Comp116 Security Final Project

Buckle Up: Let's be (Car)eful about Security

Erica Schwartz

Advised by
Ming Chow

December 13, 2016

Abstract

Two of the most alarming and well-known vehicle hacks of the past two years were the Jeep hack and the Tesla hack. These hacks were similar in that both involved remotely accessing and controlling the core elements of the car, such as the breaks. One can only imagine the safety implications involved when cars' breaks are vulnerable to remote control; as Charlie Miller, Jeep hacker, aptly put it: "This might be the kind of software bug most likely to kill someone."[7]

The Jeep hack and the Tesla hack differed in the way that the affected car companies responded to them. While the Tesla's vulnerabilities were addressed with a powerful patch within two weeks of their discovery[8], the Jeep Cherokee had to be recalled and the vulnerability was never completely fixed. It has now been over a year since the original Jeep hack, and while Jeep Cherokees are no longer vulnerable to remote control, they are vulnerable to hacks that control the core functionality of the car; hacks that take steering and breaking out of the driver's hands.[9] While the Tesla patch went more smoothly, neither car is completely flaw-free today; Tesla recently underwent another hack that may enable car thieves. Pending legislation to protect us against car hacks like these must hold car companies accountable for producing secure vehicles and punish malicious attackers without deterring white-hat hackers.

Introduction

In this paper, we examine and compare the Jeep hack and the Tesla hack: why they were possible, how they were accomplished, and how the car company responded. In doing so, we suggest how companies might minimize car vulnerabilities, and how to best handle hacks then they do occur. We also examine relevant pending legislation and how it might impact the landscape of vehicle security.

To the Community

As a society, we have a fascination and distrust for high-tech everyday items. We love to imagine the odd inventions that will become commonplace in the future, and technology is fast-approaching the science fiction that both praises it and warns of its dangers. As our cars inevitably grow more computerized, with internet access and even autonomy, will this distrust be validated? Or, will we be able to advance technology in a safe and secure way?

We're seeing the distrust for technology play out in the discussion about the recent Tesla crash. This crash occurred while the car was on autopilot: "Against a bright spring sky, the car's sensors system failed to distinguish a large white 18-wheel truck and trailer crossing the highway."[15] So, many reacted with a confirmed distrust of autonomous cars. This distrust may or may not be rational. On one hand, autopilot is safer than human driving when considering statistics alone: "This is the first known fatality in just over 130 million miles where Autopilot was activated. Among all vehicles in the US, there is a fatality every 94 million miles."[2] On the other hand, it is not a stretch to imagine what could happen if hackers had the power to cause a fatal crash such as this one.

Summary of the Hacks

The Jeep hackers were able to track the location and speed of the car, and take control of the radio, air vents, digital display, windshield wipers, and transmission completely remotely. They were also able to kill the engine, engage and disengage the brakes, and even (in reverse) control steering.[7] In the hands of a malicious individual, the power to control a car remotely to this extent can at best distract the driver and at worst cause a fatal accident. The hackers were able to remotely access these elements of the car because of a vulnerability in the cellular connection of the car's Uconnect system. The Uconnect system "controls the vehicle's entertainment and navigation, enables phone calls, and even offers a Wi-Fi hot spot." Its vulnerability allows anyone who knows the car's IP address to gain access to, track, and control the car.[7]

The Tesla hackers were able to gain remote control of the brakes, the windshield wipers, and the side mirrors, and even popped the trunk while the car was moving. While the car was parked, they could control the sunroof, some of the lights, and the door locks.[13] This hack is almost as severe and comprehensive as the Jeep hack, and had a similar cause; a vulnerability in the car's internet connection allowed attackers to access the critical components of the car. Specifically in the Tesla case, "the vulnerability compromises the CAN bus that controls many vehicle systems in the car. It requires the car to be connected to a malicious wifi hotspot to take control and works via the in-car web browser."[6]

