los-peligros-de-internet_45949/
- Amazon.** (2012). Inateck Compact USB Bluetooth 4.0 Low Energy USB Adapter Dongle. [En línea] Estados Unidos [Consulta: 22 de octubre 2016] Obtenido de <https://www.amazon.co.uk/Inateck-Bluetooth-Bluesoleil-Authorised-Compatible/dp/B00ATXZ6XO>
- Amazon.** (2013). Eteckcity Wireless Remote Control Electrical Outlet Switch. [En línea] Estados Unidos [Consulta: 28 de octubre 2016] Obtenido de https://www.amazon.com/Eteckcity-Wireless-Electrical-Household-Appliances/dp/B00DQELHBS/ref=sr_1_2?ie=UTF8&qid=1491758395&sr=8-2&keywords=etecckcity+outlet
- Amazon.** (2015). GE Link Starter Kit. [En línea] Estados Unidos [Consulta: 28 de octubre 2016] Obtenido de https://www.amazon.com/GE-Starter-65-Watt-Equivalent-Amazon/dp/B00TJ4WMZE/ref=sr_1_1?ie=UTF8&qid=1491758636&sr=8-1&keywords=ge+link+kit
- Arroyo, R.** (2014). Fortinet desvela las preocupaciones que genera el Hogar Conectado. [En línea] Europa [Consulta: 4 de noviembre 2016] Recuperado de <http://www.channelbiz.es/2014/06/25/fortinet-preocupaciones-genera-hogar-conectado>
- Balakrishnan, A.** (2016). *Londoners lost some sleep over Brexit, their fitness trackers show.* CNBC [En línea] Estados Unidos [Consulta: 8 de noviembre 2016] Recuperado de <http://www.cnbc.com/2016/06/27/londoners-lost-some-sleep-over-brexit-their-fitness-trackers-show.html>
- Barker, I.** (2015). *Companies add more physical security to combat BYOD risks.* Betanews [En línea] [Consulta: 16 de noviembre 2016] Recuperado de <https://betanews.com/2014/11/12/companies-add-more-physical-security-to-combat-byod-risks/>
- Beltov, M.** (2016). La herramienta Bluetooth de código abierto Blue Hydra puede ser utilizada por delincuentes [En línea] Bulgaria [Consulta: 4 de noviembre 2016] Recuperado de

<http://bestsecuritysearch.com/open-source-bluetooth-tool-blue-hydra-can-used-criminals/>

- Bernal, C.** (2013). *Métodología de la investigación*: Pearson. 3ª. ed. [En línea] México ISBN: 978-958-699-128-5 [Consulta: 4 de noviembre 2016] Recuperado de <https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf>
- Benaim, J.** (2017). *Ubertooth One*. Project Ubertooth. [En línea] [Consulta 22 de marzo 2017] Recuperado de <https://github.com/greatscottgadgets/ubertooth/wiki/Build-Guide>
- Brustein, J** (2013). *Smartwatches From Samsung and Other Big Names Are Coming. Does That Matter?*. Bloomber. [En línea] [Consulta: 21 de noviembre 2016] Recuperado de <https://www.bloomberg.com/news/articles/2013-08-16/smartwatches-from-samsung-and-other-big-names-are-coming-dot-does-that-matter>
- Caldas, A.** (2014). *Internet de las Cosas, Hogar Inteligente y Ahorro*. IES Castro Alobre. [En línea] Mexico. p.7[Consulta: 1 de diciembre 2016] Recuperado de http://www.edu.xunta.gal/centros/iescastroalobrevilagarcia/system/files/Trabajo%20de%20investigaci%C3%B3n_Internet%20de%20las%20cosas%20Cahorro%20y%20hogar%20inteligente_Alberto%20Est%C3%A9vez%20Caldas.pdf
- Cas-Chile.** (2009). *Vulnerabilidad*. Colombia: Caschile. [En línea] [Consulta: 12 de diciembre 2016] Recuperado de <https://www.caschile.cl/>
- Castejron, E.** (2013). *Breve historia de las tablets*. Webadictos. [En línea] [Consulta 26 de marzo 2017] Recuperado de <https://webadictos.com/2013/05/19/breve-historia-de-las-tablets/>
- Cayetano, F.** (2012). La internet de las cosas una breve reseña. *Tecnología IOT*. [En línea] México: Mc Graw Hill. pp.37-48 [Consulta: 21 de diciembre 2016] Recuperado de <https://www.internetsociety.org/wp-content/uploads/2016/09/report-InternetOfThings-20160817-es-1.pdf>
- CEPAL.** (2015). *La nueva revolución digital Del Internet del consumo a la Internet de la Producción*. [En línea] Santiago de Chile: CEPAL [Consulta: 6 de enero 2017] Recuperado de <https://www.cepal.org/es/publicaciones/38604-la-nueva-revolucion-digital-la-internet-consumo-la-internet-la-produccion>
- COMPSMAG.** (2015). Las mejores aplicaciones de seguridad de Android [En línea] [Consulta: 10 de enero 2017] Recuperado de <https://www.compsmag.com/best-android-security-apps/>
- Corletti, A.** (2011). *Seguridad por niveles*. [En línea] Madrid: DarFE. pp. 346-355[Consulta: 10 de enero 2017] Recuperado de <http://index-of.co.uk/INFOSEC/341.seguridad-por-niveles.pdf>

