Sistemas Operativos Modernos. Riesgos y Soluciones.

César Derian Estrada Gómez

Universidad Nacional Autónoma de México

Junio 2019

Introducción

Distintas series de televisión han mostrado en sus episodios a sujetos que corrompen sistemas de automóviles u otros dispositivos para cometer sus actos criminales

Si bien, esto es ficción, el hackeo de dispositivos comunes es más real de lo que parece.

Introducción - Ejemplos

En 2007, el BMW X5 blindado de David Beckham fue robado 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, 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.

Sistemas Operativos Modernos

Marcapasos Medtronic

Afinales de 2018 y principios de 2019, la marca Medtronic estuvo en el ojo del huracán debido a que sus marcapasos 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.

Marcapasos Medtronic

La firma de seguridad Clever Security descubrió que el protocolo de telemetría de radiofrecuencia *Conexus* (medio 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).

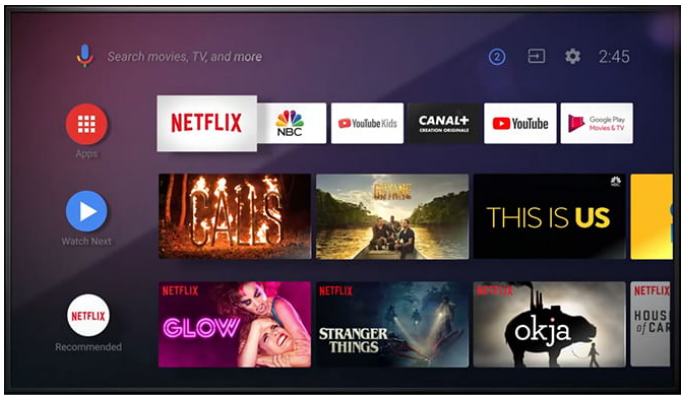
Peor aún, el protocolo no tiene medios de autenticación para que los dispositivos legítimos demuestren que están autorizados para tomar el control de los dispositivos implantados.

Ataque a Medtronic

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.

Smart TV

Las Smart TV adquieren mayores funcionalidades asimilándose cada vez más a un smartphone , sin embargo, las Smart TV cuentan con un software más sencillo por lo que resulta relativamente fácil corromper su sistema.



El riesgo no está en que el atacante ponga vídeos de YouTube de forma aleatoria. Sino en que, a través de la conexión WiFi podrían aprovechar el ataque para afectar a otros dispositivos.

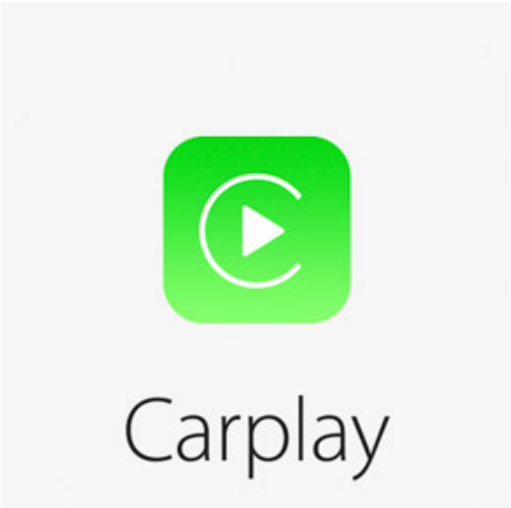
Smart TV

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.

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

Una memoria USB infectada puede colocarse y ejecutar scripts maliciosos o tener la capacidad de explotar vulnerabilidades.

Android y Apple han extendido su tecnología para aplicarla a vehículos inteligentes, ambas presumen que hace que manejar sea más seguro ya que minimiza las distracciones.



Sistemas Operativos en Automóviles

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

Un automóvil promedio tiene más de 150 millones de líneas de código de computadora.

Toda esa complejidad crea un riesgo real de ataque cibernético Tam-

bién las aplicaciones que funcionan alarmas de seguridad, como **Pandora** y **Viper** son vulnerables, según un análisis hecho por la consultora *Pen Test Partners*.

