IDENTIFYING & MITIGATING CYBER SECURITY THREATS IN VEHICULAR TECHNOLOGIES

Anil Lamba[1], Satinderjeet Singh[2], Natasha Dutta[3], Sivakumar Sai Rela Muni[4]
Department of Computer Science, Charisma University, Turks and Caicos Islands

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.

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

Citation: Anil Lamba, 2016."IDENTIFYING & MITIGATING CYBER SECURITY THREATS IN VEHICULAR TECHNOLOGIES", International Journal for Technological Research in Engineering, Volume 3 Issue 7, pp.5703-5706, 2347-4718.

I. 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 Service (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 HS812 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.

II. 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.

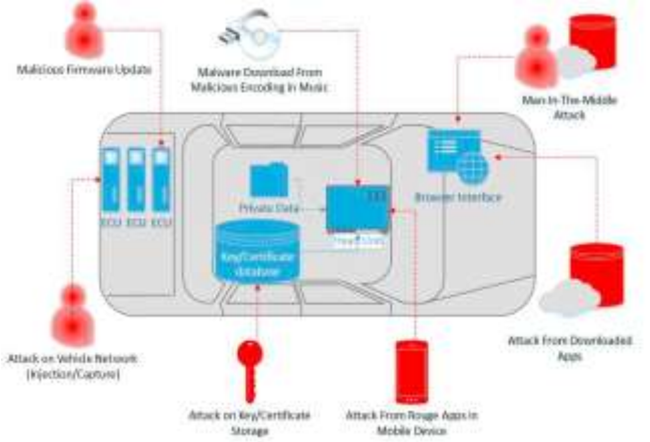
Malicious Firmware Update
Malware Download From Malicious Encoding in Music
Man-In-The-Middle Attack
ECU ECU ECU
Private Data
Browser Interface
Key/Certificate database
Attack on Vehicle Network (Injection/Capture)
Attack From Downloaded Apps
Attack on Key/Certificate Storage
Attack From Rouge Apps in Mobile Device

Fig. 1. Potential threat vector for CAR networks

2.1. DOS Attacks

A DoS is an attack where a large number of packets are sent towards a single location. The packets are fake as they are spoofed and are full of random values. The attack floods the buffer memory of a network and loads up the bandwidth, thus using all of the computational resources [4]. This usually leads to extreme slowness or even a complete halt of the system. In vehicles, a DoS attack could be much more detrimental than it would be within a computer system [5]. In a vehicle, an attacker could flood an important component. This could lead to safety concerns, especially with certain components. For instance, a DoS attack on the Electronic Throttle Control System (ETC) could cause malfunction and lead to a stuck or inoperable throttle [5]. The safety of the occupants of the car as well as anyone in the immediate area can be affected directly by a DoS attack on a vehicle. Car companies are starting to understand the risks that their vehicles have in relation to connecting them to the IoT world. Some DoS attacks can affect the infotainment sector with others affecting critical parts of the car such as the controller area network (CAN) bus [6]. The critical parts include brakes, throttle, and steering. These components could be disabled by an overload of processes or an overhead on the thus affecting the how the car responds in real time [6]. Some less harmful attacks within the infotainment sector include performing a DoS attack against the radio so it cannot be used [6]. Bryan Parno et al. [7] suggest inspection to the technological infrastructure. They also suggest performing the inspection during the yearly inspection that automobiles already go through to decrease the inconvenience for the consumer [7]. Maxim Raya [8] suggests that the use of an event data recorder may suffice. These recorders would act similar to a black box in the way that they register and record what goes on within the vehicle communications before an accident [8].

2.2. Replay Attacks

Replay attacks are one of the many stepping stones for car hacking. These attacks focus entirely on the authentication side of network and car security. Replay attacks in general are when a malicious user "sniffs" out a signal between two parties. The sender will be verified by the receiver as a legitimate user; while this exchange is safe, this is where the malicious user comes into play [9]. The malicious user uses the "sniffed" signal, and mimics the signal to the original receiver. This, in turns, makes the receiver think that this is the original sender, but it is actually the malicious user gaining access to unauthorized information using the "replay" of the authenticated user's signal. These types of attacks that can be used on cars are characterized as PKES system [9].

The PKES system is the Passive Key Entry and Start system. This system is used on numerous car models and relies solely on the communication between the key fob and the car itself [9]. This may seem small on the scale of possibilities with car hacking, especially when thinking about getting access to a car's safety ramifications and so on and so forth. However, these replay attacks on cars are merely a stepping stone to the rest of a car's vulnerabilities. The replay attacks allow a malicious user to gain access to the inside of a car, and give them further access to a car's ODB-II port. This would allow the malicious user to access a car's CAN network and possibly allow them to download malicious software to the car's systems. This could give the user access to things like the brakes and power to the car itself.

