Sí, un hacker podría robar su auto

El futuro planteado en películas como "Blade Runner" o "I Robot" de autos guiados en superautopistas podría ser más cercano de lo pensado si se toman en cuenta los adelantos en ingeniería de las principales casas fabricantes. Sin embargo, abrir al mundo esa posibilidad podría conllevar severos riesgos si no se toman en cuenta los desafíos en materia de seguridad que esto representa. Presentamos en exclusiva un análisis del futuro de la industria automotor en el tema de seguridad informática.

Los autos actuales ya poseen componentes inteligentes; entre ellos, una computadora que registra todos los sensores de aire, combustible o calor. El futuro va más lejos.

1913
Ford Motor Company comenzó con el desarrollo en serie de vehículos con su modelo de leyenda: el Ford T.

2012
la industria es dominada por fabricantes asiáticos y entre sus metas está el desarrollo de sistemas de autoguíado.

ROSA MARTÍNEZ
REVISTAS@LAPRENSAGRAFICA.COM

En enero, durante el International CES 2012, el mundo fue testigo de la ola de nuevas tecnologías que las empresas automovilísticas están implementando para las próximas generaciones de automóviles. Capacidades como la conducción de forma semiautónoma, estacionarse casi por sí solos y recibir y transmitir información en tiempo real son ejemplos de lo que la industria promete en un futuro cercano.

Tradicionalmente, la mayoría de los autos poseen sistemas informáticos integrados, pero muy rudimentarios, que solo cumplen funciones básicas, como medir la cantidad de combustible, hacer la transmisión más suave u optimizar el rendimiento y el consumo de gasolina.

"Muchas de las funcionalidades computacionales de los automóviles, que antes veíamos solo en las películas, son hoy una realidad. La gran mayoría de estos vehículos poseen alta tecnología y son controlados completamente por una o más computadoras en la forma de sistemas embebidos, conocidas como Engine Control Unit (ECU)", asegura Gabriel Acevedo, investigador en seguridad de McAfee.

Considerando que la industria automotriz ha empezado a lanzar al mercado autos con navegadores capaces de determinar la ubicación del mismo o que incluyan sistemas de información embebidos, nos preguntamos: ¿qué tan lejos estamos de observar fraudes electrónicos o scams que se aprovechen de la situación?

Vale la pena mencionar que los exploits de navegadores en plataformas más tradicionales tienen ya un largo y amplio listado de fallos y vulnerabilidades que han sido aprovechados por los ciberdelincuentes.

Si pensamos que los autos estarán cada vez más dotados de altas prestaciones informáticas capaces de asistir en la conducción con información relevante, ¿no podría ser esta una nueva y fecunda plataforma para fines delictivos? La respuesta es sí.

Hace un año, durante el Black Hat 2011, se realizaron demostraciones donde expertos vulneraron la seguridad de un automóvil que utilizaba tecnología inalámbrica. (Ver video: "The Hack and the Furious").

Durante la demostración, dos informáticos fueron capaces de desbloquear las puertas de un automóvil y encender el motor de forma exitosa. El método empleado les permitió enviar comandos de forma remota a un

El sector automotriz toma en serio el futuro de la conducción. Herramientas como Google Maps o sistemas comunitarios como Waze ya se enfocan en identificar rutas y evitar atascos.

>>Vicente Díaz,
analista de Kaspersky

“Cada modelo utiliza distintas tecnologías, por lo que no es fácil dar una solución genérica. Si bien es cierto que muchas firmas ya tienen en cuenta la seguridad en el diseño.”

>>Limor Kesser,
experta de EMC–RSA

“La industria sufre un ataque de robo de datos cada cinco días (...) Sin embargo, cualquier inconveniente que ocurra durante ese proceso podría traer serias consecuencias.”

>> Hellmuth Sole,
Toyota Motor Corporation

“Al final del día, no serán las corporaciones las que decidan cuáles serán los aspectos por definir en el tema de los autos interconectados, sino que serán los gobiernos.”

>>Guillermo Cortez,
Widefense

“Solo bastaría alguien con intenciones maliciosas con acceso al código de la computadora controladora en el taller automotriz para hacer la ingeniería inversa.”

automóvil modelo Subaru Outback, quitar los seguros e incluso encenderlo sin siquiera tocarlo, romper algún cristal o manipular el switch de encendido.

Uno de los hackers, Don Bailey, asegura que puede abrir cualquier auto con solo enviar mensajes de texto desde su teléfono Android.

Ahí quedó demostrado que los exploits que utiliza Java –y que muchas veces funcionan de forma independiente al sistema operativo– podrían perfectamente afectar un automóvil que utilice alguna aplicación desarrollada en ese lenguaje.

“Un vehículo que utilice alguna aplicación como Java podría prestarse al robo de información almacenada en la computadora del mismo o incluso traer consecuencias mucho más graves, como permitir que se abran sus puertas, convirtiéndolo en un objeto de fácil sustracción”, dice Rodrigo Calvo, ingeniero de preventa de Symantec para el norte de América Latina.

Según especialistas en seguridad informática, lo primero que necesita un atacante es poder comunicarse con el automóvil, ya sea mediante contacto físico o utilizando cualquier medio de comunicación (GPS, Bluetooth, acceso a internet o a un teléfono integrado).

