# MODELO DE DEFENSA ANTE ATAQUES A EQUIPOS IOT APLICADO A SMART TV BASADO EN VULNERABILIDADES IDENTIFICADAS CON OSSTMM.

**RICO MACIAS VICTOR HUGO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD**
**ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**

**CALI**
**2020**

# MODELO DE DEFENSA ANTE ATAQUES A EQUIPOS IOT APLICADO A SMART TV BASADO EN VULNERABILIDADES IDENTIFICADAS CON OSSTMM

**RICO MACIAS VICTOR HUGO**

**Proyecto de Grado – Monografía presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA**

**Director {a}:**
**ING. EDWARD ANTONIO MANTILLA TORRES**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD**
**ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**

**CALI**
**2020**

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

## DEDICATORIA

Este trabajo es gracias primero a DIOS que es el ser que me da día a día su amor y me mantiene en pie de lucha por ser una persona feliz, y dedicado a mi familia que ponen su grano de arena con la paciencia y apoyo permanente para que yo cumpla mis sueños.

## AGRADECIMIENTOS

Este trabajo es producto de un esfuerzo que no hubiera podido darse sin la ayuda de DIOS como dador de vida, y seguidamente del motor que tengo como es mi esposa y mis hijos.

Y agradecimientos muy especiales a todos mis tutores, personas a las cuales respeto y admiro mucho, son profesionales que han estado permanentemente comprometidos en dar lo mejor de sí para que yo como aprendiz tenga el conocimiento suficiente para perfeccionarme en el campo que me apasiona como es la seguridad informática, y de esta manera crecer, conocer y actuar en pro de aplicar esta seguridad informática en las empresas, lo cual plasmo en mi trabajo siempre.

Gracias a todos DIOS les siga bendiciendo.

## CONTENIDO

## LISTA DE TABLAS

**Pag.**

## LISTA DE FIGURAS

**Pág.**

## GLOSARIO

**Ataque Informático**: Actividad considerada ilícita la cual por medo del aprovechamiento de una vulnerabilidad se compromete la seguridad del dispositivo con fines específicos no legales.

**Enumeración**: Proceso parte de la fase 3 del ciclo de vida de un ataque que busca validar que los datos obtenidos del escaneo del objetivo sean verdaderos, es decir que los servicios que el sistema dice tener activos se puedan ver en la práctica.

**Escaneo**: Proceso parte de la fase 2 del ciclo de vida de un ataque que busca conocer por medio de herramientas técnicas datos específicos de un objetivo como son sus puertos, sistema operativo, los servicios que corren y sus versiones.

**Hacking Ético**: Es el proceso que se lleva a cabo para realizar pruebas de seguridad en infraestructuras específicas basadas en una metodología, los que realizan estas pruebas son denominados pentester o auditores de seguridad.

**Herramientas de Hacking**: Conjunto de herramientas de software o hardware por medio de las cuales el auditor logra sus objetivos en cada una de las fases del ciclo de vida de un ataque.

**Intrusión**: Proceso parte de la fase 4 del ciclo de vida de un ataque, donde después de conocer y analizar las vulnerabilidades de un sistema se logra penetrarlo o accederlo son consentimiento o provechando las vulnerabilidades encontradas.

**IoT**: Se define como una nueva tecnología denominada el Internet de las cosas, y no es más sino un conjunto de aparatos o equipos de uso diario en el mundo que pasan a tener un contexto de inteligencia al conectarse a internet y generar transferencia o trasmisión de datos para fines específicos.

**Riesgos Informáticos**: Riesgos a los que se encuentran expuestos sistemas que aún no cumplen con la implementación de las medidas adecuada de seguridad.

**Smart TV**: Dispositivo considerado de las tecnologías IoT el cual es un televisor inteligente al contar con tecnologías que permiten por medio de aplicaciones específicas conectarse a internet y reproducir jugos, conectar a canales de TV en internet, conectarse con dispositivos de almacenamiento y reproducir música entre otros beneficios.

**Vulnerabilidades**: debilidades de un sistema las cuales están dadas por la fábrica o por malas prácticas o malas configuraciones de los administradores del sistema analizado.

## RESUMEN

Las nuevas tecnologías del IoT {internet de las cosas} son cada día más usadas en empresas colombianas, por esto, los ciber-delincuentes ven estas tecnologías como objetivos importantes para controlar remotamente estos los mismos, conseguir información confidencial de las empresas, generar prácticas de espionaje empresarial, manipular remotamente sus aplicaciones y dispositivos, infectar sus sistemas informáticos con malware y lograr denegar servicios, entre otras formas de ataque.

Si tenemos en cuenta que los Smart TV en las empresas colombianas son los dispositivos más usados fuera de los computadores en procesos empresariales como mercadeo, marketing, gestión de reuniones y capacitaciones, entre otros; estos Smart Tv se convierten en un elemento importante a analizar para el objetivo de este trabajo.

Esta monografía se basa en la investigación de estadísticas en los ataques más comunes a los Smart TV durante los últimos 2 años y en prácticas de laboratorio propias en entornos virtualizados o controlados para comprobar qué vulnerabilidades hoy en día aún se muestran como NO solucionadas y son por ende vulnerabilidades vigentes, se determinarán también qué vulnerabilidades no son vigentes por el aseguramiento que dan los fabricantes a sus sistemas desde la salida de fábrica de los Smart TV.

Por lo anterior, y en búsqueda de las empresas tengan un control de estos posibles ataques, proponemos con este documento, un modelo de defensa que pueda implementarse en estas empresas colombianas orientado a prevenir ataques informáticos aplicados a Smart TV. El modelo se basará en la aplicabilidad de acciones técnicas en los sistemas operativos de cada marca y de

buenas prácticas las cuales son el resultado de un análisis de las vulnerabilidades que hoy en día siguen vigentes frente a los resultados de pruebas en ambientes controlados de virtualización o de algunos televisores reales en marcas LG y Samsung.

Palabras clave: Seguridad, información, OSSTMM, Smart TV, vulnerabilidad, base de Datos, IoT.

## ABSTRACT

The new technologies of the IoT {internet of things} are increasingly used in Colombian companies, for this reason, cyber-criminals see these technologies as important objectives to remotely control them, get confidential information from companies, generate practices of corporate espionage, remotely manipulate your applications and devices, infect your computer systems with malware and achieve denial of services, among other forms of attack.

If we take into account that Smart TVs in Colombian companies are the most used devices outside of computers in business processes such as marketing, marketing, meeting management and training, among others; These Smart TVs become an important element to analyze for the purpose of this work.

This monograph is based on statistical research on the most common attacks on Smart TVs during the last 2 years and on own laboratory practices in virtualized or controlled environments to verify which vulnerabilities today are still shown as NOT solved and are by In the case of current vulnerabilities, it will also be determined which vulnerabilities are not in force by the assurance that manufacturers give their systems since the Smart TV leaves the factory.

Therefore, and in search of companies to have control of these possible attacks, we propose with this document, a defense model that can be implemented in these Colombian companies aimed at preventing computer attacks applied to Smart TV.

The model will be based on the applicability of technical actions in the operating systems of each brand and of good practices which are the result of an analysis of the vulnerabilities that are still in force today compared to the results of tests in

controlled virtualization environments or of some real TVs on LG and Samsung brands.

Keywords: Security, information, OSSTMM, Smart TV, vulnerability, Database, IoT.

# INTRODUCCIÓN

La presente monografía tiene como fin principal proponer un modelo básico de aseguramiento de entornos Smart Tv basado en acciones técnicas de configuración y buenas prácticas que son el resultado de la identificación de vulnerabilidades que son vigentes y que fueron identificadas con la metodología OSSTMM aplicado únicamente a las marcas Samsung y LG buscando imitar os ataques o basado en conocimientos de hacking validar otras posibles vulnerabilidades.

En este documento, se describe primeramente como las tecnologías IoT en Colombia están ya inmersas en las empresas por medio de diferentes equipos que están en este rango de IoT Internet de las Cosas, se describen cifras que permiten ver los diferentes ataques y el uso de los Smart TV como equipos en las empresas, cifras que permiten conocer que en Colombia son 3 o 4 las marcas que tienen los liderazgos en ventas y que el mercado va en crecimiento día a día.

Se logra evidenciar que entre la gran cantidad de marcas y de tecnologías en los Smart TV, la monografía se centrará en la verificación de las vulnerabilidades y posibles ataques que puedan darse en los Smart TV en las dos marcas más conocidas como son Samsung y LG, basados en los datos identificados de ataques en los documentos de investigación, buscando mostrar si estas vulnerabilidades son al día de hoy aún vigentes o por el contrario han sido solucionadas por las fábricas.

# 1. DEFINICIÓN DEL PROBLEMA

## 1.1 ANTECEDENTES DEL PROBLEMA

Colombia es un país que ha adoptado las nuevas tecnologías de IoT tanto para el uso personal en hogares como empresarial, desde el año 2017 se ha evidenciado un crecimiento importante en el uso del Smart TV con un porcentaje de uso y adquisición del 30% en toda la población en Colombia (Valero, s.f.)[1].

En los últimos 3 años estadísticas demuestran que los Smart TV Samsung son los más vendidos en Colombia, seguidos por Sony y LG, con búsquedas indexadas del 61%, para Samsung, 20% Sony y 18% LG, reportes encontrados en los portales de venta más importantes en Colombia (Colombia B. L., 2017)[2].

Las empresas son uno de los mayores consumidores de televisores en Colombia, no solo los hogares y personas del común, son los sectores como el hotelero, mercadeo, marketing, educativo y publicitario que adquieren estas tecnologías como parte importante de su negocio.

Pero al ser los Smart tv considerados equipos del segmento de los IoT y al estar estos permanentemente conectados a internet se convierten en objetivos muy interesantes para delincuentes informáticos y son uno de los elementos que más atacan en el mundo, especialmente en Latinoamérica y en Colombia, lo que ha generado en Colombia en el primer trimestre del 2019 un incremento del 55% en

[1] Consumo móvil en Colombia, Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Consumo%20movil%202018.pdf.
[2] Los televisores más buscados de la región, recuperado de: https://blog.linio.com.co/los-televisores-buscados-la-region/

los ataques a dispositivos IoT siendo esto la preocupación número 1 en algunos sectores. (Aumenta el ransomware y ataques de IoT, 2019)[3]

Los ataques a dispositivos IoT es una actividad que ven lucrativa los delincuentes informáticos, por lo cual se crea la necesidad de poder implementar medidas específicas y modelos de protección prácticos y aplicables hacia la prevención de estos ataques que cada día serán más comunes e impactantes.

Las marcas fabricantes no son ajenas al problema de la inseguridad, el robo de datos personales y otros riesgos a los que están expuestos los usuarios de los Smart TV, han generado medidas que buscan implementar cada día elementos de defensa, como medidas efectivas que en un principio mitiguen algunos ataques, y progresivamente esto aportará a la seguridad, aunque no siempre sea suficiente (Colombia S. N., 2018)[4].

Muchos de los usuarios, entre estos empresas han sufrido ataques importantes los cuales han dejado muchas pérdidas de dinero con al menos 34 millones de dólares en los últimos 2 años y pérdidas de información valiosa la cual ha sido borrada, accedida, secuestrada o eliminada; y se han realizado ataques aprovechando nuevas vulnerabilidades, lo que ha generado una alerta muy alta en las empresas. Estudios han dejado como dato que 8 de cada 10 empresas están muy preocupadas por el tema de la seguridad en las tecnologías IoT y ven que muchas de las empresas se quedan cortas en la implementación de medidas de seguridad efectivas en estas tecnologías (Colombia C. , Pérdidas corporativas por fallas de seguridad en IoT, 2018)[5]

---

[3] Aumenta el ransomware y ataques de IoT, recuperado de: https://computerworld.co/aumenta-ransomware-como-servicio-y-ataques-de-iot/

[4] Samsung garantiza la seguridad de los Smart tv, recuperado de: https://news.samsung.com/co/conozca-como-samsung-garantiza-la-seguridad-en-sus-smart-tvs

[5] Perdidas e las empresas por fallas de seguridad en dispositivos IoT, recuperado de: https://computerworld.co/perdidas-corporativas-por-fallas-de-seguridad-en-iot/

## 1.2 FORMULACIÓN DEL PROBLEMA

De acuerdo a lo anterior se crea una pregunta de investigación o solución:

**¿Cómo proteger los Smart TV de ataques informáticos basados en un modelo de defensa que sea efectivo para las organizaciones o empresas?**

# 2 JUSTIFICACIÓN

En nuestro país se han dado ataques de seguridad a dispositivos IoT en los últimos años dejando algunas áreas en las empresas afectadas con un alto impacto económico, estas han experimentado consecuencias como: Pérdidas y daños monetarios, Pérdida de productividad, Multas legales y de cumplimiento, Pérdida de reputación en su sector y el mercado, además de la caída en el precio de sus acciones.

Los delincuentes informáticos cada día avanzan y se especializan más, al parecer como si fueran siempre ganando esta guerra y están un paso delante de las autoridades.

El consumo de equipos de IoT en Colombia está creciendo día a día, tanto así que para el 2020 se pronostican inversiones de los consumidores por casi USD $ 1.494 millones en dispositivos de estas tecnologías, con USD $ 5.000 millones en el mercado minorista. Y no solo en el gasto sino en la instalación de sistemas de gestión en IoT con aproximadamente 37 millones en el transito vial, lo que quiere decir que muchos de los dispositivos pueden ser Smart TV y serán también mayores los ataques que estos dispositivos sufran (Colombia C. , IoT, otro escenario para ataques, 2018)[6]

En cuanto al mercado colombiano en el uso de dispositivos IoT se estima que ya TELEFÓNICA empresa de servicios en telecomunicaciones tiene 600.000 servicios IoT conectados a 14.000 clientes empresariales, lo que hace que los delincuentes informáticos vean a Colombia como un lugar para sus prácticas y

[6] IoT Escenarios de ataques, recuperado de: https://computerworld.co/iot-otro-escenario-para-ataques/

lucrarse, con ataques que se basan en ocasiones con malware que es el tipo de ataque más usado (Portafolio.co, 2018)[7].

Específicamente el mercado de los Smart Tv en Colombia se movió en 4,18 Billones de pesos en el 2018 y se estima que esto se crezca para el 2023 al 37, 6% en ventas. Lo que indica que los Smart Tv son unos dispositivos de mucho uso en Colombia y en cuanto a las marcas que más se mueven está Samsung que es en la que nos enfocaremos. Además de estas marcas la investigación de Euro monitor indica que las más vendidas en el 2018 fueron: Samsung con 34, 7%, seguido de LG con 25, 7% y Kalley con 7, 2%. En cuarta y quinta posición se encuentra Challenger y Hyundai. El modelo investigará las vulnerabilidades de Samsung y LG, al ser las marcas líderes del mercado en Colombia (Republica.co, 2019) [8]

[7] Colombia tendrá una red exclusiva para el internet de las cosas, recuperado de: https://www.portafolio.co/negocios/empresas/colombia-tendra-una-red-exclusiva-para-el-internet-de-las-cosas-520354

[8] Samsung y Kalley tienen el 67.6% del mercado colombiano en televisores, recuperado de: https://www.larepublica.co/empresas/samsung-lg-y-kalley-tienen-676-del-mercado-de-televisores-en-colombia-2853252

# 3 OBJETIVOS

## 3.1 OBJETIVO GENERAL

Proponer un modelo básico de aseguramiento de entornos Smart Tv específicamente en las marcas Samsung y LG, basado en vulnerabilidades identificadas con la metodología OSSTMM.

## 3.2 OBJETIVOS ESPECÍFICOS

- Examinar las tecnologías, sistemas y protocolos que componen los Smart TV susceptibles de ataques en la actualidad.
- Establecer los ataques a que han sido sometidos dispositivos Smart TV en los últimos 2 años.
- Identificar las vulnerabilidades que tienen los sistemas de los Smart TV hoy en día según datos específicos de documentos recientes.
- Formular un modelo de aseguramiento que permita a los compradores implementar prácticas técnicas y procedimentales que los protejan de los ataques modernos más comunes a los Smart TV.

# 4 MARCO REFERENCIAL

## 4.1 MARCO TEÓRICO

### 4.1.1 Hacking Ético

Cuando se habla de hacking ético se hace referencia a pruebas de intrusión las cuales se ejecutan bajo ambientes controlados hacia los sistema de información de una empresa, o los llamados objetivos de auditoría, el objetivo inicial es encontrar la mayor cantidad de vulnerabilidades en los objetivos y definir con un análisis de estas vulnerabilidades las posibilidades de que se puedan explotar; el hecho de que sea en ambientes controlados genera que no se pone en riesgo la operatividad de los servicios de la organización.

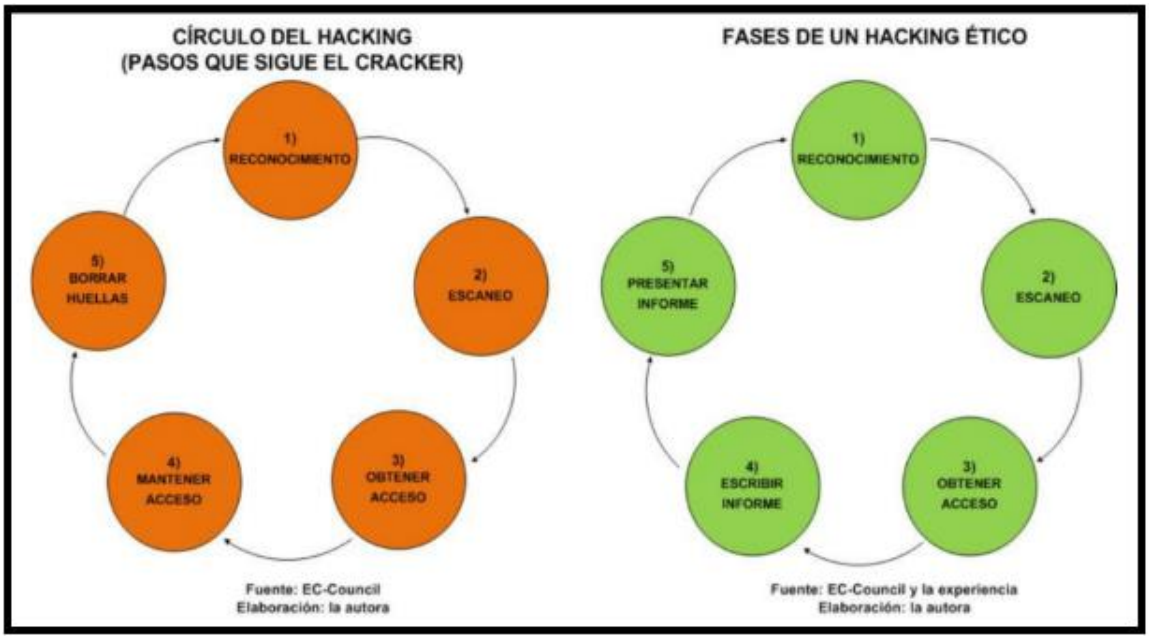
Un analista de seguridad debe tener conocimientos en diferentes temas especialmente en desarrollo o programación, redes de comunicaciones, protocolos e infraestructura de equipos y sistemas operativos, arquitectura de redes y de sistemas de hardware, y en lo posible experiencia en estas actividades, aunque estas se van adquiriendo junto con las actividades que se realizan. De acuerdo con la posición que tome el auditor una actividad de hacking de dividen en:

**Hacking ético interno**: Se ejecuta ubicado al interior de la infraestructura del cliente, hace las veces de empleado o de un atacante interno, debe tener acceso a un punto de red ya sea cableado o inalámbrico. Normalmente los auditores encuentran más vulnerabilidades en este ambiente que en el externo, lo anterior debido a que los administradores muchas veces se confían y generan o mantienen configuraciones por defecto en los quipos o infraestructuras de sistemas operativos o acceso de impresoras por ambientes web o de protocolos como ssh entre los sistemas operativos.

**Hacking ético externo:** Son actividades de hacking ético o de identificación de vulnerabilidades que se realizan desde fuera de la organización, es decir desde la red pública, desde este ambiente o posición se puede tener acceso a portales web aplicaciones expuestas a internet y equipos de red expuestos como UTM, routers entre otros (B., 2013) [9].

