A Study On Vehicle And Counter Measure

Gourav Sachdev, Aayush Goyal, Arihant Jain, Aman Kumayu, Mr. Jayesh Surana
Information Technology, SVITS
Gram Baroli, Sanwer Road, Indore, MP, India

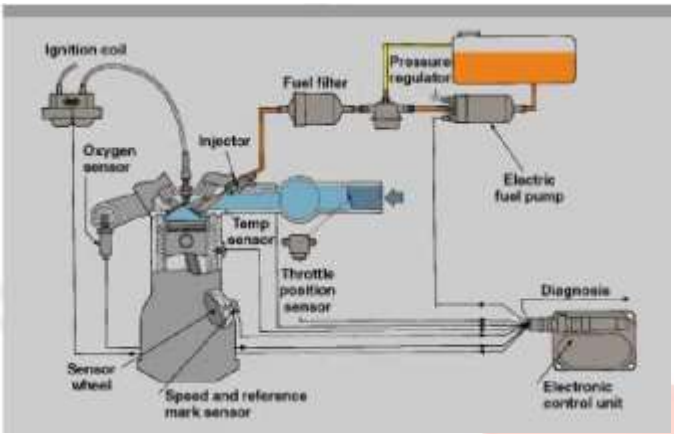
Abstract— **The modern automobile is a complex network of information systems. As the car becomes increasingly computerized, so too does its attack surface increase. With security researchers recently demonstrating a series of vulnerabilities in automotive systems, it is becoming clear that auto manufacturers have not placed enough emphasis on developing secure vehicular information systems. Indeed, the field of automotive systems security is in its infancy. Automakers are struggling to come to grips with the need to secure vehicles' on-board systems. As a result, the modern passenger vehicle presents an attractive target, with a broad attack surface and a multitude of potential vulnerabilities to exploit. This paper analyses recent research into automotive security vulnerabilities and reflects on the need for more secure vehicles.**

I. INT RODUCT ION

In the developed world, there is arguably no appliance more prevalent in people's lives than the automobile. Certain ly, in the United States, there is scarcely a household without access to a car or some other form of vehicular transportation. Statistics fro m the Un ited States Department of Transportation (2015) show that in recent years, over 250 million highway vehicles have been registered per year in the U.S. And, this number continues to grow steadily. Growing at an even faster rate is the prevalence of co mputers in modern auto mobiles. Co mputers began to find their way into passenger vehicles in the early 1980s with the advent of the Engine Control Unit (ECU). By managing basic engine functions, early ECUs brought about imp rovements in performance and fuel efficiency, while also lo wering vehicle emissions (Eyal, 2007).

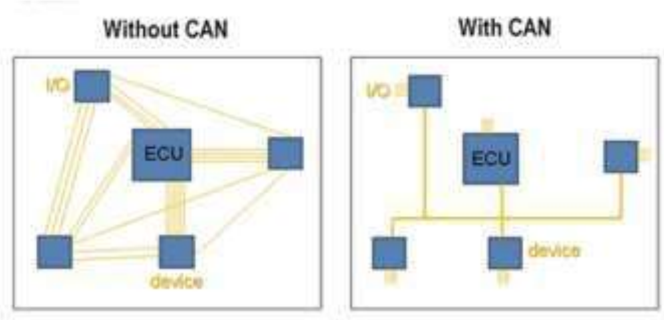
An ECU works by interfacing with different engine components including the fuel pump, fuel injectors, throttle body, spark plugs, and various sensors (Eyal, 2007). Develop ments in Car Hacking 3 The ECU receives inputs fro m the sensors and makes adjustments to a series of actuators controlling the function of the engine's physical components accordingly. This allows for ignit ion timing and fuel/air mixture to be dynamically adjusted in real-time, which can save fuel and optimize performance. Prior to the use of ECUs for engine management, these functions had to be controlled mechanically (Eyal, 2007). The Engine Control Unit has been found in almost every vehicle manufactured since the mid-80s (Micheli & Ernst, 2002). Unlike in the

