Universidad Nacional Autónoma de México
Facultad de Ciencias

Ciencias de la Computación
Sistemas Operativos 2019-2

Sistemas Operativos Modernos.
Riesgos y Soluciones.

César Derian Estrada Gómez

1. Introducción

En diciembre de 2012, en el episodio 22 de la serie de espionaje *Homeland*, los guionistas crearon una trama en la que un grupo terrorista planea un complot para hackear el marcapasos del Vicepresidente de los Estados Unidos.

También, en el capítulo 19 de la serie policíaca *CSI Cyber*, expuso como un hacker colocaba en automóviles un dispositivo que contenía una tarjeta SIM y, por ese medio, tenía total control del auto, desde el estéreo hasta los seguros y el motor.

Estos ejemplos parecen demasiada ficción, sin embargo, el hackeo de dispositivos comunes es más real de lo que parece. Algunos ejemplos de hackeo de aparatos populares son los siguientes:

- En 2007, el BMW X5 blindado valuado en US $100,000 de la estrella de fútbol, David Beckham, fue robado no una, sino dos veces por dos ladrones que únicamente ocuparon una laptop para abrir y arrancar el motor del vehículo.
- En 2015, un hacker veterano llamado Samy Kamkar construyó un dispositivo por menos de US $100 que, según dijo, podría encontrar, desbloquear e iniciar de forma remota cualquier automóvil de General Motors equipado con el sistema de comunicaciones *OnStar*.
- También en 2015, Fiat Chrysler retiró 1.4 millones de autos y camionetas después de que Chris Valasek y Charlie Miller demostraron que podían controlar de forma remota los frenos, la radio, los limpiaparabrisas y otras funciones de un Jeep Cherokee al acceder a través de su sistema de información y entretenimiento *UConnect*.
- En 2016 muchos usuarios se vieron afectados por el secuestro de televisores a través de *ransomware* para Android.
- En 2019, una agencia de seguridad de Estados Unidos, *Homeland Security*, emitió un aviso a todos los pacientes que utilizarán un desfibrilador marca *Medtronic* que tuvieran cuidado porque la compañía había detectado fallas de seguridad y problemas que dejaban a los dispositivos sin protección ante un ataque cibernético.

En un intento por ir un paso adelante en la mercado, las marcas agregan características y cualidades innovadoras a sus distintos productos pero en su intento de hacerlo, se adelantan también a ellos mismos y por este motivo no siempre piensan en las vulnerabilidades existentes.

A continuación, se abordará más a detalle el caso de *Medtronic*, así cómo otros casos de hackeo a sistemas operativos modernos de dispositivos que utiliza cualquier individuo.

2. Marcapasos Medtronic

A finales de 2018 y principios de 2019, la marca *Medtronic* estuvo en el ojo del huracán debido a que sus marcapasos modelo *Adapta*, *Versa*, *Sensia*, *Relia*, *Attesta*, *Sphera* y *Vitatron* sufrieron un 'error de software' que producía una falta de estimulación que podía provocar en los pacientes latidos cardíacos lentos, presión arterial baja, mareos, desmayos e incluso la muerte.

La firma de seguridad *Clever Security* descubrió que el protocolo de telemetría de radiofrecuencia *Conexus* (los medios patentados de Medtronic para que los monitores se conecten de forma inalámbrica a los dispositivos implantados) no proporcionan cifrado para las comunicaciones seguras (no manda conexión cifrada por HTTPS). Y peor aún, el protocolo no tiene medios de autenticación para que los dispositivos legítimos demuestren que están autorizados para tomar el control de los dispositivos implantados.

La falta de autenticación, combinada con una serie de otras vulnerabilidades, hace posible que los atacantes reescriban completamente el *firmware* del desfibrilador.

Cabe destacar que sus dispositivos para la alineación de la columna vertebral también presentaron vulnerabilidades y 'errores de software'.

2.1. Descripción de un ataque a un marcapasos

Los investigadores, Billy Rios y Jonathan Butts, dijeron que: un hackeo en particular explota las vulnerabilidades de los sistemas servidores de software que Medtronic usa en su red interna. Una vez hecho esto, el hacker podría unirse a una red privada virtual y modificar maliciosamente el proceso de actualización.

Después de que realizaron este proceso, los investigadores decidieron no adentrarse más al sistema de Medtronic y pues hubieran afrontado problemas legales.

