V. May Tomic
Professor Kurt Teichert
ENVS 0070C
December 6, 2015

Research Proposal: Cybersecurity in the Automobile Industry

The basic purpose of the automobile has changed little in the past century: with its internal combustion engine and noxious exhaust, the modern car seems to be hardly more than a large mechanical tool for getting from one place to another. However, as automakers have increasingly incorporated computerized and network-connected elements into their new vehicle technologies, the electronic subsystems that underlie the physical control and safety of automobiles have grown more complex and more integral to proper vehicle performance. Despite the cybersecurity risks inherent to this increased level of computerization and connectivity, many of which have been verified as significant threats by third-party researchers, automakers continue to deny that car-hacking presents any serious danger to consumers. In order to ensure the safety of the vehicles of the future, it will be necessary for the car companies that have attempted to “turn the modern automobile into a smart phone” (Greenberg) to take responsibility for the consequences of this rapid innovation and begin conducting cybersecurity threat analysis and penetration testing throughout their design and manufacturing process. The question that remains to be answered, then, is exactly how and at what cost major automakers can alter their current practices to include this type of fully process-integrated security testing.

Understanding how computerization creates vulnerable attack surfaces in current and future vehicles requires a basic understanding of recent developments in electronic automotive control systems. Modern automobiles now come equipped with a range of computer-based components, called Electronic Control Units or ECUs, which manage sets of particular vehicle features and actions. ECUs, between twenty and one hundred of which can be found in any modern vehicle on the road, monitor and control everything from air-conditioning and radio settings to steering wheel angle and automatic braking systems. In the past, ECUs only needed to communicate internally with one another in order to share information about the current state of the vehicle between the car’s various electronic subsystems. Increasingly, however, vehicular ECU’s must also be made to send and receive information from external, wirelessly connected systems. Examples include cellular connections that allow hands-free calling from within vehicles, radio systems that gather song and artist information from internet sources over Wi-Fi, and a slew of other connectivity and networking-related features. It would be reasonable to expect that the ECUs accepting input from external networks and those directly managing vehicle safety and control systems would be separated by physical and telecommunication-based barriers in order to prevent unauthorized external parties from gaining remote access to the system-critical ECUs which comprise a vehicle’s control area network, or CAN, bus. As it turns out, this is rarely the case. Although car-manufacturers claim to keep these systems separated, in reality there often exists at least one unprotected or vulnerable line of communication between externally accessible ECUs, such as those found in many modern car entertainment or telematics systems, and those ECUs which are capable of sending CAN messages that will directly alter a car’s physical behavior, such as steering, braking, or acceleration. As modern vehicles come to increasingly communicate with outside information networks, these internal electronic control systems will grow only more highly connected, more complex, and more susceptible to attack. The research that has already been conducted in the area of remote vehicle hacking – which has largely been pioneered by “white hat” hackers who exploit computerized systems but are committed to releasing their findings for the public good — not only reveals specific threats, but also highlights the critical need for further research.

Knowing the general structure of the electronic automobile control system described above, the worst-case car-hacking scenario may seem a little far-fetched: could it really be possible for an attacker to execute control messages that might kill the transmission, cut the brakes, or track the GPS coordinates of your car without ever even seeing the vehicle? In October of 2015, a pair independent computer security specialists, Charlie Miller and Chris

Valasek, decided to put computer-connected vehicles to the test by attempting to implement this kind of remote takeover. They spent the winter attempting to hack into an unaltered and legally street-safe vehicle – a regular 2014 Jeep Cherokee released by Fiat Chrysler Automobiles. In spring of 2015 they began disclosing their findings to FCA, finally submitting a pre-release of their completed research to FCA on July 16th, 2015. On July 24th, more than 1.4 million Chrysler vehicles were recalled as a result of Miller and Valasek's report. It was not until the two white hat hackers presented at the DEF CON hacking conference in August 2015 that the technical details and catastrophic implications of their exploit were revealed: using only existing hacking tools and freely-available manufacturer data, Miller and Valasek were able to gain full CAN bus access by attacking a network-connected entertainment/telematics system found in every Chrysler vehicle released after 2013. This hack was executed not through physical access to the car, but rather through the completely remote manipulation of an unprotected server port that is part of the Chrysler Uconnect system. This port was found to be accessible via WiFi or any Sprint cellular network in the country, making it easy for anyone with Miller and Valasek's research in hand to scan for vulnerable vehicles and, with a few lines of CAN bus commands, make a car on the other side of the country veer off the road, lose control of its brakes, or even become "bricked" – totally non-functional – in a matter of minutes. Miller and Valasek estimated that hundreds of thousands of vehicles currently on the road are vulnerable to potentially deadly cyberthreat. But, if the Chrysler recall of 1.4 million vehicles is any indication, it would seem that their estimate is too conservative by an order of magnitude. What, then, have automakers done to address the obviously credible threat of large-scale automotive cyberattacks? The answer, as hackers wearing black hats instead of white are certainly beginning to discover, is nearly nothing.