1980s, however, the modern automobile now relies on computerization for almost everything fro m engine management to steering, braking, climate control, navigation, infotain ment, and much mo re. A group of researchers recently found that the average modern high-end car now contains over 100 million lines of code – more than an F-35 fighter jet or a Boeing 787 passenger airliner (Doughty -White & Quick, 2015). This heavy reliance on co mputers, therefore, means that the modern automobile has a very broad attack surface and the potential for a plethora of vulnerabilit ies. Today, in 2015, auto motive systems security is a hot topic. Several recent high-profile car hacking demonstrations have brought med ia attention to the fact that the modern automobile is a largely insecure platform; an insecure platform that the public has come to rely on heavily, and one wh ich plays an integral role in most people's lives. The imp lications of automotive system security vulnerabilities range fro m the mundane – such as an attacker being able to act ivate a vehicle's horn or flash its lights – to the downright terrify ing – an attacker remotely gaining control of a vehicle and running it off the road at speed with occupants inside.



II. EVOLUT ION

At the heart of any modern vehicle's interconnected systems is the Controller Area Network bus, or CAN bus. The CAN bus is a single, centralized network bus on which all of a vehicle's data traffic is broadcast. The CAN bus carries everything from operator commands such as "roll down the windows" or "apply the brakes", to readouts from sensors reporting engine temperature or tire pressure. The advent of the CAN bus brought about improvements in efficiency and a reduction in complexity while also reducing wiring costs.



that appears to change dynamically in real time. CAN bus include cabin temperature, tire pressure, steering input, vehicle speed, and many more

Prior to the development of CAN bus technology, any two vehicular components needing to communicate with each other would have required a dedicated point-to-point connection between them (National Instruments, 2014) . The diagram shown above in Figure 3 demonstrates how a CAN network can significantly reduce the amount of wiring needed in a vehicle by eliminating the old point-to-point topology in favour of a more efficient, centralized approach. Whereas the pre-CAN architecture diagram places the ECU at the centre of the logical network, the CAN diagram highlights the network bus itself as the focal point, removing point-to-point connections between devices and lessening the involvement of the ECU (National Instruments , 2014).

What sets the CAN bus apart from other common network bus topologies is that data constantly flows on the CAN bus whether it is actually requested or not. An example of this can be illustrated using the vehicle's tachometer, which displays the number of revolutions per minute (RPM) being performed by the engine. For the tachometer to display the engine RPM, it does not first need to send a query to the engine; instead, the engine's ECU constantly broadcasts the engine RPM out over the CAN bus to any listening controllers. All the tachometer's controller needs to do is monitor CAN bus traffic for RPM messages, and when one is detected, the tachometer's display is updated with the new information. By repeating this action many times per second, the driver sees a tachometer readout that appears to change dynamically in real time.

What sets the CAN bus apart from other common network bus topologies is that data constantly flows on the CAN bus whether it is actually requested or not. An example of this can be illustrated using the vehicle's tachometer, which displays the number of revolutions per minute (RPM) being performed by the engine. For the tachometer to display the engine RPM, it does not first need to send a query to the engine; instead, the engine's ECU constantly broadcasts the engine RPM out over the CAN bus to any listening controllers. All the tachometer's controller needs to do is monitor CAN bus traffic for RPM messages, and when one is detected, the tachometer's display is updated with the new information. By repeating this action many times per second, the driver sees a tachometer readout