With the current security of cars' PKES systems, a user could gain access to a car with ease. For example, if the owner of a car enters a parking garage, a malicious user could set an antenna near the entrance and then another one near the car. When the owner of the car parks his car within the garage, they would leave their car unattended as they lock it and walk away. As the PKES system is constantly receiving signals from the fob, the owner passes the first malicious antenna. The first antenna can then in turn pick up the fobs signal strength and patterns. The malicious user then would use a second antenna near the car itself to allow the first antenna to transmit the mimicked fob signal to the car which in turn unlocks the car. This would give the user access to the car as if they had the key, and if the car has a "push to start option," they would be able to even drive the car away [9].

Aurelien Francillon et al. [9] provided a comprehensive discussion on how many different mitigation techniques work for automobiles, but they all come with pros and cons. They start with more simple ideas like physically shielding the key and removing the battery to control the software within the key fob itself [9]. This would in theory disable the PKES system until the driver is within a certain distance - something that is a very short distance between car owner and the car itself. Moreover, the authors discussed just adjusting the hardware for a switch to be used on the fob to turn the PKES system on and off [9]. The true issue with the replay attacks is that a malicious user can gain access to and start a targets car by replaying the signal that your key fob generates. The attacker could even replay with the shortened distance signal transmitting from the fob. The way this works in a lot of cases is that the "sender" (the car) sends a challenge to the "prover," (the key fob) and the "sender" then reads how long it took to get a reply since the time it sent the original challenge. Specifically, it references to the protocols simply having to do with the reply time, which is down to the nanosecond. The car simply reads how strong the signal is and the pattern that the signal is being transmitted; a malicious user could replicate these patterns and signal strengths with cheap technology.

III. THE HYBRID SECURITY SYSTEM

To address DoS and Replay attacks within a car network, we propose a Hybrid Security System (HSS) that consists of multiple layers of security. Specifically, each layer of the proposed HSS consists of multiple modules responsible to provide specific security defense mechanisms [10]. Each Electronic Control Unit (ECU) would be assigned a program acting like a firewall. By implementing this system, we can prevent unauthorized access to important bus systems and modules. The system deviates from the applied security protocols and systems that are already in-placed since it is implemented as a standalone program that provides a several lines of defense to the network while keeping pre-existing systems and protocols currently protecting the architecture. With whitelists currently protecting the internal systems, the hybrid security program (HSP) provides multiple layers of security distributed across different components. If one of these security measures is compromised, the second layer of security can stop a potential intrusion.

Our proposed hybrid solution not only helps to further secure the car but also provides a generic design that can be implemented on any underlying automobile platform. We envision our proposed HSS as an overall system (i.e., the most outer layer of the architecture) that serves as an "umbrella" on top of the two lower layers. The layer underneath the HSS is the Hybrid Security Program (HSP). The HSP is the layer/program that communicates between the HSS recourses layer and the Firewall Like Program layer [10]. The HSP is also known as the executer and decision maker of the architecture. It is also mainly in charge of the Firewall Like Programs (FLP). The FLPs are individual programs that are installed on each module, creating a firewall that examines each incoming packet to determine whether the packet should be allowed to enter into the module or deny access. The HSP and the FLP differ (despite both being "programs") because the HSP is located with the HSS, which is in a separate location of the FLPs. The FLPs are explicitly focused on filtering through packets on each module. By focusing on packets and not the entire message of packets, the hacker would have to work harder in mimicking the normal traffic messages

3.1. The Stateful Hybrid Adaption

Originally the Hybrid Security System's architecture was only using the stateless firewalls. By following this architecture, the security system was susceptible to vulnerabilities found in stateless firewalls. If an attacker compromised a stateless FLP, the compromised FLP would not be able to mitigate the attack. To combat the vulnerability in the FLP, an implementation of Stateful firewall would replace all FLPs assigned to modules that are external gateways for the vehicular network. These modules would include Bluetooth, WiFi, and wireless sensors as shown in Fig. 2.