- Corporation, I. D.** (2014). Programa Acelerador de IDC: el paquete que necesitan los innovadores de tecnología disruptiva [En línea] Needham-Estados Unidos [Consulta: 12 de enero 2017] Recuperado de www.idc.com.
- Craig Smith, D. M.** (2015). *Internet of things research study*. Hewlett Packard. [En línea] Rusia [Consulta: 12 de enero 2017] Recuperado de <https://dl.acm.org/doi/abs/10.1145/2794381>
- Cuthbertson, A.** (2014). *eBay Hack: Outdated Password System Means Huge Cyber-Attacks are 'The New Normal'*. International Business Times. [En línea] Australia [Consulta: 4 de marzo 2017] Recuperado de <http://www.ibtimes.co.uk/ebay-hack-outdated-password-system-means-huge-cyber-attacks-are-new-normal-1449726>
- Dani, P.** (2011). *Domotica*. [En línea] [Consulta: 16 de enero 2017] Recuperado de <http://domoactualidad.blogspot.com/2011/05/introduccion-los-inicios-de-la-domotica.html>
- Diaz Tarascó, D.** Creación de un portal Web a partir de las necesidades de alumnos. [En línea] Loja-Ecuador [Consulta: 27 de enero 2017] Recuperado de [www.monografias.com: http://www.monografias.com/trabajos81/creacion-portal-web-partir-necesidades-alumnos/creacion-portal-web-partir-necesidades-alumnos2.shtml](http://www.monografias.com/trabajos81/creacion-portal-web-partir-necesidades-alumnos/creacion-portal-web-partir-necesidades-alumnos2.shtml)
- Digi-Key.** (2017). *Digi-Key Electronics*. [En línea] Estados Unidos [Consulta: 4 de febrero 2017] Recuperado de <https://www.digikey.com/catalog/en/partgroup/cc2540-usb-evaluation-module-kit/32432>
- Espinosa, A.** (2010). Análisis de Vulnerabilidades de la Red LAN de la UTPL. [En línea] Loja: Universidad Técnica Particular de Loja. [Consulta: 6 de febrero 2017] Recuperado de http://dspace.utpl.edu.ec/bitstream/123456789/1352/3/Espinosa_Otavallo_Ang%C3%A9lica%20del%20Cisne.pdf
- Evans, D.** (2011). *Internet de las cosas Como la proxima evolucion de Internet lo cambia todo*. CISCO. [En línea] Estados Unidos [Consulta: 6 de febrero 2017] Recuperado de https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf
- Fundación Barkinter.** (2011). *El Internet de las Cosas*. Acenture [En línea] [Consulta: 6 de febrero 2017] Recuperado de https://www.fundacionbankinter.org/documents/20183/137558/RE+PDF+ES+FTF_IOT.pdf/379ba7dd-711c-419c-a105-59e6693f502a
- Galdámez, P.** (2014). *Seguridad informatica*. Actualidad TIC. [En línea] Valencia [Consulta 16 de marzo 2017] Recuperado de https://issuu.com/_iti_/docs/actualidad_n1
- García Salvatierra, A.** (12 de Julio de 2012). El Internet de las Cosas y los nuevos riesgos para la privacidad. [En línea] Tesis (Master), E.U.I.T. Telecomunicación (UPM) [Consulta: 8 de febrero 2017] Recuperado de <http://oa.upm.es/14543/>