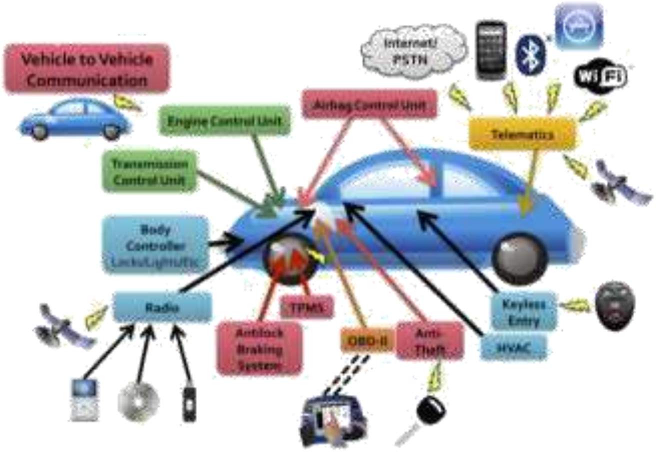
III. HISTORY

When the CAN bus was being developed in the mid-1980s, its designers certainly did not envision that one day the bus would be targeted by attackers seeking to take over or otherwise manipulate the function of an automobile. In fact, as recently as ten years ago, the concept of car hacking received little media attention and was not a worry to most vehicle consumers. It is only in the last decade, and particularly in the last several years, that car hacking has become a very real concern. In a 2015 study by Kelley Blue Book in which members of the car-buying public were polled, it was found that 78% of study participants believed vehicle hacking “will be a frequent problem in the next three years or less” (as cited in PR Newswire, 2015). This perception among the general public is due in large part to several recent high-profile vehicle hacks. The timeline below summarizes some of the more notable automotive hacks that have occurred recently.

1. 2010 – Vehicles Disabled Remotely Via Web Application - One of the first widely reported accounts of vehicle hacking came in 2010 when a disgruntled former employee of an Austin, Texas car dealership sought revenge against his former employer (Poulsen, 2010). In reality, this attack did not involve any hacking of the actual vehicles themselves. Nonetheless, the attacker was able to physically disable the vehicles of innocent owners without their knowledge or consent. The former dealership employee used stolen credentials to log into a web application that allowed remote access to functions of customers’ vehicles including the engine immobilizer and the horn (Poulsen, 2010). This web application’s intended purpose was to let dealership personnel immobilize the vehicles of customer who failed to make their loan payments on time. In fact, it ended up being used to cause mayhem as car owners found themselves locked out of their vehicles with the horns constantly honking (Poulsen, 2010).

2. 2010 & 2011 – CAESS Experimental Analysis -

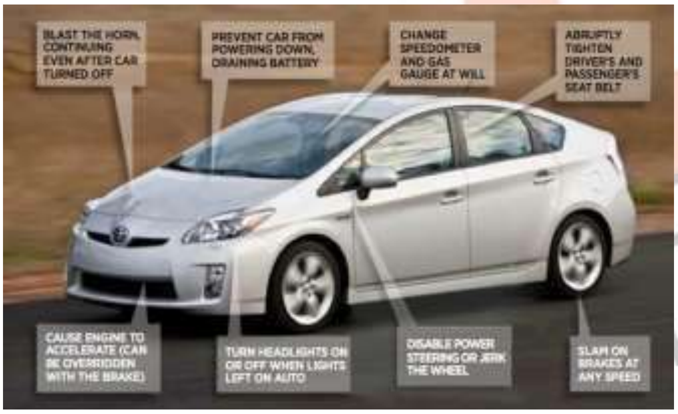
In 2010, a group of researchers from the Center for Automotive Embedded Systems Security (CAESS) – a joint venture between the University of Washington and the University of California, San Diego – released a research paper entitled “Experimental Security Analysis of a Modern Automobile” (Koscher et al., 2010). The team conducted a range of lab experiments and road tests and found that it was possible to manipulate a vehicle’s functions by injecting messages on the CAN bus (Koscher et al., 2010). The researchers successfully demonstrated that a would-be attacker could disable the brakes, selectively brake individual wheels on demand, stop the engine, falsify information on the vehicle’s speedometer, and more (Koscher et al., 2010).



3. 2013 – Miller & Valasek Physical Hack-

A more recent high-profile case of vehicle hacking came fro m researchers Charlie Miller and Chris Valasek. Working with an $80,000 grant fro m the Defense Advanced Research Projects Agency (DARPA), M iller and Valasek were tasked with finding security vulnerabilities in automobiles and published their findings in 2013 (Greenberg, 2013). The duo conducted a series of real-time demonstrations for journalists and security professionals, before going on to present their findings at the Defcon conference in Las Vegas, Nevada that same year. Specifically, M iller and Valasek targeted the systems of a 2010 Ford Escape and a 2010 Toyota Prius (Greenberg, 2013). They were essentially able to reverse engineer the vehicles' CAN bus commun ications to demonstrate "everything from annoyances like uncontrollably blasting the horn to serious hazards like slamming on the

Prius' brakes at h igh speeds" (Greenberg, 2013). The infographic in Figure 8 lists many of the vehicular functions that Miller and Valasek were able to man ipulate on their 2010 Toyota Prius test vehicle. So me of these capabilities, such as being able to jerk the steering wheel or slam on the brakes, propelled car hacking fro m a nuisance to a serious safety concern for automakers.


