The Ethics of Jeep Hack Breaking DMCA While Exposing Security Risks

Kim Arre

CSC 300: Professional Responsibilities

Dr. Clark Turner

November 18, 2015

Abstract

In July 2015 a security researcher named Charlie Miller remotely hacked into a Jeep from 10 miles away, taking over basic physical features of the car including turning on the windshield wipers, steering the car and disabling control of the transmission.[20] In doing so, he defeated Jeep's Technological Protection Measures (TPM). Miller did so to prove that car manufacturers weren't producing "unhackable" cars.[3] Was it ethical for Miller to defeat TPM in order to unveil a major security vulnerability in Jeep cars? Some contend that in order to maintain the integrity of car manufacturer's market interests, the TPM should have been respected and left alone. However, without circumventing the car's TPM, 1.4 million cars wouldn't have been recalled for the security risk.[19] The Software Engineering Code of Ethics sections 6.08 and 6.06 prove that although Miller defeated TPM, he acted in the public interest and therefore acted ethically by releasing sensitive information about security flaws in Jeeps.[31]

Contents

1 Facts

In July 2015, well known security researcher Charlie Miller and his research partner Chris Valasek successfully took remote control of an unaltered Jeep from miles away. [20]

Dr. Miller's security background includes work with the National Security Agency (NSA), as well as Twitter. [25] His research on automotive security began in 2013 when he showed that with direct access to a vehicle, he could control the physical systems of a 2010 Ford Escape and Toyota Prius. [26] After Miller unveiled his findings, Toyota released a statement that the attacks were only possible because they had physical access to the vehicles and that "[their] focus, and that of the entire auto industry, is to prevent hacking from a remote wireless device outside of the vehicle." [18]

The Uconnect system allows drivers to use their smartphones to control physical functions of the car, such as locking and unlocking doors, forwarding a GPS location to the navigation system, and starting the engine.[4]

When the automotive industry dismissed Miller after he displayed the possible threats, he followed up with further research. He was able to acheive control of an unaltered Jeep remotely from 10 miles away by taking advantage of the car's Uconnect system. [26]

By taking advantage of the Uconnect system, Miller and Valasek demonstrated remote use of the Jeep's windshield wipers, sound system, steering, and transmission. [20] The hack went viral after Miller demonstrated it to Andy Greenberg of Wired, who wrote a detailed article that was shared on Facebook over 200,000 times.[20]

Although this was a major breakthrough, Miller and Valasek's confession of hacking into cars to do automotive security research left them susceptible to legal action by Jeep, including both fines and a felony charge. [14] Although the author can find no reports of Jeep prosecuting under the law, Miller and Valasek defeated Jeep's Technological Protection Measures (TPMs) in order to determine the vulnerability, which is illegal under The Digital Millennium Copyright Act (DMCA).[1]

Only days after Greenberg's article was published on Wired, Miller's research on the topic resulted in the recall of 1.4 million Jeep, Dodge, Ram, Fiat, and Chrysler vehicles.[29]

2 Research question

Was it ethical of Charlie Miller to defeat Jeep's TPMs in order to unveil a major security vulnerability?

3 Social Implications

TPMs are widely criticized for making software secure through obscurity.[27] The general logic is that it is illegal to bypass well written and obscure software security locks. If it is illegal it doesn't matter what software lies beyond, since people won't be able to view it. The software is the company's property and no one else is allowed to reverse engineer TPMs for any reason, including life threatening situations.[5] It raises the issue of whether or not property rights should be valued above the public interest.[32]

This also raises social issues for whether or not we should trust car manufacturers. TPMs suppress the general public from figuring out if the product they're selling is safe and fulfills all promises made by the manufacturer. Threatening to punish security researchers who examine product software decreases the likelihood of discovering and fixing security flaws. An example of this risk is the Volkswagen Clean Diesel scandal. Since it was illegal under anti-circumvention law to verify the car's code, the true emission rates weren't realized until physical tests were done several years later.[27]

