Lightweight Authenticated Encryption for Vehicle Controller Area Network

by

Syed Akib Anwar Hridoy

A thesis submitted to the
School of Computing
in conformity with the requirements for
the degree of Master of Science

Queen's University
Kingston, Ontario, Canada
May 2020

Abstract

Vehicle manufacturers are installing a large number of Electronic Control Units (ECU) inside vehicles. ECUs communicate among themselves via a Controller Area Network (CAN) to ensure better user experience and safety. CAN is considered as a de facto standard for efficient communication of an embedded control system network. However, it has no built-in security features. In this thesis, the existing security solutions for the CAN protocol found in the literature are classified in terms of security enforcement procedures. The classification can facilitate the researchers to select an appropriate security technique depending on security requirements. We also propose a security framework to secure CAN communication using the Authenticated Encryption with Associated Data (AEAD). The framework ensures confidentiality, integrity, and authenticity of CAN data transmission. The experimental results show that the delay of the proposed approach can be reduced to 0.07 ms depending on hardware configurations. We consider it lightweight since it adds a low overhead regardless of performing encryption and authentication. We evaluate the approach using four metrics: communication overhead, network traffic load, cost of deployment, and compatibility with CAN specification. We show that the framework keeps the network traffic unchanged, has low deployment cost, and is highly compatible with the specifications of the protocol.

Acknowledgements

I would like to express my heartiest gratitude to my supervisor Dr. Mohammad Zulkernine for his continuous support, guidance, patience, and motivation throughout my Masters at Queen's University. Without his sincere direction and optimism, this thesis would not have been possible.

I would also like to express my appreciation to everyone in Queen's Reliable Software Technology Group (QRST) for their support. In particular, I am thankful to Md. Abu Faisal for the constructive discussions.

Finally, I wish to thank my family for their unparalleled love, encouragement, and dedication. I am forever indebted to my parents for giving me the opportunities and experiences that enabled me to achieve this milestone.

Dedication

This thesis is dedicated to the memory of my father, Syed Anwar Hossain. Although he was my inspiration to pursue my Master's degree, he was unable to see my graduation. This is for him.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

Vehicles were considered as mechanical machines before the introduction of software inside them. Components such as engines, brakes, and gears were assembled into a car in coherence with the principle of mechanics. Yet, the limited accuracy of mechanics led to undetectable failures, and vehicle safety was in threat. The automotive industry moved towards the adaption of digital electronics in the vehicle to improve the scenario. After that, manufacturers started installing electronic sensors in vehicles for driving safety and assistance. The automotive industry introduced Electronic Control Unit (ECU) in 1970 to collect information from the sensors and control the mechanical components. An ECU can request another ECU for its sensor information to make a collective decision. These ECUs form an in-vehicle network to communicate with each other. For in-vehicle communications, the most widely used medium is the Controller Area Network (CAN). CAN was released in 1986 at the Society of Automotive Engineers (SAE) conference [89].

With the revolution of ECUs, features involving artificial intelligence are added

to vehicles to enable them to make intelligent decisions. These features are providing autonomous driving support as well as safety and convenience to users. Some of the examples of these features are the Advanced Driver Assistance System (ADAS), Pre-Collision System, and Tire Pressure Monitoring System (TPMS). ADAS assists drivers in controlling different systems such as steering and acceleration. It can alert the driver upon detecting distracting behavior [52]. Pre-Collision System provides a safety system, which reduces the possibility and severity of collisions by alerting drivers with audio and visual warnings. If the signals left unattended, the system automatically activates brake assist without any human input, reducing the severity of potential accidents [78]. TPMS monitors the air pressure of tires and sends a warning to the driver if the air pressure of any tire is low [45]. TPMS is a mandatory feature for the vehicles running in the US and Europe [60].