BLAST THE HORN, CONTINUING EVEN AFTER CAR TURNED OFF
PREVENT CAR FROM POWERING DOWN, DRAINING BATTERY
CHANGE SPEEDOMETER AND GAS GAUGE AT WILL
ABRUPTLY TIGHTEN DRIVER'S AND PASSENGER'S SEAT BELT
CAUSE ENGINE TO ACCELERATE (CAN BE OVERRIDDEN WITH THE BRAKE)
TURN HEADLIGHTS ON OR OFF WHEN LIGHTS LEFT ON AUTO
DISABLE POWER STEERING OR JERK THE WHEEL
SLAM ON BRAKES AT ANY SPEED

4. 2015 – Miller & Valasek Remote Hack-

Charlie Miller and Chris Valasek made headlines again in 2015, this time fo r successfully demonstrating that an unaltered passenger vehicle – a 2014 Jeep Cherokee in this case – could be remotely exploited without the need for any physical access (Miller & Valasek, 2015, p.6). Unlike the duo's 2013 hack of a Toyota Prius and Ford Escape, this new research mimicked a real-world attack scenario in that it demonstrated both the ability to gain remote access and the ability to remotely execute code. And unlike the 2013 hack, which was largely met with incredulity by automakers, the 2015 hack prompted Fiat Chrysler Automobiles (FCA) to recall some 1.4 million vehicles for a critical security update and forced Sprint Corporation to enhance the security of its cellular carrier network. Miller and Valasek's Jeep hack took advantage of the vehicle's onboard connectivity features, in addition to the familiar lack of security controls on the CAN bus. Access was obtained through a vulnerability in Uconnect, a system that governs the vehicle's infotainment, navigation, built-in apps, and cellular communications (Greenberg, 2015a). What made the Uconnect system so attractive to the pair of researchers was that in addition to being a hotbed of connectivity, Uconnect also contains a microcontroller in its head unit which can communicate with other modules on the vehicle's CAN bus (Miller & Valasek, 2015, p.20). The hack also took advantage of a weakness in Sprint's cellular network, to which the vehicle's on-board telematics system was connected. The telematics system is used for real-time traffic data, in-car Wi-Fi, and other remote connectivity functions.

IV. SECURING THE AUTOMOBILE

The extensive media attention given to Charlie Miller and

Chris Valasek's Jeep Cherokee hack has sent automakers scrambling to better secure their vehicles. The old industry status quo of "security by obscurity" is no longer acceptable.

Researchers have published detailed accounts of how to gain access to the CAN bus and manipulate CAN messages. As such, the security of vehicle systems is no longer a topic that can simply be ignored by manufacturers. While it is to be expected that each automaker will approach the problem of vehicle systems security in its own way, outlined below are some fundamental security best practices that should be followed going forward.

Encryption

One of the most fundamental flaws of the CAN protocol is a lack of message confidentiality. As in the "security by obscurity" model, automakers rely solely on a proprietary message format that is unknown to the public as a means of security. But as has been shown, it is possible to decipher these proprietary CAN messages to uncover their function, and to then modify or replay CAN messages for malicious purposes. The most effective way to prevent CAN reconnaissance is to apply some form of encryption to the CAN protocol.

A significant limitation facing CAN encryption is the CAN protocol's maximum data field size of 8 bytes. According to

Gene Carter o f security firm Security Innovation, “CAN is an old technology with limited data streams, [therefore] it isn't possible to use encryption of any meaningful size” (as cited in

Yoshida, 2015). It is widely accepted that a strong encryption algorith m requires a 128-bit or 256-b it block size. But that hasn’t stopped several different researchers and security companies from proposing solutions for CAN encryption.

Defense in Depth

There is no single solution to the security vulnerabilities facing automotive systems. What is needed is a broad approach providing mu ltiple layers of security, also known as

“defense in depth” (McGuiness, 2001). The concept of defense in depth utilizes “a series of defensive mechanis ms such that if one mechanis m fails, another will already be in place to thwart an attack” (McGuiness, 2001).

