International Journal of Research (IJR) Vol-1, Issue-10 November 2014 **ISSN 2348-6848**

Amateurs Hack System Professionals Hack Cars

Amit Saini & Akansha Marwah

Department of Electronics and Computer Science Engineering

Dronacharya College of Engineering

Khentawas, Farrukh Nagar – 123506

Gurgaon, Haryana

Email: {amit.saini0384@gmail.com, makansha1995@gmail.com}

ABSTRACT:

Modern automobiles are no longer mere machines running on 4 wheels. They are machines being monitored by a number of digital computers coordinated via internal vehicular networks.

While this enhancing technology has provided substantial benefits to efficiency, safety and cost, it has likewise created a space for new approaches.

In this paper, we discuss the structural characteristics of the auto motive ecosystem that give rise to such attacks and high light the practical challenges in reducing them. We demonstrate the ability to control the automotive functions and completely ignore driver input -- including disabling the brakes, stopping the engine, and so on.

INTRODUCTION:

For the past 80 years, the passenger automobile industry has remained confined to a single gasoline powered internal combustion engine; four wheels, gearshift, steering wheel and brakes.

However, in the past two decades, the control systems have experienced a drastic change. Today, it's not just the wheels on which a car runs; it's also a 1000-2000 page code making it happen.

A luxury sedan now contains over 100 MB of binary code spread across 50–70Electronic Control Units (ECUs) allowing communication over one or more shared internal network buses.

Each component of a car, from the Anti-Lock Brake module to the Telematics module, can communicate with each other. The automotive industry has always considered safety an uncertain engineering concern but the question arises whether manufacturers keep in their mind the intentions of an attacker. The present scenario depicts that the enhanced computerized control is also making a room for potential threats.

As more sophisticated services and communications features are added into vehicles, the possibility of attack on modern automobiles increases swiftly. In USA it is mandatory to install the On-Board-diagnostics (OBD-II) port under the dash in all modern vehicles. OBD systems give the vehicle owner or repair technician access to the status of the various vehicle sub systems. General Motors' OnStar demonstrated Telematics systems, which provided features such as automatic crash response and stolen vehicle recovery over a long-range wireless link.

To what extent are external attacks possible, how to reduce the vulnerability? Our aim is to answer these questions through a systematic analysis of the remote attack surface.

1) <u>Characterizing Threat Model:</u>

Indirect physical access, short-range wireless access, and long-range wireless access lie under the attacker's ability to deliver malicious input into the machine. Within these 3 categories, we characterize the attack surface exposed in current automobiles.

2)Analysing Vulnerability:

Here we assess the level of actual exposure in each case. We focus on the vulnerabilities that allow the attacker to peek into the automotive machine, without gaining direct physical access to it. The major attack-prone sites in a car include media player, hands-free-Bluetooth device and the car's cellular modem.

3) Threat assessment:

The question arises that what capabilities does the vulnerability enable?
An attacker may modify a car's external interfaces for post-compromise control through the means of multiple post-compromise control channels, secret streaming of cabin audio to an outside recipient.

Before we proceed with the methods and the aftermath of this kind of hacking let us first understand the basic devices present in the cars which are attacked upon.

Electronic Control Unit:

Electronic control unit (ECU) is a generic term for any embedded system that controls one or more of the electrical system or subsystems in an automotive machine. These systems are sometimes referred to as the car's computer. Some modern motor vehicles have up to 80 ECUs. Embedded software in ECUs continues to increase in complexity, and sophistication.[2] Managing the increasing complexity and number of ECUs in a vehicle has become a key challenge for original equipment manufacturers (OEMs).

ECUs are interconnected by Controller Area Network (CAN) or Flex Ray bus. This interconnection allow convenience features such aspre-tensioning of seat-belts during a crash and automatically varying radio volume as a function of speed and provides the user with complex safety.

ECU'S communicate with each other by sending CAN packets. There is no source identifier or authentication built into CAN packets. It makes reverse engineering traffic more difficult because it is impossible to know which ECU is sending or receiving a particular packet.