3. Smart TV

Según algunos expertos, las *Smart TV* son el futuro; día a día adquieren mayores funcionalidades asimilándose cada vez más a un *smartphone* en cuanto a funciones y utilización de software, sin embargo, a diferencia de los *smartphones*, las *Smart TV* cuentan con un software más sencillo por lo que resulta relativamente fácil corromper su sistema.

El problema no es que sea posible hackear la *Smart TV* ya que lo máximo que podría hacer el atacante sería cambiar el canal o poner vídeos de YouTube de forma aleatoria. Pero sí, a través de la conexión WiFi podrían aprovechar el ataque para afectar a otros dispositivos.

3.1. Ataque a una *Smart TV*

Dentro de un informe desarrollado por la empresa de seguridad *ESET*, menciona que las técnicas de ingeniería social, las vulnerabilidades del software, las malas configuraciones y ataques físicos, son suficientes para poder ejecutar algún código malicioso en una *Smart TV*.

También, si la *Smart TV* está conectada a una conexión WiFi, el hacker puede colarse por esa red y acceder a otros dispositivos.

Otro "puerto de entrada" son las memorias USB. Un pendrive infectado puede colocarse en un televisor y ejecutar scripts maliciosos o tener la capacidad de explotar vulnerabilidades que no han sido parchadas por el usuario.

4. Automóviles

Actualmente, los sistemas operativos más usados en los teléfonos móviles han extendido su tecnología para aplicarla a vehículos inteligentes, ambas presumen que hace que manejar sea más seguro ya que minimiza las distracciones:

- *Apple CarPlay*. Tecnología donde el usuario se puede conectar con su ID, gestiona sus llamadas, mensajes, reproductor musical, y todo tipo de información. Tiene acuerdos con Honda, Mercedes-Benz, Nissan, Ferrari, Chevy, Infiniti, Kia, Hyundai, Volvo, Acura y Opel.

- *Android Auto*. Extiende las características de los dispositivos Android al tablero del automóvil. Lo utilizan autos de las compañías General Motors, Audi, Honda y Hyundai.

Los automóviles nuevos tienen características muy innovadoras como manejo automático, GPS, cámara de reversa en el tablero del conductor, sistemas de información y entretenimiento, conexiones de red entre varias otras; aunado a esto, es importante mencionar que un automóvil promedio tiene más de 150 millones de líneas de código de computadora.

Toda esa complejidad crea un riesgo real de ataque cibernético puesto que los hackers "de sombrero negro" pueden usar las conexiones de red y/o conexiones físicas para explotar las vulnerabilidades y poner en riesgo la información del usuario, además de su propia seguridad física.

4.1. Pandora y Viper

En el mundo de hoy en día, las aplicaciones móviles están al alcance de todos, sin embargo, éstas también presentan vulnerabilidades que, si se saben explotar, el atacante puede obtener los datos del usuario y tomar el control total del sistema operativo del dispositivo que están vulnerando.

Un claro ejemplo de lo anterior es el caso de las alarmas de seguridad para los automóviles. En este rubro, las marcas más populares son *Pandora Alarms* y las creadas por la empresa *Directed*: *Viper* (nombre comercial para EUA) y *Clifford* (nombre comercial para Reino Unido). *Pandora* vende sus alarmas como *'inhackeables'*. No obstante, la consultora de seguridad *Pen Test Partners* encontró serias vulnerabilidades en ambas amplicaciones .

Estos problemas afectaron aproximadamente a 3 millones de vehículos en todo el mundo, entre los cuales se encuentran: Mazda 6, Range Rover Sport, Kia Quoris, Toyota Fortuner, Mitsubishi Pajero, Toyota Prius 50 y RAV4, a los cuales, el atacante también podía cambiar la velocidad del control de forma remota.

4.2. Descripción de un ataque a un automóvil

Pen Test Partners encontró que ambas aplicaciones permiten a cualquiera crear una cuenta de prueba. Y con esa cuenta de prueba, acceder a cualquier cuenta genuina y recuperar y manipular los datos, así como actualizar la dirección de correo electrónico registrada en la cuenta, enviar un restablecimiento de contraseña a la dirección modificada (es decir, la del atacante) y hacerse cargo de la cuenta.

Todo esto permitió a los investigadores un acceso significativo de las dos aplicaciones. En *Viper* pudieron:

- Apagar el motor del automóvil mientras éste se encuentra en movimiento.