Como se puede ver en la figura 1 a continuación existe una diferencia del ciclo en un ataque y una auditoria profesional, aunque los pasos o fases sean muy similares la diferencia está siempre en la última fase, el atacante borra huellas y sale y en la auditoria se dejan las banderas y se hace un informe técnico y uno gerencial.

Figura 1 Fases de un ataque informático




Fuente: Karina Astudillo B., 2013, HACKING ÉTICO 101 Cómo hackear profesionalmente en 21 días o menos

[9] Karina Astudillo B., 2013, HACKING ÉTICO 101 Cómo hackear profesionalmente en 21 días o menos!

#### 4.1.1.1 Tipos de auditorías hacking

Según la información que le dé el cliente al pentester, el servicio de hacking ético se puede ejecutar en una de las 3 modalidades: black-box, gray-box, White-box, cada modalidad afecta el costo y la duración de las pruebas de intrusión ya que a menor información adquirida mayor tiempo de duración y mayor dificultad.

Figura 2 Modalidades del hacking - Caja negra, caja gris, prueba de caja blanca


Fuente: https://www.nbs-system.com/en/blog/black-box-grey-box-white-box-testing-what-differences/

**Black-box:** Hace referencia a pruebas de intrusión externas y en ocasiones internas, se llama así porque el cliente solo le proporciona el nombre de la empresa y posiblemente la IP del objetivo, pero para el auditor la infraestructura de la empresa es una caja negra. Son auditorías con un tiempo de duración más largo y un costo más elevado.

**Gray-box:** Se aplica a pruebas de intrusión externas, pero con más información donde el cliente proporciona las IP públicas de los equipos a auditar y el tipo de equipo, router, web-server, firewall, etc. También se ven en auditorías internas en el que el auditor tiene acceso a la red, pero sin privilegios.

**White-box:** Se aplica a pruebas de intrusión internas y se llama así porque la empresa cliente se encarga de darle toda la información sobre las redes y los sistemas a auditar. La empresa le entrega al auditor un diagrama de red, una lista de equipos a auditar, plataformas, servicios principales, etc. El auditor se evita tener que averiguar esta información por sí mismo, por lo anterior esta auditoria requiere menos tiempo y es menos costosa (B., 2013).

#### 4.1.1.2 Herramientas Usadas En Hacking Ético

**Sistemas operativos Linux**

Linux usado en grandes centros de cómputo, portátiles, pistolas, bombillas, etc. Existen muchas distribuciones usadas en hardware antiguo. Algunos usuarios consideran que Linux es más familiar y fácil de usar que Windows 10. A diferencia de Windows, Linux no tiene políticas de actualizaciones intrusivas y Linux tiene una variedad de software de código abierto.

Los tipos de Linux son:

- Linux Mint: fácil de usar e instalar.
- Debian: la distribución de Linux gratuita sin software, firmware o drivers propietario.
- Ubuntu: este es moderno y fácil de instalar y usar.
- OpenSUSE: no es tan fácil de instalar, pero es muy poderoso y estable.
- Fedora: una distribución actualizada, nuevos conceptos se incorporan mientras estén disponibles.
- CentOS: similar a Fedora, pero más estable.
- Elementary: para usuarios que prefieren interfaces estilo Mac.

#### 4.1.1.2.1 Kali Linux

Kali Linux es una distribución basada en Linux-Debian destinado a pruebas de seguridad y pruebas de penetración avanzada. Contiene un pool de herramientas divididos en varias categorías de la seguridad informática, como pruebas de penetración, investigación de seguridad forense de computadoras e ingeniería inversa. Kali Linux ha sido fundado, desarrollado y mantenido por la empresa offensive security que se dedica al entrenamiento en seguridad informática (Castro Alicia, s.f.) [10].

Kali Linux fue publicado el 13 de marzo de 2013, como una reconstrucción completa del sistema operativo BackTrack Linux sus características son:

- Incluye más de 500 herramientas para pruebas de penetración.
- Es totalmente libre.
- Amplio soporte para dispositivos inalámbricos.
- Kernel personalizado con parches para inyección.
- Está desarrollado en un entorno seguro.
- Paquetes y repositorios están firmados con GPG.
- Soporta múltiples lenguajes.
- Totalmente personalizable.14

#### 4.1.1.2.2 Nmap

Nmap es un software usado para realizar auditoría de seguridad en redes y equipos informáticos, es multiplataforma y libre. Esta herramienta nos permite averiguar información de los equipos conectados a una red, las versiones de sus

[10] Castro Alicia, Casanovas Eduardo, Gil Costa Verónica, CONICET Concejo Nacional de Investigaciones Científicas y Técnicas, Aspectos de seguridad en Internet de las Cosas-

sistemas operativos, y los puertos y servicios abiertos, usado en la fase de Scanning (Wikipedia, s.f.) [11]

Comandos.

- -A: Detalle
- -O: Información de sistema operativo
- -V: información ampliada
- -p {Número de puerto} {IP victima} : Información del puerto
- -sS: Devuelve si un puerto está escuchando, abierto, cerrado o filtrado.
- -sN: Nos presenta mayores detalles de los equipos escaneados
- -sA: Escanea y detecta firewall
- -pN: Escanear y detectar firewall
- -pO {número de puerto} {ip victima}: Ignora el ping y brinca
- -pT {número de puerto} {ip victima}: Información detallada de puerto

#### 4.1.1.2.3 Ipscanner

Desarrollado por Famatech en 2002. Es una aplicación muy usada para el escaneo de dispositivos conectadas a una red, permitiendo “recuperar de forma rápida y sencilla toda la información requerida sobre los equipos conectados a la red”. Según su sitio web oficial este ofrece la posibilidad de “apagar o encender un PC remoto, conectarse al mismo a través de Radmin y mucho más” (Advanced-ip-scanner, s.f.) [12]

[11] Nmap ( Network Mapper ), recuperado de: http://unblocked.to/unblock.php?site=aHR0cHM6Ly9lbi5tLndpa2lwZWRpYS5vcmcvd2lraS9ObWFw

[12] Advanced IP Scanner, recuperado de: https://www.advanced-ip-scanner.com/es/

#### 4.1.1.2.4 Sparta

Aplicación creada en Python que nos para hacer pruebas de penetración de infraestructura de una red de una forma más sencillas, permitiendo al usuario enfocarse más en los resultados del análisis de la red (Sparta.secforce, s.f.) [13].

#### 4.1.1.2.5 Putty

Putty es un programa Open Source Desarrollado por Simon Tatham para la plataforma Windows. Sirve como cliente Telnet y SSH.

Dentro de las actividades de hacking, existen pasos que forman parte de una metodología la cual se usa en las pruebas internas del presente documento, esto con el objetivo de buscar puertos en televisores reales e identificar los sistemas operativos, como actividades propias del proceso de recolección de información de estos Smart TV como objetivos para este caso, seguidamente se busca aplicar las técnicas de hacking para la identificación de vulnerabilidades y su posterior validación, algo que para la metodología se llama Banner Grabbing y está enmarcado como uno de los pasos en una metodología de auditoría local llamada OSSTMM, la cual es usada para auditorías de seguridad en entornos locales, esta metodología se muestra a continuación (Putty, s.f.)[14].

### 4.1.2 Metodología Osstmm

La metodología OSSTMM es una metodología que permite la identificación de vulnerabilidades en entornos de red local, es decir se logra con esta metodología tener los puntos base que todo pentester debe tener en cuenta si desea realizar una auditoría efectiva de una serie de equipos o activos dentro de una

[13] What is sparta?, Antonio Quina, Leonidas Stavliotis, recuperado de: http://sparta.secforce.com
[14] PuTTY, recuperado de: https://www.putty.org

organización, posicionándose desde el interior de la red y logrando tener acceso a los sistemas informático dejando ver las vulnerabilidades y los riesgos que estas vulnerabilidades evidencias en estos ambientes o entornos.

Esta es una metodología para probar la seguridad operativa de activos tecnológicos usados en las organizaciones y que están interconectados físicamente, en interacción con humanos y en diversas maneras de comunicaciones como inalámbricas, cableadas, analógicas y digitales.

La Metodología Abierta de Testeo de Seguridad OSSTMM es hoy en día un estándar alineado al concepto de seguridad. Siendo las pruebas ejecutadas e incluidas en el test pruebas no avanzadas, este estándar es una referencia para las entidades que quieren desarrollar un Testeo de calidad, ordenado y eficiente. OSSTMM propone el uso de categorías, que identifican claramente el alcance de cada una de las actividades a realizar en los procesos de evaluación de la seguridad, estas categorías son:

- Búsqueda de Vulnerabilidades: Se enfoca en comprobar de forma los sistemas objetivos de una red.
- Escaneo de la Seguridad: Realiza principalmente identificación de vulnerabilidades en el sistema, por medio de verificaciones manuales de falsos positivos, ubicación de puntos débiles en los sistemas y análisis de los resultados de estas pruebas.
- Test de Intrusión: Son testeos de pruebas que se centran en crackear o traspasar barreras o medidas de seguridad de un sistema definido, es decir generar una penetración o lograr la intrusión al objetivo.
- Evaluación de Riesgo: Son los análisis de seguridad por medio de entrevistas e investigación de nivel medio que incluye la justificación

negocios, las justificaciones legales y las justificaciones específicas de la industria.

- Auditoria de Seguridad: Hace referencia a la continua inspección que sufre el sistema por parte de los administradores los cuales controlan que se cumplan las políticas de seguridad definidas por la organización.
- Hacking Ético: Busca permanentemente obtener, basado en los test de intrusión, objetivos complejos dentro de la red de sistemas, como acceso a carpetas con políticas de seguridad, acceso a discos con controles de acceso entre otros (Commons, 2010) [15].

Teniendo en cuenta que para el presente documento se usará la metodología OSSTMM, para las actividades con los Smart TV se aplicarán únicamente las fases 1 y 2, la fase 1 de Identificación de vulnerabilidades apoyados en herramientas automatizadas y la fase 2 de escaneo de la seguridad donde se realizan validaciones manuales de lo que las actividades automatizadas muestran y con esto realizar el banner grabbing o demostración de que el servicio está funcional y la vulnerabilidad puede ser válida al día de hoy, con esto cumpliremos unos de los objetivos principales que es la validación respectiva en un ambiente como se dijo, controlado.

Seguidamente este documento muestra los resultados identificados en búsqueda de análisis de vulnerabilidades realizados en pruebas de hacking tratando de emular por medio de la metodología OSSTMM una identificación de vulnerabilidades a Smart TV y dejar ver los resultados que se lograron, sin ser un objetivo obligatorio de este documento hackear o lograr una intrusión real a los equipos o Televisores revisados, se busca únicamente aplicar una metodología y poder evidenciar si la vulnerabilidad es viable con nuestro proceso o realmente se muestra que no lo es.

[15] Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org

Cabe anotar que las pruebas internas o directas son en ambientes controlados como pueden ser una máquina virtual y emuladora de sistemas Smart TV o algunos Smart TV reales de las marcas a trabajar LG y Samsung y para este documento no aplican y será realizado un comparativo y un análisis de los ataques evidenciados en los últimos 2 o 3 años y estas vulnerabilidades identificadas en los sistemas operativos actuales en el 2021 y con esto verificar su las vulnerabilidades podrían estar vigentes en los sistemas actuales debido a actualizaciones no realizadas, o sistemas en versiones iguale a las de los ataques entre otros aspectos a analizar..

## 4.2 MARCO LEGAL

Durante el desarrollo de actividades de implementación de la seguridad informática en las organizaciones, y como un tema muy importante no solo para los jefes de sistemas o directivos de tecnología, sino también para la organización completa, está el aspecto legal en cuanto a qué podría impactar a la persona que sea sorprendida en acciones ilícitas en la organización, o también qué aspectos legales estarían a la mano de la organización, como herramientas jurídicas en cuanto a poder ejercer legalmente una reclamación frente a un ataque informático.

Esta herramienta es la ley, y en Colombia a partir del año 2009 se sancionó la ley 1273 de delitos informáticos, es la ley por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Es decir que la información y la data en las organizaciones pasa a ser un bien activo, como cualquier otro activo el cual al sufrir impactos negativos en cuanto a

su confidencialidad, integridad o disponibilidad desde lo que se conocen como ataques o acciones ilícitas con la data, son causa de cárcel y hasta sanciones económicas para los “atacantes” o causantes de estas violaciones a la seguridad.

Esta ley 1273 ´[16] está conformada por 4 artículos y dos {2} capítulos; así mismo existen en la ley unos artículos específicos enumerados desde la 269ª hasta la 269J donde se enuncian los diferentes y posibles delitos que están consagrados para gestionar legalmente un ataque informático.

Estos artículos podemos resumirlos de la siguiente forma:

- Artículo 269a. Acceso abusivo a un sistema informático
- Artículo 269b. Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269c. Interceptación de datos informáticos
- Artículo 269d. Daño informático.
- Artículo 269e. Uso de software malicioso
- Artículo 269f. Violación de datos personales
- Artículo 269g. Suplantación de sitios web para capturar
- Datos personales
- Artículo 269h. Circunstancias de agravación punitiva
- Artículo 2691. Hurto por medios informáticos y semejantes
- Artículo 269j: transferencia no consentida de activos

[16] Ley 1273 de delitos informáticos, Superintendencia de Industria y Comercio, recuperado de: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

# 5 DISEÑO METODOLÓGICO

Para el desarrollo de esta monografía en cuanto a la recolección de la información, el análisis y la definición de lo objetivos se ha tenido que recolectar una serie de datos que son parte de revisiones de documentos previos en universidades, empresas o entidades interesadas en mejorar la seguridad de los Smart TV como un dispositivo involucrado en lo que se llama hoy en día tecnologías IoT.

Por lo anterior, este documento tuvo que ser construido con métodos documentales muy básicos y experimentales, ya que se realizó previamente una búsqueda de aportes significativos dirigidos a conocer cuáles son las vulnerabilidades que hoy en día han sido confirmadas como viables en un ataque informático a un dispositivo Smart TV LG o Samsung, siendo estos métodos actividades parte de los objetivos planteados y que permitieron llegar a las conclusiones que el mismo deja al lector y experimentales porque se quiso realizar o simular los ataques como un método de validación de lo encontrado en la parte lectura documental de las vulnerabilidades.

Para el desarrollo se usó el método deductivo, el cual permite según conceptos de Carlos Muñoz Razo en su libro Cómo elaborar y asesorar una investigación de tesis, el razonar a partir de una porción de un todo, para este caso un conjunto de dispositivos tecnológicos dentro de un conjunto de elementos de nuevas tecnologías en el mundo, y llegar de una conclusión general de los dispositivos IoT en su seguridad frente a vulnerabilidades actuales, a llegar a conclusiones particulares o específicas al tener claras al final del proceso cuáles son las vulnerabilidades vigentes en los Smart TV específicamente las marcas Samsung y LG.

Es así como esta metodología hace posible que el tema escogido y los resultados basados en prácticas personales validaran las conclusiones sobre las cuales se basa el autor del mismo para crear el modelo de defensa o seguridad frente a ataques a estos dispositivos Smart TV LG y Samsung.

# 6 DESARROLLO DE LOS OBJETIVOS

## 6.1 IDENTIFICACIÓN DE TECNOLOGÍAS, SISTEMAS Y PROTOCOLOS EN LOS SMART TV.

### 6.1.1 Tecnología Del Internet De Las Cosas O IOT

Para explicar este concepto hay que iniciar hablando del concepto del objeto conectado a internet y objeto inteligente, este concepto se evidenció con Nikola Tesla o Alan Turing. En 1926, Nikola Tesla en una entrevista a la revista Collier {Kennedy, 1926} anticipó el crecimiento de conectividad a nivel global y la miniaturización tecnológica, este dijo “cuando lo inalámbrico esté perfectamente desarrollado, el planeta entero se convertirá en un gran cerebro, que de hecho ya lo es, con todas las cosas siendo partículas de un todo real y rítmico y los instrumentos que usaremos para ellos serán increíblemente sencillos comparados con nuestros teléfonos actuales. Un hombre podrá llevar uno en su bolsillo (Kottke, 2018) [17]”.

Así como Tesla, también fueron importantes las palabras de Alan Turing en 1950 en su artículo en el computing Machinery and Intelligence in the oxford mind journal {Turing, 1950}, en donde evidenció la necesidad futura de dotar de inteligencia y capacidades de comunicación a los dispositivos y sensores, dijo: “también se puede sostener que es mejor proporcionar la máquina con los mejores órganos sensores que el dinero que pueda comprar, y después enseñar a entender y hablar inglés. Este proceso seguirá el proceso normal de aprendizaje de un niño” Alan Turing.

[17] Nikola Tesla Predicted the Smartphone in 1926, acceso el 09 de Octubre del 2019, https://kottke.org/18/04/nikola-tesla-predicted-the-smartphone-in-1926

Hoy en día el internet de las cosas o IoT es una tecnología aplicada a diferentes dispositivos que van desde relojes, Smart TV, neveras, entre otros, y estos brindan a los usuarios servicios diferentes los cuales pueden enviar o recibir información por internet, aprovechando las bondades de la web, siendo esto un gran desafío para las organizaciones, dependiendo del uso en las organizaciones se pueden dar IoT en ambientes de salud, finanzas, infraestructuras industriales entre otras.

Este término fue introducido hacia los años 2008 y 2009 cuando la cantidad de dispositivos interconectados fue muy grande, casi superior al número de personas en su momento. En su época los equipos que estaban interconectados en la web eran PC's, servidores, Smartphones pero ya se dio la llegada a otros elementos como Tablets, Smart TV que hacia el 2013 generaron un crecimiento del 8.5% en Tablets y los Smart TV en un 78,6% (Castro Alicia, s.f.) [18].

El IoT es un componente tecnológico fundamental, hoy en día es la base de la industria 4.0, es preciso entender que el término "internet de las cosas" es bastante reciente, este data del año 2009 cuando Kevin Ashton, un profesor del MIT {El instituto de tecnología de Massachusetts} inicio el uso de la expresión "internet de las cosas {IoT}" de forma pública, en el RFID Journal {Ashton, 2009}. El RFID Journal, es una compañía de medios independiente. [19].

### 6.1.2 Arquitectura y conceptos básicos del IOT.

Dentro de las tecnologías IoT existen arquitecturas que se pueden dividir en las que han sido creadas por marcas específicas y las Open Source y que estas buscan que esta arquitectura sea para uso general. Las que son creadas por empresas o mercados globales, las que son sensores o llamados Things y que

[18] Castro Alicia, Casanovas Eduardo, Gil Costa Verónica, CONICET Concejo Nacional de Investigaciones Científicas y Técnicas, Aspectos de seguridad en Internet de las Cosas-

[19] Jordi Salazar y Santiago Silvestre, Paginas 34, TECHPEDIA, Internet de las Cosas.

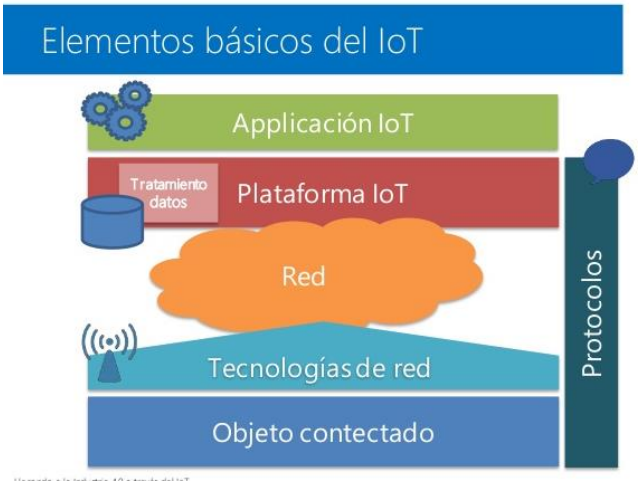
van en conexión con otro dispositivo por lo general de forma inalámbrica, con esto el aparato se conectaría a internet y con el uso de programas y servicios de terceros puede interactuar con servidores cloud o servidores nube en el intercambiando datos para objetivos especiales.