Both the Jeep hack and the Tesla hack involved exploiting a flaw in the cars' remote connections to tamper with their critical components via the CAN bus. This is not a new theme in car security; in 2011, Checkoway et al. found that there are four major types of routes for remote car hacks. These include mechanics' tools, audio devices such as CD players, short-range wireless access such as RFID and Bluetooth, and long-range wireless access such as cellular radio.[3] Once a hacker has gained access to the car's internal network (”CAN bus”) through one of these routes, they can control the entire car.[3] Since remote attacks pose the most real-world risk, we must take all of these ”attack vectors” very seriously.[3]

Companies' Responses

The reports of the Jeep hack led to a recall for 1.4 million cars.[9] This recall involved Jeep owners being sent a USB containing a software update for customers to install themselves.[11] Chrysler's statement in response to the Jeep hacks was one of minimization; they stressed that, ”The software manipulation addressed by this recall required unique and extensive technical knowledge, prolonged physical access to a subject vehicle and extended periods of time to write code,” and even that ”no defect has been found” and ”[Fiat Chrysler Automobiles] is conducting this campaign out of an abundance of caution.”[11] A statement like this one is dangerous because users without much knowledge of security may not think the vulnerability is a big deal, and therefore may not use the USB they were sent to update their vehicles.

The software on the Jeep recall USB stick was intended to resolve the flaw that let hackers access the car remotely.[9] It may well have succeeded in this endeavor. However, some of the issues the Jeep hack brought to light still remain. The original Jeep hackers recently found that ”by sending carefully crafted messages on the vehicle's internal network,” they can ”pull off even more dangerous, unprecedented tricks like causing unintended acceleration and slamming on the car's brakes or turning the vehicle's steering wheel at any speed.” However, they can only do this ”with a laptop directly plugged into the Jeep's CAN network via a port under its dashboard”[9] This is not a remote attack, but it is still an extremely dangerous one.

Tesla responded to their hack swiftly and effectively; a software update was remotely deployed to all vulnerable cars within 10 days of the hack's reporting.[6] This update directly addressed the vulnerability the hack exploited by "adding a measure that requires any new firmware written to components on the CAN bus ... be digitally signed with a cryptographic key only Tesla possesses."[8] In this way, the car's critical components will be protected from the effects of a malicious wifi hotspot. Furthermore, Tesla responded to the hack with a statement that reiterated their commitment to work with researches to enhance their cars' security. In their statement, they said, "We engage with the security research community to test the security of our products so that we can fix potential vulnerabilities before they result in issues for our customers. We commend the research team behind today's demonstration and plan to reward them under our bug bounty program, which was set up to encourage this type of research."[6]

While Tesla's patch was effective, their vehicles are still not impervious to hacks. Recently, researchers were able to, by installing a malicious Android app on a phone which also had the Tesla app installed, use the user's OAuth token (stored in plain text) to find their Tesla and open its doors.[10] The researchers could also delete the user's OAuth token, which would cause the Tesla app to prompt the user for their username and password. These credentials give the attackers the final thing they need to steal the car: the power to drive it.[10] This vulnerability is quite different from the previous one, and depends mostly upon social engineering. However, it suggests that Teslas are still not completely secure.

While Tesla's response to their hack was not perfect, there is something to be learned from their response as opposed to Chrysler's. Tesla did not try to deny their cars' vulnerabilities, and applauded and encouraged the researchers' work through their statement and through their bug bounty program. On the other hand, Chrysler tried to minimize the importance of their vulnerability in order to save face. Companies should work with the security research community, rather than against them, so that their bugs can be found and reported by researchers before they're exploited by malicious hackers. Tesla also was much faster and more thorough with their patch; they were able to quickly fix the vulnerabilities shown in the report and send a patch to all customers. Chrysler was slower in their response, and their patch was not as thorough as it could have been, so this vulnerability continues to haunt them. When a vulnerability is found, it is crucial that the company makes addressing it their number one priority, and ensures that all customers receive and install the patch. While Tesla did a better job at this than Chrysler, no company has perfect security, and Tesla continues to grapple with new vulnerabilities. At this point, it seems like finding and fixing vulnerabilities may remain a losing race between car companies and hackers.