- Acceder a los perfiles de otros usuarios para así poder cambiar las contraseñas de esas cuentas y tener un control total.

Mientras que en *Pandora* pudieron:

- Tomar el control de la aplicación de forma remota.
- Rastrear cualquier vehículo en tiempo real.
- Activar la alarma de forma remota.
- Abrir las cerraduras de la puerta.
- Arrancar el motor de un vehículo.
- Habilitar el micrófono (que en un inicio es para que el conductor realice llamadas de emergencia) de manera remota que se encuentra dentro del automóvil.

Ken Munro, socio de *Pen Test Partners*, dijo que: una vez que el atacante tiene el control de una cuenta, podría ubicar geográficamente el vehículo, seguirlo y en un punto adecuado, detener el auto apagando el motor, abrir las puertas y secuestrar el vehículo. De manera similar, podría encendar/apagar la sirena de la alarma y las luces intermitentes provocando, de igual manera que el auto se detuviera ya que el usuario bajaría a revisar qué está pasando. Después de detener el auto, podría configurar el inmovilizador y, debido a que tendría el control de la cuenta, evitar que el propietario pudiera reiniciar el automóvil.

5. El caso de Meltdown y Spectre

Meltdown. "Rompe el aislamiento fundamental que existe entre las aplicaciones de usuario y el sistema operativo". Ataque que permite a un programa acceder a la memoria (y secretos) de otros programas y del sistema operativo.

Spectre. "Rompe el aislamiento entre distintas aplicaciones". Un atacante podría usarlo para vulnerar la seguridad de aplicaciones que han sido programadas perfectamente y "siguiendo las mejores prácticas". De hecho, seguir esas prácticas acaba siendo irónicamente contraproducente, ya que hace a estos programas más vulnerables a *Spectre*.

Meltdown afecta a todos los procesadores Intel que hagan uso de la tradicional *Out-of-Order Execution*, y eso incluye básicamente a todos los que están funcionando a día de hoy, ya que estos procesadores llevan produciéndose desde 1995. Solo los Itanium y los Intel Atom desarrollados antes de 2013 están fuera de peligro.

En el caso de *Spectre*, "prácticamente todos los sistemas" están afectados por esta vulnerabilidad. Esto plantea un riesgo mayor y una amenaza para todas las computadoras, laptops, tablets, *smartphones* y cualquier otro dispositivo que cuente con un diseño de Intel, AMD o ARM.

5.1. Morpheus

Gracias a los sucesos ocurridos con Meltdown y Spectre, investigadores de la Universidad de Michigan han estado trabajando en un procesador "imposible de hackear": *Morpheus*.

Morpheus se caracteriza por ser un procesador que encripta rápidamente los datos a una gran velocidad. Además de que cambia rápidamente de algoritmo de encriptación, impidiendo que un atacante lo pueda corromper. Esto es un sistema de seguridad infinitamente superior al que pueden ofrecer los procesadores actuales.

Su seguridad radica en la capacidad de cambiar elementos de su código denominados *'undefined semantics'*. Un elemento que hace referencia a la localización, tamaño y contenido del código del programa. Datos que normalmente son fijos y un atacante puede explotar. Aquí cambian cada 50 milisegundos a unos nuevos valores. Su velocidad de modificar el código es muy superior a las técnicas de hacking más actuales.

Destacan también que la velocidad en la aleatoriedad del código puede variar según la finalidad del CPU. Además cuenta con un detector de ataque, que permite saber cuándo sufre uno y poder así, aumentar la velocidad de cambio.

6. Posible Solución

Tanto a nivel de hardware como de software, es importante reducir el riesgo de hackeo lo más que se pueda, mas si de protección de datos y seguridad hablamos. A continuación, se proponen soluciones que ayudarían a los sistemas operativos modernos a ser más seguros.

6.1. Lo que tienen que considerar los Sistemas Operativos Modernos

- Actualización constante del sistema operativo.
  - Asignar y extender un ciclo de vida en cada actualización.
  - Mejorar acciones de respuesta, en cada actualización.
  - Agregar nuevas funcionalidades de manera regular.
- Asignar un ciclo de vida de seguridad.
- Manejar prioridades para cada operación del vehículo.
- Separar el sistema de entretenimiento de los sistemas críticos del vehículo.
- Emitir advertencias en caso de comportamiento inusual.
- Bloquear el acceso al sistema de conducción.
- Altamente modulable. El sistema operativo debe ser fácil de reprogramar.