In addition to the growing features of comfort and assistance, the In-Vehicle Infotainment (IVI) system is also evolving. IVI is a combination of information and entertainment system which delivers entertainment and information to users. The IVI market is expanding rapidly and it is estimated to reach USD 30.47 billion by 2022 [13]. The automotive industry is integrating IVI with smartphones connecting thorough Bluetooth or Wi-Fi. This integration facilitates users to integrate smartphone apps into IVI [53]. Vehicle manufacturers offer proprietary smartphone applications compatible with vehicle, some of which are Toyota Entune [77], Mercedes Me Connect [55], BMW ConnectedDrive [23], HondaLink [36]. These applications provide services such as navigation, weather forecast, and hands-free phone calls.

All these features brought by the connectivity of electronic components offer a safe and comfortable experience to drivers and passengers. However, these features

expose the previously isolated vehicle system to cyberspace, which introduces the opportunity of cyberattacks. These attacks endanger the privacy and safety of a vehicle.

Miller and Valasek [33] hacked a Jeep Cherokee by exploiting the vulnerability of the Uconnect [14] telematics system. A vulnerability in the cellular connection of Uconnect gave them the access to rewrite the firmware and send commands to the in-vehicle network remotely. They controlled the car functionalities such as disabling brakes and honking horns from 10 miles away. This demonstration of attack led to a recall of 1.4 million vehicles.

In 2016, the Keen Security Lab in China displayed attacks on Tesla Model S in both parking and driving mode [48]. They abused the flaws of the web browser kit through a malicious 3G/Wi-Fi connection, which allowed them to install their software in the vehicle. Then, they reprogrammed the firmware to bypass security measures. They remotely controlled several vehicle functions such as windshield wiper swinging, unauthorized door unlocking, and brake manipulation.

In 2017, the Keen Security Lab also found 14 flaws in BMW's infotainment unit [47]. All the BMW models (i.e., i Series, X Series, 3 Series) manufactured from 2012 onwards had the vulnerabilities. They discovered that it is possible to get access to the infotainment system locally and remotely. BMW fixed the flaws through software updates [58].

NissanConnect EV [82] is a smartphone application designed for Nissan Leaf electric vehicles. This application provides services such as climate control, dashboard customization, and charge plug-in reminder. A flaw in NissanConnect EV allowed a hacker to access user settings and driving logs by simply using vehicle identification

number [91]. The hacker was able to control the fan by manipulating user settings. This can disable the car by draining battery. The analysis of driving logs can reveal the identification of an owner. Nissan shut down the application temporarily to resolve the flaws.

All these attacks control vehicle functionalities illegally. ECUs are responsible to control these functionalities and they communicate via a CAN bus. Therefore, these attacks highly relate to CAN communications and the security of these communications must be a concern.

1.2 Problem Overview

Before the introduction of CAN, the automotive industry was facing challenges in terms of wiring inside the vehicle. The two most significant purposes of CAN development were to reduce the wiring complexity and cost. At that time, the security of communication between vehicular components was not a concern as a vehicle was a closed system without communications with other devices or vehicles. Hence, the automotive engineers implemented CAN following the concept of broadcast-based serial communication. As a result, any ECU connected to the network can read or send messages.

In-Vehicle Infotainment (IVI) system is connected to the CAN bus. It increases the security risks as IVI connects external devices through the wireless medium such as Bluetooth and Wi-Fi. In addition to proprietary smartphone applications from vehicle manufacturers, there are third-party applications available to provide entertainment and navigation services [44]. BMW vehicles come with BMW ConnectedDrive [23] application. The services of BMW ConnectedDrive include remote engine

start, remote lock or unlock, real-time traffic information, on-street parking information, etc. However, the flaws in BMW ConnectedDrive compromised the control of the vehicle to hacker [47, 29]. Similarly, attackers hacked Uconnect [14] to disable brakes from 10 miles away. Furthermore, third party dongles can be plugged into the OBD-II diagnostic port to monitor the status of vehicle systems such as the engine and transmission. These dongles connect to smartphones via Bluetooth. A malicious application installed on a phone which is connected to the OBD-II dongle can help the attacker to read the network traffic [90]. The reverse engineering of recorded communication may lead to an attack. The lack of confidentiality, integrity, and authenticity are the reasons for these attacks.

