Por Tom Srail (*)

 Os fabricantes de automóveis estão preocupados em garantir uma maior segurança aos passageiros e prevenir o potencial de ataques cibernéticos dos carros "conectados".

Segundo um relatório divulgado em maio pelo BI Inteligence, em 2020, 75% dos carros lançados mundialmente irão permitir que as pessoas compartilhem músicas, procurem por filmes, acompanhem em tempo real o trânsito e as condições climáticas, e ofereçam ao motorista diversas opções de suporte como, por exemplo, o auto estacionamento.

Os pesquisadores americanos dizem que o mercado de carros conectados irá crescer anualmente cerca de 45% pelos próximos cinco anos, um incremento 10% maior que o do próprio mercado de automóveis. Segundo o BI Intelligence, dos 92 milhões de carros previstos para serem entregues em 2020, três quartos devem oferecer hardwares de conexão com a Internet.

No entanto, conforme a conexão com a Internet tornar-se mais comum nos módulos de controle dos veículos e do lançamento de um número maior de dispositivos usados em automóveis, o risco com a segurança e privacidade das informações também aumentará.

Definindo o problema

Recentes estudos da Universidade da Califórnia e da Universidade de Washington revelam que quase todos os sistemas de controle em um carro moderno podem ser comprometidos e controlados remotamente. Isso porque a maioria dos sistemas de segurança foi desenvolvida antes do surgimento das opções de conectividade existentes atualmente.

Hoje, um mercado diversificado de aplicativos de “entretenimento tecnológico” está sendo projetado especificamente para carros como, por exemplo, diagnósticos digitais, serviço de monitoramento para novos motoristas, sistemas de navegação e outros serviços pensados para toda essa nova linha de carros conectados.

Segundo a consultoria McKinsey, as vendas desses automóveis devem crescer para $220 bilhões em 2020, bem acima dos $39 bilhões gerados em 2014.

Os carros novos já sairão das fábricas com pontos de acesso wireless, sistemas de telemática, conectividade via Wi-Fi e Bluetooth, além de sistemas de scanner. À medida que os aplicativos de smartphones forem integrados aos carros, como, por exemplo, o CarPlay da Apple, oportunidades para as ações dos hackers também crescerão exponencialmente.

No entanto, poucos questionam que a rápida expansão da tecnologia de conecção dos carros já ultrapassou a capacidade dos fabricantes de automóveis em proteger os consumidores contra os ciberataques.

Em fevereiro de 2015, o senador americano Edward Markey escreveu um artigo sobre o tema. No texto, o senador detalha que encontrou montadoras que não tinham conhecimento e não conseguiam identificar a escala atual do problema, simplesmente porque não mantinham ou compartilhavam registros de possíveis invasões.

Além disso, verificou-se que quase todos os fabricantes de equipamentos originais (OEM), fornecedores de componentes para carros conectados, eram incapazes de responder aos ataques em tempo real, embora alguns tivessem sistemas de bordo que possibilitavam o registro das informações sobre as violações para uma recuperação posterior.

A conclusão do artigo foi que todas as empresas envolvidas com a indústria automobilística terão que desenvolver, rapidamente, a capacidade de se defender contra-ataques cibernéticos.

Definindo os riscos

A maioria dos especialistas em segurança acredita que a dimensão dos riscos emergentes só será plenamente compreendida quando descobrirmos a motivação dos ciberterroristas. O que os criminosos têm a ganhar?

Infelizmente, parece haver muitas razões para se conectar a um carro ligado, algumas das quais se estendem além da motivação financeira usual para ataques a computadores e smartphones pessoais. Entre as razões já levantadas estão:

Lucro ou ganho financeiro

- Roubo de propriedade, incluindo do próprio automóvel
- Conquistar uma vantagem comercial, como, por exemplo, desativar o modelo auto-maker da empresa rival para causar dano de marca
- Espionagem industrial, ou roubo de propriedade intelectual dos softwares

Crime organizado, terrorismo e vingança pessoal

- Engano ou neutralização do software e/ou hardware de restrições
- Violação de privacidade, como rastreamento ou perseguição de pessoas
- Causar danos a um motorista, passageiro, pedestre ou pessoas que estão na estrada
- Danos de infraestrutura: desabilitar e/ou controlar uma frota de carros como forma de interromper ou mesmo parar o transporte de uma cidade inteira

Qualquer incidente pode afetar as metas financeiras de empresas, o aumento de indenizações por responsabilidade civil, ou ainda impactar negativamente o valor da marca de uma montadora ou de fornecedores de componentes eletrônicos. Por estas razões, alguns setores da indústria automobilística dos Estados Unidos estão considerando os recursos possíveis para medir o risco e construir estratégias adequadas de defesa à ciberataques.

Resposta da Engenharia

Uma extensa reengenharia de arquitetura de sistemas para o suporte cibersegurança - incluindo o desenvolvimento de hardwares e softwares específicos – serão exigidos de diversos controles automotivos. Será necessário também um trabalho adicional para melhorar a proteção dos dados e a integridade dos controles que protegem o acesso a esses sistemas.

A teoria mais abrangente da indústria de design de sistemas de segurança tem que assumir que violações de segurança cibernética irão ocorrer e soluções operacionais de forma padrão devem fornecer proteção contra a intrusão, além de um monitoramento constante de comportamentos suspeitos, enquanto o carro estiver em operação.

A implantação de tal extensa tecnologia terá custos significativos para a indústria automobilística e pode levar uma década para que seja implementada integralmente. Mas os custos de não se construir sistemas de cibersegurança robustos para a nova era carros conectados serão mesuradas em despesas legais, responsabilidades civis para com os clientes, além, é claro, de perda de reputação corporativa das empresas envolvidas.

Claramente, carros conectados irão requerer soluções inteligentes.

(*) **Tom Srail** é líder regional paras as indústrias de Tecnologia, Media e Telecomunicações da Willis Towers Watson. O executivo tem mais de 20 anos de experiência nos setores de seguros e tecnologia. É responsável também por supervisionar o Centros de Excelência em Tecnologia, Media e Telecomunicações da empresa em São Francisco, Nova York e Dallas.

(15.03.2016)