A SURVEY ON SECURITY RISKS IN THE CONTROLLER AREA NETWORK

1Monica Catherine Susairaj, 2Robert Shoniwa
1Department of Information Technology, SRM University, Potheri, Chennai, Tamil Nadu 603203, India
2Department of Information Security and Assurance, Harare Institute of Technology, P.O Box BE277, Belvedere, Harare, Zimbabwe
1monicacatherine.s@ktr.srmuniv.ac.in, rshoniwa@hit.ac.zw

Abstract: Advancements in automobile-related networks have increased the sophistication in the car world. Electronic Control Units (ECUs) play a major part in a car’s architecture. These ECUs monitor and control the different subsystems of a car. Secure communication between those ECUs is very much needed in modern cars. A car has approximately 60 ECUs which are all interconnected and form a global internal network. Nowadays, devices in cars communicate with other external devices through the use of Wi-Fi, Bluetooth, and USB to name a few. However, when ECUs communicate with external devices, they may expose the internal global network to external networks which are prone to cyber-attacks. A survey of vulnerabilities and threats to vehicular networks like the Controller Area Network (CAN) is done through the analysis of techniques and tools used to undertake these activities as well as their potential impact to the vehicles. Security solutions that have been implemented so far in these vehicular networks are then discussed with emphasis on their positive characteristics and drawbacks. Ultimately, the benefits and flaws in the current mechanisms used to protect the CAN bus are highlighted in this paper and will aid in providing a more efficient protection mechanism for the CAN bus.

Keywords: CAN bus, Vehicular Security, ECUs, Denial of Service attacks, Car Hacking

1. Introduction

Automobiles today are comprised of different electronic components which control one or more functions of a vehicle. In today’s modern vehicle system, ECUs play a major part. More than 50 ECUs are used in a vehicle nowadays and the complexities of embedded systems are also growing faster[1]. These ECUs communicate with each other by means of messages through an internal network to efficiently monitor and control the different vehicular subsystems. This internal network can be connected to an external network in various ways like via Bluetooth, Wi-Fi, On-Board Diagnosis (OBD) port and thus it can be reached from an outside network. Even car to car communication (also known as Vehicle-to-Vehicle Communication or V2V) is also possible by means of recent interconnection techniques[2].

Like the other networks, the vehicular network is also prone to threats and can be exploited with attack goals such as theft, sabotage, or electronic tuning of the vehicle and Intellectual Property theft from the embedded networks within the automobile that is being attacked[3] to name a few.

Two particular classes of attacks that are of note are Replay attacks and Denial of Service/Distributed Denial of Service attacks. We will begin by looking at the replay attack. By definition, the replay attack is whereby attackers interfere with the original sender’s connection by intercepting and re-sending messages sent by the original sender[4]. In order to prevent this kind of attack, it is necessary to recognize the exact attack method that is specific to the attacker’s execution scenario so as to counteract it. With respect to replay attacks in the context of CAN, this is basically done through the interception of the channel and then re-sending of data sent by the original sender. If authentication is done at the receiver side then the attacker would also need to take some risks in performing this particular attack. Since CAN messages are broadcasted across the network, CAN is more prone to replay attacks. For example, an unauthorised device can capture a CAN message that was sent at an earlier point in time when the brakes were applied and said message can then be resent when the vehicle moves at a higher velocity which would most definitely result in potentially life threatening consequences[4].

The other class of attacks we would like to zero in on is one that has to do with the compromising of availability of services through Denial of Service and Distributed Denial of Service Attacks. Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) flooding attacks are the mostly commonly used methods in instances where the goal is to destroy
availability of resources or services that are housed or accessed via the CAN. In context, DoS attacks or DDoS attacks are an attempt to make an ECU or network resource unavailable to its intended users (in CAN, this would be another ECU on the network). DDoS attacks are also line DoS attacks but done by two or more nodes or bots while DoS attacks are done by one node or system. By definition, a bot is a compromised device created when a node (in most cases it may be a computer but in this scenario it refers to an ECU) is penetrated by software from malware or malicious code[5].

As mentioned earlier, these are not the only kinds of attacks that can be perpetrated on the internal networks housed within automobiles. They are but just a few that were taken note of in order to put the security solutions that have been developed and researched on (which will be highlighted in sections to follow in this paper) into perspective as to what exactly these possible solutions are aiming to protect and from what in particular.

ECUs in a car communicate with each other through a bus network called Controller Area Network through which messages are broadcasted to all devices connected with the CAN bus. In earlier days, vehicles had closed networks and so it was difficult to compromise any system inside the vehicle unless the internal network was accessed through some means.