- García, L. (2010).** *Metodología OSSTMM. SECURITYPORDEFAULT.* [En línea] España [Consulta: 12 de febrero 2017] Recuperado de <http://www.securitybydefault.com/2010/03/metodologia-osstmm.html>
- Garnet Technology . (2017).** *Kit Inalámbrico N°3 (Kit de Alarma A2K4-NG-RF con DGW-500, DGM-300, TX-500 y sirena MP-100 ST).* Obtenido de Recuperado de http://www.alonsohnos.com/Productos/Kits_de_Alarma/Kit-Inalambrico-N13-Kit-de-Alarma-A2K4-NG-RF-con-DGW-500-DGM-300-TX-500-y-sirena-MP-100-ST
- GE Link.** *Ge Link COnnected Bulbs.* [En línea] Canadá. [Consulta: 12 de febrero 2017] Recuperado de <http://www.gelinkbulbs.com>
- Hack, J. (2016).** *Hook: Smart Home on a Budget.* Kickstarter. [En línea] Estados Unidos [Consulta: 5 de marzo 2017] Recuperado de <https://www.kickstarter.com/projects/hackajoe/hook-home-automation-on-a-budget>
- HakShop.** *SOFTWARE DEFINED RADIO STARTER KIT.* [En línea] [Consulta: 14 de febrero 2017] Recuperado de <https://hakshop.com/products/software-defined-radio-kit-rtl-sdr>
- Haller, S. S. (2010).** *Internet of Things: An Integral Part of the Future Internet.* [En línea] New York: Pearson. p.4 [Consulta: 15 de febrero 2017] Recuperado de <https://www.alexandria.unisg.ch/46642/1/fis2008-haller-final.pdf>
- Hand, V. (2017).** *Best Fitness trackers of 2017.* CNET. [En línea] Estados Unidos [Consulta: 9 de enero 2017] Recuperado de <https://www.cnet.com/topics/wearable-tech/best-wearable-tech/best-fitness-trackers/>
- Hernández, R. (2012).** *Metodología de la Investigación.* [En línea] 6ta. ed. México: Mc Graw Hill. [Consulta: 14 de febrero 2017] Recuperado de <http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf>
- Herzog, P. (2003).** *Manual de la Metodología Abierta de Testeo de Seguridad.* [En línea] [Consulta: 18 de febrero 2017] Recuperado de <http://index-of.co.uk/INFOSEC/OSSTMM.es.2.1.pdf>
- Hewlett Packard. (2014).** *Internet of things research study.* [En línea] [Consulta: 22 de febrero 2017] Recuperado de <https://www.redalyc.org/jatsRepo/5122/512253717005/html/index.html>
- Hoyle, A. (2014).** *Sony SmartBand Talk review.* CNET. [En línea] Estados Unidos [Consulta: 9 de enero 2017] Recuperado de <https://www.cnet.com/au/products/sony-smartband-talk/review/>
- HRin (2015).** *Capitalising on the power of mobile recruitment.* [En línea] Asia. [Consulta: 22 de febrero 2017] Recuperado de <http://www.hrinasia.com/recruitment/capitalising-on-the-power-of-mobile-recruitment/>