Legislation

If we are to have secure cars, something fundamental must change about the way that car companies approach security. They must be held accountable for prioritizing security rather than treating it as an afterthought. And, lawmakers are currently trying to do just that. The SPY Car Act, introduced in 2015 after the Chrysler hack by senators Markey and Blumenthal, is currently being reviewed by the Senate Committee on Commerce, Science, and Transportation.[1] This bill would not only hold hackers accountable, but also hold car companies accountable for their vehicles' vulnerabilities. It would "set minimum standards and transparency rules to protect the data, security and privacy of drivers in the modern age of increasingly connected vehicles." These standards include that the critical components of the car be properly isolated from the rest of the car, that the car be subject to security evaluations and adjust based on those evaluations, and that precautions are in place to detect and fight hacks as they're happening.[13]

Other pending legislation takes a different approach. Senate bill no. 927, a new bill that just passed the Michigan senate, would make it so that if a car is hacked and that hack results in a death, the parties responsible can be sentenced to life in prison. If it results in "serious impairment of a body function," or if the responsible party has a prior conviction, they can be sentenced to imprisonment for 10 years and/or a 50,000 dollar fine.[12] These punishments are quite harsh, and may inadvertently discourage researchers or white hat hackers from looking into cars' vulnerabilities. This could have unintended and damaging consequences for the ability of car companies to learn of vulnerabilities before malicious hackers do. Furthermore, by outlawing this kind of tinkering, lawmakers may inadvertently create a situation where only black hat hackers fully understand car hacking. Finally, placing the blame of car hacks exclusively on the hackers sends the wrong message; we need to hold car companies accountable for their share of the responsibility for the vulnerabilities in their products.

One currently-active area of car legislation is the push to regulate autonomous cars. The California DMV's autonomous car regulations, currently on its second draft, contains an entire section on "Information Privacy."[4] This section would require that manufacturers either "provide a written disclosure to the operator of an autonomous vehicle that describes the information collected by the autonomous technology that is not necessary for the safe operation of the vehicle," or "anonymize the information that is not necessary for the safe operation of the vehicle."[4] This would encourage carmakers to minimize the information they collect to only the necessary. The US Department of Transportation's Federal Automated Vehicles Policy also addresses autonomous car security. It stresses that car manufacturers prioritize security and document the security measures they take, and that car manufacturers share data on cybersecurity: "Each industry member should not have to experience the same cyber vulnerabilities in order to learn from them."[5] Many of the security and privacy principles we see in autonomous car legislation can (and should) be generalized to other types of car legislation.

Action items

The problem of car hacks cannot be combatted by one entity alone; each of us has a part in addressing this problem as a society.

Software engineers, engineering managers, and product managers at car companies must prioritize security as an essential aspect of all software released to the public. They must recognize the risks associated with all internet-connected devices, especially cars. Systems should be designed so that untrusted websites, wifi hotspots, and applications are kept far from the crucial components of the car; both the Jeep hack and the Tesla hack were made possible by inadequate separation of these components. Customers' privacy must also be prioritized by minimizing the information collected and stored; especially login and location information. Finally, software engineers must think like hackers to consider how social engineering can be used to hack their products and close these loopholes where they exist.

Before software engineers and managers can implement secure systems, university computer science department administrators and educators must prioritize security as a crucial part of computer science and engineering management educations. Car companies must prioritize security at the highest levels, and implement bug bounty programs to encourage their customers to test the security of their products. This will improve the odds that well-meaning hackers find vulnerabilities before malicious ones.