El otro modo de arquitectura vemos la llamada OpenIoT, son implementaciones Open Source que actúan bajo servicios de IoT y que dan la posibilidad de conectar y procesar datos que le llegan de objetos o dispositivos físicos que son basados en sensores. En tecnologías abiertas está la versión 3.0 que se basa en un proyecto creado en Europa IoT-A mantenido por diferentes empresas de diferentes sectores en Europa donde han creado modelos basados en lograr confianza, privacidad y confiabilidad (Castro Alicia, s.f.) [20].

La figura 3 nos muestra más claramente éste concepto, se ve como las capas de la infraestructura están organizadas e interactúan en el modelo de usabilidad sin importar cuál sea el dispositivo, si es un reloj inteligente, o un televisor, o una nevera, etc. Se ve como las aplicaciones que son particulares de las marcas interactúan con la plataforma y las tecnologías de red o de comunicaciones hasta que el dispositivo se conecta. Y todo esto usando protocolos de comunicación y de infraestructuras conocidas.

[20] Castro Alicia, Casanovas Eduardo, Gil Costa Verónica, CONICET Concejo Nacional de Investigaciones Científicas y Técnicas, Aspectos de seguridad en Internet de las Cosas-

Figura 3 Componentes Fundamentales del IoT




Fuente:https://es.slideshare.net/BrunoCendn/llegando-a-la-industria-40-a-travs-del-iot

A continuación, es preciso explicar la magnitud de las tecnologías IoT incluidas en los equipos denominados Smart tv y lo que estos representan para las empresas hoy en día.

### 6.1.3 Tecnologías Y Componentes Smart Tv

La televisión inteligente {traducido al inglés “Smart Tv”} hace referencia a la integración de internet a la televisión digital, es decir la televisión 3D. La tecnología de los Smart Tv no solo se incorpora en los televisores, sino en otros equipos como la set-top boxes, el grabador de videos digital, los reproductores Blu-ray, las consolas de videojuegos y los llamados home cinemas, entre otros.

Estos dispositivos permiten que los usuarios busquen y encuentren videos, películas, fotografías y otros contenidos online, en un canal de televisión por cable, en un canal de televisión por satélite o almacenado en un disco duro local, muchos de ellos permiten grabar y verlos en 3D, estos Smart TV se consiguen por un

módico precio con todas estas habilidades, las cuales son hoy en día el estándar (tecnologica, s.f.) [21].

El objetivo de esta tecnología Smart TV era crecer en contenidos multimedia directamente a la televisión buscando comodidad, y más contenido multimedia integrado a internet, todo en un televisor mediante una sola única interfaz de usuario en una súper pantalla. Los fabricantes de Smart TV aprovecharon la feria internacional de electrónica de consumo, que se realizó en las vegas durante el inicio del año 2011 para promocionar los primeros televisores inteligentes.

Podemos ver a continuación en la figura 4 que los Smart TV son un elemento con computación avanzada integrada, podemos mencionar al LG ST600 Smart Tv upgrader creado por LG, una pequeña caja que actualiza un televisor que originalmente solo reproduce la salida de la antena del televisor, sin conexión a internet.

Esta caja inteligente cuenta con conexión Wi-fi y Ethernet, más funcionalidades propias de la televisión inteligente al televisor, como conexión a internet y la posibilidad de hacer Streaming de video de otros ordenadores.

La televisión inteligente permite instalar y ejecutar aplicaciones avanzadas o plugins basados en una plataforma específica, tal como se maneja en un computador tradicional integrando este en el televisor.

Los televisores inteligentes ejecutan un sistema operativo o el software completo de un sistema operativo móvil ofreciendo una plataforma para el desarrollador de software.

[21] areatecnologia, que es Smart tv características, recuperado de: https://www.areatecnologia.com/que-es-smart-tv.htm

Figura 4 Características de un Smart TV


Fuente: areatecnologia, que es Smart tv características, recuperado de: https://www.areatecnologia.com/que-es-smart-tv.htm

La televisión inteligente permite al usuario integrar diferentes aplicaciones que cubren las necesidades del mismo, entretenimiento, información noticias, redes sociales, entre otras, la figura 5 que vemos en esta página nos muestra estos elementos que se resumen en los siguientes puntos:

- Entregar contenidos de otros dispositivos de almacenamiento a la red, como fotografías, películas y música utilizando un programa de servicios, como Windows Media Player en el ordenador o NAS como dispositivo de almacenamiento, o a través de iTunes.
- Proporcionar acceso a servicios basados en internet, mediante IPTV, logrando buscar y navegar por internet en servicios de video a la carta, personalización de contenido, redes sociales y aplicaciones multimedia.
- Visualizar los contenidos en alta definición.

- Lanzar aplicaciones asociadas en un canal concreto, como videos relacionados con el contenido, sistemas de votaciones, sistemas de apuestas y participación en concursos, y publicidad interactiva.
- Reproducir el contenido de videos o música almacenado en dispositivos USB.
- Controlar de forma remota el televisor con el Smartphone del usuario, mediante aplicaciones desarrolladas por los dispositivos que cuentan con Android y el iPhone.
- Algunos cuentan con redes de telefonía IP, como Skype o Hangouts.

Figura 5 Funciones Básicas de la TV Online


Fuente: https://www.xatakahome.com/televisores/pero-realmente-que-es-un-smart-tv-especial-smart-tv

### 6.1.4 Sistemas operativos de los Smart tv

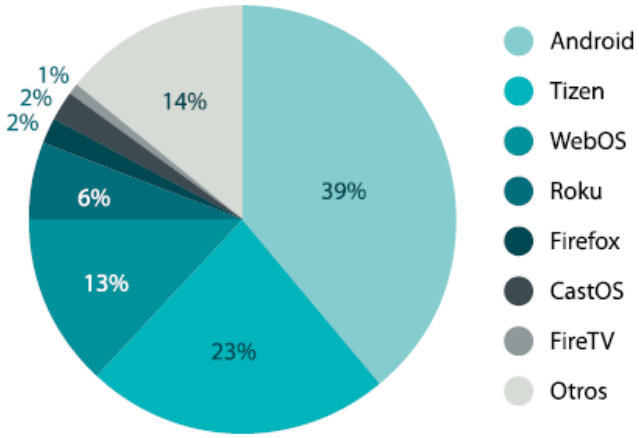
Los sistemas operativos son aplicaciones base para los televisores inteligentes que controlan lo que el hardware hace, y facilitan el uso de otras aplicaciones y del hardware por medio de una interfaz figura. Los Smart TV son una gran revolución en lo referente a disfrutar contenidos televisivos, estos nos permiten

llegar directamente al mundo digital con internet, pudiendo ver los contenidos con Streaming, navegar por la internet y hacer casi todo lo que hacemos en PC's o computadoras, de manera fácil y cómoda.

Sin embargo, para acceder a todas estas funciones, es imprescindible que el mejor Smart TV disponga de un sistema operativo eficiente, que nos facilite el acceso a todas estas funciones y que tenga la compatibilidad necesaria como para instalar las aplicaciones que más nos gusten.

La siguiente figura muestra los diferentes sistemas operativos que vienen instalados hoy en día en la mayoría de los Smart TV.

Figura 6 Sistemas Operativos de Smart TV




Fuente: IHS Markit TV Sets Intelligence Service Premium. Disponible en: https://www.broadbandtvnews.com/2018/07/17/smart-tv-share-jumps-to-70-of-tv-shipments

La marca que estamos trabajando en este documento LG tiene un sistema operativo llamado Web OS, Es un sistema propio de la marca es un sistema

llamado Palm/HP y su principal característica es la velocidad de conexión, la búsqueda y la visualización de os contenidos presentados. Además, gestiona remotamente por control accesos directos a servicios basados en el uso de botos Magic Link.

Una característica importante relacionada con la seguridad es que la plataforma ha sido certificada por sus capacidades de ciberseguridad por la UL Trasaction Security compañía independiente experta en seguridad, como una plataforma segura. Firefox OS es el sistema operativo de Panasonic, desde el 2015 se generó la implementación de este sistema basado en HTML5, este incorpora todo tipo de aplicaciones, entre ellos un potente navegador, en este se puede acceder a todo tipo de contenidos y establecer accesos directos (Gadget) [22].

La marca en estudio para este documento y como lo muestra la figura 7 es TZEN un entorno moderno y muy gráfico e intuitivo para el usuario, Samsung se monta en TZEN, esta marca coreana maneja este sistema que es de código abierto, este posee una función de auto detección la cual identifica automáticamente la fuente conectada al equipo o televisor por medio de HDMI. Como una última implementación del sistema es el sistema de reconocimiento de voz que llego para todos los sistemas posteriores a 2017.Maneja Mando a distancia y one remote para aprovechar las funciones de aplicaciones del Smart TV.

[22] Revista GADGET, ¿Sabes cuáles son los sistemas operativos que puede tener tu televisor? Recuperado de: http://www.revista-gadget.es/reportaje/sistemas-operativos-televisor/

Figura 7 Sistema Operativo TZEN

Fuente: Revista GADGET, ¿Sabes cuáles son los sistemas operativos que puede tener tu televisor? Recuperado de: http://www.revista-gadget.es/reportaje/sistemas-operativos-televisor/

### 6.1.5 Protocolos de comunicación en los Smart TV

Como equipos conectados a una red y que se conectan con internet, los Smart TV tienen esquemas de comunicación para la entrada y salida de datos basados en puertos, los cuales aprovechan los delincuentes para atacar, estos puertos están relacionados con los servicios que prestan cada una de las funcionalidades del Smart Tv, puertos que podemos conocer están en la siguiente figura la número 8 donde se muestran los protocolos que son usados en las comunicaciones a través de los puertos abiertos del Smart TV, en estos equipos los más usados son (Eliécer, 2018) [23]:

[23] Manosalva Barrera Néstor Eliécer, Universidad nacional de Colombia, Construcción de un modelo de plataforma IoT para la trazabilidad del proceso logístico de la fresa dentro del marco del corredor tecnológico agroindustrial Bogotá, 2018. Recuperado de: http://bdigital.unal.edu.co/69834/1/1032370645.2018.pdf

Figura 8 Protocolos de los Smart TV

| PROTOCOLO | TARNSPORTE | QoS | Arquitectura | Seguridad | 2G,3G,4G(1000s) | Recursos de computo |
|---|---|---|---|---|---|---|
| CoAp | UDP | SI | Req/Resp | DTLS | Excelente | 10Ks/RAM Flash |
| MQTT | TCP | SI | Req/Resp | TLS/SSL | Excelente | 10Ks/RAM Flash |
| XMPP | TCP | NO | Req/Resp, Pub/Sub | TLS/SSL | Excelente | 10Ks/RAM Flash |
| REST | HTTP | NO | Req/Resp | HTTPS | Excelente | 10Ks/RAM Flash |
| WebSocket | TCP | NO | Pub/Sub | HTTP | | |

Fuente: Adaptado de Karagiannis et al. [2015], Olubusayo Richard Adeyemo Supervised by Paul Lin [2016], Estep [s.f.]

Como lo muestra esta figura 8, que representa una tabla de datos de los protocolos usados en los SmartTV en sus sistemas operativos, estos usan comunicaciones basadas en TCP y UDP para las comunicaciones con el exterior del equipo y con otros equipos o aplicaciones.
Estos puertos son normalmente atacados en los procesos de hacking a estas tecnologías, cada uno cumple unas funciones dentro del Smart, a continuación, se conocerá que hace cada uno de estos protocolos en el sistema operativo.

**CoAP {Constrained Application Protocol}** es un protocolo software a nivel de aplicación usado en dispositivos electrónicos simples permitiendo comunicarse sobre Internet (bdigital.unal.edu.co, s.f.) [24].

**MQTT {Message Queue Telemetry Transport}** es un protocolo de transporte de mensajes Cliente/Servidor basado en publicaciones y subscripciones a los denominados “tópicos”. Cada vez que un mensaje es publicado será recibido por el resto de dispositivos adheridos a un tópico del protocolo. El protocolo MQTT se ha convertido en uno de los principales pilares del IoT por su sencillez y ligereza. Ambos son condicionantes importantes ya que los dispositivos de IoT,

[24] RFC 7252 Protocolo de aplicación restringida, COAP, recuperado de: http:// https://coap.technology/

regularmente tienen limitaciones de potencia, consumo, y ancho de banda (tst-sistemas, s.f.) [25].

**Extensible Messaging and Presence Protocol**, más conocido como XMPP {Protocolo extensible de mensajería y comunicación de presencia} {anteriormente llamado Jabber1}, es un protocolo abierto y extensible basado en XML, originalmente creado para mensajería instantánea. Con el protocolo XMPP queda establecida una plataforma para el intercambio de datos XML que puede ser usada en aplicaciones de mensajería instantánea. La adaptabilidad y sencillez del XML son heredadas de este modo por el protocolo XMPP (XMPP, s.f.) [26].

**REST** - Si bien el término REST se refería originalmente a un conjunto de principios de arquitectura —descritos más abajo—, en la actualidad se usa en el sentido más amplio para describir cualquier interfaz entre sistemas que utilice directamente HTTP para obtener datos o indicar la ejecución de operaciones sobre los datos, en cualquier formato {XML, JSON, etc} sin las abstracciones de los protocolos basados en patrones de intercambio de mensajes, como SOAP (Simões, s.f.) [27].

**WEBSOCKET** es una tecnología que proporciona un canal de comunicación bidireccional y full-dúplex sobre un único socket TCP. Está diseñada para ser implementada en navegadores y servidores web, pero puede utilizarse por cualquier aplicación cliente/servidor. El protocolo WebSocket propone un modelo sencillo de comunicaciones para la Web que no rompe con las tecnologías ya existentes. El RFC 6455 habla de este protocolo (Blogspot, 2013) [28].

---

[25] MQTT - Protocolo de conectividad M2M / IoT, recuperado de: https:// http://www.tst-sistemas.es/mqtt/
[26] Sobre XMPP, recuperado de: http:// https://xmpp.org/about/
[27] Chiyana Simões , REST vs WebSocket. ¿Qué diferencias hay?, recuperado de: http:// https://www.itdo.com/blog/rest-vs-websocket-que-diferencia-hay/
[28] Qué es WebSocket, recuperado de: http:// http://queeswebsocket.blogspot.com/2013/01/que-es-websocket.html

¿Qué diferencia hay entre REST y WebSocket? Como hemos dicho anteriormente, REST es un estilo de arquitectura y WebSocket un protocolo, por tanto, tiene sentido si comparamos HTTP con WebSocket.

Los anteriores protocolos de comunicación de las tecnologías Smart TV trabajan en protocolos de comunicación básicos con otras tecnologías como internet, por lo cual están relacionados con ataques que los aprovechan como se menciona en el documento Smart-TV security analysis: practical experiments, cuando en los laboratorios desarrollados de seguridad para Smart TV LG donde se ve que en las actualizaciones de los firmware entre los módulos no se usa por parte del software de fábrica parámetros de seguridad en el cifrado de los datos que pasan de un módulo a otro generando comunicaciones en XML lo que permite que se hagan ataques de Hombre en el medio (Yann Bachy, 2015) [29].

Esto da claridad sobre el primer objetivo específico de este documento para así llegar a identificar más adelante cuales son los tipos de ataques más actualizados o más ejecutados por medio de estos protocolos en estas tecnologías Smart TV.

Después de conocer las características de los sistemas Smart TV, los sistemas operativos y los protocolos, es importante conocer qué proceso se debe seguir para la búsqueda de vulnerabilidades y posiblemente llegar desde un entorno controlado pero real, a encontrar y EXPLOTAR brechas de seguridad o vulnerabilidades en los Smart TV. A continuación, se presenta el concepto de Hacking Ético y qué herramientas se usan para llegar a conocer y encontrar estas vulnerabilidades.

[29] Smart-TV security analysis: practical experiments, recuperado de: https://www.semanticscholar.org/paper/Smart-TV-Security-Analysis%3A-Practical-Experiments-Bachy-Basse/5dd526542309915c1b67facec3355ca59e156902

## 6.2 ATAQUES IDENTIFICADOS EN INVESTIGACIONES EXTERNAS A LOS SMART TV.

Para lograr identificar los ataques más efectivos a los que han sido sometidos los dispositivos Smart Tv hoy en día, es preciso contar con la información anteriormente descrita como los protocolos, las vulnerabilidades que presentan estos protocolos y bueno también las formas en que los delincuentes o atacantes informáticos realizan sus acciones, y de acuerdo con las diferentes fuentes consultadas y buscando cumplir con el segundo objetivo del documento, vemos que los ataques más importantes son los siguientes:

### 6.2.1 Ataque a las particiones de almacenamiento:

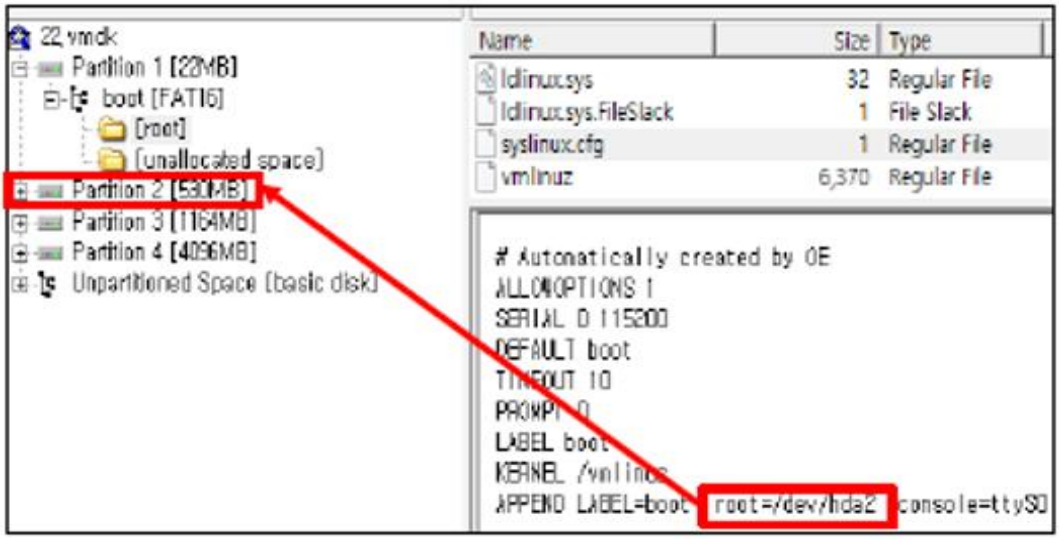
Des-encriptando los datos de los archivos que almacenan los hash de los usuarios que se loguean al sistema Smart TV, usan herramientas como kali Linux con unos llamados decrypters, después de acceder a los archivos basados en el conocimiento de las rutas de los archivos (Mingeum, 2017) [30].

**Primero** encuentran la ruta donde están los archivos en el sistema WebOS.

En la figura 9 presentada a continuación, vemos como en el Smart tv se puede ubicar para este ataque en el vmdk o disco virtual la partición 2, donde en sus características se ve que está ubicado en esa partición la ruta de una carpeta que en los Linux almacena los datos de los usuarios y sus claven, algo que para un atacante es muy importante al inicio del proceso de escaneo y de enumeración.