Additionally, consumers are left susceptible to being taken advantage of by people from foreign countries who aren't required to operate under the same laws as us.[32] The major current events as of this paper's writing are the ISIS terrorist attacks.[8] Specifically, ISIS killed nearly 128 people in shootings and bombings on November 13, 2015.[8] With increasing technological advances it's important to consider the public good with respect to whether our everyday vehicles are subject to hijacking by terrorist organizations such as ISIS. [32]

4 Arguments

4.1 Arguments Affirmative

4.1.1 Discouraging the research of vehicles prevents us from unveiling potential dishonesty from manufacturers

As seen in the recent unveiling of Volkswagen's scandal, physical research was essential for uncovering Volkswagen's dishonesty regarding their Clean Diesel technology. [22] Without this research, we wouldn't have discovered the true emission rates.

Volkswagen went on for years promoting their Clean Diesel technology, with the true emission rates going unnoticed. There's no telling how many other companies – automotive or any other industries – could be doing the same. In order to test the integrity of these products, we need validation of the software it runs on, but the DMCA's section 1201 on anti-circumvention law deters us by making it illegal. Instead, our only legal option is to put our trust in the companies and hope that they're behaving ethically without any definitive evidence. [14]

When manufacturers are dishonest, there's a potential for people to die as a result. In the Volkswagen case, 4000 people may have died from Volkswagen's dishonesty.[16] Had security researchers, such as Charlie Miller, been able to investigate the vehicles freely those deaths could have been avoided.

4.1.2 Manufacturers should be doing more to ensure their vehicles are safe by allowing for more extensive tests

When Toyota made the statement that they weren't concerned with security risks [18] before Miller proved them wrong, it's unclear if they genuinely believed their security was rock solid. There's a possibility that they hadn't done enough testing but assumed that security by obscurity would be enough to protect the internal software from end users[14]. Car manufacturers should follow in the footsteps of Uber who hires researchers like Miller and Valasek to ensure the security of their vehicles[24].

4.2 Arguments Negative

4.2.1 The software TPMs were put in place to protect Jeep's copyright and prevent their code from being stolen or sold to other car manufacturers

In order for vehicle companies to stay competitive with the others in their field, they must use TPMs to ensure that their intellectual property is safe from being stolen or used against them in the market. [27]

Anti-circumvention law promotes creativity by assuring that the creators and copyright holders have control over their intellectual property so that it won't be used in ways that they don't approve of.[27] Ensuring their intellectual property is only accessible by them encourages more creative and innovative products to be created by both the original company, as well as their competitors. [27]

4.2.2 Allowing malicious actors to view or modify software responsible for safe vehicle operation would put public safety at risk.

By circumventing the TPMs of cars, Miller put all cars affected at risk when he published the specifics on how he did it[26] for potential wrong-doers to find. TPMs provide a barrier that deter people who may wish to do harmful things to drivers and their cars. [27]

5 Analysis

5.1 Why the Software Engineering Code of Ethics is applicable to this problem

The Software Engineering Code of Ethics states that software engineers "are those who contribute by direct participation or by ... the analysis ... and testing of software systems."[2] Did Charlie Miller "directly participate" to the analysis of a "software system"?

The definition of "direct" is "without intervening factors or intermediaries."[5] Miller and Valasek published a paper on the specifics of how they hacked the Jeep. [26] Additionally, they gave a talk at the DEF CON 23 Hacking Conference on how they did it. [3] During both, Miller and Valasek took responsibility for the hack by using their own names.[26][3] Since there were no intermediaries between the Jeep car and the security researchers, Miller and Valasek were directly participating.

A "software system" [6] is defined as an "interface between hardware and user applications." [6] The software system applied to this case is the Jeep's Uconnect system, along with the TPMs that prevent the code from being viewed.