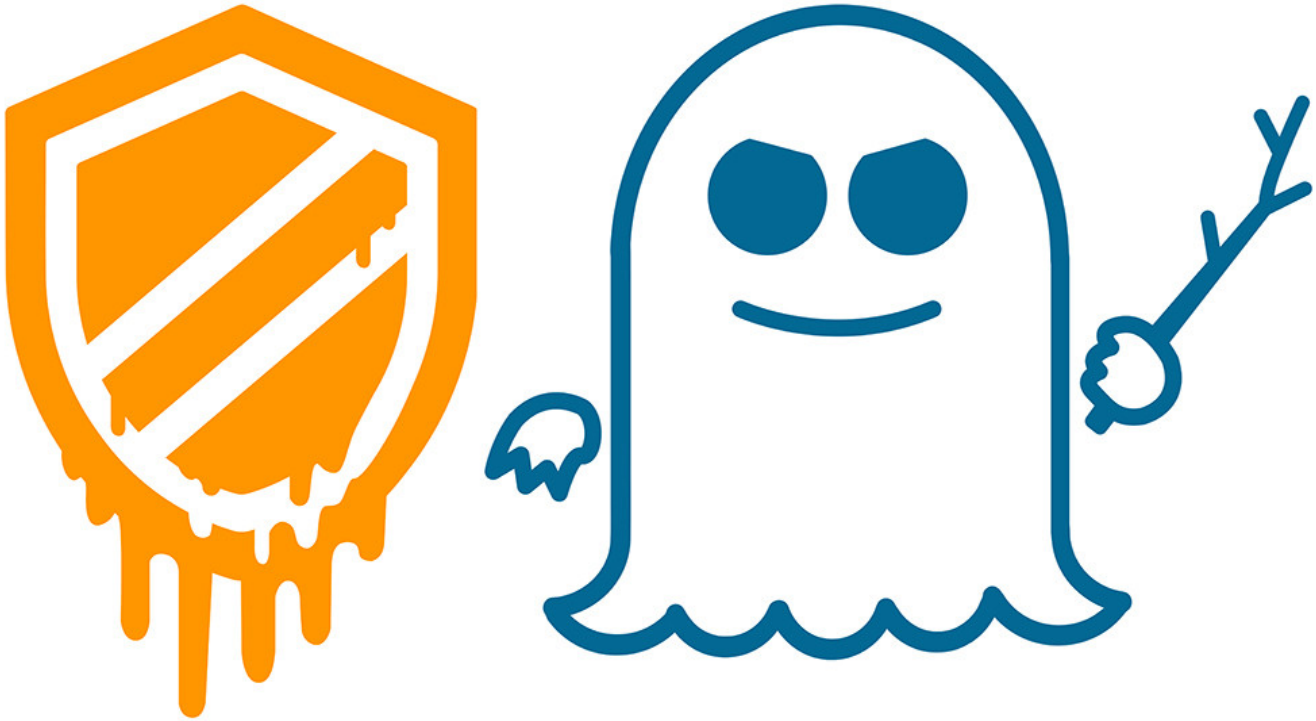
Descripción de un ataque con Pandora y Viper

Ambas aplicaciones permiten a cualquiera crear una cuenta de prueba y con ella acceder a cualquier cuenta genuina, recuperar y manipular los datos, actualizar la dirección de correo electrónico registrada en la cuenta, enviar un restablecimiento de contraseña a la dirección del atacante y hacerse cargo de la cuenta.

Uuna vez con el control de una cuenta, se podría ubicar geográficamente el vehículo, seguirlo y en un punto adecuado, detener el auto apagando el motor, abrir las puertas y secuestrar el vehículo.

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.

El caso de Meltdown y Spectre



El caso de Meltdown y Spectre

Meltdown

- Ataque que permite a un programa acceder a la memoria y demás de otros programas y del sistema operativo.
- Afecta a todos los procesadores Intel que se han producido desde 1995. Solo los Itanium y los Intel Atom desarrollados antes de 2013 están fuera de peligro.

Spectre

- Se puede usar para vulnerar la seguridad de aplicaciones que han sido programadas perfectamente y "siguiendo las mejores prácticas".
- Prácticamente todos los sistemas están afectados debido a que es una amenaza para todos los dispositivos que cuenten con un diseño de Intel, AMD o ARM.

Morpheus

- Investigadores de la Universidad de Michigan han estado trabajando en un procesador “imposible de hackear”: Morpheus.
- 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 cambian cada 50 milisegundos a unos nuevos valores.
- Encripta y cambia el algoritmo de encriptación rápidamente.
- La velocidad en la aleatoriedad del código puede variar según la finalidad del CPU.
- Cuenta con un detector de ataque, que permite saber cuándo sufre uno y poder así, aumentar la velocidad de cambio.

Posibles Soluciones en los Sistemas Operativos

- 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.

Posibles Soluciones en los Sistemas Operativos

Cuando un Sistema Operativo interactúe con un dispositivo externo tiene que tener en consideración lo siguiente:

- 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.

Posibles Soluciones - Apps Móviles

- Aplicar mecanismo de autenticación como *usuario/contraseña*.
- Aplicar control de autorización y autenticación del lado del servidor.
- Tener auditoría de cualquier movimiento realizado en la aplicación.
- Evitar realizar intercambio de datos, descargas y actualizaciones vía HTTP.

Cuando el uso de la aplicación sea fuera de línea:

- Instrumentar verificaciones de integridad local dentro del código para detectar cualquier cambio de código no autorizado.

Posibles Soluciones - Desarrolladores de Apps Móviles

Los desarrolladores no tienen control sobre cambios y/o fallas de los sistemas operativos, por lo que deben realizar ataques a su aplicación y al sistema operativo para observar como se manejan en los siguientes aspectos:

- *Logging*
- Almacenamiento en caché de URL.
- Almacenamiento en caché de ingreso de datos.
- Almacenamiento en caché de copiar/pegar.
- Almacenamiento de datos HTML5.
- Objetos de cookies del navegador.
- Datos enviados a terceros.

Posibles Soluciones - Usuarios

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.

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.