[30] Are you watching TV now? Is it real?:Hacking of smart TV with 0 day, Lee Jongo and Kim Mingeum, 2017, security analysis and evaluation SANE Lab

**Figura 9. Identificación de rutas de archivos**




Fuente: Are you watching TV now? Is it real? Hacking of smart TV with 0 day

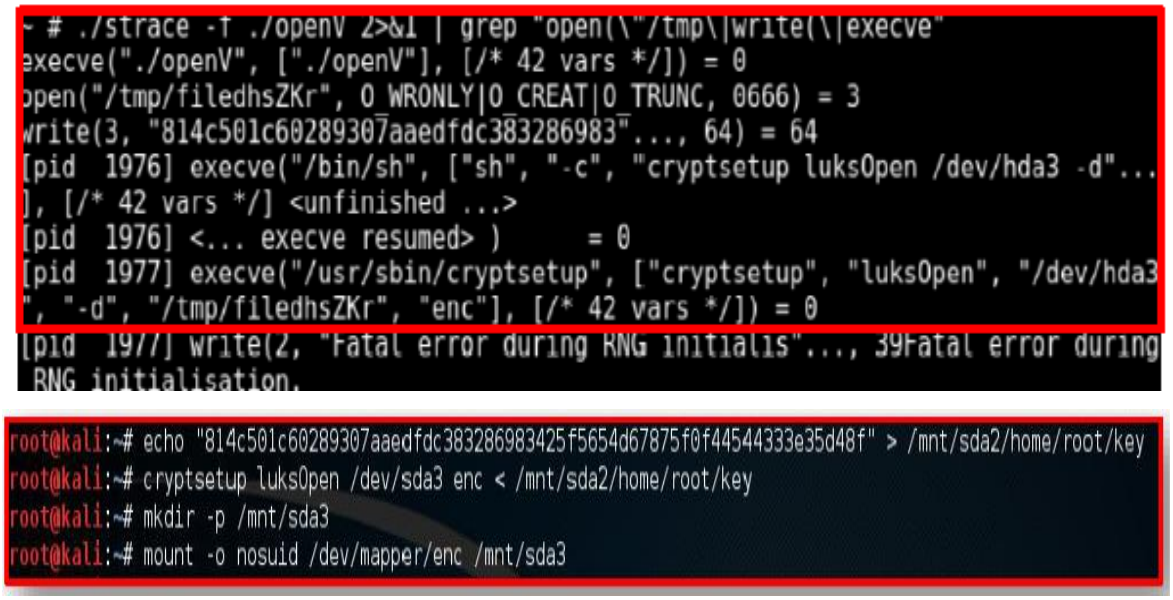
**Segundo paso identificación:** La herramienta con la que des-encriptaran los archivos. Un script personalizado para descifrar el archivo de usuarios OPEN V.

Figura 10 Identificación de herramienta OPEN V


Fuente: Hacking of smart TV with 0 day – Korea University - Jongho Lee, Mingeun Kim*, Seungjoo Kim**

**Tercer paso Des-encripción,** Se muestra en la figura 11, cómo se desarrolla la des-encripción de los archivos necesarios para llegar a tener las claves respectivas y conformar el ataque.

Figura 11 **Tercer paso:** des-encripción de la partición y ubicación de los archivos




Fuente: Hacking of smart TV with 0 day - Korea University, Jongho Lee, Mingeun Kim*, Seungjoo Kim**

**Cuarto paso** es la modificación del archivo {**dropbear**} que está en la ruta del usuario que esta con la sesión abierta, con la identificación del algoritmo de cifrado que es RSA.

La figura 12 muestra cómo se logra en la ruta identificada modificar el contenido del archivo con comandos y códigos parte del ataque y que son favorables para el atacante, todo con un script como se ve en la figura en el cuadro rojo, llamado 12.sh o una Shell que se ejecuta dentro del Smart víctima.

Figura 12 Paso cuarto modificación del archivo.


Fuente: Hacking of smart TV with 0 day - Korea University, Jongho Lee, Mingeun Kim*, Seungjoo Kim**

Después se logra descifrar los archivos encontrados y se consigue el usuario y la clave respectiva para entrar como root del sistema.

La figura 13 muestra como con el paso anterior se rootea o se accede con usuario root el sistema del Smart TV y se secuestra prácticamente el dispositivo ya que con el usuario root activo se tiene todo el poder sobre el Smart algo que es una evidencia de ataque o intrusión satisfactoria.

El recuadro enmarcado en roja muestra lo que se digita en los comandos del proceso que se lleva para el ataque, esto para dejar claro que actividades hacen posible esta paso.

Figura 13 Descifrado de archivos encontrados


Fuente: Hacking of smart TV with 0 day - Korea University, Jongho Lee, Mingeun Kim*, Seungjoo Kim**

**Quinto paso**. Finalmente se usa putty para la conexión y se logra des-encriptar los archivos ubicados en el sistema que se accedió, sr generan ataques de intrusión como este aprovechando las vulnerabilidades de los sistemas de cifrado el sistema WebOS (Mingeum, 2017) .

### 6.2.2 Ataque DirtyCOW Vulnerability (Mingeum, 2017) [31]

La siguiente vulnerabilidad esta llamada **DirtyCOW Vulnerability** está catalogada desde el 2016 como posible con el CVE-2016-5195 donde se permite leer el área

[31] Hacking of smart TV with 0 day - Korea University, Jongho Lee, Mingeun Kim*, Seungjoo Kim**

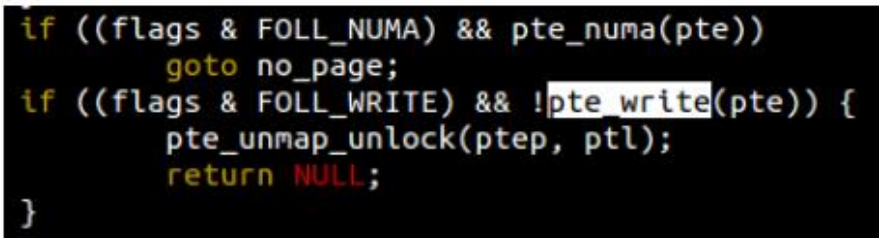
usando una condición mientras se ejecuta un código pasado en una función Linux, esto lo ejecuta el exploit que está diseñado para esto.

**DirtyCOW Vulnerability:**

**Primero** se deja ubicado el código que se ejecutará. Es decir se chequea el código del Kernel del sistema.

La figura 14  a continuación presentada, se pasa un parámetro en las variables ptep y ptl, parámetro que estará escrito y quedará implantado en el sistema, por la función pte_write. Esto hace referencia a la modificación de los parámetros del kernel del sistema del Smart TV desde donde se hace el ataque inicialmente.

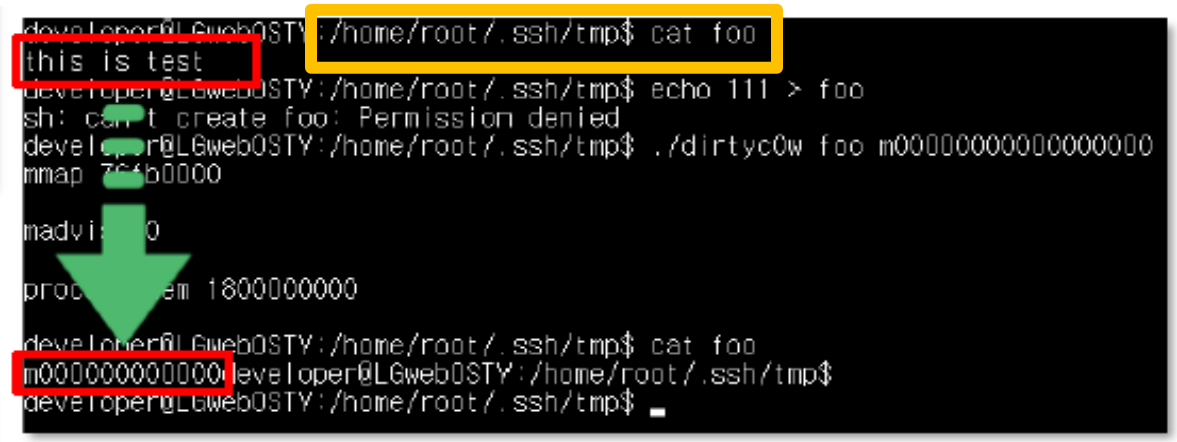
Figura 14 Ataque DirtyCOW




Fuente: Hacking of smart TV with 0 day - Korea University, Jongho Lee, Mingeun Kim*, Seungjoo Kim**

**Segundo,** Como lo muestra la figura 15, después se accede por comandos al TV y se testea si en la ruta /home/root/.ssh en color amarillo, y se ubica el archivo de datos o FOD por sus siglas en inglés, File of  Data que contiene el código temporal que se usará para el ataque. Como se ve el ataque es testeado dejando visto el segmento COW que se requiere para hacer el ataque, es decir si es posible.

Figura 15 Acceso por comandos al sistema del TV




Fuente: Hacking of smart TV with 0 day - Korea University, Jongho Lee, Mingeun Kim*, Seungjoo Kim**

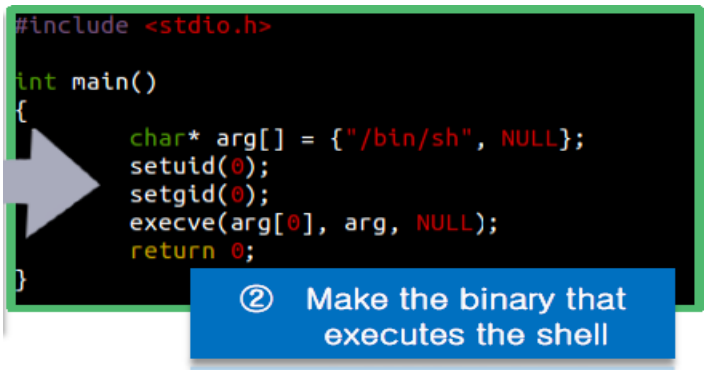
Como el sistema WebOS es basado en un Kernel de Linux se ubican las rutas de los archivos **shadow** que son los que almacenan los usuarios y claves del sistema especialmente las del root, es algo que todo atacante realiza siempre, ubicar usuarios y claves con privilegios de administrador o root.

Figura 16 Ubicación de las rutas del sistema


Fuente: Hacking of smart TV with 0 day - Korea University, Jongho Lee, Mingeun Kim*, Seungjoo Kim**

Luego se ejecuta el código pasando como parámetro la ruta del archivo, /bin/.sh.

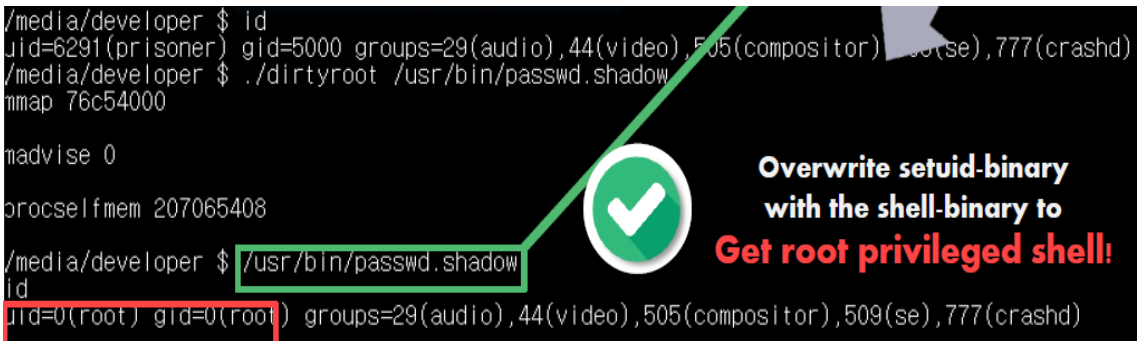
Figura 17 Ejecución del código con parámetros de pasada




Fuente: Hacking of smart TV with 0 day - Korea University, Jongho Lee, Mingeun Kim*, Seungjoo Kim**

Finalmente se logra sobre escribir la ruta y el archivo deja ver las credenciales del root del sistema, como se muestra en la figura 18 esto se logra usando siempre código que está diseñado especialmente para estos temas, es decir que podría verse como un ataque con exploits o malware., logrando editar el archivo passwd.shadow en la ruta descrita. Y encerrada en color rojo.

Figura 18 Ubicación y edición del archivo de las claves y usuarios Passwd




Fuente: Hacking of smart TV with 0 day - Korea University, Jongho Lee, Mingeun Kim*, Seungjoo Kim**

### 6.2.3 Ataque de MiTM Man in the Middle u hombre en el medio

Es un tipo de ataque normalmente usado en combinación con otros elementos como malware, generalmente estos dos elementos del ataque son muy usados, se dice que es un ataque de hombre en el medio ya que donde el atacante se pone en medio de la ruta de comunicación entre el Smart TV y el usuario, generando un control en la comunicación sin dejar que esta fluya, pero a su conveniencia, y en la gran mayoría de los casos para extraer o robar datos.

Es un tipo de ataque que es posible por las comunicaciones que generan las aplicaciones del TV con el exterior y con los dispositivos que internamente se conectan como el dispositivo de decodificador del proveedor de televisión. El ataque se da cuando un atacante se ubica técnicamente hablando, en la misma ruta de red o de comunicación con el usuario para llevar a cabo la captura de la data en la comunicación, cuando se realiza desde se aprovecha mediante la captura de la contraseña de Wi-Fi o del secuestro de las solicitudes DNS, que el Smart TV hace hacia internet.

De acuerdo a lo anteriormente mencionado es un tipo de ataque muy frecuente ya que NO todas las conexiones realizadas por la TV utilizan el cifrado SSL, algunas lo hacen, pero no verifican el certificado a profundidad, por ejemplo, algunos aceptan certificados SSL firmados que son fáciles de crear para los atacantes, o en la mayoría de os casos los sistemas operativos y los sistema de cifrado no son actualizados y manejan versiones viejas u obsoletas de protocolos y métodos de cifrado como por ejemplo TLS 1.0 o el uso de RC4.[32] (https://infoweek.biz, 2019)

[32] INFOWEEK, Cómo se Infectó mi televisor con ransomware, https://infoweek.biz 18/06/2019

### 6.2.4 Ataque de Adopción de TLS

Transport Layer Security, al ser este protocolo de seguridad en el transporte de datos en las tecnologías de Samsung se logró evidenciar que las comunicaciones al ser resteadas podrían llegar a tener tráfico de alguna data en texto plano, en un trabajo realizado en la Universidad de Ruhr en Alemania se evidenciaron posibles ataques de este tipo.

El atacante logró llegar a identificar aplicaciones con la opción de inicio de sesión en tráfico Http donde entran a formularios y las credenciales estaban en texto plano. Con este ataque se lograría secuestrar las credenciales de inicio de sesión si él escucha a escondidas la conexión no encriptada de la víctima y si una de la aplicación vulnerable es utilizada por la víctima al mismo tiempo y hora. Para realizar un ataque de TLS aprovechando las vulnerabilidades de la versión 1.0 del protocolo.

### 6.2.5 Ataque a vulnerabilidades de XML y XXE.

Extensible Markup Language {XML} el cual es un formato de W3C. Se utiliza para transmisión, validación e interpretación de datos en diferentes aplicaciones que van desde servicios web y aplicaciones de oficina hasta configuración archivos utilizados en varios servidores y dispositivos. El problema de la vulnerabilidad estaba en que número de escenarios de aplicación que adaptan la tecnología XML resultó en una gran cantidad de especificaciones de extensión que permiten definir esquemas para documentos XML o para aplicar primitivas criptofiguras directamente en el nivel XML. En este se usa el estándar de llamado a topos de documentos {DTD} y este permite la declaración de nuevos bloques de construcción XML en el prólogo de un documento XML. Estos bloques de construcción se llaman entidades XML. Las entidades XML se insertan en el documento XML.

Cuando un analizador XML procesa dicho documento, primero lee las entidades en el prólogo XML. Luego, se resuelve todas las ocurrencias de la entidad en el documento: & title; es reemplazado con un archivo de configuración de texto y & ext; se reemplaza con el contenido del archivo: ///text.txt. Esto es muy peligroso ya que si un atacante controla el contenido de los archivos XML procesados podría inyectar los que desee.

### 6.2.6 Ataque de Autorización delegada

OAuth. OAuth es un marco para autorización delegada. En contraste con el inicio de sesión único Sistemas como OpenID y SAML, la idea de OAuth no es iniciar sesión en una aplicación, sino otorgar derechos de acceso sobre recursos específicos para ello. En la mayoría de los casos, la aplicación, denominada Cliente OAuth, es solo autorizado para acceder a un subconjunto de recursos propiedad de usuario. Hay algunas variantes de OAuth: OpenID Connect y Facebook Connect. Ambos se basan en OAuth y deben referirse a estos tres con el término OAuth.

Después de identificar los ataques más comunes, causa curiosidad el determinar si estos ataques respondían a realmente las vulnerabilidades más comunes y es muy pertinente saber de antemano que, al ser estos dispositivos cada vez más inteligentes y tener más apps, las Smart TV manejan cada vez más datos sensibles, como nuestra cuenta de usuario de Google, Netflix, HBO, o cualquier plataforma de Streaming o web en la que hagamos login a través del navegador, entre otros muchos tipos de datos. Por ello, estos son los 5 peligros a los que se exponen los usuarios si no se protege la Smart TV según Check Point en su documento de seguridad en IoT.

Como complemento a los anteriores ataques evidenciados en consultas realizadas a documentos es preciso dejar como datos importantes algunas

vulnerabilidades que se dan cuando los Smart TV no están protegidos o se tienen malas prácticas de configuración o están por defecto desde fábrica, se muestran en este documento como peligros comunes cuando el equipo está sin protección (Nikos Sidiroupoulos, 2013) [33].

### 6.2.7 Ataques al Firmware del TV:

**Importancia del firmware**

El firmware es el elemento central de cualquier sistema electrónico que comprende memoria persistente o memoria permanente, código de programa y datos. En el caso de Smart TV, el firmware es el sistema operativo responsable de administrar los recursos de hardware disponibles de la TV y de proporcionar servicios comunes y necesarios a los programas de uso e interacción con el usuario en el TV.

**Sobre el firmware**

La versión en ejecución del firmware del televisor es 1029, mientras que las actualizaciones 1030 y 1031 están disponibles a través del sitio de soporte de productos de Samsung. Esta marca no proporciona ningún tipo de registro de cambios a las versiones que proporciona a través de su sitio web. Hay tres procedimientos de actualización que se pueden seguir: En línea {Internet} - USB o Señal de transmisión

**Evaluación de la vulnerabilidad**

El firmware no proporciona ningún tipo de acceso de Shell, por lo que desde ese punto de vista parece seguro pero inmanejable desde la perspectiva del usuario.

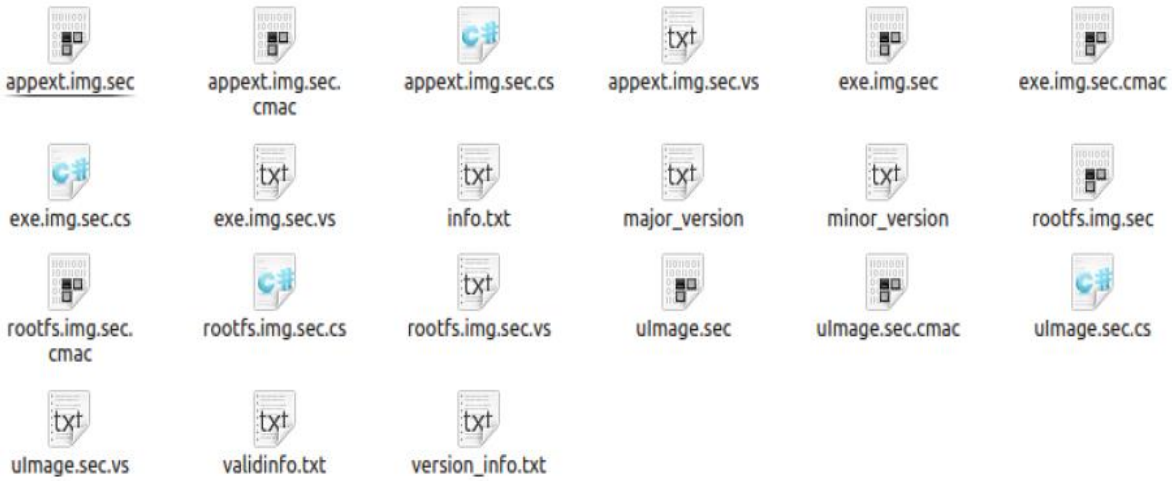
[33] Nikos Sidiroupoulos, Periklis Stefopoulos, Smart TV, University of Amsterdam, 2013

Pero, ¿qué sucede si puede modificar el firmware para obtener acceso root e instalarlo utilizando cualquiera de los procedimientos de actualización mencionados anteriormente? ¿Cómo previene Samsung que tal cosa suceda?

Todos los firmwares disponibles para descargar e instalar a través de USB están encriptados, pero no de la mejor manera posible. El método de cifrado {cifrado de dos capas: AES + XOR} se demostró deficiente. Un equipo de desarrollo de unos de los equipos de seguridad más importantes en el mercado de la seguridad como s es Samygo.tv ha creado una herramienta para descifrar / cifrar la mayoría de los firmwares de TV Samsung.