ECUCoupling:

Many features require complex inter actions across ECUs for example, modern Electronic. Stability Control (ESC) systems monitor individual wheel speed, steering angle, and various accelerometers. The ESC modulates engine torque and wheel speed on its own to increase traction when the car's line stops following the steering angle. If brakes are applied they must also interact with the Antilock Braking System (ABS).

Active Cruise Control (ACC) systems scan the road ahead and automatically increase or decrease the throttle depending on the presence of slower vehiclesinthe path (e.g., the Audi Q7 will automatically apply brakes, completely stopping the vehicle if necessary, with no user input).

Telematics:-

GM's OnStar provides a myriad of services. An OnStar-equipped car can analyse the car's On Board Diagnostics(OBD) as it is being driven, proactively detect likely vehicle problems, and notify the driver that a trip to the repair shop is warranted. OnStar ECUs monitor will automatically place emergency calls, provide audio-links between passengers and emergency personar. These systems even enable properly authorized OnStar personnel to remotely unlock cars, track the cars' locations.

Instead, we focus primarily on what an attacker could do to a car if she was able to maliciously communicate on the car's internal network.Insert a malicious component into a car's internal network via the ubiquitousOBD-II port (typically under the dash). The attacker may leave the malicious component permanently attached to the car's internal network or, as we show in this paper, they may use a brief period of connectivity to embed the malware within the car's existing components and then disconnect.

Car Security Challenges:

Since CAN packets are both physically and logically broadcast to all nodes, a malicious component on the network can easily send packets to any other node on the network. CARSHARK grips this property, allowing us to reverse-engineer packets, as well as to inject new packets to induce various actions.

No Authenticator Fields:

CAN packets contain no authenticator fields i.e., that any component can indistinguishably send packet to any other component. This means that any single compromised component can be used to control all of the other components on that bus,

Attack Methodology:

These can be the few major approaches that can help a hacker peek into the car without gaining direct physical access to it.

Packet Sniffing and Targeted Probing:

CARSHARK can be used to observe traffic on the CAN business order to determinee how ECUs communicate with each other. It can also tell which packets were sent if we activate various components.

It can be used to discover how to control the radio, and a number of the Body Control Module (BCM) functions.

Fuzzing

Ssignificant attacks do not require a complete understanding or reverse-engineering of even a single component of the car. In fact, because the range of valid CAN packets is rather small, significant damage can be done by simple fuzzing of packets. Indeed, for attackers seeking indiscriminate disruption, fuzzing is an effective attack by itself.

Reverse-Engineering:

For a small subset of ECUs, code can be dumped via the CAN Read Memory service and used third-party debugger (IDA Pro) to explicitly understand how certain hardware features were controlled.

Consequences:

Here are the following aftermaths which may occur or in other words can be triggered by the hacker in an individual's car.

Brakes:

Unification of the Electronic Brake Control Module allows discovering how to lock individual brakes and sets of brakes, notably without needing to unlock the EBCM with its Device Control key. By posting a random package, one can not only occupy the front left brake, but can lock it to manual override even through a power bike and battery removal. To rectify this, we had to resort to continued fussing to find a package that would override this result.

Generic Denial of Service:

We can disable the communication of individual parts on the CAN bus.Disabling communication to/from the ECM when the wheels are whirling at 40 MPH reduces the car's reported speed immediately to 0 MPH. Disabling communication to/from the BCM freezes the instrument panel cluster in its current state (e.g., if communication is disabled when the car is going 40 MPH, the speedometer will continue to report 40 MPH).

Lights Out:

One can disable certain interior and exterior lights on the car. One can disable all of the car's lights when the car is traveling at speeds of 40 MPH or more, which is particularly dangerous when driving in the dark. This lets in the headlights, the brake lights, the auxiliary lights, the interior dome light, and the elucidation of the instrument panel cluster and other display lights inside the automobile. This approach requires the lighting control system to be in the "automatic" setting, which is the default context for most drivers.

Self-destruct:

In this a 60-second countdown is displayed on the Driver Information Center (the dash), accompanied by clicks at an increasing rate and horn honks in the last few seconds. It goes with killing the engine and activating the door lock relay (preventing the occupant from using the electronic door unlock button).

