technology review.es
Published by MIT

Segunda-feira, 11 de agosto de 2014

Black Hat: Segurança em Carros Deve Piorar, Dizem Pesquisadores

Aplicativos a bordo de automóveis e conectividade sem fio são uma bênção para hackers que visam atacar carros.
Por Robert Lemos

À medida que a conectividade sem fio e os aplicativos se tornam mais comuns nos carro, mais deles se tornarão vulneráveis a hackers potencialmente perigosos, advertiram dois importantes pesquisadores na quarta-feira durante a conferência de segurança Black Hat que ocorreu em Las Vegas.

Em um estudo com cerca de 20 veículos diferentes, Charlie Miller, engenheiro de segurança do Twitter, e Chris Valasek, diretor de pesquisa em segurança veicular da empresa de serviços de segurança IOActive, concluíram que a maioria dos sistemas de controle não foi projetada com foco na segurança e pode ser comprometida remotamente. A dupla criou classificações de segurança cibernética para os veículos, que serão publicados em um artigo no final desta semana.

"Quando você está buscando um carro para comprar, você pode pegar uma revista e ela vai dizer: 'Aqui estão as características de segurança deste carro", disse Valasek. "Por que nós não podemos, como indústria de segurança, começar a fazer relatórios que dizem: 'Estes carros têm boa segurança cibernética e estes carros não têm boa segurança cibernética'?"

À medida que a indústria automotiva acrescenta mais sistemas de controle e computadores integrados, os veículos tornaram-se mais fáceis de hackear. Em 2011, pesquisadores da Universidade de Washington e da Universidade da Califórnia, São Diego, analisaram um sedã de classe média e descobriram que ele poderia ser comprometida inserido-se um disco no seu leitor de CD, o equipamento de diagnóstico utilizado pelos mecânicos ou uma conexão de celular.

Desde então, outros grupos de pesquisa têm estudado a segurança dos carros e demonstrado maneiras de tomar o controle de freios, aceleração e outras funções. Veículos de alto desempenho geralmente têm controle computadorizado de freios e aceleração para prevenção de colisões, controle de velocidade e direção automática para permitir o estacionamento automatizado e permanecer dentro da faixa.

Ataques a sistemas de controle automotivo envolvem três etapas, de acordo com Valasek e Miller. O invasor precisa primeiro encontrar uma maneira de invadir um sistema do veículo, em seguida, usar essa vulnerabilidade para enviar um comando para a unidade de controle eletrônico (ECU) e, finalmente, fazer com que a ECU execute o comando.

Devido à proliferação do acesso sem fio em veículos, em especial a conectividade Bluetooth e celular, a execução remota é, cada vez mais, possível. A viabilidade do envio de comandos a unidades de controle eletrônico que gerenciam diferentes funções do veículo depende do projeto do carro.

As empresas de veículos precisam projetar seus sistemas para detectar tentativas de invasão e impedir que a segurança seja comprometida, Miller disse: "Queremos tornar cada um destes três passos mais difícil para o invasor".

Mas, com as montadoras competindo em recursos, a adição de aplicativos ao carro, desde navegação até streaming de música, poderia deixar o veículos mais vulnerável, acrescentou Miller. "Aplicativos para uso dentro do carro e recursos estilo desktop representam grandes ameaças futuras", disse ele.

Incorporar segurança em veículos é especialmente importante porque a implementação de reparos de software é problemática. Atualizar o software de um carro significa trazer o veículo a uma revendedora para assistência, algo que a maioria dos proprietários não quer fazer.

"Quando você começa a receber avisos [de RECALL] via e-mail, você começa a ignorá-los",

disse Valasek. "Vai ser muito difícil, se uma vulnerabilidade real aparecer, de corrigir o problema".