Journal of Information Security and Applications 36 (2017) 90–100

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Cyber security attacks to modern vehicular systems

L. Pan [a,*], X. Zheng [a], H.X. Chen [b], T. Luan [a], H. Bootwala [a], L. Batten [a]

[a] School of Information Technology,Deakin University, Geelong, Victoria, 3220, Australia
[b] State Key Laboratory of Automotive Safety and Energy, Tsinghua University, Beijing, China

ARTICLE INFO

Article history:

Keywords:
CAN bus
Security
Vehicle systems
Security attacks
Smartphone

ABSTRACT

Security is a fundamental concern in modern vehicular systems. The advancement in modern vehicular systems provides many benefits such as reducing traffic congestion and improving safety and fuel economy via vehicular networks. However, many vehicular experts in industry take it for granted that Controller Area Network (CAN) bus being the most important part of a vehicle is secured and cannot be easily hacked; furthermore, cyber security experts have limited exposure to CAN bus. This paper provides in-depth explanation of CAN bus and feasible scenarios where a vehicle is no longer safe after its CAN bus is compromised. Furthermore, the inclusion of CAN bus attacking codes in a mobile malware is cost-effective for the malicious attackers but very challenging for vehicle engineers to mitigate the security risks. Based on a variety of security attacks, we analyze potential attacks and their impact on the safety of the vehicle users. A number of vulnerabilities and attack scenarios are exposed which allows malicious attackers to hamper the vehicular control systems and cause harm to the vehicle even the passengers. In this paper, we do not report on our own implementation of attacks on real vehicles; our aim is to motivate further research to improve the security of the modern vehicular systems.

1. Introduction

There is a huge increase in the complexity of current vehicular systems. As the technology increases, new features are rapidly introduced and installed in modern vehicles. Engineering-wise, each modern vehicle has a number of electronic control units (ECUs) that are interconnected via bus systems. The ever increasing functionality of a vehicle might be handy for a driver but it incurs more security vulnerabilities. Attackers can misuse the system for their own purposes which can be harmful to vehicle and passengers. The second reason of concern is how to safeguard the large volume of information that is transmitted between a vehicle and the outside world (e.g., through internet, wifi, or bluetooth). For example, a number of cyber attacks are easily generated and infiltrated to the vehicle via the infotainment systems [1].

Considering these trends and the ever expanding gap between security attacks and existing safety measures, security in vehicular systems is therefore an important area of research. Vulnerabilities in vehicular systems' security can not only leak sensitive personal information but also can endanger the lives of humans.

Controller Area Network (CAN) bus system plays an important role in vehicles. It has a protocol for serial communication. Besides providing high level of security, it supports distributed real-time control of electronic control units (ECUs) [2]. CAN, comparing with other networks, does not have a concept of a central bus master. That is, CAN bus does not send a large amount of data from one point to other. Instead, it sends a number of short messages which are broadcasted to the entire network, which immediately posts many security issues like eavesdropping. Vehicular engineers adopting CAN bus listed its strengths below [3]:

- Compared to other data transmission protocols, CAN provides very good performance/price ratio.
- It provides up to 1,000,000 bits per second (1 Mbps) which is a fast transmission speed for moving data.
- CAN protocol is successfully implemented in real-time systems.
- Data in CAN is reliable in nature and error detection mechanisms are robust.
- Large data blocks in the network are not been sent by CAN from one point to another. Short length messages like engine RPM data or temperature are transmitted to the whole network.

The modern CAN bus becomes increasingly complex for engineers to work with. That is, ISO 11,519, also known as Low Speed CAN, is the first version of CAN which is used for applications with low bit rates up to 125 kbps. Each CAN bus packet consists of a 11-bit identifier. ISO 11,898 (1993) is the second version of

* Corresponding author.
E-mail addresses: l.pan@deakin.edu.au (L. Pan), xi.zheng@deakin.edu.au (X. Zheng), herschel.chen@gmail.com (H.X. Chen), tom.luan@deakin.edu.au (T. Luan), hbootwal@deakin.edu.au (H. Bootwala), lynn.batten@deakin.edu.au (L. Batten).

http://dx.doi.org/10.1016/j.jisa.2017.08.005
2214-2126/

CAN with 11-bit identifiers and signaling rates from 125 kbps to 1 Mbps. It is also referred to as Standard CAN Version 2.0A. It provides $2^{11} = 2048$ different message identifiers. ISO 11,898 amendment (1995) is the current version of CAN which has extended to support 29-bit identifier. It is also referred to as Extended CAN Version 2.0B. It provides $2^{29} = 537$ million identifiers [3]. With the increasing number of identifiers, simple security solutions such as blacklisting struggle.

Once gained access to the CAN bus (e.g., through a maintenance port [4] or via USB cable [5]), the attacker can perform numerous malicious activities which can harm the vehicle as well as the human. Attackers can stop the engine of the vehicle at any point of time. If the automobile is traveling at a speed of 100 km/h and the engine shuts down suddenly, it would cause a catastrophic impact to the human and the vehicle. Moreover, the attacker can cheat the speedometer of the vehicle, turn off door locks, change lights and so on. In short, the attacker has full control over the vehicle and can harm it according to his or her intention [5].

