Universidad nacional autónoma de México

Sistemas Operativos

Sistemas operativos en la vida real

Barbosa Carranza Andrés Luisós 313055407

0.1 Introducción.

Para este documento se realizó una lectura de 4 noticias, además de otros ejemplos de hackeos en sistemas operativos los cuales presentan fallas de seguridad en los diversos sistemas. Se identificó a nivel de sistema operativo cuales eran los problemas, además de hacer sugerencias para posibles correcciones o características que deberían presentar dichos sistemas para evitar errores.

La creación, desarrollo y evolución de los sistemas operativos han sido básicos para el acercamiento al consumidor particular de productos especialmente sensibles para el gran consumo, como son los ordenadores y los teléfonos móviles; ahora en la actualidad debido a la gran tendencia de la tecnología, ha habido un enorme crecimiento en dispositivos que se controlan por software, lo cual hace indispensable el uso de un sistema operativo.

Un sistema operativo se considera el nexo de la unión entre la computadora y una persona común. Es el software que gobierna una máquina, el conjunto de procesos que determinan lo que se ve y lo que se desea haga un dispositivo con cada acción que realiza el usuario. Dada la enorme tendencia del mundo actual, las empresas se han inclinado a que sus productos sean manipulados por software lo cual deja expuestos a peligros informáticos, los cuales se presentan a continuación en diversos casos.

En noticias recientes se han presentado casos de violaciones a los sistemas de seguridad de los sistemas operativos, como tal es el caso del vehículo Jeep Cherokee, donde un par de hackers pudieron acceder de manera remota al sistema operativo del vehículo, pudiendo cambiar la velocidad, aplicar los frenos, manejar el radio, limpiaparabrisas y manipular los cambios.

Otro caso de hackeo fue el del BMW X5 blindado perteneciente al jugador de futbol, David Beckham, el cual fue robado por ladrones, los cuales usaron una laptop para acceder al vehículo y poder acceder a el y arrancar el motor.

En el pasado, los ladrones usaban palancas para robar un vehículo, en la actualidad les basta con una laptop.

0.2 Riesgos en automóviles

0.2.1 El problema

Dada la tendencia de los vehículos a incluir más equipo electrónico y conducción automática estos se vuelven un nuevo objetivo para los hackers o piratas informáticos. Lo cual provoca un extenso esfuerzo para proteger la seguridad de los usuario. Ocurrieron casos en donde piratas informáticos podían acceder a un vehículo de manera remota y activar o bloquear funciones del mismo, además de rastrear su ubicación. Algunos piratas informáticos como es el caso de Samy Kamkar trabajan en conjunto con empresas para identificar vulnerabilidades y ayudar a eliminarlas.
Un ataque puede resultar en el control total del vehículo, de tal forma que se podría manipular la conducción automática y dirigir el vehículo donde se plazca.
Un automóvil tiene alrededor de 150 millones de lineas de código y dicha complejidad puede llevar a un ataque cibernetico, el cual puede ser ignorado como riesgo. Por tal motivo, las empresas se ven obligadas a proporcionar un sistema de seguridad para los vehículos, pues el riesgo podría no ser solo costoso.

Una manera de hackear un vehículo es mediante las redes inalambricas que tiene, pues de manera remota se puede conectar al sistema y empezar a usar diversas funciones, lo cual estaría involucrando un problema de seguridad enorme pues no se tiene un exacto control sobre los dispositivos conectados al sistema, además de que los sistemas críticos del vehículo pueden ser manipulados por medio de software, lo cual pone en riesgo la seguridad del conductor.

Los hackers de "sombrero blanco" pueden ser los encargados de identificar las vulnerabilidades del sistema y trabajar en conjunto con las empresas para eliminar los riesgos. Sin embargo, cualquier persona con malas intenciones puede explotar dichas vulnerabilidades.

Algunos ejemplos de sistemas operativos para automóviles pueden ser:
OSEK/VDX que nació en 1993 por la unión de los desarrollos realizados por las empresas alemanas BMW, Bosch, DaimlerChrysler, Opel y Siemens entre otros, está diseñado para requerir un mínimo de recursos de hardware

y funciona incluso con microprocesadores de 8 bits.

Jaspar que es una iniciativa impulsada por el gobierno japonés y que reúne a diez compañías japonesas de automóviles e informática. Toyota, Nissan, Honda y Toshiba entre otros, se han unido para desarrollar un sistema operativo propio para vehículos que incluye módulos específicos para cada uno de los modelos.

0.2.2 Una posible solución

Pedir una autorización e identificación a cada dispositivo que se conecta a la red del vehículo.
Una alternativa podría ser la de añadir una encriptacion a las instrucciones que reciben los sistemas críticos, para que sea difícil acceder o interferir con las comunicaciones del sistema. Parecido al sistema de los aviones, los cuales tienen un sistema prácticamente impenetrable.
La complejidad del código del vehículo también puede considerarse como una vulnerabilidad, por lo que un código separado por módulos puede ser una opción. Manejar actualizaciones para parchar posibles vulnerabilidades y asignar un ciclo de vida a cada actualización y un ciclo de vida de seguridad, pueden mejorar bastante la seguridad llevando una revisión diaria. Cada actualización debe mejorar acciones de respuesta y agregar funcionalidades nuevas, además de extender el ciclo de vida de cada actualización.