6.2. Sistemas Operativos Modernos y su Interacción con el exterior

- Emitir un aviso cuando un dispositivo quiera conectarse.
- Pedir una validación para permitir la conexión del dispositivo.
- Pedir una dirección IP del dispositivo que quiera conectarse.
- Matener un registro de los dispositivos que quieran conectarse.
- Manejar redes *ad-hoc* para comunicación con vehículos cercanos.
- No permitir que comandos digitales puedan activar acciones físicas.

6.3. Lo que tienen que considerar las Aplicaciones Móviles

Las aplicaciones móviles también son una puerta por la que los hackers pueden entrar y vulnerar el sistema operativo, por ello, es importante que los desarrolladores de iOS y Android tengan en consideración los siguientes aspectos:

- Aplicar mecanismo de autenticación como *usuario/contraseña*.
- Aplicar control de autorización y autenticación del lado del servidor.
- Tener auditoría de cualquier movimiento realizado (por el usuario y/o por el proveedor) en la aplicación.
- Cifrar los canales de comunicación
- Evitar realizar intercambio de datos, descargas y actualizaciones vía HTTP.
- Cuando el uso de la aplicación sea fuera de línea, implementar verificaciones de integridad local dentro del código para detectar cualquier cambio de código no autorizado.

6.4. Lo que tienen que considerar los desarrolladores de Aplicaciones Móviles

Las aplicaciones móviles tienen que interactuar con los sistemas operativos que no son propiedad de los desarrolladores; es importante que los desarrolladores realicen una buena evaluación de la interacción de la aplicación con elementos del sistema operativo del dispositivo para el cual están desarrollando la aplicación.

- *Logging*
- Almacenamiento en caché de URL (Solicitud y respuesta).
- Almacenamiento en caché de ingreso de datos.
- Almacenamiento en caché de copiar/pegar buffer.
- Almacenamiento de datos HTML5.
- Objetos de cookies del navegador.
- Datos enviados a terceros.

6.5. Capa 8

Debe haber mayor difusión para los usuarios sobre la seguridad de suss computadoras y dispositivos, las acciones que debe realizar como las que debe evitar para mantener la integridad de su equipo, sus datos y su salud física.

7. Apunte Final

La mayoría de los hackers necesitan información de usuario que puedan vender y obtener una ganancia a cambio. Debido a eso, la mayoría de aquellos que se dedican a hackear autos, televisiones, etc. son de "de sombrero blanco", sin intención criminal, porque hoy en día no existen incentivos atractivos para ellos. A pesar de ello, los casos de hackeo tienen que ser una buena llamada de atención para las empresas que muchas veces subestiman la seguridad de los dispositivos que venden.

8. Referencias

Noticias de hackeo de marcapasos

1. El hackeo de los dispositivos médicos de Medtronic
2. Código malicioso, potencialmente mortal, en marcapasos cardíacos

Noticias de hackeo de *Smart TV's*

1. Expertos explican como 'hackean' a través de una Smart TV
2. ¿Sabías que tu Smart TV se puede hackear?

Noticias de hackeo de automóviles

1. Agujeros de seguridad encontrados en las alarmas de automóviles de grandes marcas.
2. Investigadores hackean alarmas de automóviles de terceros para tomar el control de los vehículos
3. Los autos se convierten en computadoras sobre ruedas
4. Los ingenieros de automóviles advierten que tu auto podría ser más fácil de hackear de lo que crees
5. Roban el auto de David Beckham con una laptop
6. El futuro es ahora: Hackeo de auto
7. Hackers 'matan' remotamente un Jeep en una carretera

Sistemas Operativos de Automóviles

1. Sistemas operativos en el auto. El futuro del automóvil
2. 9 formas terroríficas en las que los hackers pueden controlar tu auto
3. Vehículos con los 3 Sistemas Operativos
4. Android Auto
5. ¿Qué es y cómo funciona Android Auto?

Meltdown y Spectre

- Meltdown y Spectre: la pesadilla de Intel, AMD y ARM

Morpheus

- Morpheus, el procesador imposible de hackear

Seguridad en Sistemas Operativos

1. Seguridad de Sistemas Operativos

Vulnerabilidades en las aplicaciones móviles

1. Top 10 de OWASP de vulnerabilidades en aplicaciones móviles
2. Vulnerabilidades en aplicaciones móviles y el mal uso de HTTP
3. Data Leakage - Fuga de Datos