Although the positive impact of independent researchers like Miller and Valasek cannot be overestimated, the need for large-scale, automaker funded and approved research is clear. The 1.4 million Chrysler vehicles recalled earlier this year represent only a small fraction of the millions of cars projected to enter public roadways equipped with insecure computerized control systems in the near future. When Senator Edward Markey sent a letter to twenty automakers requesting information regarding the risks and precautions surrounding car-hacking in 2013, the sixteen companies that responded “all confirmed that virtually every vehicle they sell has some sort of wireless connection, including Bluetooth, Wi-Fi, cellular service, and radios,” (Greenberg) while almost none claimed that they had conducted any serious security testing of these features. Although sweeping recalls may soon be replaced by over-the-air updates that allow security patches to be delivered to vehicles remotely, the stakes are far too high to rely on these retroactive methods of ensuring vehicle safety. Even with such measures in place, it is neither logical nor safe to assume that significant threats will always be discovered by individuals for whom public safety is a primary concern: for every white hat hacker interested in sharing vulnerabilities before they can be exploited, there are many more hackers motivated by malicious goals, who are unlikely to be concerned about the potentially deadly consequences of their actions. Thus it is critical that manufacturers start thoroughly testing for vulnerabilities before at-risk vehicles are released for public use. However, as vague automaker responses regarding computer security protocols make clear, little has been done to research the critical question that must be concretely answered before an industry-wide cybersecurity crack-down can occur: how and at what cost can extensive software testing be integrated into existing automobile manufacturing practices?

The general methodology that I propose for conducting the research needed to answer this question is as follows: assign teams of independent cybersecurity analysts to each of the twenty major automobile manufacturers implicated by Senator Markey’s letter on the dangers of car-hacking, and have each team spend six months collecting information about the level of risk for a given company’s vehicles and assessing the company’s current methods of defending against cyberthreats. After comparing these existing methods to those used in more highly cybersecure fields, each group would generate a detailed report specific to their assigned company recommending concrete, cost-effective, and easy-to-implement strategies for improving software security testing practices. One element key to the effectiveness of this research approach is the use of unaffiliated third-party analysts who, unlike company-hired security specialists, are not primarily motivated by minimizing production time and maximizing profits. Another important aspect of the proposed research methodology is the extended length of the study: by deeply investigating each company's design and production practices over the span of many months, the security experts would be equipped to propose software testing solutions that could be incorporated into a particular company's design process at every stage. Perhaps even more important than these general guidelines, however, are the specific questions and methods used by each investigation group to collect this data on difficult to quantify concepts like factor of risk and level of security.

In order to make recommendations tailored to the needs of particular automakers, each of the security research groups must begin by developing a quantitative understanding of the potential vulnerabilities associated with a given company's vehicles. A critical piece of data collected in this stage of research would be an enumeration of the ECU's contained within each vehicle, classified by factors such as capability of connecting to external data networks, level of access to sensitive user information, and ability to control physical functionality of the automobile. This information would be supplemented by the creation of a diagram for each vehicle's network architecture, which is essentially a detailed map of the physical and telecommunications connections which comprise an electronic system's framework (Fig 1). With this type of data in hand, the security specialists would begin investigating the company's existing software testing procedures: they would collect data such as the types of tests currently performed, the number of employees directly involved with each testing initiative, the amount of time spent testing each element of the electronic control system, and the frequency with which testing is performed. Finally, the cybersecurity analysts would combine this company-specific information with their expertise in the broader world of computer security: utilizing their knowledge of software testing procedures in fields highly concerned with computer security, such as aerospace/aviation, national intelligence, and banking, each analyst would develop a set of specific recommendations for how their assigned company should alter its existing practices to incorporate rigorous cybersecurity testing. This final report would include a detailed summary of the costs associated with the proposed changes, providing concrete statistics like the estimated number of new employees to be hired and the projected amount of revenue lost during prolonged testing periods. Ultimately these findings would be disclosed to the relevant executive entities at each of the investigated car companies, with the goal of getting them to implement some or all of the suggested changes by providing a concrete, well-researched, and company-specific plan of action for improved cybersecurity.