In recent cars however, those closed networks can be accessed from outside world by means of the technologies like Wi-Fi and Bluetooth and hence they can be accessed from outside world by means of the technologies like Wi-Fi and Bluetooth and hence they are more vulnerable to most of the network attacks that are occurring nowadays. In this manner, attackers taking control of the entire control system has become a possibility as well.

The remaining sections of this paper consist of the following: in section II, networks that are used in modern cars are described. Then in section III, possible threats and security approaches for those highlighted loopholes are then discussed. Finally, section IV will summarise the paper in the form of a conclusion.

2. Networks Used in Vehicles

With the increased usage of embedded units in modern cars, communication of two ECUs through point to point connection is no longer efficient[6].

Based on this growth rate and related requirements, many technologies have been introduced to improve this efficiency.

A. Controller Area Networks (CAN)

Controller Area Networks [7] is a serial bus which is used for real-time message delivery between distributed control systems. In recent times CANs have been used in many areas such as elevators, medical devices, cars and robots. In modern cars, ECUs are connected by multiple CAN buses and for transmitting messages it follows Carrier Sense Multiple Access/Collision Detection (CSMA/CD) and priority based arbitration. The data transmission rates also tend to go up to 1Mb/s[6].

The arbitration id is usually treated as message type but when OBD-II diagnostics is done it is used as the controller source or a destination identifier. Logical zero state is considered as dominant and logical one state is “recessive” in arbitration. Most of the CAN applications follow ISO 11898-2 which specifies two lines, CAN_H and CAN_L which are connected to each other with a 12Ω terminating resistor.

Also, from vehicle to vehicle the types of CAN messages differ. Even a different version of the same type of car use different frames. For example, the CAN frame to activate the wipers on one vehicle may be used to close and open the windows in another car.

B. Flex Ray

Flex Ray is a flexible and high-speed communication protocol with a speed of 10 Mb/s. It supports fault tolerant communication between electronic devices. It also functions in two ways, where one is time-triggered and another one is event-triggered. Initially it is used for the electronically controlled damper of the BMW X5 series. To add to that, it provides two channels for communication. A single node can be connected to both of these channels. It is recognized in some circles as the successor to CAN. It has also replaced steer by wire, brake by wire techniques and so on[3].

C. MOST

Media Oriented Systems Transport (MOST) supports multimedia data in vehicular network. According to the MOST150 Standard, the maximum possible bandwidth is 150 Mb/s. Because of this bandwidth it is much more suitable for multimedia data transfer than CAN[8].

Among the in-vehicle networks highlighted, the CAN is the most preferred but it is also very vulnerable. This means there are many possible entry points for cyber-attacks because it is lacking when it comes to security. The various attack goals as well as possible internal and external attacks are briefly described in paper[3]. In the next section, a few methods of exploitation highlighted in Fig. 1 and security approaches are going to be described.

3. Can Threats & Security Approaches

A. CAN Vulnerabilities

Ian Foster and Karl Koshcher[9] stated that CAN buses are not created to withstand malicious attacks, instead they are designed only for reliability. Because of its shared broadcast nature, it is more vulnerable. By
altering the CAN messages, a car can be partially controlled by an attacker. This was proven by Miller and Valasek[10] by a demonstration in which they controlled the steering wheel of a Jeep by spoofing parking assist.

CAN is also of a relatively fragile nature and so an attacker can actually override messages. For example, the speedometer reading was made false and displayed 100 MPH minus the actual speed by the UW/UCSD researchers. This was done by simply flooding the CAN bus with spoofed messages. Speedometer messages sent by other ECUs can be detected and the attacker can assert a dominant bus state which makes all other receivers reject such messages as invalid. Even the control of brakes can be compromised when a car is moving at a very high speed.

“Read Memory By Address” is another diagnostic service that can be used in such a way that an attacker can read arbitrary pieces of an ECU’s address space. Using this service, sensitive values like authentication keys can be leaked.[9]

These services should be restricted but unfortunately, that is not true in many cases and in some other cases, security mechanisms can also be defeated. Also, aftermarket devices that plug into the On-Board Diagnosis port (such as dongles that can track driving for insurance purposes) are potential entry points. It can even be exploited by SMS in some instances.[9]

B. Authentication in CAN using HMAC

Nicolas Bravo et al [11] addressed the authentication issue in CAN, which is also very important considering the number of components on a car that communicate over the CAN bus as illustrated in Figure 2 which highlights a few of these components. Typically, the CAN frame has no authentication field and the 8-byte long data field makes it difficult to add a large-key for authentication. So, both at sender side and receiver side, authentication is not performed in the original CAN network.