Prácticamente, todos los automóviles modernos poseen sistemas de diagnóstico a bordo, conocido como On–Board Diagnostics (OBD), que proveen acceso directo a las redes internas del automóvil.

Muchos de estos vehículos proveen también interfaces inalámbricas con rangos de distancia cortos, como el Bluetooth, o distancias mucho mayores, como las redes celulares, lo que abre una ventana para que los sistemas puedan ser vulnerados si alguien logra acceder a estas redes.

Un ejemplo es el robo de vehículos que controlan el acceso en forma computarizada y que requieren un

Los modelos más recientes de las casas automotrices incluyen elementos de nueva generación, como sistemas de navegación por GPS.

En la edición 2011 del CES de Las Vegas, las casas de fabricantes automotrices presentaron al público más cualidades tecnológicas en sus bólidos.

El panorama del sector en la región

Consultamos a varios firmas que venden automóviles en la región para ver qué tanto estaban al tanto de esta realidad. En Hyundai nos informaron, a través de su agencia de relaciones públicas, que no poseen datos de este tema, por lo que preferían no referirse al respecto.

En el caso de Ford, supimos que el fabricante comenzó a inicios de agosto de este año una serie de pruebas en vehículos, como parte de un programa de investigación destinado a avanzar las comunicaciones coche–a–coche y coche–a–infraestructura en las carreteras europeas, con el fin de expandir sus resultados al resto del mundo.

"Las comunicaciones coche–a–coche y coche–a–infraestructura representan los próximos avances de gran importancia en materia de seguridad. Ford está comprometido a realizar pruebas reales aquí y en todo el mundo con el objetivo de implementar estas tecnologías en un futuro cercano", expresó el jefe técnico y vicepresidente de innovación e investigación de Ford, Paul Mascarenas.

Por su parte, Toyota Motor Corporation trabaja de la mano con Intel para definir la próxima generación de sistemas de información y entretenimiento a bordo de automóviles. La alianza empezó en 2006 y es parte de los avances que Toyota tiene en la materia.

Hellmuth Sole, gerente de educación para América Latina y el Caribe de Toyota Motor Corporation, considera que al final del día no serán las corporaciones las que decidan cuáles serán los aspectos por definir en el tema de los autos interconectados, sino los gobiernos, ya que no pueden arriesgarse a colocar vehículos en las calles que terminen siendo un peligro para la seguridad nacional (escuchar audio: "Entrevista a Hellmuth Sole").

También consultamos a empresas, como AutoStar, Agencia Datsun, Veinsa, Porshe y Excel Automotriz; pero, para el momento, aún no habíamos recibido sus respuestas.

Una de las vulnerabilidades encontradas en los autos de nueva generación, hasta ahora, es que podrían ser infectados incluso por medio de discos compactos de música.

Los autos de alta gama son los primeros en incorporar adelantos. Más allá de las computadoras que registran funciones básicas, los nuevos diseños prometen el autoguíado.

token de seguridad, generalmente una key fob. Según los expertos de McAfee, se ha demostrado que en varios modelos de estos automóviles es posible reprogramar el sistema que lee las llaves, para así acceder al vehículo sin autorización.

Otro ejemplo son los centros de entretenimiento. Si el usuario quiere que el mismo esté basado en Android, para conectar su teléfono y descargar aplicaciones que muestren el estado del motor, deberá haber una conexión entre ambos sistemas.

En caso que se produzca una infección, ya sea intencionada o casual en el sistema Android, el resto de sistemas interconectados se pueden ver afectados y actuar de forma inesperada ante la presencia de un componente desconocido.

"Hay que pensar que la mayoría de componentes de la industria que controlan distintos subsistemas del auto (como la dirección, la tracción o el motor) fueron diseñados hace años sin tener en cuenta ningún tipo de medida de seguridad informática, por lo que son un objetivo muy sensible en caso de una hipotética infección", asegura Vicente Díaz, analista senior de malware en Kaspersky Lab.

Según Díaz, incluso podemos ver algunos escenarios de ataque –que ya se han probado vulnerables– como infectar vehículos a partir de la lectura de un CD. No hace mucho, investigadores de las universidades de California y Washington explotaron una vulnerabilidad en el decodificador de Windows Media Audio presente en el reproductor de CD, logrando acceder a los sistemas internos del automóvil.

Podemos pensar en un atacante subiendo un CD a cualquier servicio de compartición de ficheros con un nombre atractivo, como "Mejores temas para conducir" para posteriormente infectar todos los vehículos vulnerables que lo reproduzcan.

Piénselo un momento: en la actualidad, cualquier ingeniero o técnico automotriz es capaz de conectarse a la computadora de auto y solicitar toda la información que este registra o ver y diagnosticar el estado.

Esto se realiza a través de un computador que está diseñado para comunicarse e intercambiar la información que esas computadoras registran y las instrucciones que el mecánico automotriz ingresa.

"Creo que bastaría con que alguien con intenciones maliciosas tenga acceso al código de la computadora controladora en el taller automotriz para hacer la ingeniería inversa. Así como el software le abre todo un mundo de posibilidades a las automotrices, también lo hace para los hackers", comenta Guillermo Cortez, product manager para Widefense.