0.3 El caso de Pandora y Viper

0.3.1 El problema

Con motivo de resolver el problema de la inseguridad en automóviles modernos, marcas como Pandora, Viper y Clifford se dedican a crear sistemas de seguridad para vehículos. Dichos sistemas consisten en alarmas de seguridad supuestamente inhackeables. Sin embargo, investigaciones recientes revelan que estos sistemas tienen fallos enormes.
Se encontró que en los sistemas desarrollados de Pandora se permite al usuario restablecer la contraseña y/o correo electrónico de cualquier cuenta prácticamente desde cualquier otra cuenta y esto sin ninguna autentificación. Gracias a esa facilidad de cambios se podía tomar el control de forma remota,

rastrear cualquier vehículo en tiempo real, activar la alarma, abrir cerraduras, arrancar el motor, entre otras funciones.
Mientras que en Viper se encontró que se podía usar una cuenta para acceder a los perfiles de otros usuarios y cambiar contraseñas.
Un atacante puede ser capaz de secuestrar el vehículo por completo, pues gracias a ambas aplicaciones, el atacante puede rastrear su ubicación, detenerlo e incluso meterse con el acelerador y frenos, incluso escuchar lo que dicen las personas al interior del vehículo. Así mismo, el atacante puede ser capaz de bloquear el sistema para que el usuario sea incapaz de tener acceso a el.

0.3.2 Una posible solución

El error en estos casos fue provocado gracias a la aplicación de la alarma más que al sistema operativo del vehículo. Se menciona que fue gracias a una actualización que no fue verificada correctamente que ocurrió el error. Por lo que como sugerencia se debería tener en cuenta el proceso de verificación de actualizaciones. Así como al igual que en el caso anterior se deben cifrar las comunicaciones con el sistema para que sea muy difícil para cualquier atacante mandar instrucciones. Se debe proporcionar para la aplicación un sistema de seguridad eficiente y un sistema de control y autenticacion de lado del servidor y de manera local. Se debería de igual manera llevar una bitácora de las instrucciones seguidas.

0.4 Hackeo a scooters

0.4.1 El problema

Una cantidad de scooters es hackeada, permitiendo acceso a su archivo de audio, cambiándolo y poniendo en su lugar otros archivos de audio ofensivos. Sin embargo el hackeo no ponía a los usuario en ningún riesgo físico.
La compañía aclaró que modificar su sistema operativo requería de un conocimiento intimo de su software e ingeniería. Sin embargo es preocupante pues al parecer un usuario con un smartphone puede acceder al sistema del scooter y alterar su funcionamiento.
Se notifica que a través de un dispositivo Bluetooth se puede bloquear un scooter e insertar un malware que tomara control sobre el, pudiendo acelerar o frenar de manera inesperada. El problema está en que se puede acceder

de manera remota desde un dispositivo con autorización Bluetooth al sistema del scooter, lo cual representa una falta de control en los dispositivos que pueden conectarse al dispositivo, así como de las instrucciones para el scooter.

0.4.2 Una posible solución

Como sugerencia se podría que las instrucciones estuvieran encriptadas para que sea difícil comandar instrucciones al scooter sin saber el código. Se debería también de pedir una autentificacion para los dispositivos conectados al sistema del scooter, o en su defecto tener una lista de dispositivos permitidos y que está estuviera también encriptada.

0.5 Hackeo a smartwatches

0.5.1 El problema

Según una investigación sobre los dispositivos electrónicos, se revela que los dispositivos que se visten, en este caso, los smartwatches presentan una gran oportunidad para los hackers. Según los especialistas, estos equipos y todos los que dependan de una aplicación para su configuración, cuentan con tres grandes problemas de seguridad: el dispositivo (la tecnología bluetooth por ejemplo), las apps y la nube (el software), esto, sumado al poco tiempo de desarrollo no es suficiente para hacer frente a cualquier ataque.

Como puntos débiles para estos dispositivos se puede encontrar que:

almacenan en texto plano muchos datos, como los mensajes que el dispositivo usa para las indicaciones por voz, así como el nombre del usuario del smartwatch. El reloj es capaz de compartir esos datos con otras aplicaciones o cuando se conecta al móvil mediante Bluetooth. En este proceso se envían todo tipo de datos, como mensajes, llamadas o información biométrica. Lo cual puede ser interferido por un hacker y el mismo podría robar información.

Muchos relojes comparten datos con servicios almacenados en la nube para posteriormente verlos en el computador y analizarlos. Sin embargo, una mala configuración puede hacer que se filtren estos datos, pudiendo identificar a

una persona, su dispositivo, y consecuentemente sus información personal.