Preventions:

In that respect is always a path to avoid somebody from peeking in your car's system and thus keeping your precious spirit. Researchers and programmers are working upon the same.

Towards Security:

These are just a few of many potential defensive directions and associated tensions. They are deep-rooted tussles surrounding the security of cyber physical vehicles, and it is not yet clear what the "right "solution for security is or even if a single "right" solution exists. More likely, there is a spectrum of solutions that each tradeoff critical values (like security vs. support for independent auto shops). Thus, we argue that the future research agenda for securing cyber-physical vehicles is not merely to consider the necessary technical mechanisms, but to also inform these designs of what is feasible practically and compatible with the interests of a broader set of stakeholders. This work serves as a critical piece in the puzzle, providing the first experimentally guided study into the real security risks with a modern automobile.

Ford has offered the so-called Sync technology service it co-developed with Microsoft in most of its Ford, Lincoln, and Mercury vehicles since 2008. The technology lets drivers run their Bluetooth-enabled mobile phones and digital media players via their vehicles and use voice commands to operate them, for instance. The automaker said March 8 that the second generation of its Sync technology — due out later this year and to include a full Windows CE operating system with a new driver interface called MyFordTouch — will come with a built-in browser and secured Wi-Fi access. The Wi-Fi will be broadcast via Sync using a USB-based modem, and Ford has updated its on-board firewalls to protect both the Wi-Fi network as well as the vehicle operations. The Wi-Fi network is set by default to Wi-Fi Protected Access 2 (WPA2) encryption for secured access to the wireless network. It also will provide anti-malware protection.

McAfee Security Researcher Barnaby Jack just joined the hacking team to attack embedded devices and protect vehicles from viruses; Jack is a member of the McAfee TRACE (Threat Research and Central Intelligence Experts) team who specialize in embedded device security. Jack is part of the TRACE team investigating how to protect embedded systems, hardware and devices from next-generation hacking attacks. That research includes finding and fixing vulnerabilities such as those in medical devices and car systems. As we read about the endless attack vectors on the computer with four wheels in which we sit inside and drive at high speeds, it makes us feel a bit better to know Jack is on the job.

Future Scope:

Hacking is always assumed as the dangerous practice; in fact, it is but if looked with the different angle of view we can use this in a positive way.

Car hacking can help the Army to track the extremists and prohibit them from absconding. In the same way CBI agents, CID members, Cops and Raw agents can use this technique to catch the criminal and spying agents respectively.

Conclusions:

Vehicles have been planned with safety in mind. Even so, you cannot have safety without security. If an assailant (or even a corrupted ECU) can send CAN packets, these might bear on the safety of the vehicle. This paper has shown, for two different automobiles, some physical changes to the part of the machine, including safety implications, that can occur when arbitrary CAN packets can be transported on the CAN bus. The promise is that by freeing this information, everyone can have a candid and informed discussion about this issue. With this information, individual researchers and consumers can propose ways to make ECU's safer in the bearing of a hostile CAN network as well as ways *to detect and stop CAN bus attacks. This will contribute to safer and resilient vehicles in the hereafter. So next time when you're driving and suddenly a similar scene out of Mission Impossible befalls, then better be worried that a malicious hacker has launched a "Self Destruct" attack on your vehicle. DRIVE SAFE!!*

References:

[1] Hartmann, B., Doorley, S., & Klemmer, S. R. (2008). Hacking, mashing, gluing: Understanding opportunistic design. *Pervasive Computing, IEEE*, *7*(3), 46-54.

[2] Hartmann, B., Doorley, S., & Klemmer, S. R. (2008). Hacking, mashing, gluing: Understanding opportunistic design. *Pervasive Computing, IEEE*, *7*(3), 46-54.

[3] Tapscott, D., & Williams, A. D. (2007). Hack This Product, Please. *The Business Week Wikinomics Series, Business Week, February, 23*.

[4] Long, J. (2011). *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Syngress.

[5] Beaver, K. (2012). *Hacking for dummies*. John Wiley & Sons.