- INCIBE** (2016). *Seguridad Bluetooth Fortalezas y Debilidades*. [Consulta 26 de marzo 2017]
Recuperado de <https://www.incibe-cert.es/blog/seguridad-bluetooth-fortalezas-y-debilidades>
- Instituto Nacional de Tecnologías de la Comunicación.** (2010). *¿Que son las vulnerabilidades del software?* Inteco. [Consulta: 24 de febrero 2017] Recuperado de https://www.incibe.es/extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/Vulnerabilidades/cert_inf_vulnerabilidades_2011_semestre_2.pdf
- iStart.** (2014). *Family homes become the latest IoT battleground*. Newsdesk [En línea] Nueva Zelanda [Consulta: 5 de marzo 2017] Recuperado de <http://istart.co.nz/nz-news-items/family-homes-become-the-latest-iot-battleground/>
- Lazaro, L.** Installing bluehydra on raspberry pi. [En línea] [Consulta: 5 de marzo 2017]
Recuperado de <https://www.lazaro.com.ar/Bluehydra-raspberrypi>
- Leland, T.** (2014). *Wireless Power Outlets*. [En línea] [Consulta:7 de marzo 2017] Recuperado de <https://timleland.com/wireless-power-outlets/>
- López, A. T.** (2014). Seguridad en el internet de las cosas. Madrid: Centro de Apoyo a la Innovación Tecnológica (CAIT).
- LOQUI, Y. C.** (2015). Desarrollo y modelación de solución domótica para la asistencia a personas con diversidad funcional motora utilizando hardware libre. [En línea] Escuela Superior Politécnica del Litoral. Guayaquil: [Consulta:7 de marzo 2017] Recuperado de <http://www.dspace.espol.edu.ec/xmlui/handle/123456789/30297>
- Maroto, P.** (2014). *Introduccion a la Internet de las Cosas*. [En línea] España [Consulta 10 de marzo 2017] Recuperado de <https://pacomaroto.wordpress.com/about/introduccion-a-la-internet-de-las-cosas/>
- Martinez, P.** (2013). *Internet de las cosas: objetos interconectados y dispositivos inteligentes*. [En línea] ICT. Madrid: Audiovisual de madrid. [Consulta: 24 de febrero 2017]
Recuperado de https://www.academia.edu/22661485/Internet_de_las_cosas
- Matthinsen, H.** (2015). Domotica met Raspberry Pi . *Blog Henri Matthinsen*. [Entrada de blog] [Consulta 11 de marzo 2017] Recuperado de <https://eye-vision.homeip.net/domotica-met-raspberry-pi/>
- NEXTPOWERUP.** (2014). *Android Is Now The Leading Tablet OS: Gartner*. Egham [En línea] Reino Unido [Consulta 10 de marzo 2017] Recuperado de <http://www.nextpowerup.com/news/7796/android-is-now-the-leading-tablet-os-gartner/>
- Open Editions Book.** (2015). Defining the Internet of the things. [En línea] New York [Consulta 15 de marzo 2017] Recuperado de <http://books.openedition.org/editionsms/97>
- Ossmann, M.** (2011). *UbertoohOne*. Proyecto Ubertooh [En línea] [Consulta 22 de marzo 2017] Recuperado de <http://ubertooh.sourceforge.net/hardware/one/>

- Pérez, J., & Merino, M.** (2008). *Definición de Seguridad Informática*. [En línea] [Consulta 19 de marzo 2017] Recuperado de <http://definicion.de/seguridad-informatica/>
- Philco, O.** (2014). *Los riesgos en transacciones electrónicas en línea y la criptografía como modelo de seguridad informática*. Gaceta Sansana [En línea] Quito. [Consulta 19 de marzo 2017] Recuperado de <http://publicaciones.usm.edu.ec/index.php/GS/article/view/44>
- Ronda, K. R.** (2011). *Semántica*. México: Mc Graw Hill. p.39
- Rootear.** (2013). *Vulnerabilidades de una red Wifi*. [En línea] España [Consulta 24 de marzo 2017] Recuperado de <https://rootear.com/seguridad/vulnerabilidades-una-red-wi-fi>
- Ruiz, J.** (2013). *Internet de las cosas*. [En línea] España: Trillas. [Consulta 25 de marzo 2017] Recuperado de <http://www.seeci.net/cuiciid2013/PDFs/UNIDO%20MESA%20%20DOCENCIA.pdf>
- Ryan, M.** (2017). *Crackle*. GitHub [En línea] [Consulta 26 de marzo 2017] Recuperado de <https://github.com/mikeryan/crackle>
- Smarththings.** (2016). *Samsung Smarththings*. [En línea] [Consulta 26 de marzo 2017] Recuperado de <https://www.smarththings.com>
- Tecnofullshop.** (2017). *Samsing Galaxy S6 Edge +*. Donweb [En línea] [Consulta 28 de marzo 2017] Recuperado de http://www.tecnofullshop.com.ar/index.php?route=product/product&product_id=251
- Tomlinson, K.** (2016). *Raspberry Pi Projects You Can Actually Do - Part 4: Home Automation with Siri and a Raspberry Pi*. [En línea] [Consulta 26 de marzo 2017] Recuperado de <https://blog.kurttomlinson.com/posts/raspberry-pi-projects-you-can-actually-do-part-4-home-automation-with-siri-and-a-raspberry-pi>
- Totality Services.** (2016). *Why cybercriminals are targeting small London based businesses*. Totality Services [En línea] Londres [Consulta 26 de marzo 2017] Recuperado de <http://totalityservices.co.uk/why-cybercriminals-are-targeting-small-london-based-businesses/>
- Tuzovic, A.** (2015). *The Internet of your things Microsoft's Vision for IoT*. Microsoft BiH.
- Villavicencio, J.** (2011). *Estudio de las vulnerabilidades en tecnologías de virtualización con vmware en microcomputadoras*. [En línea] Guayaquil: UNIVERSIDAD DE GUAYAQUIL . [Consulta 26 de marzo 2017] Recuperado de <http://repositorio.ug.edu.ec/handle/redug/6744>
- Wikipedia.** (2017). *ARM11*. [En línea] [Consulta 28 de marzo 2017] Recuperado de <https://en.wikipedia.org/wiki/ARM11>
- Wright, J., & Cache, J.** (2017). *Hacking Wireless Exposed*. New York: McGraw-Hill. 3ª ed. pp.189-193