Here, they have implemented a public-key/shared-key authentication scheme for CAN using HMAC. This is done by providing one secret key and one public-key pair for each node through which it sends its signed messages. It is tested with 256-bit public/private key pairs, 32-bit authentication tags and 256-bit HMAC keys.

However, brute force attacks may be possible after $2^{32}$ trials. Its limitations are low latency, high response time, memory overhead because of the authentication facility, as well as susceptibility to Denial of Service and injection attacks. The Homebrew CAN software simulation was used for testing in this case.

C. Cryptographic Approach to CAN

Jennifer Ann Bruten[12] demonstrated cryptographic approaches for improving the security of the CAN bus with specific constraints. AES and RC4 were used for encryption, HMAC was used for authentication and SSL/TLS was used for the distribution of keys.

One of the drawbacks, however, is its small message length (4 bytes) and hence larger messages need to be divided into two or more smaller messages. In this case, the increase in message time was less than 1 millisecond which is relatively acceptable with respect to other options.

D. CAN Message injection & counter measures
Tobias Hope et al. demonstrated injection of messages on control systems and they discussed about certain preventative measures. Four attacks were tested on control systems for the window lift, warning light and airbag as well as the central gateway. It was stated in their paper that hardware implementation of cryptographic algorithms performs much better than software implementation but on the downside, it is also harder to maintain.

In this case, applied cryptographic measures should then be updated regularly to face the continuous progress in cryptanalysis. They also recommended the implementation of an intrusion detection system as well as IT-forensic measures in car networks also.[3].

**E. Signal-based Authentication in CAN[1]**

Murvay et al.[14] performed authentication based on signals from transceivers and Frame IDs. Based on the difference in CAN signals, the sender can be identified. They used three techniques in their research which included mean square-based separation, convolution-based separation and mean value-based separation for source identification. Ten samples were collected and comparisons were made based on these samples.

The drawbacks in this case were; the communication overhead, computational overheads and fitting an authentication tag in addition to the message within 8 bytes was not feasible.

**F. CAN bus security attacks & countermeasures**

Chung-Wei Lin et al.[16] addressed the problem of secure communication over the CAN bus with less overhead and high degree of tolerance to fault. This paper focused on the masquerade attack and the replay attack. It particularly addressed runtime authentication.

However, in this case security is concentrated after the ignition key is set to on and the security secret keys have been distributed to the ECUs. Hence it does not focus on the aspects of initial security like critical key assignment and distribution.

**G. CAN message compression & security**

Wu, Yujing, et al.[17] developed security software for CAN2.0 using CANoe software and the bus load was measured using CANcaseXL device. Authentication and encryption of CAN messages were done in this paper with average message delay being less than 0.13ms.

Also, a CAN data compression algorithm (ECANDC) was used for compressing the CAN messages. Therefore, in this case the bus load was reduced by 18.41%. Typically, without compression the bus load reached 43.09%. AES-128 was also used for encryption and HMAC was used for authentication.

The test was performed with 20 ECUs and it was then observed that it could be used for in-vehicle networks.

**H. Hardware-based CAN Security Module**

Wang, Eric, et al.[15] proposed a secure hardware based module for controller area network security. In this case, a separate ECU (Security ECU) especially for security was developed for key distribution, message verification and to defend against malicious messages. Because of this additional Security ECU (SECU) changes in software of other ECUs would then also be necessary. Compression of CAN messages was also done to increase the entropy and to fit the CAN message and Message Authentication Code (MAC) in the same frame which would then make the authentication process faster.

However, the drawbacks were that it would be expensive to make custom hardware and that additional memory and processing power would be needed for the ECUs to decode messages.

**4. Conclusion**

The Controller Area Network plays a major role in today’s automotive industry. With the growing number of threat actors interested in compromising cars, its insecure communication is now a great threat to the world of automobiles. As highlighted in the paper, even complete control of a car can be gained if its CAN bus is exploited. In this paper, we have discussed the possible security measures that can be implemented as well as their respective corresponding drawbacks. It is also prudent to note that all the highlighted security measures had not yet been tried in real time scenarios yet. This is because due to the typically short frame length, implementing strong encryption/authentication algorithms is very difficult as this must be factored in before deploying into real time scenarios. Based on the discussed ideas a strong but light-weight algorithm should be implemented in the CAN network to prevent it from malicious messages while also not compromising the effectiveness of the CAN and ultimately, it would have to be tried and tested in real time as well.

**References**