"Software testing" is defined as "any activity aimed at evaluating ... capability of a program or system and determining that it meets its required results."[28] A form of software testing is one in which you try to break the existing functionality. [28][30] The existing functionality in this case would be both the Jeep's TPM, as well as the UConnect system that allowed the researchers to gain control.

Therefore, Miller and Valasek directly

tested and broke the Jeep's TPM and UConnect system, which qualifies them as software engineers and "shall adhere to the [Software Engineering] Code of Ethics."[2]

5.2 SE Code sections 6.06

SE Code 6.06 states that software engineers are to **"Obey all laws governing their work, unless in exceptional circumstances, such compliance is inconsistent with the public interest."** [2]

The definition of a "law" is "any written or positive rule or collection of rules prescribed under the authority of the state or nation, as by the people in its constitution."[5] The "laws" being applied to this problem are the DMCA's anti-circumvention law.

The meaning of "work" is "exertion or effort directed to produce or accomplish something" [5]. Charlie Miller made an effort to use his knowledge in security research in order to accomplish finding security vulnerabilities in Jeep cars.[26]

The definition of "exceptional" is "forming an exception or rare instance; unusual." [5] Typically, laws are made to protect the people under which they govern. Therefore, an example of an "unusual" circumstance would be when the law endangers the people it governs.

Public Interest

"Public interest" is defined as "the welfare or well-being of the general public."[5] Further, "public" is defined as "affecting a population or a community as a whole."[5] In this case, the affected community consists of anyone who interacts with vehicles on the road. This includes drivers, pedestrians, and insurance companies. Their well-being may be defined as their safety in terms of money, property, and health.

The driving community must consider the well-being of people who don't drive. Pedestrians' lives can can be gravely affected by cars each time they cross a street or crosswalk.

Drivers most immediately interact with motor vehicles. Their well-being depends on keeping their life, personal property, and passengers safe. "While health and wellbeing is important in every part of lifes activities, driving may be considered an extreme activity that depends on the awareness and performance of the driver."[23] Drivers' actions while operating a car can have fatal effects, such as death or psychological damage.

Lastly, the well-being of car insurance companies are affected by hacked cars as well. Every car on the road is required to have insurance by law,[9] so any incident that occurs will affect an insurance company financially. Not only does this include property damage of the car, but life threatening circumstances as well. "Liability insurance ... is almost always mandatory because it helps protect other people and their property."[9] When cars are compromised on the road, insurance companies need to pay out for damages, making it their interest for cars to be as safe as possible.

5.2.1 Substituted Code 6.06: Charlie Miller should obey the DMCA's anti-circumvention law while doing security research on Jeep cars, unless such law threatens the well-being of drivers, pedestrians, or insurance companies.

Obeying Anti-circumvention law

In order for Charlie Miller to uncover the security vulnerabilities, he needed to bypass the car's TPMs. [14] The Anti-Circumvention law, Section 1201(a.1.A) of the DMCA, states: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[1]

The articles on Miller's demonstration refer to it as a Jeep "hack", but what does this word actually mean? The definition of "hack" is to "use a computer to gain unauthorized access to data in a system."[5] Unauthorized access is considered not having official permission or approval. [5] Presence of the Jeep's TPM indicates that he did not have permission or approval to view the vehicle's code.

Therefore, the only way he could have control of a Jeep system was by defeating the TPMs to gain unauthorized access to the Jeep car, which was not legal under Anti-Circumvention Law.[1]

Now that we've determined that Charlie Miller did not obey the law, the only way his actions were ethical under this code was if he was acting consistently with the community's well-being.

Public Well-Being

Charlie Miller had an ethical obligation to base his actions on the well-being of the community. [2] The well-being of a community is based on their health, property, and money.

Pedestrians

Pedestrians' well-being is threatened when their lives are at risk of being hit by a compromised vehicle. Research shows that if a car is traveling at 40 miles per hour and hits a pedestrian, it has a 90% chance of killing them.[7] A compromised car has the potential to take the lives of pedestrians when the driver no longer has the ability to keep them safe from harm.