In the Information Security field, it is a common ly accepted reality that perimeter defenses will fail at some point. Boundary defense alone is not enough to secure an informat ion system. It must be assumed that an attacker is capable of bypassing perimeter defenses and will eventually find himself within the internal network. When that happens, there must be a sufficient arsenal of other security controls in place to keep him fro m maneuvering within the system or otherwise being successful in performing an attack. A holistic approach to securing a vehicle’s systems should include – at the very least – better network segmentation, locking down of external interfaces, controller authentication, and data encryption.

Security by Design

A major obstacle to the development of secure automobiles is the archaic CAN bus technology that lies at the core of almost every modern car. According to Kathleen Fisher, a p rofessor at Tufts University, “the CAN bus is hopelessly insecure

[because] it was developed decades before cars were connected to the Internet and lacks features to block malware programs or reject co mmands fro m unauthorized intruders”

(as cited in Bray, 2015). Because of the significant limitations of CAN, automakers will be forced to implement “Band -Aid” fixes for CA N until a fundamental overhaul of vehicle networking architecture occurs. Ideally, security should be designed into vehicle systems fro m the ground up. Security should never be an afterthought, nor should security features be applied reactively. As automakers exp lore the prospect of replacing CA N with a more fundamentally secure infrastructure, Ethernet has shown promise as one possible solution.

Device Authorization

Another key element in preventing an attacker fro m being able to transmit malicious messages on the CAN bus is to require authentication or authorization of devices. Previous attack demonstrations have utilized devices – generally laptop computers – wh ich should have no leg itimate reason for transmitting data on the CAN bus.

V. THE CAN HACKING TOOL (CHT)

Recently, security researchers Alberto Garcia Illera and Jav ier Vazquez-Vidal presented the CAN Hacking Tool (CHT), a $20 smartphone-sized apparatus that can compro mise an automobile's co mputer system. In o rder fo ra hacker to do that, however, he needs physical access to the car. The CHT has four wires that go into several outputs of an auto's CAN. A cheap computer chipset bypasses encryption on the car prior to reading/writ ing data fro m vehicle's memory residing in its engine control unit. After that, it can wirelessly control vital car's functionalities as steering and brakes. The words of Vazquez-Vidal attested to the simplicity of the process: "It can take five minutes or less to hook it up and then walk away. We could then trigger it to do whatever we have programmed it to do."

a) Indirect Physical Channels

Today's automobiles provide a nu mber of physical interfaces for easy access to the car's networks.

Door Locks

In modern automobiles, the power-locking system is interconnected to other car mechanisms in order fo r doors to lock auto matically when a car is in drive, for instance, or unlock in case the airbags have been released or the car keys are forgotten inside.

MP3 MALWARE: iPod, Disc, and USB.

Virtually all manufacturers integrate media devices into their products. Researchers proved that malicious input can be delivered by encoding it into an MP3 file or a CD. As a result, an adversary may deceive the user or recourse to social engineering techniques just to prompt him into playing a CD or a song file that has a malicious code. Alternatively, compro mising user's phone or iPod with a malware that insidiously engages the automobile's media system when connection takes place, is another viable modus operandi. If you think that taking over a CD player system alone is not a pervasive threat, think again of the how CAN bus is interconnected in such a style so as to even med ia systems not be standalone units. Furthermore, corrupted audio files of such a nature may spread in a worm-like manner if the user under attack decides to share them through peer-to-peer networks, for instance.

b) Remote Hacking Wireless Communication Units

Every wireless network is potentially dangerous because a person can never know if someone is lurking in the dark, preparing to intercept his data. The good news is that: firstly, WiFi range may be limited in d istance; secondly, utilizing a Wi-Fi/Bluetooth signal blocker may prove sufficient to b lack out any wireless connections, trustful or corrupt, around your car.

Troels Oerting, the d irector of the Eu rope's Cybercrime

Centre, opines that car hacking might be a real security concern very soon: "W ireless technology is integrated into practically everything nowadays and if there's wireless access to anything there's a possibility to remotely control it."

In the same spirit is the opinion of Roesner: "Cars are not only becoming more co mputerized internally, but that they are becoming increasingly connected to the outside world. Automobiles most at risk include those with more co mponents under computer control and without manual overrides, and those that are more connected to the outside world via the

Internet or wirelessly." She further defines this trend in interconnectedness as "concerning".