Car companies will likely not change their attitudes towards security on their own. So, lawmakers must pass laws that force car companies to put security first, and must not discourage well-meaning white hat hackers and researchers. The National Highway Traffic Safety Administration could put in place a five-star security rating system, similar to the five-star safety rating system they already use to evaluate cars. Finally, we as citizens and consumers must put pressure on our elected officials to pass these laws, and we must put pressure on car companies to provide us with secure products. The blame for car hacks cannot be solely placed on the shoulders of the software engineer whose code contains a vulnerability; it is up to all of us.

Conclusion

Too often, we see companies only addressing security vulnerabilities as an afterthought, when they're exposed in the media. There is plenty to be learned from how Tesla handled their vulnerability as opposed to how Jeep handled theirs. Tesla was able to send a patch to all clients within ten days of receiving the report and encouraged further research with a financial reward. Jeep, on the other hand, denied the extent of the serious vulnerability and while they did recall their vehicles, many of the original vulnerabilities linger today. However, even Tesla has new vulnerabilities to grapple with. All car companies should be held accountable for their insecure products, and should acknowledge and fix any flaws, ideally before they're released to clients.

We cannot count on bottom-line-driven car companies to do this without any outside incentives; we must enact legislation to force car companies to prioritize privacy and security. As developers, we must keep security as a necessary priority throughout the development process. When vulnerabilities come up, it is important to prioritize fixing them over covering them up. We as a society must not fall victim to security afterthought syndrome, worrying about car security only after a vulnerability leads to a fatal disaster. We should think about security before it's too late; when cars are involved, people's lives may be in danger.

References

1. "114th Congress (2015-2016): SPY Car Act of 2015." Congress.gov. Library of Congress, 21 July 2015. Web. 27 Nov. 2016.

2. "A Tragic Loss." Tesla. Tesla Motors, 30 June 2016. Web. 27 Nov. 2016.

3. Checkoway, Stephen, et al. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." USENIX Security Symposium. 2011.

4. "Deployment of Autonomous Vehicles for Public Operation." California Department of Motor Vehicles. State of California, 19 Oct. 2016. Web. 13 Dec. 2016.

5. "Federal Automated Vehicles Policy." Transportation.gov. U.S. Department of Transportation, 22 Nov. 2016. Web. 13 Dec. 2016.

6. Golson, Jordan. "Car Hackers Demonstrate Wireless Attack on Tesla Model S." The Verge. The Verge, 19 Sept. 2016. Web. 23 Oct. 2016.

7. Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway-With Me in It." Wired.com. Conde Nast Digital, 21 July 2015. Web. 20 Oct. 2016.

8. Greenberg, Andy. "Tesla Responds to Chinese Hack With a Major Security Upgrade." Wired.com. Conde Nast Digital, 27 Sept. 2016. Web. 20 Oct. 2016.

9. Greenberg, Andy. "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse." Wired.com. Conde Nast Digital, 1 Aug. 2016. Web. 20 Oct. 2016.

10. Kumar, Mohit. "Researchers Show How to Steal Tesla Car by Hacking into Owner's Smartphone." The Hacker News. The Hacker News, 26 Nov. 2016. Web. 04 Dec. 2016.

11. Mearian, Lucas. "Update: Chrysler Recalls 1.4M Vehicles after Jeep Hack." Computerworld. Computerworld, 24 July 2015. Web. 20 Oct. 2016.

12. Michigan Legislature. "SENATE BILL NO. 927." Michigan Legislature - Senate Bill 0927 (2016). 20 Oct. 2016. Web. 27 Nov. 2016.

13. Peterson, Andrea. "Researchers Remotely Hack Tesla Model S." Washington Post. The Washington Post, 20 Sept. 2016. Web. 23 Oct. 2016.

14. "Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & 'Cyber Dashboard' Rating System." Senator Ed Markey. Markey.senate.gov, 21 July 2015. Web. 27 Nov. 2016.

15. Yadron, Danny, and Dan Tynan. "Tesla Driver Dies in First Fatal Crash While Using Autopilot Mode." The Guardian. Guardian News and Media, 30 June 2016. Web. 23 Oct. 2016.