1.3 Overview of the Proposed Approach

Confidentiality, integrity, and authenticity have to be ensured to secure CAN communications. Therefore, the sender ECU has to encrypt the data, and receiver ECU has to validate data integrity and authenticity. Data encryption keeps the data confidential from the illegitimate nodes and resists against the reverse engineering process. Receiver ECU has to check the integrity and authenticity to inspect data accuracy. Also, it has to verify sender legitimacy. To achieve confidentiality, integrity, and authenticity, we propose to implement a lightweight Authenticated Encryption with Additional Data (AEAD) cipher. Authenticated encryption ensures the privacy and authentication of data. The cipher can check the integrity and validate additional data. In the proposed approach, we authenticate and encrypt the CAN payload for confidentiality and integrity. To ensure authenticity, we feed CAN message identifier to AEAD cipher as additional data. To find the best applicable AEAD cipher in

CAN, we explore both block and stream ciphers. Our analysis shows that ChaCha20-Poly1305 has the best credibility in low powered ECUs.

AEAD cipher uses Message Authentication Code (MAC) for authentication, which has to be transmitted from sender to receiver. To accommodate the MAC into a fixed-length CAN frame, we propose to use the CRC field. In standard CAN, the CRC field is used for error detection. Error detection is part of data integrity process [61]. Since the proposed approach ensures data integrity, we replace the CRC data with MAC. By using the CRC field to transmit MAC, the proposed method keeps the network traffic unchanged. Otherwise, additional message transmission is required for MAC transmission, which at least doubles the network traffic. Increasing traffic intensity will make other ECUs wait for the completion of MAC transmission. As a result, it will have a significant impact on the real-time communication of the protocol.

The keystream block generation in resource-constrained ECUs adds significant communication overhead. To minimize the delay, we adapt forward keystream block generation, which means that after the transmission of a message, we calculate the keystream for the next message. Therefore, during the transfer of the next message, the required key stream will be ready to process that reduces the delay.

1.4 Contributions

In summary, the contributions of this thesis are as follows:

- We classify the CAN security solutions based on the security enforcement procedures.
- We propose the integration of the ChaCha20-Poly1305 cryptographic algorithm

to ensure the confidentiality, integrity, and authenticity of data. ChaCha20-Poly1305 is not used in CAN protocol security.

1.5 Organization of Thesis

The remainder of the thesis is organized as follows. In Chapter 2, we discuss ECU and in-vehicle CAN protocol in brief. Also, we explain authenticated encryption. Later, in Chapter 3, we discuss the related work by providing a classification of CAN security solutions. Chapter 4 presents the proposed approach and discusses the challenges of it. In Chapter 5, we describe the implementation details, present the experimental results, and evaluate the proposed approach. We conclude the thesis, discuss limitations, and suggest future work in Chapter 6.

Chapter 2

Background

The evolution of vehicle Electronic Control Unit (ECU) has facilitated the automotive engineers to implement advanced features to improve safety and comfort. However, the software used in the ECUs and the communication network introduce many security risks. In this chapter, the background knowledge required for a better understanding of ECU and its communication security is discussed. We illustrate an in-vehicle Controller Area Network (CAN) along with some security attacks demonstrated on it. We also explore some of the cryptographic concepts related to this work.

2.1 Electronic Control Unit (ECU)

ECU is responsible for controlling different systems or subsystems of a vehicle based on the sensor information. Every sensor inside a car is connected to an ECU. ECUs collect the sensor information and process it to control its system or to share it with other ECUs to provide assistance. For example, front display ECU gathers information from the seat belt controlling ECU to show the driver if the passengers are wearing seat belts. Engine control, airbag control, powertrain control, adaptive