VI. UNAUTHORIZED APPS

Similarly, to the smartphone business in which a mult itude of programs is developed by third-party enterprises and contractors, carmakers are forced by the advent of the digitalisation era to expand their in fotain ment services and provide downloadable software to their clients. Unfortunately, there are always rogue apps that contain viruses or malware, which can contaminate your car without you having a clue about it. What may give you co mfort is the fact that carmakers usually very strictly select app developers and permit only a handful of preapproved programs. Besides, the number of apps available for infotain ment systems is far less than those envisaged for smartphone users.

Short-range Wireless Access -

Devices under attack in this category are Bluetooth, WiFi, Keyless Entry, RFIDs, Short Range and Tire Pressure Monitoring Systems. For a successful attack, researchers assume that an adversary will need to place a wireless transmitter within 5 and 300 meters fro m the car’s receiver, depending on the channel.

KEY FOB

A wireless key fob is used by a car owner to unlock and start the car when they utilize the device in close proximity to the car. Swiss researchers, however, figured out how to intercept the signal within a radius of 30 feet with gadgets that cost less than $100.

If there is a vulnerability in the ECU software entrusted with parsing messages through channels, then the evildoer may exploit the ECU, and by extension, the integrity of the entire vehicle plainly by transmitting malware content from a short - range distance.

VII. CONCLUSION

Well, although cars are computerized, they do not function like PCs or smartphones. Hackers need to put a lot more effort to assume control of a vehicle than, for example, to steal someone's banking credentials and siphon off his money. Cars are not built to take randomly forced in commands, and even if that works, the effect would only remain for that intended car. The motives? They vary from a reputation showing off to more serious crimes like erasing information from in -car event data recorders, theft, kidnapping, and assassination. Despite the fact that there are no significant real life cases of car hacking to date, the threat is scientifically proven and it is out there for gifted but malevolent minds to exploit.

VIII. GLOSSARY AND ABBREVIATION

ECU (Engine Control Unit): Main control of the vehicle engine.

RPM (Revolutions Per Minute): The number of revolutions per minute (RPM) being performed by the engine.

CAN (Controller Area Network): The CAN bus is a single, centralized network bus on which all of a vehicle's data traffic is broadcast.

CHT (CAN Hacking Tool): It can wirelessly control vital car's functionalities as steering and brakes.

IX. REFERENCES

Eyal, N. (2007). Vehicle Lab – Engine Control Unit. Retrieved November 26, 2015, from http://www.vehicle-lab.net/ecu.html

Fortin Electronic Systems. (2006). What is CAN Bus? Retrieved November 12, 2015, from http://canbuskit.com/what.php

Greenberg, A. (2013). Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel. Retrieved November 14, 2015, from http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-mebehind-the-wheel-video

Greenberg, A. (2015a). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Retrieved November 15, 2015, from http://www.wired.com/2015/07/hackersremotely-kill-jeep-highway

Greenberg, A. (2015b). 5 Lessons from the Summer of Epic Car Hacks. Retrieved November 16, 2015, from http://www.wired.com/2015/10/five-car-hackinglessons-we-learned-this-summer

Lambert, F. (2015). Tesla hired Chris Evans from Google's Project Zero to lead the company's security team. Retrieved

November 16, 2015, from http://electrek.co/2015/08/06/tesla-hired-chris-evans-from-googles-project-zero-to-lead-thecompanys-security-team

National Instruments. (2014). Controller Area Network (CAN) Overview. Retrieved November 27, 2015, from http://www.ni.com/white-paper/2732/en/

OpenXC. (2015). Vehicle Interface Concepts. Retrieved November 13, 2015, from http://openxcplatform.com/vehicle-interface/concepts.html

OWASP. (2009). Avoid Security by Obscurity. Retrieved November 16, 2015, from https://www.owasp.org/index.php/Avoid_security_by_obscurity

Wikipedia. (2014). File:CAN-Bus-frame in base format without stuffbits.svg. Retrieved November 27, 2015, from https://commons.wikimedia.org/wiki/File:CAN-Busframe_in_base_format_without_stuffbits.svg

Wojdyla, B. (2012). How it Works: The Computer Inside Your Car. Retrieved November 12, 2015, from http://www.popularmechanics.com/cars/how-to/a7386/how-itworks-the-computer-inside-your-car