A more extreme example of an attack would be public figures and other influential leaders. In an interview, Valasek suggested that "it's not too early for national leaders and others who might face targeted attacks to think about the security risks of their car's technological features."[15]

Drivers

Drivers are concerned about attacks in the form of having their vehicle taken over during operation. [26] The worst consequences of which would be a fatal collision that results from a hijack.

The demonstration of the Jeep hack was a very controlled example of how the driver could be affected by someone taking over any feature of the car. However, even such a controlled experiment had its risks. When Miller and Valasek took over functions of the car that were considered to be less dangerous, such as windshield wipers and fluid, the driver of the demonstration couldn't see and was still fearful of his surroundings.[21][20]

Car accidents can cause psychological damage to drivers as well, which affect their well-being. Drivers may experience post-traumatic stress disorder and experience high amounts of anxiety and stress.[12] This takes a direct toll on their health, or well-being.

Insurance Companies

Both drivers and insurance companies must consider an attack in the form of stealing. Cars aren't only vulnerable while they're in use. If not secure, they can be taken advantage of by remotely unlocking the doors and starting the engine. [15]

Additionally, insurance gets complicated for the case of a hacked vehicle. Who is at fault for the actions of a compromised vehicle? The driver who's the usual operator of the car? The manufacturer for producing a car with security vulnerabilities? The hacker? How do you know who the hacker is, or even prove that the car was hacked? [11] In order for insurance companies to accommodate such complications, insurance costs go up, which affect both the driver and the insurance company. [32]

Now that we've established who the public interest is, we need to determine if the threat to the public well-being was worth breaking the law.

Should Charlie Miller obey the DMCA's anti-circumvention law?

It's sometimes hard to tell if a manufacturer is being trustworthy when they're so secretive of what lies beyond the TPMs. In an interview, Valasek stated "Car manufacturers generally say little about what they are doing to mitigate the risks of systems."[15]

"The problem is, people want to get their technology out there really quick, so you dont have programmers sitting there looking at everything line by line to make sure that everything is secure."[17]

Unfortunately, it's easier for car manufacturers to put a security lock on their software than it is to thoroughly test to eliminate as many vulnerabilities as possible. [27] However, security through obscurity can only be so secure.[27] It's often prevalent for companies to weigh the financial costs of allowing people to die versus testing and better securing their software. [32] Often times, it turns out that it's cheaper for them to ignore the problems and let people die, which is a direct influence on the public's well-being. [32]

Charlie Miller's discovery of the vulnerability may have saved pedestrians their lives, drivers their property and mental health, and insurance companies money. Fortunately, we won't know how many peoples' well-being would have been negatively affected by the vulnerability since it resulted in the recall of all the affected vehicles. [19] Jeep, Chrysler, Dodge, and Ram cars and their drivers are more secure because of his discovery. [19]

Discussion Summary

The problem of compromised cars opens up a plethora of complications for insurance and risks for the lives of pedestrians and drivers involved. When anti-circumvention law prevents security researchers from discovering vulnerabilities, car manufacturers often aren't doing all they can to be sure their systems are as safe as possible. [15]

Although Charlie Miller violated anti-circumvention law, by uncovering a major security vulnerability, he protected the public's well-being in terms of health, money and property. Charlie Miller's action was consistent with the well-being of drivers, pedestrians and insurance companies, and therefore ethical under SE Code 6.06.

SE Code 6.06: Laws vs. Public Interest
Charlie Miller: Ethical

5.3 SE Code section 6.08

Section 6.08 of the SE Code states the Software Engineers shall **"take responsibility for detecting, correcting, and reporting errors in software ... on which they work."**[2]

The definition of "responsibility" is "the state ... of being responsible, answerable, or accountable for something within one's power ..."[5]

"To detect" means "to discover the existence of"[5], or find.