ANEXOS

ANEXO A: INSTALACIÓN DE UBERTOOTH EN RASPBIAN

1. Se recomienda actualizar Raspbian con las últimas versiones de paquetes y programas con los siguientes comandos.

```
apt-get -y update  
apt-get -y upgrade
```
2. Se debe instalar las dependencias que requiere Ubertooth, el script siguiente se detalla todas las dependencias necesarias.
 - ```
apt-get -y install cmake libusb-1.0-0-dev make gcc g++ libbluetooth-dev libncurses5-dev libnl-dev pkg-config libpcap-dev python-numpy python-pyside python-qt4
```
3. Ubertooth requiere de la librería libbtbb para decodificar las captura de los paquetes de bluetooth.

```
wget https://github.com/greatscottgadgets/libbtbb/archive/2015-10-R1.tar.gz -O libbtbb-2015-10-R1.tar.gz
tar xf libbtbb-2015-10-R1.tar.gz
cd libbtbb-2015-10-R1
mkdir build
cd build
cmake ..
make
make install
ldconfig
```

4. Instalación de las herramientas de Ubertooth para el uso y configuración del dispositivo
  - ```
wget https://github.com/greatscottgadgets/ubertooth/releases/download/2015-10-R1/ubertooth-2015-10-R1.tar.xz -O ubertooth-2015-10-R1.tar.xz  
tar xf ubertooth-2015-10-R1.tar.xz  
cd ubertooth-2015-10-R1/host  
mkdir build  
cd build
```

```
cmake ..  
make  
make install  
ldconfig
```

5. Instalación de la herramienta Kismet para que sea usada por Ubertooth para el interpretado de paquetes

```
wget http://www.kismetwireless.net/code/kismet-2016-01-R1.tar.xz  
tar xf kismet-2016-01-R1.tar.xz  
cd kismet-2016-01-R1  
ln -s ../ubertooth-2015-10-R1/host/kismet/plugin-ubertooth ./  
./configure  
make deb  
make && make plugins  
make suidinstall  
make plugins-install
```

6. Configuration de Writeinterval

```
sed -i "s/writeinterval=300/writeinterval=10/g" /usr/local/etc/kismet.conf
```

7. Instalación de Wireshark

- apt-get install wireshark wireshark-dev libwireshark-dev cmake
- (SE RECOMIENDA PARA COMPATIBILIDAD CON UBERTOOTH Y KISMET INSTALAR LAS VERSIONES 1.12.x)

```
cd libbtbb-2015-09-R2/wireshark/plugins/btbb  
mkdir build  
cd build  
cmake -DCMAKE_INSTALL_LIBDIR=/usr/lib/x86_64-linux-  
gnu/wireshark/plugins/1.12.x ..  
make  
sudo make install
```