0.5.2 Una posible solución

Los desarrolladores deberian aplicarar un cifrado adecuado al enlace wearable-a-smartphone e implementar Bluetooth correctamente.

Ser precavidos con la información que se envía por medio de bluetooth pues este puede generar fugas de información ya que cualquier dispositivo podría conectarse a esa red.

Guardar la información en distintas bases de datos para reducir el hackeo a los servidores y proteger la información en varias bases.

0.6 Ataques ransomware de Wannacry

0.6.1 El problema

WannaCry es el nombre que se le asigna al criptogusano por el medio del cual se hacen ataques informáticos dirigidos al sistema operativo de microsoft Windows. Durante el ataque, los datos de la victima son encriptados y se solicita un rescate economico pagado con la criptomoneda bitcoin para poder recuperar los datos.

Este se trata de un ataque masivo que empezó en mayo de 2017 y ha infectado a más de 230,000 computadoras a lo largo del mundo. Los ataques ransomware normalmente infectan una computadora cuándo un usuario abre un email phishing (de suplantación de identidad) y, a pesar de que presuntamente emails de esta clase serían los causantes de la infección WannaCry, este método de ataque no ha sido confirmado. Una vez instalado, WannaCry utiliza el exploit conocido como EternalBlue, desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA), para extenderse a través de redes locales y anfitriones remotos que no hayan recibido la actualización de seguridad más reciente, y de esta manera infecta directamente cualquier sistema expuesto.

0.6.2 Soluciones propuestas

Se lanzo una actualización con parche crítico emitido por Microsoft el 14 de marzo de 2017 para eliminar la vulnerabilidad subyacente para sistemas soportados por Microsoft en la actualidad, lo cual se dio casi dos meses antes del ataque, sin embargo, muchas organizaciones no llegaron a aplicarlas. Las máquinas usando sistemas más antiguos, para los que Microsoft no publica actualizaciones, como Windows XP y Windows Server 2003, se encontraban en una situación de riesgo, sin embargo Microsoft ha tomado la decisión inusual de publicar actualizaciones para estos sistemas operativos. Poco después de que habia comenzado el ataque, el investigador de seguridad web, MalwareTech, accionó sin advertirlo un "botón de apagado" propio del gusano, al registrar un nombre de dominio hallado en el código del ransomware. Esto retrasó la difusión de la infección, pero se han detectado nuevas versiones que carecen de este "botón de apagado".

0.7 Conclusión

Con la creciente tendencia de las empresas a introducir software a sus productos, estos casos de hackeos deben ser una llamada de atención para los mismos. Por lo cual deben de mejorar los sistemas de seguridad e incentivar a los hackers que detectan las vulnerabilidades a trabajar con ellos. Hackear un sistema operativo en la mayoría de veces no es nada fácil, pues el hacker necesita de un amplio conocimiento del sistema, sin embargo es posible, por lo cual es un peligro bastante presente para los usuarios y las compañías. Por eso se deben tomar las medidas de seguridad necesarias para proteger la seguridad de los datos del usuario y con el crecimiento de la tecnología, su misma seguridad física.

0.8 Bibliografía

- Javier Costas. (2014). Sistemas operativos en el coche, el futuro del automóvil. 12 de junio de 2019, de motorpasion Sitio web: `https://www.motorpasion.com/tecnologia/sistemas-operativos-en-el-coche-el-futuro-del-aut`

- Steve Lawless. (2019). Carhacked! (9 Terrifying Ways Hackers Can Control Your Car). 12 de junio de 2019, de Purple Griffon Sitio web:

https://purplegriffon.com/blog/carhacked-9-terrifying-ways-hackers-can-contro

- Dimitar Kostadinov. (2014). The Future is Now: Car Hacking. 12 de junio de 2019, de Infosec Sitio web: https://resources.infosecinstitute.com/future-now-car-hacking/#gref.

- Peter Holley. (2019). In Australia, hacked Lime scooters spew racism and profanity. 12 de junio de 2019, de The washinting post Sitio web: https://www.washingtonpost.com/technology/2019/04/24/australia-hacked-lime-sc?noredirect=on&utm_term=.5f33a7c49774.

- anonimo. (2014). How hard or easy is it to hack the computer of a car?. 12 de junio de 2019, de Quora Sitio web: https://www.quora.com/How-hard-or-easy-is-it-to-hack-the-computer-of-a-car.

- Jim Motavalli. (2019). Locking More Than the Doors as Cars Become Computers on Wheels. 12 de junio de 2019, de The New York Times Sitio web: https://www.nytimes.com/2019/03/07/business/car-hacks-cybersecurity-safety.html.

- anonimo. (2017). Ataques ransomware WannaCry. 12 de junio de 2019, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Ataques_ransomware_WannaCry.

- Rosselyn Barroyeta. (2018). Los smartwatch son más vulnerables al hackeo de información. 12 de junio de 2019, de TekCrispy Sitio web:https://www.tekcrispy.com/2018/03/22/smartwatch-vulnerables-hackeo/.