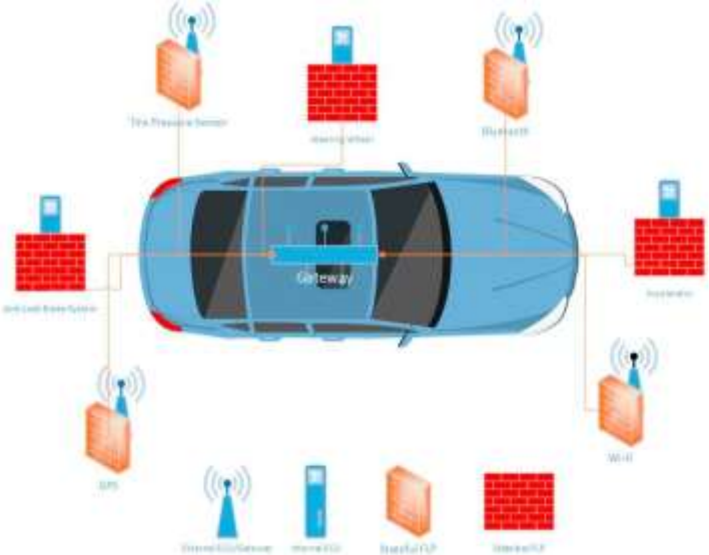

Fig. 2. An illustration of stateful firewall

When a packet passes through a Stateful FLP, the FLP determines if the packet is a trusted or untrusted packet. If trusted, the FLP allows the packet to pass through. However, if the packet is unknown or has requested access over 'x' amount of times, the FLP blocks the packet. In addition, the FLP generates an error ticket to the FLP Independent Log and a flag is generated - eventually causing a system wide black list. The HSS flag system has two types of flags that can be generated. The first flag is the Yellow Flag. The yellow flag is generated by the ‘x’ number of same source packets that are being dropped. When a yellow flag is generated, it is sent to the Flag Log in the HSS layer. If the Flag Log receives ‘x’ number of yellow flags, the HSP generates a Black Flag. When a black flag is generated, it generates a filtering rule update that adds the malicious packet source to the block table. This rule is then sent to every FLP on the network alerting every FLP of the rouge packet. The details of Stateful firewall are given below:

- Packets attempt to enter another external module, USB.
- The packets are declined by FLP ID:*x* and the errors are sent to the log.
- After *x* number of packets are denied *x* amount of times by FLP ID: *x*, a yellow flag is generated and sent to the flag log (Steps 1-3 are repeated until there are x number of yellow flags).
- After *x* number of yellow flags are generated by *x* amount of FLPs, a black flag is generated and distributed throughout the network.
- The black flag updates the filtering rules for every FLP.

IV. CONCLUSION

With technology in the vehicles progressing and smarter connected cars becoming more of a consumer demand, automotive manufactures must take automotive cyber security more seriously. While the connected cars become much safer on the road the networks that hold the critical safety components are becoming critically unsafe. To maintain safety of the safety features, the security and automotive industry must establish and maintain strong security systems. With vulnerabilities and threats such as the DoS and replay attacks, it could cause detrimental repercussions for the safety of the driver, passengers and others near the vehicle. Though our research and development of the Hybrid Security System is still on going, the HSS will help proactively fight against these attacks. With the Statefull Hybrid Adaption, we can bring a larger impact in further securing the state of the art in car security.

REFERENCES

[1] M. Khurram, H. Kumar, A. Chandak, V. Sarwade, N. Arora and T. Quach, "Enhancing connected car adoption: Security framework", 2016International Conference on Connected Vehicles and Expo (ICCVE), 2016.

[2] US Department of Transportation - National Highway Traffic Safety Administration, "Cybersecurity Best Practices for Modern Vehicles", 2016.Yadav, G. Bose, R. Bhange, K. Kapoor, N. Iyengar and R. Caytiles, "Security, Vulnerability and Protection of Vehicular On-board Diagnostics", International Journal of Security and Its Applications, Vol. 10, No. 4 (2016), pp.405-422, http://dx.doi.org/10.14257/ijsia.2016.10.4.36.

[3] H. Wang, L. Xu and G. Gu, "OF-GUARD: A DoS Attack Prevention Extension in Software-Defined Networks", Proceedings of the 2015 45thAnnual IEEE/IFIP International Conference on Dependable Systems and Networks, Pages 239-250, June 22 - 25, 2015.

[4] T. Hoppe, S. Kiltz and J. Dittmann, "Adaptive Dynamic Reaction to Automotive IT Security Incidents Using Multimedia Car Environment", 2008 The Fourth International Conference on Information Assurance and Security, 2008.

[5] T. Perry, "Why the Next Denial-of-Service Attack Could Be Against Your Car", IEEE Spectrum: Technology, Engineering, and Science News,

[6] 2016. [Online]. Available: http://spectrum.ieee.org/view-from-the-valley/transportation/safety/why-the-next-denial-of-service-attack-could-be-against-your-car.

[7] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[8] M. Raya and J. Hubaux, "Security Aspects of Inter-Vehicle Communications", in Swiss Transport Research Conference, Monte Verita, Ascona, Switzerland, 2005.Francillon, B. Danev and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars", in 18th Annual Network& Distributed System Security Symposium (NDSS Symposium 2011), San Diego, CA, USA, 2011

[9] S. Rizvi, J. Willett, D. Perino, T. Vasbinder and S. Marasco, "Protecting an Automobile Network Using Distributed Firewall System", in SecondInternational Conference on Internet of Things and Cloud Computing Proceedings, Cambridge, United Kingdom, 2017. – In Press