8. Instalación del plugin Wireshark para leer paquete BLE (Bluetooth Low Energy)
 - apt-get install wireshark wireshark-dev libwireshark-dev cmake
 - cd libbtbb-2015-09-R2/wireshark/plugins/btbredr
 - mkdir build
 - cd build
 - cmake -DCMAKE_INSTALL_LIBDIR=/usr/lib/x86_64-linux-gnu/wireshark/plugins/1.12.x ..
 - make
 - make install

ACTUALIZACIÓN DE FIRMWARE Y COMPROBACIÓN DE VERSIÓN DE UBERTOOTH ONE

- Descargar la última versión del firmware del link:
<https://github.com/greatscottgadgets/ubertooth/releases/>
- Extraer y pasarse al directorio ubertooth-one-firmware-bin
 - cd ubertooth-one-firmware-bin/
- Ejecutar el comando siguiente para actualizar el firmware
 - ubertooth-dfu -d bluetooth_rtx.dfu -r
- Comprobar la versión del firmware de Ubertooth actual con ubertooth-util -v, se mostrará algo como lo siguiente:
 - \$ ubertooth-util -v
 - Firmware revision: 2014-02-R1
 - \$ ubertooth-util -V
 - ubertooth 2014-02-R1 (dominicgs@mercury) Wed Jan 29 23:10:46 GMT 2014

(Project Ubertooth, 2017)

ANEXO B: FORMULARIO DE ENCUESTAS DIRECCIONADO A LAS PERSONAS QUE UTILIZAN LAS NUEVAS TECNOLOGIAS



**ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**

FORMULARIO DE ENCUESTAS DIRECCIONADO A LAS PERSONAS QUE UTILIZAN LAS NUEVAS TECNOLOGIAS Y SU IMPACTO EN EL CONTROL DE VULNERABILIDADES INFORMÁTICAS EN DISPOSITIVOS IOT (INTERNET OF THE THINGS) PARA REDES HAN (HOME ÁREA NETWORK).

Objetivo

Recabar información acerca de la necesidad de una guía metodológica para el control de vulnerabilidades informáticas en dispositivos IoT (Internet of the things) para redes han (home área network).

Contenido:

1.-¿Conoce que son los Cyber Ataques?

SI ()

NO ()

2.-¿Conoce los riesgos a los que se expone al sufrir un Cyber Ataque?

SI ()

NO ()

3.-¿Cómo ha enfrentado el peligro de una vulnerabilidad informática ante un Cyber Ataque?

Mantenimiento permanente ()

Capacitación personalizada ()

Ninguno ()

4.-¿Sabe implementar controles para minimizar las vulnerabilidades informáticas?

SI ()

NO ()

5.-¿Para usted cual es el riesgo que se presenta al momento de no contar con una adecuada protección ante vulnerabilidades informáticas?

Robo de información personal ()

Contagio de virus informáticos ()

Perdida de información importante ()

Acceso a la red de Internet de su casa ()

Mal funcionamiento de dispositivos electrónicos ()

6.-¿Ha enfrentado el peligro de una vulnerabilidad informática?

Si ()

No ()

7.-¿De qué elemento depende para usted la existencia de un control de vulnerabilidad informática?

Desconocimiento de las vulnerabilidades informáticas ()

Inexistencia de herramientas de control ()

Equipos que presentan fallas en su seguridad ()

De las anteriores ()

8.- ¿Conoce el riesgo que se presenta al momento de no contar con una protección informática?

Si ()

No ()

9.-¿De qué manera enfrenta el riesgo de una vulnerabilidad informática?

Consulta información relacionada en Internet ()

Permanente actualización del software de protección informática ()

Permanente actualización del firmware de los dispositivos electrónicos ()

Asesoría profesional ()

Ninguna ()

10.- ¿Tiene usted una protección en el sistema informático y de internet que maneja?

Si ()

No ()

11.-¿Cuenta Ud. con una protección ante vulnerabilidades informáticas en la red de Internet o datos de su hogar

Si ()

No ()

12.-¿Cómo le gustaría acceder al control de la vulnerabilidad?

Guías especializadas

Acceso por Internet

13.-¿Cómo desearía implementar controles de seguridad informática para minimizar las vulnerabilidades informáticas en su hogar?