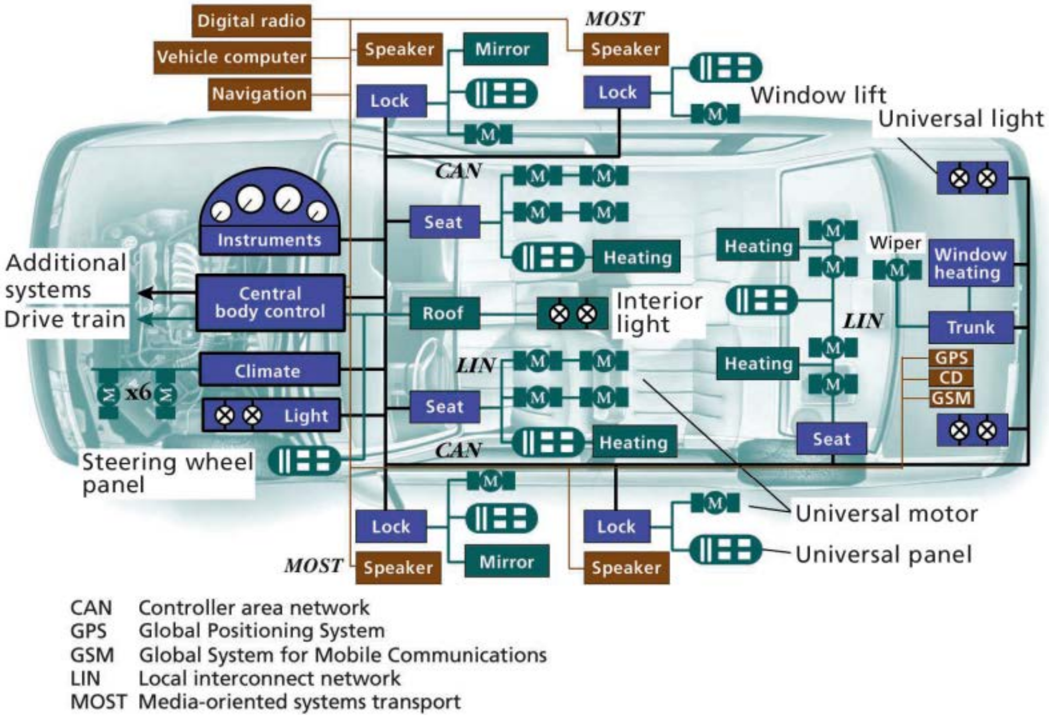

Fig 1: Example of network architecture diagram for an automobile (Source: InTech Open)

Research conducted in the past five years has indicated repeatedly that modern vehicles, no matter what automakers claim, are not safe from the software security risks that affect laptops, smart phones, and other computer-connected technologies. As Joshua Corman, another presenter at the 2015 DEF CON hacking conference, put it: “Modern cars are computers on wheels and are increasingly connected and controlled by software. Unlike your home computer, the consequences of compromise are far more severe.” Herein lies the most critical reason that research into improving the safety of computerized automobile control systems can be delayed no longer: the cost of failing to integrate rigorous software security testing into vehicle development may soon come to be measured not just in loss of stock value and sensitive user information, but also in loss of human life.

Bibliography

Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, and Tadayoshi Kohno. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." Center for Automotive Embedded Systems Security. University of California, San Diego, 11 Aug. 2011. Web. 8 Nov. 2015.

Koscher, Karl, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno. "Experimental Security Analysis of a Modern Automobile." *IEEE Symposium on Security and Privacy* (2010). Web. 8 Nov. 2015.

Miller, Charlie, and Chris Valasek. "Adventures in Automotive Networks and Control Units." DEF CON 21. Las Vegas. 20 Dec. 2013. Web. 27 Nov. 2015.

Miller, Charlie, and Chris Valasek. "Survey of Remote Attack Surfaces." N.p., 6 Aug. 2014. Web. 27 Nov. 2015.

Miller, Charlie, and Chris Valasek. "A Survey of Remove Automotive Attack Surfaces." DEF CON 22. Las Vegas. 6 Jan. 2015. Web. 27 Nov. 2015.

Miller, Charlie, and Chris Valasek. "Remote Exploitation of an Unaltered Passenger Vehicle." DEF CON 23. Las Vegas. 21 Aug. 2015. Web. 27 Nov. 2015.

Greenberg, Andy. "How Hackable is Your Car? Consult This Handy Chart." WIRED 6 Aug. 2014: 17 pars. Web. 27 Nov. 2015.

Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway – With Me in It." WIRED 7 July 2014: 53 pars. Web. 27 Nov. 2015.

Greenberg, Andy. "Here's the Letter a Senator Sent to 20 Auto Makers Demanding Answers on Car Hacking Threats." Forbes 4 Dec 2013: 7 pars. Web. 27 Nov. 2015.

Perlroth, Nicole. "Security Researchers Find a Way to Hack Cars." New York Times 21 July 2015. Web. 27 Nov. 2015.

Perlroth, Nicole, and Mike Isaac. "Uber Hires Two Engineers Who Showed Cars Could be Hacked." New York Times 28 Aug 2015. Web. 27 Nov. 2015.

Paul. "BMW Fixes ConnectedDrive Flaw with Over the Air Patch." Security Ledger 2 Feb 2015: 11 pars. Web. 27 Nov. 2015.

Arkin, Brad, Scott Stender, and Gary McGraw. "Software Penetration Testing.". IEEE Computer Society, Feb. 2005. Web. 27 Nov. 2015. <https://buildsecurityin.us-cert.gov/sites/default/files/bsi6-pentest_0.pdf>.