Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 114 (2017) 100–105

Procedia Computer Science

www.elsevier.com/locate/procedia

Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems, CAS October 30 – November 1, 2017, Chicago, Illinois, USA

A Threat to Vehicular Cyber Security and the Urgency for Correction

Syed Rizvi*, Jonathan Willet, Donte Perino, Seth Marasco, Chandler Condo

Department of Information Sciences and Technology, Penn State University, Altoona PA, 16601, USA

Abstract

In the past decade, technologies in vehicles have been rapidly advancing creating both a new type of "on the road" entertainment and safer environment while driving. Technologies such as anti-lock brake systems, steering assist, and in some cases autonomous driving, manufactures nearly eliminated the dangers of driving. To maintain the advances in safe technologies, it is vital to establish a strong security system for automotive networks and is crucial to advance the state of the art in automobile security. Motivated by this, one of the main goals of this research paper is to define a threat environment for CAR networks by discussing the existing security vulnerabilities and threats/attacks that an automobile network is currently facing. To address these security challenges, we also present a distributed firewall system to protect a CAR network from both internal and external networks.

Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems.

Keywords: Vehicles; Cyber Security; CAN; Connected Car; Network

1. Introduction

In a technological world, the practice of cyber security is detrimental when it comes to confidentiality, integrity, and availability of a technological infrastructure. Every IT security expert understands that a lack of security can cause problems in any system or network. When computer systems become vulnerable, hackers can exploit their targets to steal credit card information, read and sell sensitive files, and block services. Vulnerabilities for computing networks and architectures can cause headaches for IT departments, but usually administrators and developers can create patches and updates that help combat against the upcoming attacks that may surface at any moment. If a Denial of Servic[e

* Syed Rizvi. Tel.: +1-814-949-5292
E-mail address: srizvi@psu.edu

1877-0509
Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems.
10.1016/j.procs.2017.09.021

(DoS) attack occurs, network admins will work to mitigate the attack and relocate services that had been taken offline or bogged down.

Unfortunately, when dealing with vehicular technologies, cyber security experts and automotive manufactures cannot treat automotive networks and its digital recourses as they would with computing networks. Modern vehicles are no longer just a big metal box on wheels; it now is a sophisticated computer that in some cases makes life saving decisions within seconds of potential bodily harm. Due to the technology in cars today and constant Internet of Thing (IoT) connectivity, vehicles are gradually becoming equally susceptible to hacking vulnerabilities just as computers are in an office building.

As of now, vehicular cyber security is a free for all or in the "wild west" stages of IT development. The implementation of technologies in cars has spiked dramatically causing much innovation and luxury for consumers, but government security regulations and new security architecture has not yet been set in stone. Several manufactures are moving vehicular networks from a closed network to more of an open network with an increase in connectivity [1]. Only recently, May of 2016, the National Highway Traffic Safety Administration (NHTSA) published DOT HS 812 333, which gave federal recommendations for guidance on securing modern vehicles to manufactures [2]. Before 2016, best practice vehicular cyber security was nearly nonexistent. Networks that interconnect critical devices together within a vehicle were created to regulate commands sent across a network [3]. These networks such as the (Car Area Networks) CAN were never designed for encryption, giving an extreme vulnerability to the cars. These networks are unprotected and do not shield from malicious attacks. The On-Board Diagnostic II Port (OBD-II) has some security by using access control with four different security access levels, but the security itself is still weak [3]. The weakness in the OBD-II is the incorrect use of algorithms that can be circumvented with diagnostic tools that need little to no knowledge to use [3]. Seed Key Algorithms are used to protect diagnostic services but is often the secret key is usually used across the entire network. If a hacker was able to obtain the secret key, they would be able to access the entire production network and all ECUs [3].

As experts in the cyber security field, there must be a new strive to find a valid solution to the security of vehicles and its networks. It's becoming easier to gain access to simple tools that allow thieves to gain access to a car and commit grand theft auto. As of now, remote access of a car has been proven within controlled lab environments, but how long will it take a hacker to successfully gain control of the driver assist modules? An increase in vulnerabilities and exploits are surfacing causing a higher risk of attack. Autonomous vehicles are now becoming popular with consumers, this will introduce a higher chance of hacking because of the idea of a computer nearly hacking complete decision making and control of the vehicle.

It is critical to establish a strong security system for automotive networks, and is crucial to advance the state of the art in car security. Motivated with this, one of the main goals of this research paper is to define a threat environment for CAR networks by discussing the existing security vulnerabilities and identifying the threats/attacks that an automobile network is currently facing. To address these security challenges, we also present a distributed firewall system to protect a CAR network from both internal and external attacks.

2. Threats For Automotive Networks

With the computing architecture being introduced into vehicles, there is an introduction of computing vulnerabilities that come with it. The threat of malicious attack of vehicle's network is very much real. These common computing threats within a vehicle exacerbates the problem of causing much overhead or taking down an entire network due to the lack of available recourses given in the automotive pipeline (network). We believe that the current cyber security industry cannot come up with a strong security system for protecting CAR networks unless they have a clear understanding of the existing vulnerabilities and potential threats that an automobile network is facing. In next subsequent sections, we present some of the common security threats to CAR networks. An illustration of such attacks is shown in Fig.1.