Universidade Federal de Pernambuco
Centro de Informática
Graduação em Engenharia da Computação

In-Vehicle Network Security : Attacks and Countermeasures

Proposta de Trabalho de Graduação

Aluno: Caio Augusto Pereira Burgardt (capb@cin.ufpe.br)
Orientador: Divanilson Rodrigo Campelo (dcampelo@cin.ufpe.br)
Área: Segurança em Redes Automotivas

19/09/2018

Resumo

Redes automotivas estão crescendo em tamanho e complexidade. Essas redes utilizam várias tecnologias diferentes e agora a indústria está adicionando Ethernet aos veículos. Para proteger qualquer ambiente conectado, são necessárias soluções de segurança para lidar com as possíveis ameaças para cada tecnologia utilizada. Ataques recentes mostraram que as redes automotivas, apesar de parecerem isoladas, podem ser atacadas com uma certa facilidade; se o atacante tem acesso à rede interna, não existem soluções de segurança eficientes para impedi-lo de afetar funções de um automóvel. Neste trabalho de graduação, serão estudados ataques e medidas que a indústria automotiva vem adotando para se proteger. Também será proposto um modelo de segurança para a Ethernet automotiva baseado em MACsec.

Introdução

Os automóveis de hoje podem ser considerados como redes de computadores sobre rodas. Os nós nessas redes são tipicamente *Electronic Control Units* (ECUs) responsáveis por várias funcionalidades do carro. Embora as ECUs sejam dispositivos frequentemente vulneráveis por não tratar suas entradas, redes intraveiculares costumavam ser uma superfície de ataque isolada e de difícil acesso, o que tornava os automóveis alvos de ataque não atraentes para *hackers*. Essa crença de que os carros sempre seriam simples demais e isolados demais para serem atacados resultou em redes automotivas que evoluirem em complexidade e tamanho sem a consideração de falhas de segurança, demonstradas, por exemplo, no design do protocolo Controller Area Networks (CAN) [1] . Os veículos de hoje têm muitas tecnologias diferentes de rede dentro de si, mas a CAN é indiscutivelmente a principal tecnologia de rede interna em uso e um padrão ISO. No entanto, o CAN é um protocolo de transmissão orientado por mensagens que, por si só, não tem suporte para autenticação ou criptografia. Há tentativas de corrigir esses recursos de segurança, como a autenticação do quadro CAN no Secure Onboard Communications [2] do AUTOSAR. Trabalhos recentes mostraram que uma vez que um invasor tenha acesso à rede interna do veículo, ele pode controlá-lo facilmente [3]. Hoje em dia, com a adição de conectividade à Internet e outros sistemas de comunicação populares (por exemplo, Bluetooth), foi demonstrado que ataques remotos podem ser possíveis mesmo sem acesso físico prévio à rede intraveicular [4].

A indústria automotiva agora está adicionando a Ethernet como uma nova tecnologia de rede intraveicular em carros, especialmente após a padronização da Ethernet 100BASE-T1 [5]. A flexibilidade, escalabilidade e popularidade do protocolo Ethernet, juntamente com a relação custo-eficácia da solução 100BASE-T1, tornam a Ethernet uma escolha cada vez maior para os fabricantes de ECUs. No entanto, o protocolo Ethernet tem uma quantidade considerável de falhas de segurança presentes, como não tem autenticação, confidencialidade e integridade [6]. A ausência de qualquer tipo de autenticação e criptografia permite, por exemplo, ataques que ainda são recorrentes em redes domésticas e corporativas, como ARP (Protocolo de Resolução de Endereço) e DHCP (Protocolo de Configuração de Host Dinâmico) *spoofing* [6].

Objetivos

O objetivo deste trabalho é analisar a segurança de redes automotivas internas, com o foco em Controller Area Network (CAN) e Ethernet automotiva. Será verificado se as mitigações propostas pela indústria e outros trabalhos realmente são eficientes contra possíveis atacantes e será proposto o nosso próprio modelo de segurança baseado em MACsec para a Ethernet Automotiva.

Metodologia

Na etapa de revisão bibliográfica, será feita a análise dos ataques de Charlie Miller e Chris Valasek [4], assim como os padrões para CAN e outras tecnologias com padrões abertos. Serão estudados os requisitos de segurança de cada tecnologia seguindo o modelo CIA e as mitigações de ataques propostas por outros pesquisadores.

Para a análise de cada tecnologia prepararemos um modelo de ameaça para um invasor na rede intraveicular, confeccionaremos ataques para cada tipo de rede e, quando possível, também apresentaremos casos reais de vulnerabilidades ou ataques.

Após isso, mergulharemos em Ethernet Automotiva. Serão apresentados os prós e contras em segurança comparando com outras tecnologias. Por fim, será proposto um modelo de segurança para a Ethernet Automotiva baseado em MACsec.

Cronograma

	Período															
Atividade	Ago		Setembro				Outubro				Novembro				Dez	
Revisão bibliográfica	X	X	X	X	X											
Analisar vulnerabilidades em CAN				X	X	X										
Analisar ataques em CAN					X	X										
Defesas em CAN						X	X									
Analisar outras tecnologias							X									
Ethernet e MACsec								X	X	X	X					
Escrita do TG						X	X	X	X	X	X	X	X	X		
Preparação da apresentação														X	X	

Referências

[1] Specification, C. A. N. "Version 2.0." *Robert Bosch GmbH* (1991).

[2] Much, Alexander. "Automotive security: challenges, standards, and solutions." *Softw. Qual. Prof* 18.4 (2016).

[3] Koscher, Karl, et al. "Experimental security analysis of a modern automobile." *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010.

[4] MILLER, Charlie; VALASEK, Chris. Remote exploitation of an unaltered passenger vehicle. **Black Hat USA**, v. 2015, p. 91, 2015.

[5] Matheus, Kirsten, and Thomas Königseder. *Automotive ethernet*. Cambridge University Press, 2017

[6] Kiravuo, Timo, Mikko Sarela, and Jukka Manner. "A survey of Ethernet LAN security." *IEEE Communications Surveys & Tutorials* 15.3 (2013): 1477-1491

Possíveis Avaliadores

Prof. Ruy J. Guerra B. de Queiroz

Prof. Abel Guilhermino da Silva Filho

Assinaturas

Recife, ___ de _____ de _____

_____

Caio Augusto Pereira Burgardt

(Aluno)

_____

Divanilson Rodrigo Campelo

(Orientador)