As the technology improves, more and more features are introduced to the connected vehicular environment. Some of the features include connecting vehicle's entertainment system with smartphone application connected via bluetooth or WiFi etc. Modern vehicles have equipped with key-less access in which the user is not required to carry a physical key to get access to a vehicle. Some applications provide an interface with vehicle's internal system which allows control of basic functions of a vehicle like steering, door access etc. From an attacker's point of view, targeting directly towards CAN bus is not the only option to launch any attack. Attacker can get access to the vehicle's CAN bus via smartphone applications [6].

The contributions of this paper are:

1. We present strong motivation for researchers in the security domain of modern vehicle systems and IoT/Cyber Physical Systems applications.
2. We analyze attack scenarios and countermeasures which showcase the vulnerabilities in CAN bus and various attacks that may occur on the CAN bus.
3. We emphasize the importance of addressing the remote attacks via long-range wireless connection facilitated by malicious applications of compromised smartphones.

The rest of this paper is structured as follows: In Section 2 we briefly describe the related work on the analysis of CAN bus security. In Section 3 we discuss security analysis of attacks on CAN bus. In Section 4, we discuss possible attacks launched from newly introduced vehicle features (e.g., Infotainment Systems and In-Vehicle networks) to CAN bus. In Section 5, we discuss some possible solutions to mitigate the attacks. Section 6 concludes the paper with the summary and future scope of the research.

2. Related work

Lots of research has been done in the field of vehicle security. Our research holds a great importance in vehicle security as it would provide valuable information about CAN bus attacks. Many independent groups have contributed to this area and showcased the faults and limitations of CAN bus system.

Ellims et al. [7] develop a project which provides an enhanced communication network for safety-related applications. It would include central ECU and many distributed actuators. CAN 2.0B protocol is used for network data layer. Main ECU, ignition model and air/fuel ratio controllers are connected by the network. The proposal consists of additional connections to network with additional ECU and I/O devices. A number of techniques have been used such as scheduling and hazard analysis to resolve reliability and safety issues. Hazard analysis includes identification of hazards at system level using Hazop (Hazard and operability) analysis standard [8]. It was introduced by a chemical industry and then adopted by U.K. Ministry of Defense. Many hazards were identified based on air flow, fuel, RPM and ignition. CAN protocol is used for scheduling analysis to find out whether the messages were transmitted in a timely manner. The analysts operated the CAN bus at a high bit rate which would provide 10 to 20% utilization of bus. Results of the analysis revealed that it was unfeasible to schedule the system with communication link at 250 kbps; instead, the schedule of system was possible at 500 kbps bus rate.

Miller and Valasek [5] describe the vulnerabilities in CAN bus system. The authors introduce the concept of security attacks to vehicular systems. They have provided details of attacks which can be launched by an attacker on a vehicle. After gaining entry in to the CAN bus, attacker can perform a number of malicious activities with different parts of the vehicle such as engine, doors, lights, and other controllable parts. Miller and Valasek have provided a framework which would allow the development of tools that can easily interact with the modern vehicles. In addition, they have proposed different mechanisms for detecting security attacks. Our contribution is further developed on the basis of this work: We provide the malicious activities performed by the attacker; we also provide technical details of the security attacks on vehicles.

Carsten et al. [4] have discussed several ways in which a vehicle can be attacked. Features of CAN have been highlighted such as robust mechanism for error checking. Vulnerabilities have been shown in CAN system such as the packets in CAN protocol do not carry the address of sender or receiver. Due to this, individual node cannot decide for whom the packet is intended for and from where the packet came. CAN has no feature of authentication for CAN nodes. Hence, attackers can easily send spoofed messages and the receiving nodes would believe that the sender is legitimate. The authors have discussed about *FlexRay* [9] which is a high speed bus and can possibly be more secure than CAN. Many attack methods demonstrate how to steal sensitive information and data by interacting with CAN bus, and how to hack into the vehicle system. The authors have given potential solutions for preventing the attacks which focus on data management, monitoring algorithmic approach, using a system of encryption and attestation for identification of nodes etc. Our work instead focus on the vulnerabilities and loopholes in the CAN bus. The pathway from which the attacker gets an entry in to the CAN bus would be described in our work.

Hoppe et al. [10] list CAN bus vulnerabilities and tests which have been performed to exploit these vulnerabilities on different parts of the automobile. Attack on electric vehicle window is considered by adding few lines of malicious code in the appropriate ECU. After a pre-defined condition, code runs and replays CAN message which allows the attacker to gain control over the window. Another test was performed on warning lights which would switch the light on and off as per the intention of the attacker. Test were performed on airbag control system in which the system's login could be removed. In case of an accident or collision, the system would not work and would lead to a huge damage. Last test was performed on gateway ECU which interconnects to several internal and one external subnetworks of CAN. This would lead an attacker to eavesdrop sensitive internal information of a human. Our work would be similar to this as we would provide different attacks on the CAN bus. We will describe case studies which will include the attacks on different parts of a vehicle thorough CAN bus. Our research will include potential solutions which can be future research scope in vehicle security.

To best capture the cyber security attacks against vehicles presented in the literature, Table 1 aggregate their key facts including attack types, vulnerabilities, and attack surfaces. Furthermore, we observe that almost every attack was launched from laptop PCs in-