Además, para cada archivo en este paquete de actualización de firmware {actualización USB} también hay otro archivo que contiene **una firma cmac {figura 19 a continuación}.** Esta firma garantiza la integridad y autenticidad del firmware. Por lo tanto, el procedimiento de actualización USB del televisor requiere un firmware que esté firmado criptofiguradamente por Samsung.

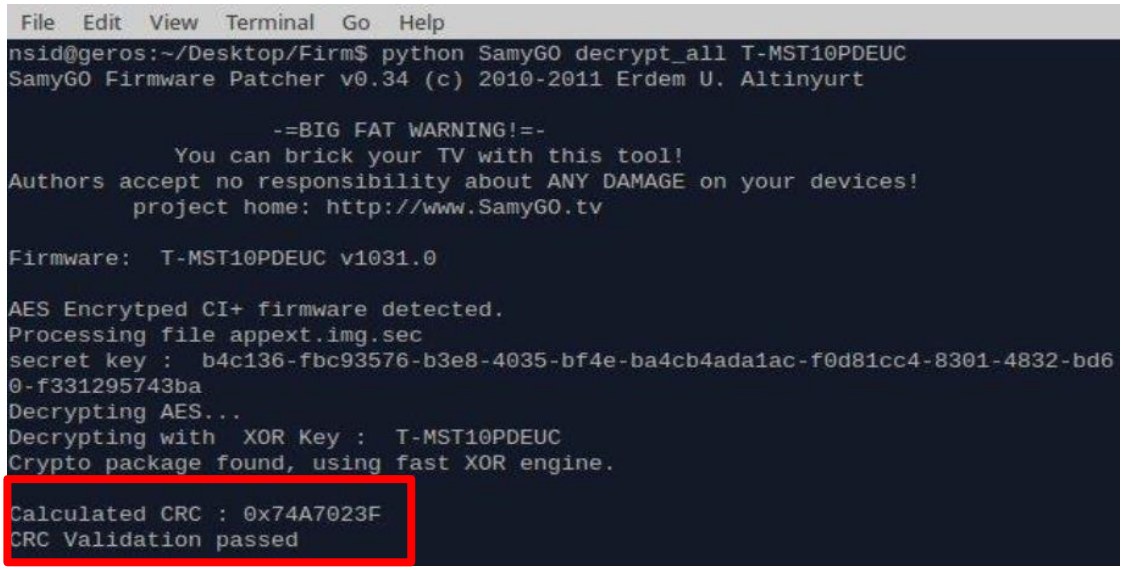
Figura 19 Archivos de la firma de Samsung




Fuente: Nikos Sidiropoulos Periklis Stefopoulos, 2013, Research Project 1 Smart TV Hacking

Usando SammyGoFirmwarePacher.py 5, se descifró el firmware y se derivaron los siguientes archivos. A continuación la figura 20 muestra cuales son los archivos logrados con el uso de la herramienta, se muestra que se ha pasado recuadro rojo el descifrado del dato.

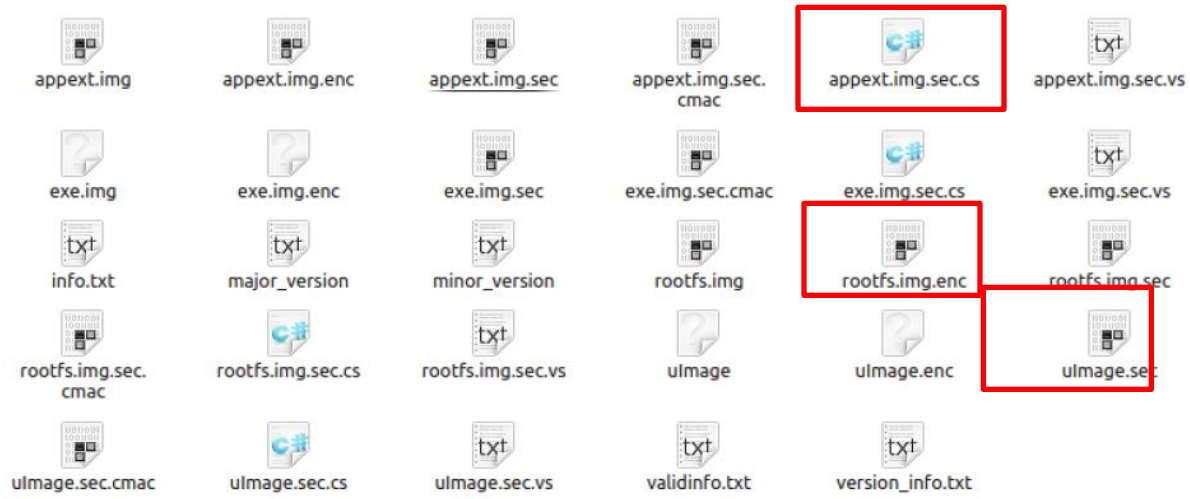
Figura 20 Uso de la herramienta SammyGoFirmware




Fuente: Nikos Sidiropoulos Periklis Stefopoulos, 2013, Research Project 1 Smart TV Hacking

Se muestran los archivos des encriptados con la herramienta. La figura 21 muestra como los archivos appext, rootfs y ulmage son archivos descifrados.

Figura 21 Archivos des encriptados




Fuente: Nikos Sidiropoulos Periklis Stefopoulos, 2013, Research Project 1

### 6.2.8 Smart Tv Hacking

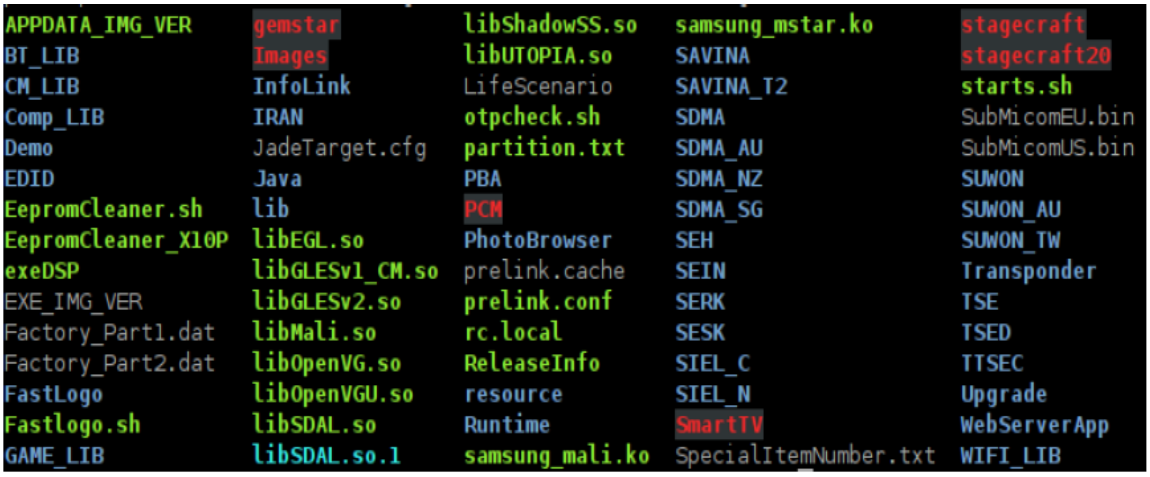
UImage es la imagen del núcleo basada en "VDLinux", mientras que rootfs.img y appext.img son el sistema de archivos y las imágenes auxiliares de datos / programas respectivamente. La imagen más importante es exe.img porque contiene el exeDSP, que es el ejecutable principal para ejecutar el procesador de señal digital {DSP}, como se muestra en la figura 22.

El siguiente paso fue montar esas imágenes e inspeccionarlas a fondo. Exe.img contiene rc.local que define el orden de arranque del sistema, así como los diferentes tipos de bibliotecas que se utilizan.

La carpeta WIFI_LIB contiene los controladores compatibles con el hardware Wifi, así como la herramienta iperf. Además, la carpeta Java tiene todas las bibliotecas Java compatibles. En la siguiente figura {Figura 23} también se puede ver toda la estructura del archivo exe.img (Nikos Sidiroupoulos, 2013) [34].

[34] Nikos Sidiropoulos Periklis Stefopoulos, 2013, Smart TV Hacking, Research Project 1

Figura. 22 Archivos de exe.img




Fuente: Nikos Sidiropoulos Periklis Stefopoulos, 2013, Research Project 1

Al montar rootfs.img fue posible ver la estructura completa del sistema de archivos. La mayoría de las carpetas son enlaces simbólicos que apuntan al área común de lectura / escritura {mtd_rwcommon}, que es el "entorno limitado" para las aplicaciones. Al explorar "/ etc /" podemos encontrar rc.local que revela todos los puntos de montaje.

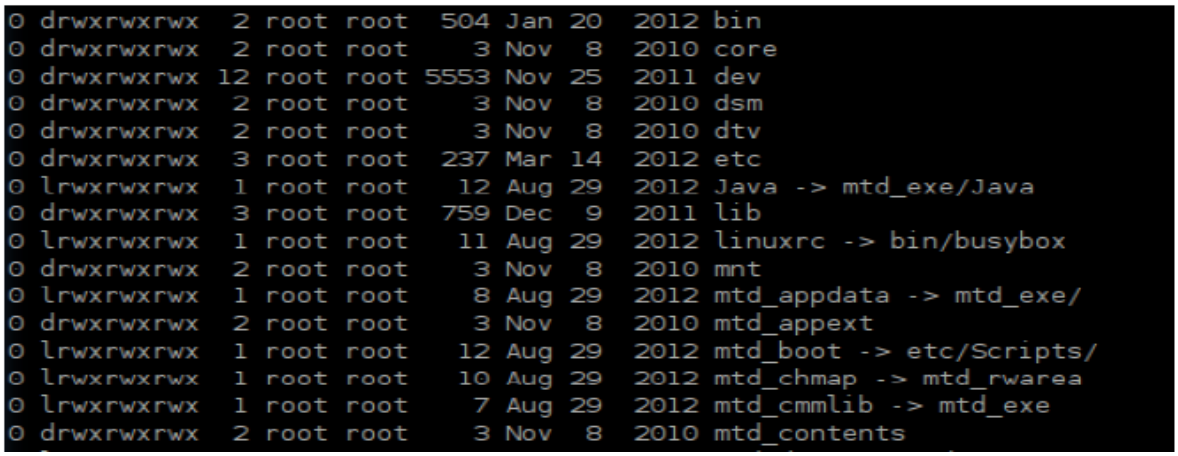
Figura 23 Archivo de ruta de /etc/rc.local

```
echo "================================================================
echo "  ROOTFS VERSION : "$ROOTFS_VERSION
echo "================================================================

# mount ramdisk
mount -n -t proc proc /proc
mount -n -t sysfs sysfs /sys
mount -t tmpfs tmpfs /dev/shm
mount -t tmpfs tmpfs /dtv -o size=40M,mode=1777
mount -t tmpfs tmpfs /tmp -o size=36M,mode=1777
mount -t tmpfs tmpfs /dsm -o size=12M,mode=1777
mount -t tmpfs tmpfs /core -o size=30M,mode=1777
```

Fuente: Nikos Sidiropoulos Periklis Stefopoulos, 2013, Research Project 1

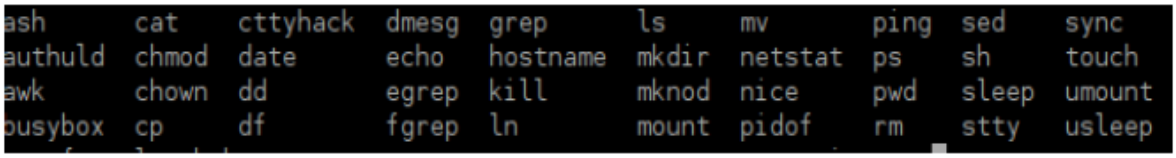
Figura 24 Ruta montada rootfs.img




Fuente: Nikos Sidiropoulos Periklis Stefopoulos, 2013, Research Project 1

Al investigar la carpeta "/ bin" nos permitió comprender qué tipos de comandos están disponibles. Todos estos comandos están vinculados {simbólicos} a busybox.

Figura 25 Carpeta /bin




Fuente: Nikos Sidiropoulos Periklis Stefopoulos, 2013, Research Project 1

Los archivos de firmware descargados mediante el procedimiento en línea no están firmados. Entonces, al descifrar, modificar y luego volver a cifrar el firmware, alguien puede actualizar fácilmente el firmware del televisor con su propia versión personalizada.

Sin embargo, crear una versión personalizada es muy peligroso, teniendo en cuenta la posibilidad de que su televisor Samsung sea "bloqueado". "Brick" es un

término utilizado por la comunidad de piratería cuando un dispositivo no está operativo debido a una falla de actualización de software. Suponiendo que el firmware personalizado se desarrolló correctamente, puede actualizar el televisor a través del procedimiento de actualización en línea.

Esto en conclusión hace referencia a la manipulación de los archivos del firmware pudiendo manipular bloqueos a gusto del atacante. Se da principalmente por la falencia en la fortaleza de los sistemas de cifrado de archivos de firmware (Nikos Sidiroupoulos, 2013) .

### 6.2.9 Ataque de Procedimiento

Basado en **Wireshark**, con la captura de tráfico del TV en su entorno, se encontró que el procedimiento de actualización en línea comienza con una conexión TLS / SSL con [www.samsungotn.net](http://www.samsungotn.net).

Figura 26 Certificado del sitio www.samsungotn.net


Fuente: Report smart tv hacking - Nikos Sidiropoulos Periklis Stefopoulos

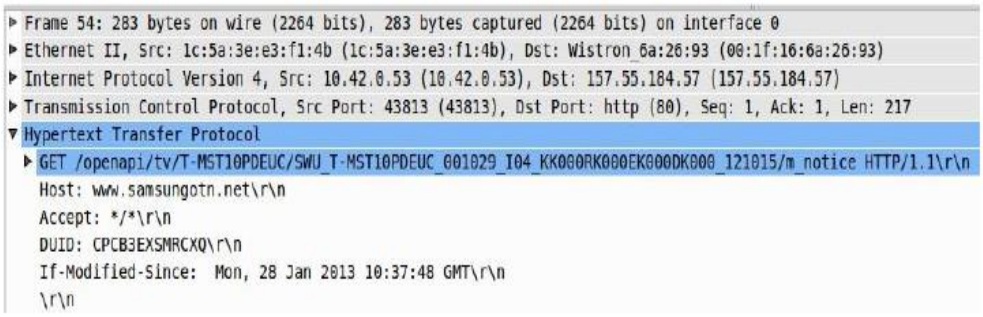
El certificado está firmado con la clave privada de Samsung Hubsite. Con Burp Suite, se realizó un ataque Man in The Middle {MiTM}, pero el televisor mostró un error de red debido a la denegación del certificado autofirmado de Burp Suite.

Figura 27 Certificado denegado


Fuente: Report smart tv hacking - Nikos Sidiropoulos Periklis Stefopoulos

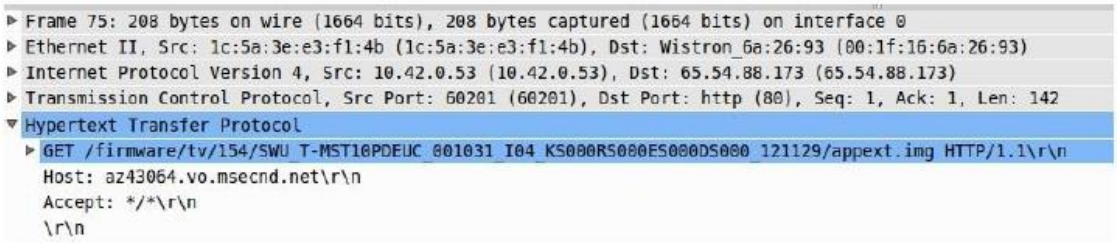
Al observar de cerca la comunicación capturada entre las dos entidades {Samsung TV - Samsung Web Server}, se descubrió que después de esta conexión HTTPS inicial con www.samsungotn.net, se estableció una conexión HTTP {no segura} con el mismo servidor web para verificar La disponibilidad de una nueva actualización {Figura 5}. Posteriormente, se estableció otra conexión HTTP con "az43064.vo.msecnd.net" para descargar realmente los archivos de firmware.

Figura 28 Chequeo de actualización de firmware inseguro




Fuente: Report smart tv hacking - Nikos Sidiropoulos Periklis Stefopoulos

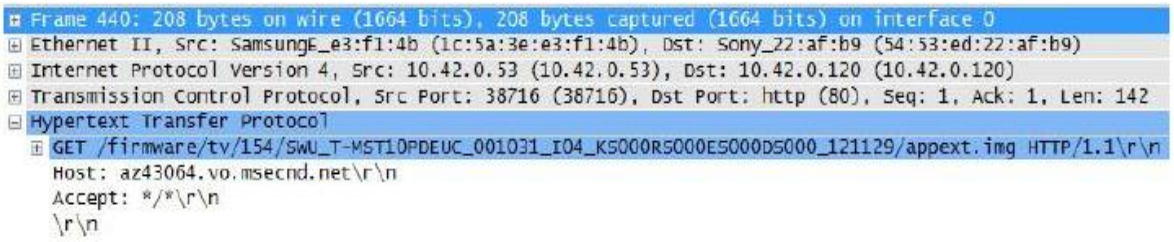
Figura 29 Firmware inseguro descargado




Fuente: Report smart tv hacking - Nikos Sidiropoulos Periklis Stefopoulos

Con base en los hechos anteriores, agregamos una entrada DNS estática al archivo "hosts" para reenviar la solicitud HTTP GET a un servidor web local, que se ejecuta en la otra computadora portátil, en lugar del servidor web de actualización de Samsung {az43064.vo.msecnd}. Además, al usar el enlace de descarga6 proporcionado por el archivo capturado de Wireshark, se descargó el primer archivo {appext.img} necesario para el proceso de actualización. Lo único que faltaba era probar si el procedimiento de descarga aceptaría el archivo proporcionado por nuestro servidor web Apache. Como se esperaba, el archivo fue aceptado con éxito.

Figura 30 Servidor local actualizado




Fuente: Report smart tv hacking - Nikos Sidiropoulos Periklis Stefopoulos

Figura 31 Firmware local descargando


Fuente: Report smart tv hacking - Nikos Sidiropoulos Periklis Stefopoulos

### 6.2.10 Ataque del navegador

**Importancia del navegador**

Los navegadores son las aplicaciones fundamentales que cualquier sistema operativo "inteligente" puede proporcionar, teniendo en cuenta que la terminología inteligente deriva del hecho de que interactúa con Internet. Por otro lado, la mayoría de los servicios que proporcionan los navegadores web {para Smart OS} han sido reemplazados por las aplicaciones en términos de velocidad y facilidad de uso. Samsung Apps {tienda} aún se encuentra en una etapa temprana de desarrollo y faltan aplicaciones populares o existen con una funcionalidad limitada. Por lo tanto, la mayor parte de la interacción con Internet debe hacerse a través del navegador y con la facilidad que proporciona un teclado / mouse USB.
Sobre el navegador

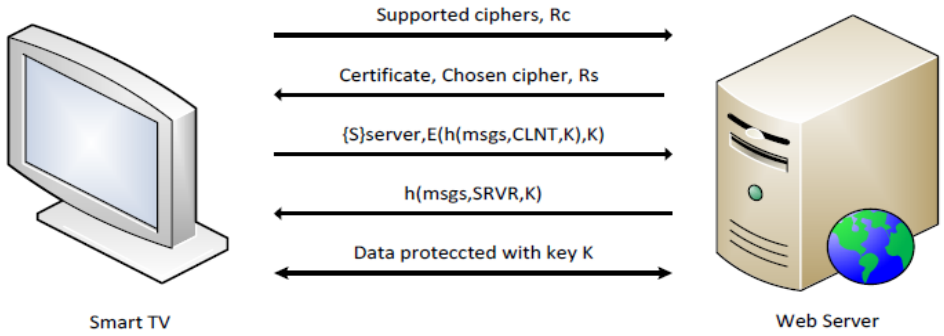
El navegador se basa en una versión desactualizada de Firefox {versión 5, basada en cadenas de usuario} y admite extensiones básicas como Java, flash y también puede administrar cookies. Además, es compatible con SSL / TLS sobre HTTP.