Internet ()

Asesorías eventuales ()

Guía metodológica ()

Capacitación permanente ()

14.-¿Conoce usted que son los dispositivos IoT (Internet de las Cosas)?

Si ()

No ()

15.-¿Qué objetos IoT o dispositivos electrónicos tiene usted conectado a las redes inalámbricas de su hogar?

Teléfonos celulares ()

Tablet ()

Computadores ()

Relojes inteligentes ()

Sistemas de automatización del hogar ()

Modem ()

Router ()

Otros ()

16.¿Cree usted que los dispositivos electrónicos IoT que utiliza en el hogar son seguros?

Si ()

No ()

17.-¿Considera usted que ha ingresado información personal en los dispositivos IoT con los cuales interactúa en el hogar?

Si ()

No ()

18.- ¿Sabe usted si sus datos personales que almacena, procesa y transmite los dispositivos IoT de su hogar están seguros?

Siempre ()

Casi siempre ()

Nunca ()

No lo sabe ()

19.-¿ La observación del uso diario a los dispositivos IoT de su hogar serviría para conocer el comportamiento y hábitos de las personas?

Si ()

No ()

20.-¿Qué medidas ha tomado para mejorar la seguridad de los dispositivos IoT de su hogar?

- Asesoría profesional ()
- Configuración y actualización de dispositivos ()
- Adquiere marcas de dispositivos reconocidas ()
- Coloca los dispositivos de su en lugares seguros ()
- Ninguna ()

21.-¿Cuál factor considera más importante para establecer seguridades informáticas en los dispositivos IoT que se encuentran en la red de su hogar ?

- Factor Humano ()
- Factor tecnológico ()
- Ambos ()

GRACIAS POR SU COLABORACIÓN

ANEXO C: MATRIZ DE VALIDACIÓN DE CONTENIDO DE LA ENCUESTA

Informe de validación del instrumento de recolección de datos

Matriz de validación de contenido de la encuesta

Evaluador 1: Ing. Pablo Armijos

Fecha: 02-02-2017

En el formato de validez cada evaluador apreciara la importancia del contenido de las preguntas según su criterio, para ello se utilizó la siguiente escala evaluativa.

Escala Evaluativa

1= Deficiente 2= Regular 3= Bueno 4= Muy Bueno 5= Excelente

Contenido			Evaluación				
Ítems	Criterios Generales	Observaciones	1	2	3	4	5
20	Pertinencia con variables						X
	Pertinencia con dimensiones						X
	Pertinencia con los objetivos					X	
	Redacción y Terminología					X	

Ing. Pablo Armijos

**INGENIERO DE SEGURIDADES E INFRAESTRUCTURA GRUPO RADICAL CIA
LTDA**

Informe de validación del instrumento de recolección de datos

Matriz de validación de contenido de la encuesta

Evaluador 1: Ing. Paúl Torres

Fecha: 02-02-2017

En el formato de validez cada evaluador apreciara la importancia del contenido de las preguntas según su criterio, para ello se utilizó la siguiente escala evaluativa.

Escala Evaluativa

1= Deficiente 2= Regular 3= Bueno 4= Muy Bueno 5= Excelente

Contenido			Evaluación				
Ítems	Criterios Generales	Observaciones	1	2	3	4	5
20	Pertinencia con variables						X
	Pertinencia con dimensiones						X
	Pertinencia con los objetivos						X
	Redacción y Terminología						X

Ing. Paul Torres

ANEXO D: TABLA DE DISTRIBUCIÓN

TABLA DE DISTRIBUCIÓN



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

**DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE
UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL**

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 05/05/2021

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: David Rodrigo Mena Galarza
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: Magíster en Seguridad Telemática
f. Analista de Biblioteca responsable: Lic. Luis Caminos Vargas Mgs.

LUIS
ALBERTO
CAMINOS
VARGAS

Firmado digitalmente por LUIS
ALBERTO CAMINOS VARGAS
Nombre de reconocimiento
(DN): c=EC, L=ROBAMBA,
serialNumber=0602766974,
cn=LUIS ALBERTO CAMINOS
VARGAS
Fecha: 2021.05.05 16:14:38
+05'00'



0034-DBRAI-UPT-IPEC-2021