Sistemas operativos en la vida real

Barbosa Carranza Andrés Luisos

Universidad nacional autónoma de México.

Junio 2019

Introducción

Para este documento se realizó una lectura de 4 noticias que presentan problemas con los sistemas operativos actuales. 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.

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 las 4 noticias que trata este documento.

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. Un ataque puede resultar en el control total del vehículo, de tal forma que se podría dirigir el vehículo donde se plazca.

Sugerencias de solucion

Pedir una autorización e identificación a cada dispositivo que se conecta a la red del vehículo.

añadir una encriptacion a las instrucciones que reciben los sistemas críticos, para que sea difícil acceder o interferir con las comunicaciones del sistema.

Riesgos en automóviles 2

El caso de Pandora y Viper

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.Sin embargo, investigaciones recientes revelan que estos sistemas tienen fallos enormes.

Sugerencias de solucion

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.

Tercera noticia: Hackear tu vehículo puede ser más fácil de lo que crees

El problema

Los automóviles actuales cada vez tienen más tendencia a ser controlados por medio de software, lo cual los deja expuestos a vulnerabilidades de seguridad del software, pues se vuelven accesibles a hackers que usan redes para explotar las vulnerabilidades. Un acceso a la red del vehículo puede poner en riesgo la información del usuario además de su propia seguridad física.

Sugerencias de solucion

Encriptar los comandos digitales que puedan activar acciones físicas.

Pedir una validación e identificación o dirección IP para cada dispositivo que quiera conectarse.

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. 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.

Sugerencias de solucion

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.

Hackeo en scooters 2

El problema

Se revela que los dispositivos que se visten, en este caso, los smartwatches presentan una gran oportunidad para los hackers. Como puntos débil para estos dispositivos se puede encontrar que almacenan muchos datos, como el nombre del usuario del smartwatch. El reloj es capaz de compartir esos datos como mensajes, llamadas, etc.

Sugerencias de solucion

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.

Hackeo en smartwatches 2

Ataques ransomware de Wannacry

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.

Sugerencias de solucion

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.