**Fondo SSL / TLS**

SSL está diseñado para ejecutarse en la parte superior de la capa 4 y proporciona una conexión TCP confiable, encriptada y protegida con integridad a la aplicación. La operación principal se describe a continuación:

- El cliente se pone en contacto con el servidor, entrega la lista de algoritmos criptográficos compatibles y un número aleatorio Rc.
- El servidor envía su certificado, más el algoritmo más alto que ambos admiten y también un número aleatorio Rs.
- Si el cliente acepta {confía} el certificado {contiene la clave pública del servidor}, el cliente elige un número aleatorio S y lo cifra utilizando la clave pública. Junto con el número aleatorio cifrado S, el cliente también envía un hash codificado cifrado, del secreto maestro K = h {S, Rc, Rs} y los mensajes de saludo.
- El servidor demuestra que conoce las claves de sesión y asegura que los mensajes anteriores llegaron intactos enviando un hash con clave de todos los mensajes anteriores más el secreto maestro K.
- La conexión se establece y protege con la clave maestra K hasta que la sesión es terminado.

Figura 32 Protocolos TLS/SSL

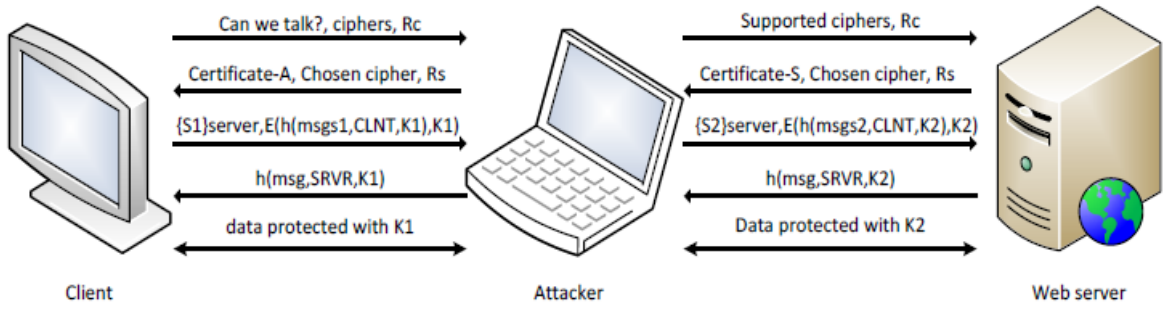



Fuente: Report smart tv hacking - Nikos Sidiropoulos Periklis Stefopoulos

### 6.2.11 Ataque el hombre en el medio {MiTM}

El ataque más común para el SSL es el ataque Man in the Middle. Se describe el método en la siguiente figura:

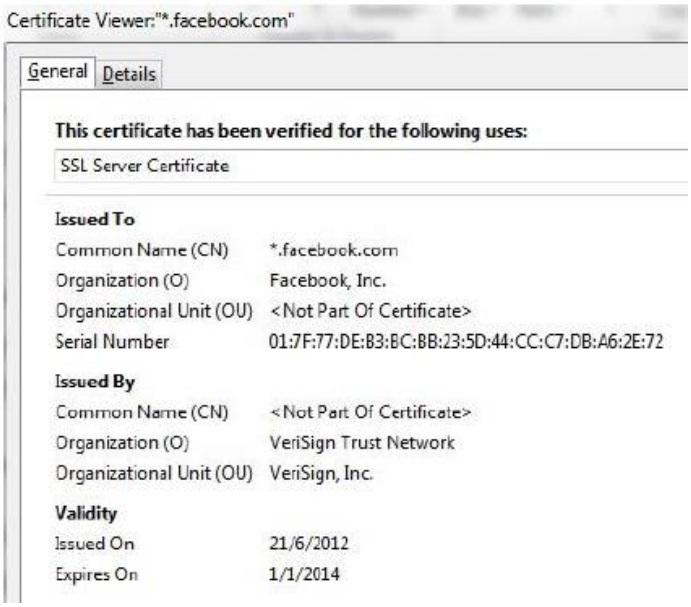
Figura 33 TSL/SSL MiTM




Fuente: Report smart tv hacking - Nikos Sidiropoulos Periklis Stefopoulos

El cliente establece una conexión SSL con el atacante, utilizando la clave maestra K1. El certificado es aceptado por el cliente. Mientras tanto, el atacante establece una conexión SSL para el servidor que el cliente tiene intención de conectar utilizando una clave maestra K2. Ahora, el atacante puede leer o modificar cualquier conversación intercambiada entre el cliente y el servidor. Este tipo de ataque se puede evitar verificando automáticamente la validez del certificado. Si este no es el caso, siempre se debe preguntar al usuario si el certificado debe ser confiable o no.

Figura 34 Ejemplo del Certificado




Fuente: Report smart tv hacking - Nikos Sidiropoulos Periklis Stefopoulos

Un certificado de servidor SSL contiene la clave pública del servidor, el nombre común del servidor, el día de inicio de la validez y el día de vencimiento, todos firmados por una Autoridad de Certificación. Un navegador común tiene certificados preinstalados de autoridades de certificación confiables para verificar la validez de cualquier certificado dado. Además, verifica si el dominio solicitado coincide con el CN para el que se firmó el certificado y también verifica si la duración de la validez del certificado coincide con la hora local.

**Procedimiento de ataque {SSL MiTM}**

Para aplicar dicho ataque MiTM, se utilizó un servidor proxy {Burp Suite} con un certificado autofirmado. Como se muestra, la computadora portátil Samsung desempeña el papel de un enrutador. Mediante configuración de iptables7 paquetes cuya IP de origen es igual a la IP del televisor y cuyo puerto de destino es igual a "443" se reenvían al puerto 8080, en "eth0" que escucha Burp Suite.

Como parte del complemento que desea este documento dejar al lector están una serie de aspectos que aunque no con a veces vulnerabilidades técnicas 100%, si son vulnerabilidades por malas prácticas que se dejan implementadas en ocasiones al interior de las empresas cuando se usan estos dispositivos. A continuación, se muestran los peligros más comunes cuando se usan los Smart TV.

## 6.3 VULNERABILIDADES DE LOS SMART TV HOY EN DÍA.

Teniendo en cuenta los ataques sufridos por estos dispositivos Smart TV en los últimos años en primera instancia, comprobando que los sistemas operativos atacados en los años 2019 y 2020 fueron versiones NO muy lejanas de las versiones actuales de los Smart TV que se venden hoy en día en el 2021 como dato complementario del análisis, y finalmente desde lo técnico, que los protocolos de comunicación y las tecnologías que se usan para las actividades más comunes como son: actualizarse automáticamente {si está configurado así}, conectarse a internet, generar actualizaciones de las aplicaciones complementarias, almacenar datos y conectarse con hábitos que los humanos tenemos como es despertarnos, apagarse, colocar música según nuestro estado de ánimo entre otras muchas actividades que pueden realizar; siguen siendo las mismas, es muy posible que las vulnerabilidades aprovechadas en aquellos ataques sigan siendo hoy en día un permanente punto de peligro para nuevos ataques.

Basados en estos análisis podremos demostrar que las vulnerabilidades aprovechadas en aquellos ataques siguen siendo hoy en día un punto importante para poder construir nuestro MODELO DE ASEGURAMIENTO para Smart TV contra ataques cibernéticos para los usuarios de estos equipos del grupo IoT.

Pero antes de poder realizar este análisis o identificación de las vulnerabilidades actuales como objetivo central de este capítulo, es importante mencionar o comentar cuales son en general los peligros más importantes a los que se ven expuestos los Smart Tv para que sean un blanco vulnerable de ataques informáticos.

### 6.3.1 Peligros más comunes en Smart TV Sin protección

#### 6.3.1.1 Smart TV sin protección

Las Smart TV son susceptibles también de tener malware. Fabricantes como Samsung incorporan en ellas un antivirus, pero hay otros que no lo hacen, por lo que no comprueban si hay malware instalado. Por ello, es recomendable actualizar tanto el sistema operativo del televisor como las aplicaciones que hay instaladas.

#### 6.3.1.2 Acceso a otros dispositivos conectados en la misma red

Uno de los mayores peligros de tener un televisor conectado a nuestra red local es que un malware puede saltar a otros dispositivos que tengamos conectados en el hogar, ya que hay vulnerabilidades que le permiten transmitirse a otros dispositivos por red. Por ello, un malware que se cuele en el televisor puede descargar contenido malicioso en el router, el NAS, o en el mismo ordenador (Alberto, 2019)[35].

#### 6.3.1.3 Robo de datos

Como se mencionó, en el televisor al loguearse {digitar usuario y clave} en aplicaciones para ver contenido en directo, series, música, etc. Por lo anterior una

[35] García Alberto, 2019, Adlzone.net, Estos son los 5 peligros a los que está expuesta tu Smart TV.,

mala protección dejaría el dispositivo expuesto al robo de credenciales si el dispositivo carece de las configuraciones adecuadas. Esto es peor aún si se reutilizan claves con otros aplicativos o servicios, podrían ser hackeadas otras cuentas.

#### 6.3.1.4 Espiar por la cámara o el micrófono

La incorporación de micrófonos en los dispositivos SMART VT hoy en día y también cámaras para realizar video llamadas, genera un vector de ataque para un hacker, éste puede tomar el control de ambos elementos, ya que pueden espiar nuestras conversaciones o incluso grabarnos en nuestra intimidad.

#### 6.3.1.5 Minar criptomonedas

El último vector de ataque hace que los Smart TV puedan ser utilizados para minar criptomonedas. Aunque incorporan procesadores ARM que consumen poco, estos chips son cada vez más potentes. Si a este escenario le adicionamos que los usuarios no podemos de manera sencilla saber el consumo de recursos de la CPU de nuestro televisor, a no ser que tengamos la información técnica lo cual muy pocos o casi nadie lo sabe, el atacante puede estar aprovechando los recursos de hardware sin que nos demos cuenta (Alberto, 2019) [36].

Como se ve no solo las vulnerabilidades son parte fundamental de los ataques, sino también acciones que vienen de fábrica y que son ajenas al usuario, otras directamente responsabilidad el usuario como lo es la gestión efectiva de actualizaciones de los programas y los sistemas operativos, que son medidas que todo fabricante pone a disposición de sus usuarios, y finalmente malas prácticas de parte de los usuarios como lo es el uso de contraseñas genéricas para todas las aplicaciones y que son fáciles de adivinar o de intuir. La seguridad hoy en día

[36] García Alberto, 2019, Adlzone.net, Estos son los 5 peligros a los que está expuesta tu Smart TV

está dada por las vulnerabilidades de tipo técnico y las que se ajustan a las malas prácticas de los usuarios de los sistemas de información en estos Smart TV.

Para tener presente cuales son las vulnerabilidades que se evidenciaron en los ataques anteriormente descritos, y que son elemento de comparación para confirmar la existencia de las mismas hoy en día, se muestra a continuación una tabla resumen de estas vulnerabilidades.

Tabla 1 Vulnerabilidades identificadas en ataques

| Ataques | Vulnerabilidad | Descripción |
|---|---|---|
| Ataque a las particiones de almacenamiento | Identificación de rutas | Usan herramientas como kali Linux con unos llamados decrypters, y conociendo rutas por defecto acceden a los archivos basados en el conocimiento de estas rutas. Buscan rutas del Sistema |
| | Descifrado de archivos | Descifran los archivos del sistema, aprovechando una debilidad en sus algoritmos en versiones anteriores al 2020 |
| Ataque DirtyCOW | Descubrimiento de código | Ataque protocolo upnpd Buffer Over Flow. Se chequea el código del Kernel del sistema, al lograr leerlo se pasa un parámetro escrito que quedará implantado en el sistema, por la función pte_write, la cual está habilitada por defecto. Y se ubican rutas del sistema basado en LINUX, /shadow y pasando como parámetro la ruta del archivo, /bin/.sh se logra ver las credenciales del root del sistema. |
| | Descubrimiento de rutas | Después se accede por comandos al TV y se testea si en la ruta /home/root/.ssh existe el archivo FOD que contiene el código temporal |

| | | |
|---|---|---|
| Ataque de MiTM Man in the Middle | Interceptación de tráfico | Se generan escaneos de los datos que están pasando por las conexiones con el Smart TV, ya sea por cable o inalámbrico. |
| | Hombre en el Medio | Interceptación de tráfico y manipulación del mismo entre el Smart TV y el usuario. |
| Ataque de Adopción de TLS | Protocolo Transport Layer Security TLS Vulnerable | Por los problemas e validación del protocolo se pueden rastrear los contenidos de las comunicaciones en las conexiones. Con esto robar las credenciales de las conexiones. |
| Ataque a vulnerabilidades de XML y XXE | Protocolo Extensible Markup Language {XML} | Cuando un analizador XML procesa dicho documento, primero lee las entidades en el prólogo XML. Luego, se resuelve todas las ocurrencias de la entidad en el documento: & title; es reemplazado con un archivo de configuración de texto y & ext; se reemplaza con el contenido del archivo: ///text.txt. Esto es muy peligroso ya que si un atacante controla el contenido de los archivos XML procesados podría inyectar los que desee. |
| Ataque de Autorización delegada | Parámetro OAuth | Se ataca este parámetro que es el que otorga derechos sobre los recursos del SmartTV, y esto es aprovechado para ganar acceso a los recursos del sistema dominando el Smart Completo. |
| Ataques al Firmware del TV | Firmware de los SmartTV | Todos los firmwares disponibles para descargar e instalar a través de USB están encriptados, pero no de la mejor manera posible. El método de cifrado {cifrado de dos capas: AES + XOR} se demostró deficiente |

| | | |
|---|---|---|
| Ataque de Procedimiento | Procedimiento de actualización del sistema con conexión TLS insegura | Se usa ataques de hombre en el medio y escaneo del tráfico del Smart TV cuando está actualizando el sistema, la vulnerabilidad está en que se permitía descartar archivos por una conexión NO SEGURA que se generaba después de validar el certificado SSL del sitio de Samsung. Todo escaneando las comunicaciones, lo cual podría hacer que se inyecte o descargue en el server archivos maliciosos o shells malignas. |
| Ataque del navegador | • Desarrollos tempranos de parte de fabricantes.<br>• Funcionalidad limitada.<br>• Compatibilidad de protocolos vulnerables de cifrado de las comunicaciones como TLS/SSL sobre Http. | Son ataques que aprovechan las vulnerabilidades de fabrica de los navegadores como el de Samsung que se basaba en una versión vieja de Firefox como es la versión 5 para su implementación en sus sistema operativo para los Smart TV. Adicionalmente el uso de protocolos de comunicaciones o de cifrado obsoletos o con soporte para versiones vulnerables como lo es la versión 1.0 y 1.1 de TLS sobre Http. |

Para dar solución a este punto del documento es preciso identificar desde los fabricantes, pasando por los críticos e investigadores y los portales especializados, cuales son estas medidas de seguridad que se han identificado,

se han enunciado por los fabricantes y que son en realidad implementadas en las versiones nuevas a partir de la 5.0 hasta la fecha que existen las versiones 6.0 de cada uno de los sistemas de los Smart TV Samsung y LG.

Inicia el análisis identificando qué versiones están hoy en día implementadas en las versiones nuevas que vienen con los televisores a partir del último trimestre del 202 a la fecha.

Teniendo en cuenta que la última versión de WEB OS [37] de LG es la 6.0 y de TZEN [38] en Samsung es la 6.0 igualmente lanzada para el año actual 2021, analizaremos las aplicaciones que están siendo involucradas en estos sistemas y se podrán verificar que estas aún son o pueden ser de versiones vulnerables.

Hoy en día sigue la preocupación de que el sistema operativo de los Smart TV sean blancos de más ataques ya que desde el 2017 cuando varios sitios dieron a conocer que el sistema Tizen de Samsun tenía muchas vulnerabilidades y que según un investigador llamado Amihai Neiderman, quien en ese año dijo que era prácticamente el peor desarrollo que había visto en la vida. [39]
Esto es preocupante ya que los sistemas Tizen no solo están en Smart Tv sino en relojes y otros elementos IoT de Samsung. Hoy en día ya es muy disiente que Samsung esté pensando en cambiar su sistema operativo Tizen y haya iniciado por los relojes inteligentes, como se comenta en un post de un portal importante llamado hipertextual.com, donde expresa que en estos elementos se usara WEAR OS en lugar de TIZEN.[40]

---

[37] ADLZONE, García Rocío, marzo 2021, https://www.adslzone.net/reportajes/tecnologia/sistema-operativo-smart-tv/
[38] TZEN 6.0 public reléase, TZEN organization, https://www.tizen.org/blogs/bighoya/2020/tizen-6.0-public-m2-release-0
[39] Kaspersky, Smart TV tiene 40 vulnerabilidades nuevas, 2017 abril, https://www.kaspersky.es/blog/tizen-40-bugs/10336/
[40] Hipertextual.com, Márquez Javier, Abril 1 de 2021, https://hipertextual.com/2021/04/nuevo-samsung-galaxy-watch-usara-wear-os-en-lugar-de-tizen

Sobre la seguridad de Tizen y de WebOS no se habla mucho pero es evidente que investigaciones realizadas por especialistas como Pablo San Emeterio que es un research de ElevenPaths una empresa muy reconocida en España, dice que los Smart TV aun en el 2020 “Normalmente suelen venir con versiones antiguas, tanto su sistema operativo como sus navegadores, y en realidad son aparatos que no están pensados para estar conectados a internet, y al conectarlos empiezan a salir problemas”, esto es algo preocupante desde la perspectiva de que se encontrará en el 2021. [41]

Hacia finales del 2020 el investigador Rafael Sheel dice que “el 90% de los televisores inteligentes podrían ser ‘hackeados’ aun sin que el ciber atacante tenga acceso físico al dispositivo. A menudo, tienen navegadores normales y sistemas operativos basados en Linux. Por lo tanto, los televisores inteligentes se ven afectados por los mismos problemas que los ordenadores, pero generalmente ofrecen una protección menor y tardan más en actualizarse con parches de seguridad”. [42]

Es un porcentaje muy alto para ser curado en el 2021, por lo cual e identificando qué vulnerabilidades están hoy en día vigentes las siguientes líneas detallan en las versiones actuales después del 2020 cuales son las vulnerabilidades que persisten y que son las que vamos a incluir en las buenas prácticas y las actividades técnicas que se deben ejecutar en el modelo de seguridad que se diseñará para que sean implementados por los usuarios e ingenieros en las empresas hoy en día y que serán útiles en el sentido de que serán muchos los ataques bloqueados.

[41] PRODATOS, Aznar Raúl, abril 17 2020, https://www.prodatosalcarria.es/comprar-una-smart-tv-es-una-idea-horrible-el-90-se-pueden-secuestrar-a-distancia/
[42] PRODATOS, Aznar Raúl, abril 17 2020, https://www.prodatosalcarria.es/comprar-una-smart-tv-es-una-idea-horrible-el-90-se-pueden-secuestrar-a-distancia/

Adicionalmente se menciona los esquemas de seguridad que se han implementado a la fecha y que ayudan a que los sistemas Tizen y WebOS sean a la fecha más seguros que desde las versiones anteriores como la 4.5 o la 4.0.

Samsung ha implementado seguridad frente a los virus o malware en general, algo que es importante ya que este tipo de ataques es muy usado hoy en día, infectar los sistemas operativos es la clave de muchos ataques específicos y las medidas implementadas son a nivel de la plataforma o Sistema Operativo, las aplicaciones y el hardware.

**A nivel de plataforma están:**

- Cifrado preventivo de claves y usuarios antes de su almacenamiento. Esto mitiga ataques de MinTheMiddle y de esnifeo de data que corre vía wifi u otros medios.
- Bloqueo de códigos no autorizados al acceder a las configuraciones de la plataforma, usan teclado seguro o virtual.

**A nivel de Aplicaciones:**

- Bloqueo de sitios de fishing.
- Detecciones de sitios emisores de software malicioso.
- Herramienta de seguridad a nivel de NAVEGADORES, detectores de sitios emisores de malware.
- Antimalware inmerso en el sistema.

**A nivel de hardware:**

- Separación de espacios físicos del hardware en los Chips del software central o los procesos del Sistema Operativo. [ [43]]

[43] News.samsung.com, Conozca cómo Samsung protege sus SmartTV sw Virus, Ago 18 2019, https://news.samsung.com/co/conozca-como-samsung-protege-sus-smart-tvs-de-virus

Por su lado LG con su sistema WebOS no solo ha implementado esquemas de diseños nuevos sino de seguridad, y ha determinado que expandirá el acceso de su código a otras marcas o fabricantes de Smart TV y esto abre la posibilidad de mejorar el código que ha sido desde 2017 una de las causas de que sea clasificado como uno de los sistemas más inseguros de la actualidad. [ [44]]

**Entre las medidas de seguridad que WebOS Ha Implementado están**:
Seguridad en canales y aplicaciones, incorporando seguridad activa con implementación de PIN para entrar o activas estas funciones. Con esta medida que es prácticamente un doble factor se evitan accesos no autorizados a estas funciones de gestión del Smart TV. [[45]] [[46]]

Si se mira el S.O. Tizen con relación al Kernel del sistema que fue atacado, este estaba en la versión 3.0 o 3.5 y el sistema actual del TIZEN tiene Kernel for Raspberry Pi 4 has been upgraded to versión 5.4.50. Por lo cual la vulnerabilidad fue curada con la actualización según datos del fabricante.

El análisis realizado frente a las vulnerabilidades identificadas en los ataques entre el 2018 y 2020 nos deja como vulnerabilidades saneadas o solucionadas desde lo técnico un conjunto de mejoras en los sistemas operativos desde fabrica y que sin ser la única fuente de acciones de mejora, son importantes para la seguridad actual de estos dispositivos, por lo cual tomando la tabla de vulnerabilidades aprovechadas en los ataques desde el 2018 al 2020, podemos dejar como vulnerabilidades solucionadas las siguientes.

---

[44] LG Lleva su sistema WebOS a troas fabricantes, García Alberto, febrero 2021, https://www.adslzone.net/noticias/streaming-tv/powered-by-webos-lg-licencia-smart-tv/
[45] LG con WebOS trucos y funciones para tu Smart TV, Fernández Yubal, Junio 2020, https://www.xataka.com/basics/lg-webos-trucos-funciones-para-tu-smart-tv
[46] WebOS opciones de Seguridad, febrero 2021, LG Corp, https://www.lg.com/es/posventa/microsites/television/webos-2-opciones-seguridad-bloqueo-programas-canales

Tabla 2 Vulnerabilidades mitigadas al 2021| en los sistemas actuales

| Control Actual | Vulnerabilidad Solucionada | Descripción de la Solución | Mitiga Ataques |
|---|---|---|---|
| PIN Para accesos a aplicaciones y la plataforma. | Ataque a las particiones de almacenamiento e Identificación de rutas y descifrado de archivos. | Para acceder a la plataforma a las configuraciones y a aplicaciones se requiere de un PIN asignado por el sistema y validado para cada usuario. | De Descubrimiento de rutas ya que las configuraciones están validadas por un PIN requerido, Un ataque automatizado no daría resultado. |
| Cifrado preventivo de claves y usuarios antes de su almacenamiento | Ataque de MiTM Man in the Middle | Al entrar a la configuración se necesita usuario y clave, así mismo al conectarse a sitios de descarga con la cuenta del dueño, se toman las claves y usuarios y se cifran antes de almacenarse y luego se almacenan en sitios alternos. | Espionaje y captura de tráfico. Interceptación de tráfico cuando el Smart TV se comunica hacia el exterior o con otros dispositivos. Robo de claves y de información confidencial. |
| Bloqueo de códigos no autorizados al acceder a las configuraciones | Infección de malware | Cuando se van a acceder a configuraciones el sistema instala bloqueos de | Infecciones o inyecciones de malware para combinarlo con otro tipo de ataques, |

| | | | |
|---|---|---|---|
| de la plataforma, usan teclado seguro o virtual | | identificación de malware | ejemplo propagaciones a otros dispositivos, espionaje y activación de elementos del Smart TV como Micrófono y Cámara. |
| Bloqueo de sitios de fishing | Infección de malware, robo de datos financieros, robo de dinero | El sistema tiene implementado un sistema de detección de malware o de sitios fraudulentos basados en una base de datos específica, igual que los antimalware por firmas o por relacionamiento de características y comportamiento. | Infección de Malware<br>Robo de data financiera<br>Robo dinero. |
| Herramienta de seguridad a nivel de NAVEGADORES. | Infección de malware | Implementaron detectores de sitios emisores de malware. | Infecciones de malware, robo de datos, inyección de código malicioso |
| Separación de espacios físicos del hardware | Accesos no autorizados | Separación del espacio físico en los chips de procesamiento y de | Inyección de código malicioso y descifrado de datos |

| | | | |
|---|---|---|---|
| en los Chips del software central | | memoria de la gestión del software del sistema operativo en sus procesos, con esto hasta que no sea necesario no hay interacción en el chip, BIOS o Almacenamiento del Firmware. | del sistema o archivos del sistema. |
| VPN para conectividad [47] | Accesos no autorizados | Se pueden implementar esquemas de conectividad segura de manera remota con servicios VPN Virtual Private Network | Accesos no autorizados al sistema desde la red local o red externa. |
| Seguridad en canales y aplicaciones, incorporando seguridad activa con implementación de PIN | Accesos no autorizados a configuraciones del sistema | Se debe implementar y digitar un PIN enviado al usuario del sistema para desbloquear los accesos a las configuraciones del Smart TV y a las aplicaciones. | Infecciones de malware y accesos no autorizados a los esquemas de configuración del sistema. |
| | | | |

[47] Configura una VPN en tu Smart TV para evadir bloqueos regionales, Lorenzo José Antonio, Agosto 2020, https://www.redeszone.net/tutoriales/vpn/configurar-vpn-smart-tv/

En conclusión, al haber una serie de acciones de mejora y mitigación que han tomado los fabricantes, a continuación, mencionamos las vulnerabilidades que son importante dejar identificadas como vigentes.

Tabla 3 Vulnerabilidades vigentes en sistemas Smart TV Samsung y LG

| Vulnerabilidad Vigente | Ataque | Impacto y Probabilidad del Ataque |
|---|---|---|
| Versionamiento del protocolo TLS/SSL en las comunicaciones externas | Ataque de Procedimiento de actualización del sistema con conexión TLS insegura | Aún es posible que, por la versión del protocolo de cifrado de las comunicaciones hacia internet en las actualizaciones del sistema o las conexiones con otros dispositivos, se pueden hacer ataques de descifrado del protocolo o de las llaves usadas ya que este protocolo por defecto aún está vigente en la |
| Descubrimiento de código y Descubrimiento de rutas | Ataque DirtyCOW | Al no tener evidencias actuales de los archivos del sistema de los sistemas operativos, los cuales todos son basados en LINUX como Kernel principal, y teniendo en cuenta que sus rutas de archivos del sistema siguen siendo las mismas, esta vulnerabilidad sigue vigente, y más cuando se han evidenciado que sistemas operativos como WebOS no son desarrollos precisamente seguros. |

| | | |
|---|---|---|
| Protocolo Extensible Markup Language {XML} | Ataque a vulnerabilidades de XML y XXE | Igualmente, que se menciona en la vulnerabilidad anterior, al no tener evidencias técnicas de la solución del uso o Versionamiento en el uso de estos protocolos basados en lenguajes esta vulnerabilidad sigue vigente y es muy probable que se sigan presentando este tipo de ataques. |
| | | |

## 6.4 MODELO DE SEGURIDAD PARA DEFENSA DE DISPOSITIVOS IOT SMART TV EN MARCAS SAMSUNG Y LG

### 6.4.1 Qué es el Modelo Básico de Aseguramiento para Smart TV.

Un modelo básico de aseguramiento para dispositivos Smart TV, como plan de defensa ante ataques informáticos en las empresas, es un conjunto de actividades tanto técnicas como de buenas prácticas que alineadas a un estándar de seguridad y basado en un Checklist para cada tipo de dispositivo, son la solución a implementar por ingenieros en las empresas en Colombia.

Uno de los objetivos específicos del MODELO propuesto es la mitigación de todos los ataques BÁSICOS que se presentan en la actualidad y que usan técnicas de escaneo de puertos, identificación de configuraciones por defecto o aprovechamiento de aplicaciones y servicios vulnerables al no tener un versionamiento actualizado.

El elemento central del Modelo de Defensa contra ataques a Dispositivos IoT aplicado a Smart TV, es un Checklist, el cual se propone aplicar en cada uno de los Smart TV que la empresa tenga. Este conjunto de acciones o actividades tanto técnicas como procedimentales son la LINEA BASE de la seguridad que las empresas implementarán en su infraestructura involucrando a los Smart TV como equipos o activos importantes dentro de la seguridad informática de las mismas.

Cabe anotar que este Checklist aplica a cualquier Smart TV marca Samsung o LG y está compuesto por actividades de buenas prácticas alineadas a controles de la ISO 27002 y acciones técnicas en cada uno de los sistemas operativos de estas marcas.

### 6.4.2. Checklist de Verificación de Seguridad en los Smart TV

Al ser este proceso de verificación una actividad de implementación básica de los controles mínimos que deben quedar implementados para cada uno de los activos Smart TV y que inicialmente están alineados a la ISO 27001 como estándar de seguridad, la siguiente tabla deja referenciados los controles que a la luz de la ISO 27001 se deben tener en cuenta.

Es preciso anotar que estos controles hacen referencia a aspectos básicos que tienen directa relación con lo que en primera instancia todo profesional encargado dentro de la empresa de la seguridad de los dispositivos IoT aplicará inicialmente.

Tabla 4 Checklist de controles para configuración segura de SMART TV alineados a ISO 27001

| **El análisis de controles en dispositivos IoT Smart TV: estado de aplicación de ISO 27001** | |
|---|---|
| **ISO 27001 cláusulas** | **Requisito obligatorio para el SGSI** |
| **5** | **Políticas de Seguridad de la Información** |
| **5,1** | **Directrices Establecidas Por La Dirección Para La Seguridad De La Información** |
| 5,1 | Brindar desde la dirección, apoya permanente para la seguridad de la información, basado en los requerimientos del negocio, las leyes y reglamentos pertinentes. |
| 5.1.1. | Política de seguridad de la información |
| 5.1.2. | Revisión de las políticas para la seguridad de la información. |
| **6** | **Organización De La Seguridad De La Información** |
| 6.1. | ORGANIZACIÓN INTERNA |

| | |
|---|---|
| 6.1.1. | Roles y responsabilidades para la seguridad de la información |
| 6.1.2. | Segregación de Funciones |
| **7** | **Seguridad En El Recurso Humano** |
| **7.2.** | **Durante La Ejecución Del Empleo** |
| 7.2.2. | Toma de conciencia, educación y formación en la seguridad de la información |
| **8** | **Gestión De Activos** |
| **8.1.** | **Responsabilidad Por Los Activos** |
| 8.1.1. | Inventario de Activos |
| 8.1.2. | Propiedad de los Activos |
| **9** | **Control De Acceso** |
| **9.1.** | **Requisitos Del Negocio Para Control De Acceso** |
| 9.1.2. | Acceso a redes y servicios de red |
| | |
| **9.2.** | **Gestión De Acceso A Usuarios** |
| 9.2.1. | Registro y cancelación de registro de usuarios |
| 9.2.2. | Suministro de acceso a usuarios |
| **9.4.** | **Control De Acceso A Sistemas Y Aplicaciones** |
| 9.4.1. | Restricción de acceso a la información |
| 9.4.2. | Procedimiento de Acceso {LOG ON} |
| **11** | **Seguridad Física Y Del Entorno** |
| **11.2.** | **Equipos** |
| 11.2.1. | Ubicación y protección de los equipos |
| 11.2.4. | Mantenimiento de los equipos |
| 11.2.6. | Seguridad de equipos y activos fuera de las instalaciones |
| **12** | **Seguridad De Las Operaciones** |
| **12.1.** | **Procedimientos Operacionales Y Responsabilidades** |

| | |
|---|---|
| 12.1.1. | Procedimientos de operación documentados |
| **12.2.** | **Protección Contra Código Malicioso** |
| 12.2.1. | Controles contra códigos maliciosos |
| **12.5.** | **Control De Software Operacional** |
| 12.5.1. | Instalación de software en sistemas operativos |
| **12.6.** | **Gestión De La Vulnerabilidad Técnica** |
| 12.6.1. | Gestión de vulnerabilidades técnicas |
| **13** | **Seguridad De Las Comunicaciones** |
| **13.1.** | **Gestión De La Seguridad De Las Redes** |
| 13.1.2. | Seguridad de los servicios de red |
| 13.1.3. | Separación de redes |
| **14** | **Adquisición, Desarrollo Y Mantenimiento de Sistemas** |
| **14.2.** | **Gestión De Seguridad En Los Procesos De Desarrollo Y Soporte** |
| 14.2.8. | Pruebas de Seguridad de Sistemas |

Los aspectos que directamente están relacionados con procedimientos y controles base son los siguientes:

- **Control de Interfaces de Acceso:** El objetivo de este control es el control de todos los puntos de acceso al dispositivo, ya que en muchos de los casos estos puntos de acceso requieren autenticación. Se habla de Aplicaciones con autenticación, Acceso al sistema operativo, Acceso Físico, Acceso a interfaces de conexión como conectores Corriente, HDMI, Infrarrojos, Ethernet, entre otros. La idea es que en los casos de que cuenten con accesos con usuario y clave por defecto estos sean desactivados o modificados quitando los que se traen de fábrica.

- **Actualización del Dispositivo:** Se debe tener un control de las versiones de las aplicaciones y del sistema operativo del dispositivo, ya que los desarrollos de fábrica tienen siempre vulnerabilidades o brechas que corregir.

- **Configuración segura de la red local:** Como punto crítico del proceso de aseguramiento y en esta primera actividad donde se busca correr procedimientos técnico básicos para cerrar brechas que hacen que los ataques más comunes sean mitigados, el aseguramiento de la red de comunicaciones entre los Smart TV y el medio exterior es básico.

  Este Checklist busca que el profesional de seguridad gestione con su firewall como equipo de seguridad de perímetro o de red interna las configuraciones respectivas para que las comunicaciones con el Smart estén vigiladas y ajustadas a las comunicaciones estrictamente necesarias. Es decir que en el Smart solo los protocolos, puertos y aplicaciones usadas sean las que este disponibles en funcionamiento. Así miso el tener la red de Smart en una vlan o en un segmento diferente a la red local como recomendación inicial. Para realizar una configuración adecuada, se recomienda emplear reglas de NAT o de Port Forwarding {Redirección de Puertos}.

- **Identificación y Control del uso de servicios en la nube {cloud Services}:** En este paso es muy importante verificar que las conexiones por software del Smart frente a los sitios CLOUD que el fabricante pone a disposición del recurso sean identificados, monitoreados, filtrados y controlados desde todo punto de vista.

- **Uso de aplicaciones móviles para dispositivos IoT:** Este punto de control o de aseguramiento hace referencia a la interacción entre dispositivos móviles como Smartphones con los Smart TV, ya que existen aplicaciones que generan tráfico y actividades dentro del Smart como por ejemplo descargas

de aplicaciones, actualizaciones de sitios que no son los aprobados o reconocidos por el fabricante, entre otras actividades maliciosas. Se recomienda al profesional de seguridad denegar el acceso a la información que no considere estrictamente imprescindible, y en segundo lugar comprobar exhaustivamente si la fuente desde la que se ha obtenido es confiable.

- **Buenas prácticas en cultura de seguridad**: Es permanente la recomendación del uso de buenas prácticas las cuales se recomienda implementar desde las políticas de seguridad. Teniendo en cuenta que se socializa frecuentemente que el eslabón más débil es el usuario los empleados de la organización serán los primeros expuestos a la ingeniería social. Se recomienda que se verifique que existen planes de capacitación donde los conocimientos en ataques de fishing, con malware, ingeniería social, violación de controles de acceso, y robo de contraseñas, entre otros serán enfocados en estos usuarios.

### 1.1.3 Prácticas de aseguramiento técnico práctico por cada marca.

Para el desarrollo de las actividades técnicas en el aseguramiento de los sistemas SMARTTV se deben seguir los siguientes pasos base.

Partimos del Checklist para los SAMSUNG y LG: Este Checklist presenta las opciones que de manera técnica se deben tener en cuenta en las configuraciones de los Smart TV con la edición y selección de opciones específicas para la seguridad controlada y de análisis automático del sistema.
La siguiente tabla de Excel muestra las opciones del Checklist a tener en cuenta:

Tabla 5 Checklist para configuraciones técnicas en SMART TV Samsung y LG

| Actividades Técnicas Para La Seguridad Del Smart Tv | |
|---|---|
| **1** | **Seguridad De Datos Por Defecto** |
| 1.1. | Cambiar la clave por defecto del usuario administrador |
| 1.2. | Crear un usuario administrador o con altos privilegios alterno |
| **2** | **Configuración De Seguridad Inteligente** |
| 2.1. | Correr procesos de análisis de seguridad |
| 2.2. | Configurar seguridad inteligente con análisis de seguridad |
| **3** | **Configurar Bloqueos De Seguridad** |
| 3.1. | Configurar bloqueos de programas |
| 3.2. | Configurar bloqueos de canales |
| 3.3. | Configurar bloqueos de aplicaciones |
| 3.4. | Configurar bloqueos de Entradas |
| **4** | **Configuración De Actualizaciones** |
| 4.1. | Configuración de actualizaciones automática de sistema |
| 4.2. | Configuración de actualizaciones automáticas de aplicaciones |
| **5** | **Seguridad En Las Comunicaciones** |
| 5.1. | Asignación de una dirección Ip estática o dinámica conocida por la empresa |
| 5.2. | Configuración de VPN para conexiones remotas de usuarios |

#### 6.4.1.1 Aseguramiento Técnico - Modelo Samsung

**Smart TV MU7500 - ACTIVAR SEGURIDAD INTELIGENTE**

Paso 1 del aseguramiento técnico del Smart TV (Samsung, 2019)[48]

Paso 1. Acceda al menú, sitúate sobre General y pulsa la TECLA ENTER del control remoto.

**Figura 35 Acceso al menú para aseguramiento del sistema**


Fuente: Seguridad del Smart TV Samsung, recuperado de: https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-enable-smart-security/

[48] Fuente: Seguridad del Smart TV Samsung, recuperado de: https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-enable-smart-security/

Paso 2. Bajar hasta Administración del sistema e ingresar clickeando la tecla Enter del control remoto.

Figura 36 Administración del Sistema


Fuente: Seguridad del Smart TV Samsung, recuperado de: https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-enable-smart-security/

Paso 3. Desplazarse hacia la parte inferior del menú utilizando la rueda de dirección del control remoto. (Samsung, 2019)

Figura 37 Deslizar mouse hacia dirección de control


Fuente: Seguridad del Smart TV Samsung, recuperado de: https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-enable-smart-security/

**Paso 4.** Selecciona Seguridad inteligente y presiona en Enter

Figura 38 Seguridad inteligente


Fuente: Seguridad del Smart TV Samsung, recuperado de: https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-enable-smart-security/

Paso 5. Selecciona Buscar y presiona la tecla Enter del control remoto. (Samsung, 2019)

Figura 39 Búsqueda de opción de seguridad


Fuente: Seguridad del Smart TV Samsung, recuperado de: https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-enable-smart-security/

**Paso 6. Espera a que finalice el análisis.**

Figura 40 Análisis de seguridad


Fuente: Seguridad del Smart TV Samsung, recuperado de: https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-enable-smart-security/

Paso 7. Listo, el análisis ha terminado. Haz clic en Aceptar para finalizar

Figura 41 Final de Análisis


Fuente: Seguridad del Smart TV Samsung, recuperado de: https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-nable-smart-security/ [49]

**Seguridad general de los Smart TV WebOS para programas de TV, Aplicaciones y Entradas**

**Bloqueo de Programas**

Evita que NNA niños, niñas o adolescentes vean determinados programas de TV de contenido para adultos por medio de una clasificación bajo unos límites establecidos. Dicha clasificación varía según el país.

1. Seleccionar Bloqueos de programas de TV.
2. Elegir la clasificación de programas que deseas bloquear.

[49] Fuente: Seguridad del Smart TV Samsung, recuperado de: https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-enable-smart-security/

Esta función se activa basado de datos recibidos de la cadena. Por consiguiente, si la señal presenta información errónea, ésta no se activará. En el momento de estar activado, se evidenciará una alerta cuando el equipo detecte uno de los programas bloqueados, solicitará una contraseña para ingresar a ver el contenido de dicho canal. Sólo es compatible con el modo de recepción digital {TDT}.

**Bloqueo de canal:** Permite bloquear canales a tu elección:

1. Selecciona Bloqueo de canal.
2. Elige el canal o canales a bloquear.

Los canales bloqueados se pueden seleccionar, pero en la pantalla no aparece ninguna imagen y el sonido se silencia. Para poder ver un canal bloqueado, introduce la contraseña.

**Bloqueo de Aplicaciones:** Puede el usuario bloquear aplicaciones del sistema WebOS:

1. Selecciona Bloqueo de aplicación.
2. Selecciona las aplicaciones que deseas bloquear.

La función de bloqueo no está disponible inmediatamente para la aplicación que se está ejecutando actualmente.

**Bloqueo de Entradas:** Puede el usuario activar o desactivar el bloqueo de entradas de señal {HDMI, etc.}.

1. Selecciona Bloqueo de entrada.
2. Selecciona las entradas que deseas bloquear.

**Restablecer código PIN**

Esta opción te permite cambiar tu contraseña de bloqueo si la has olvidado o quieres cambiar la que viene por defecto, que es "0000" {cuatro ceros}.

### 6.4.1.2 Aseguramiento de modelos LG.

**SMART TV LG Modelos 500D en adelante.**

Los pasos para la configuración de Seguridad de un Smart TV LG frente a la seguridad de bloqueo de canales y accesos son los siguientes:

**WebOS 3.0 y 3.5 o posteriores**

Paso 1. Con el Control - Magic Control, pulsar la tecla de Ajustes. Si utilizas el mando estándar o tradicional, aprieta la tecla Smart o Settings.

Figura 42 Configuración ***Smart***


Fuente: Seguridad en WebOS 3.0 y 3.5, recuperado de https://www.lg.com/es/posventa/guias-y-soluciones/television/control-parental

Paso 2. Aparecerá una barra de iconos lateral a la derecha, selecciona el de abajo del todo, Toda la Configuración.

Figura 43 ingreso a la configuración


Fuente: Seguridad en WebOS 3.0 y 3.5, recuperado de https://www.lg.com/es/posventa/guias-y-soluciones/television/control-parental

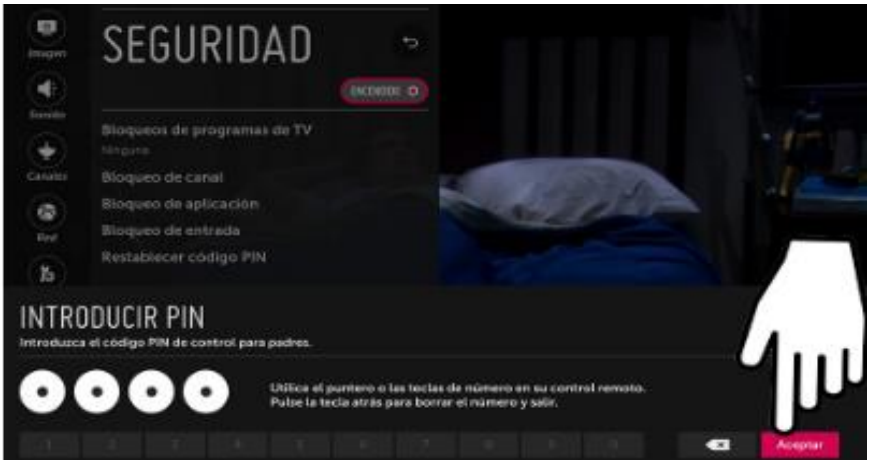
Paso 3. Entra en el menú de Seguridad y actívalo pulsando en APAGADO.

Figura 44 Activación seguridad


Fuente: Seguridad en WebOS 3.0 y 3.5, recuperado de https://www.lg.com/es/posventa/guias-y-soluciones/television/control-parental

Paso 4. Introduce el código/PIN {por defecto 0000} para el bloqueo de canal y pulsa en ACEPTAR.

Figura 45 Pin de gestión de bloqueo




Fuente: Seguridad en WebOS 3.0 y 3.5, recuperado de https://www.lg.com/es/posventa/guias-y-soluciones/television/control-parental

Paso 5. Selecciona Bloqueo de canal.

Figura 46 Bloqueo de canales innecesarios según rol del TV


Fuente: Seguridad en WebOS 3.0 y 3.5, recuperado de https://www.lg.com/es/posventa/guias-y-soluciones/television/control-parental

Paso 6. Escoge los canales pulsando en el botón Ok o con el cursor del mando Magic control.

Figura 47 Gestión de programas según rol del Dispositivo


Fuente: Seguridad en WebOS 3.0 y 3.5, recuperado de https://www.lg.com/es/posventa/guias-y-soluciones/television/control-parental

Paso 7. Al finalizar, pulsa el botón rojo del mando o selecciona el candado.

Figura 48 Activación de bloqueo


Fuente: Seguridad en WebOS 3.0 y 3.5, recuperado de https://www.lg.com/es/posventa/guias-y-soluciones/television/control-parental

Paso 8. Revisa si el candado aparece en los canales bloqueados. [50]

Figura 49 Verificación de canales bloqueados


Fuente: Seguridad en WebOS 3.0 y 3.5, recuperado de https://www.lg.com/es/posventa/guias-y-soluciones/television/control-parental

[50] Seguridad en WebOS 3.0 y 3.5, recuperado de https://www.lg.com/es/posventa/guias-y-soluciones/television/control-parental

### 6.4.2 Buenas Prácticas De Políticas Y Protocolos Organizacionales

Uno de los elementos que no deben faltar en el modelo de defensa frente a ataques a dispositivos IoT como son los Smart TV es la política de seguridad, las políticas hacen enmarcar lo que la empresa va a cuidar o va a cumplir frente a un tema específico, y en este caso de la seguridad a los IoT, se recomienda que la empresa si no la tiene la construya, apruebe, socialice e implemente.

Los que debería llevar una política básica y efectiva frente a la seguridad de dispositivos IoT se enmarca en los siguientes puntos recomendados:

La base de una apropiada política de uso y seguridad de IoT la conforman 4 áreas, que es muy importante y no debería ser punto de negociación el establecer directrices y pautas para:

**Seguridad** – Es básico y obligatorio que este tema sea ajustado a la seguridad y al sistema de gestión de la seguridad de la empresa, con esto se manejará un enfoque de defensa y gestión de acciones de resistencia a los ataques;

**Privacidad** – Esto es lo que desde la seguridad vemos como un DERECHO fundamental para todos los usuarios de las tecnologías de la información, y para este caso de dispositivos IoT mucho más al ser este un tema supuestamente novedoso y actual. La privacidad y la confidencialidad como uno de los pilares de la seguridad debe tenerse en cuenta en la política base.

**Gobernanza** – Cuando hablamos de gobernanza, estamos diciendo que desde las directivas debe existir la intensión clara de gestionar seguridad, privacidad, controles de acceso y mitigación d riesgos en el uso de dispositivos IoT, lo cual generaría un equilibrio total entre estos elementos que acompaña la seguridad, por lo cual esto es algo necesario dentro del proceso de construcción y gestión de la política de IoT.

**Gestión de datos** – La gestión de los datos en el uso de dispositivos IoT debe ser liviana, abierta y manteniendo la privacidad y el control de acceso a los mismos, por lo cual el tener en cuenta el cumplimiento como lo es en el caso de la protección de datos personales según la ley 1581, es algo que la política no debe dejar por fuera.

Si bien la profundidad de las directrices en una política de IoT no son iguales entre las diferentes empresas, si debe tener un modelo de identificación, gestión y tratamiento de riesgos que cubra todos los dispositivos IoT de la organización.

### 6.4.3 Aplicabilidad Del Modelo

El modelo tiene completa aplicabilidad a los escenarios actuales de las empresas ya que está enmarcado en una serie de actividades técnicas y la implementación de buenas prácticas dentro de la seguridad de la organización.

Como se evidencia en la lectura del documento, en las acciones técnicas de cada marca y en las buenas prácticas y las políticas internas de la organización, perfectamente un área de tecnología puede realizar estas actividades y tener un Checklist básico de valoración el cual está en el presente trabajo en los numerales 5.4.3 y 5.4.2.

Nuestra recomendación desde la perspectiva del consultor es que se inicie con un inventario de los activos Smart TV definiendo en su inventario la ip, la marca y el rol que cumple alineado al área al que está asignado.

Posteriormente debe tenerse una hoja de vida del cada Smart TV para determinar la configuración básica que tiene en el momento. Con esta información y conociendo las configuraciones base que deben darse técnicamente generar un comparativo y determinar qué actividades o configuraciones hacen falta en cada uno de los activos y así programar su ejecución.

Seguidamente debe realizarse un análisis de la situación del control de accesos físico hacia los Smart TV y las configuraciones base de accesos y claves o contraseñas de cada una de las aplicaciones del Smart TV con esto y las recomendaciones que modelo generar las acciones requeridas para corregir los faltantes.

Finalmente crear la política de gestión de información en los Smart TV como una política de Tratamiento de la seguridad de la información en los dispositivos IoT y así socializarla con los funcionarios y generar acciones de seguimiento y control para el sistema de seguridad de la información.

# 7 CONCLUSIONES

La conclusión de esta monografía se expresa en dos aspectos que son muy importantes, el primero es que se logra aplicar los conceptos aprendidos en los cursos desarrollados, en un entorno real, como lo es la seguridad que hoy en día tienen los Smart TV como dispositivos IoT en nuestro país.

Se logra identificar las tecnologías de estos elementos, las estructuras de los sistemas operativos, y las vulnerabilidades más comunes, siendo estas la base del análisis de las brechas de seguridad se analiza basado en las mejoras seguridad de los sistemas operativos actuales Tizen y WebOS al 2021, si estas vulnerabilidades están identificadas como vigentes por el uso de puertos y servicios que los Smart TV tienen a disposición de los usuarios.

Posterior a este análisis se logra determinar qué mejoras o qué brechas de seguridad se han curado o sean mitigado basados en los nuevos esquemas de seguridad de los sistemas operativos actuales y esto nos deja un sobrante sin determinar que son las vulnerabilidades actualmente vigentes y que sin data confiable sobre su mitigación o remediación aún se toman como vigentes.

Con base en estas vulnerabilidades vigentes se realiza un diseño de un modelo de aseguramiento de Smart TV Samsung y LG el cual consta de los dos elementos básicos hoy en día, como son, las buenas prácticas a nivel de usuario final y de usuario técnico y las configuraciones básicas de manera directa en los Smart TV y que dejan en cierta forma blindado el sistema para mitigar ataques comunes que se hacen hoy en día a estos equipos en las empresas.

Finalmente se deja una base fundamental para otras investigaciones de más profundidad desde lo que estas vulnerabilidades podrían llegar a significar para un atacante y el impacto que un ataque podría tener en el activo, posterior a esto

se podrá estimar que medidas de seguridad hoy en día deben ser implementadas para la mitigación de los riesgos que estos equipos tienen.

Teniendo en cuenta que existen aún muchas otras vulnerabilidades que usan no solo ataques de protocolos de red y de aplicaciones con técnicas de ingeniería social y la inyección de malware, sino que usan otros medios de comunicación que no es el protocolo tcp/ip sino medios como infrarrojos, atacando el esquema de comunicación del Smart TV con el control remoto, y del sistema de bluetooth, es preciso que se hagan desde la perspectiva de los profesionales en seguridad informática hacia los usuarios técnico y no técnicos de estos Smart una serie de recomendaciones que complementan de manera específica la aplicabilidad del MODELO propuesto y que son pautas directas para mitigar eficientemente ataques a estos dispositivos.

# 8. RECOMENDACIONES

Las recomendaciones que se dejan planteadas desde este documento son las siguientes:

- Tener claro el entorno en que se va a trabajar con el Smart TV, es decir definir qué actividades realizará para la compañía, si es educativo, informativo y de publicidad, o de apoyo en información a usuarios finales de servicios específicos, o simplemente para entretenimiento de los usuarios en la empresa. Esto define la recomendación siguiente.

- Definir que protocolos de comunicación se tendrán un uso para así poder generar las configuraciones necesarias para mitigar riesgos de ataques específicos a estos protocolos y deshabilitar los servicios de los protocolos que no se usarán.

- Definir los procedimientos que se usaran para las actualizaciones tanto del sistema operativo de los Smart como las aplicaciones que manejará en su aplicabilidad.

- Realizar un plan de asignación y gestión de contraseñas para la administración de los servicios del Smart TV y asignar los responsables respectivos a estas tareas de aseguramiento y monitoreo de la seguridad y los eventos que pasen en un tiempo definido.

- Preparar y generar u inventario controlado de los Smart en la empresa y las funciones o roles que cumplen cada uno.

- Tener una bitácora de las configuraciones realizadas a cada Smart y los objetivos que se cumplen para cada uno.

- Generar un agendamiento para verificar la seguridad de los Smart TV con procedimiento de identificación de vulnerabilidades y planes de auditorías de seguridad con pentesting o Ethical hacking.

- Involucrar estos dispositivos en la gestión general del riesgo en el área de T.I. y darles la importancia que merecen haciendo partícipes a las directivas dándoles a conocer las posibles brechas que se tienen, los ataques que se podrán dar y el impacto en caso de que uno de estos ataques sea perpetrado, así como el valor del mismo activo dentro de la organización y dejarles ver la lista de riesgos asumidos y residuales que los análisis de riesgos de estos dispositivos IoT realizados por tecnología.

# 9 BIBLIOGRAFÍA


ADVANCED-IP-SCANNER. {s.f.}. {En línea} disponible en: https://www.advanced-ip-scanner.com/es/

G. Alberto, *Estos son los 5 peligros a los que está expuesta tu Smart TV*. {En línea} {2019}. Disponible en https://www.adslzone.net/2019/07/18/smart-tv-peligros-vulnerabilidades/

AUMENTA EL RANSOMWARE Y ATAQUES DE IOT. ComputerWorld.co: {en línea} {25 de Julio de 2019}. Disponible en https://computerworld.co/aumenta-ransomware-como-servicio-y-ataques-de-iot/

B., K. A. HACKING ÉTICO 101 Cómo hackear profesionalmente en 21 días o menos! bdigital.unal.edu.co. {s.f.}. *Protocolo de aplicación restringida, COAP* {en línea} Disponible en RFC 7252: http:// https://coap.technology/

BLOGSPOT. *Qué es WebSocket*. {en línea} {13 de enero de 2013} Disponible en http://queeswebsocket.blogspot.com/2013/01/que-es-websocket.html

CASTRO Alicia, C. E. {s.f.}. *Aspectos de seguridad en internet de las cosas*. {en línea} Disponible en sedici.unlp.edu.ar: http://sedici.unlp.edu.ar/handle/10915/63929

COLOMBIA, B. L. *Los televisores más buscados de la región,* {en línea} {23 de Marzo de 2017} Disponible en https://blog.linio.com.co/los-televisores-buscados-la-region/

Colombia, C. *IoT, otro escenario para ataques*. {en línea} {10 de octubre de 2018}. Disponible en https://computerworld.co/iot-otro-escenario-para-ataques/

Colombia, C. *Pérdidas corporativas por fallas de seguridad en IoT*. {en línea} {28 de diciembre de 2018}. Disponible en https://computerworld.co/perdidas-corporativas-por-fallas-de-seguridad-en-iot/

Colombia, S. N. *Samsung.com*. {en línea} {15 de Agosto de 2018}. Disponible en https://news.samsung.com/co/conozca-como-samsung-garantiza-la-seguridad-en-sus-smart-tvs

COMMONS, I. C. Attribution-Non-Commercial-NoDerivs {en línea} {2010}. Disponible en Creative Commons 3.0: www.isecom.org

M. B Eliécer, *Construcción de un modelo de plataforma IoT para la trazabilidad del proceso logístico de la fresa dentro del marco del corredor tecnológico agroindustrial*. {en línea} {2018} Disponible en http://bdigital.unal.edu.co/69834/1/1032370645.2018.pdf

GADGET, {s.f.} ¿Sabes cuáles son los sistemas operativos que puede tener tu televisor? *Gadget*, {en línea} Disponible en: http://www.revista-gadget.es/reportaje/sistemas-operativos-televisor/

Como se infectó mi televisor con ransomware, {en línea} {19-06 de 2019}. Disponible en https://infoweek.biz: https://infoweek.biz/2019/06/18/como-se-infecto-mi-televisor-con-ransomware/

KOTTKE, J. {en línea} {09 de abril de 2018}. Disponible en *https://kottke.org/*. https://kottke.org/18/04/nikola-tesla-predicted-the-smartphone-in-1926

MINGEUM, L. J. Are you watching TV now? Is it real?:Hacking of smart TV with 0 day. {2017}.

NIKOS Sidiroupoulos, P. S. Smart TV Hacking. En P. S. Nikos Sidiroupoulos. Amsterdam. {2013}.

PORTAFOLIO.CO. *Portafolio.co*. Colombia tendrá una red exclusiva para el internet de las cosas {en línea} {23 de Agosto de 2018}. Disponible en: https://www.portafolio.co/negocios/empresas/colombia-tendra-una-red-exclusiva-para-el-internet-de-las-cosas-520354

PUTTY. {s.f.}. *Putty.org*. {en línea} Disponible en https://www.putty.org

REPUBLICA.CO, L. *Larepublica.co*. Disponible en Samsung, LG y Kalley tienen 67,6% del mercado de televisores en Colombia: {en línea} {22 de abril de 2019} Disponible en. https://www.larepublica.co/empresas/samsung-lg-y-kalley-tienen-676-del-mercado-de-televisores-en-colombia-2853252

Samsung, S. t. *samsung.com*. {en línea} {19 de 06 de 2019}. Disponible en https://www.samsung.com/co/support/tv-audio-video/smart-tv-mu7500-how-to-enable-smart-security/

J. S. Silvestre, {s.f.}. *INTERNET DE LAS COSAS*. upcommons.upc.edu.ar, {en línea} Disponible en :https://upcommons.upc.edu/bitstream/handle/2117/100921/LM08_R_ES.pdf

SIMÕES C., {s.f.}. *REST vs WebSocket. ¿Qué diferencias hay?* REST vs WebSocket. ¿Qué diferencias hay?: {en línea} Disponible en http:// https://www.itdo.com/blog/rest-vs-websocket-que-diferencia-hay/

SPARTA. SECFORCE. {s.f.}. *sparta.secforce.com*. {en línea} Disponible en http://sparta.secforce.com

TECNOLOGICA, a. {s.f.}. *QUE ES SMART TV CARACTERISTICAS*. {en línea} Disponible en areatecnologica.com: https://www.areatecnologia.com/que-es-smart-tv.htm

TST-SISTEMAS. {s.f.}. *MQTT*. {en línea} Protocolo de conectividad M2M / IoT: Disponible en http://www.tst-sistemas.es/mqtt/

VALERO, N. {s.f.}. *Consumo móvil en Colombia Siempre conectado: ¿Bendición o maldición?* {en línea} Disponible en https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Consumo%20movil%202018.pdf

WIKIPEDIA. {s.f.}. *Wikipedia.com*. {en línea} Disponible en http://unblockit.eu/unblock.php?site=aHR0cHM6Ly9lbi5tLndpa2lwZWRpYS5vcmcvd2lraS9ObWFw

XMPP. {s.f.}. *Una descripción general de XMPP*. {en línea} Disponible en xmpp.org: https://xmpp.org/about/technology-overview

YANN Bachy, F. B. *Análisis de seguridad de televisores inteligentes:* experimentos prácticos, {en línea} {2015}: Disponible en https://www.semanticscholar.org/paper/Smart-TV-Security-Analysis%3A-Practical-Experiments-Bachy-Basse/5dd526542309915c1b67facec3355ca59e156902