"Reporting" is described as "an account or statement describing in detail an event."[5]

"Errors in software" when applied to this problem correspond to the security vulnerabilities that existed in Jeep cars.

Vulnerabilities are defined as "flaws in computer software that create weaknesses in the overall security of the computer or network."[13] By this definition, a TPM itself can be considered a security vulnerability.

5.3.1 Substituted code 6.08: Charlie Miller should be held accountable for discovering security vulnerabilities in Jeep vehicles and describing them in detail.

In order to evaluate if Charlie Miller was acting ethically under SE code 6.08, we must analyze three parts of the substituted code. These parts include whether or not Charlie Miller was considered accountable, whether or not there were security vulnerabilities, and whether or not he described such vulnerabilities in detail.

Accountability

In this case, being "accountable" means to spot a problem and take action if it's within your power.[32]

Charlie Miller has extensive knowledge and history with software security systems. This is illustrated by his former experience with the NSA and Twitter[25] as proof that security research is well 'within his power.'

Miller dedicated months of research on detecting security vulnerabilities with Jeep, Ford and Toyota vehicles.[26]

Because of these reasons, Miller is considered accountable for finding the security flaws because he has the knowledge in security research that the common public doesn't.

Security vulnerabilities

Jeep's TPMs made it difficult to determine the presence of security vulnerabilities in software since they often operate under conditions of security through obscurity. [27] If we're not allowed to examine the code, how do we know if the product really is safe?

In an interview, Charlie Miller believes we should never consider software completely "unhackable."[10][3] "Most complex systems tend to have errors because as humans we are not that great at writing secure code." [10]. Part of the reason for this is because it's impossible to account for every possible case, or test for absolutely everything. [32] Therefore, all software must contain vulnerabilities in some way.

If manufacturers use TPMs as an attempt to hide all of the other security risks, it makes it easier for malicious hackers to take advantage of the system. When TPMs are too heavily relied on, manufacturers are less likely to put effort into ensuring the rest of the software is secure. [32] It's easier for malicious hackers to figure out one puzzle in order to access everything, as opposed to many smaller puzzles throughout the software. Therefore, TPMs promote weaknesses in the overall security of the Jeep.

Describing in detail

The definition of "describe" is "to tell or depict in written or spoken words."[5] Applied to this case, Charlie Miller depicted in written words by publishing a paper on the details of the background and specifics of what the vulnerability was and how he took advantage of it. [26]

He depicted using spoken words when he gave a talk about the hack at the DEFCON 23 Hacking Conference which is still publicly available on YouTube. [3] Additionally, his demonstration of the hack on Wired is an example of both written and spoken words.[20]

Miller made multiple attempts to describe the vulnerabilities in detail. This specific hack wasn't the first he had done, but it was the one that manufacturers took seriously. [19] On multiple occasions before, Miller tried to spread awareness in car manufacturers about vulnerabilities in their products but each time manufacturers were able to come up with an excuse to dismiss it.[26] However, each time, Miller properly documented the vulnerabilities.

He reported these errors both to the public and to the car manufacturers themselves so the problems could be remedied, eventually resulting in a Jeep recall of the vehicles to be updated with a security patch.[19] Therefore, he effectively described the problem in detail.

Discussion Summary

Charlie Miller is accountable for discovering security vulnerabilities because of his extensive background in security research.[25] He effectively described in detail when he published a paper and gave a conference talk on the hack.[3] There will always be security vulnerabilities in software because it's impossible to test absolutely everything. [32]

Because these three factors are present, Charlie Miller was acting ethically under SE Code section 6.08.

SE Code 6.06: Detect, correct, report
Charlie Miller: Ethical

5.4 SE Code 2.05

SE Code section 2.05 states that software engineers are to **"Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law."**[2]

"Confidential" means to speak or write about something only in strict privacy or secrecy.[5]

"Private" is defined as "confined to or intended only for the persons immediately concerned."[5] Therefore keeping something "private" would be to not share any of the information gained in researching the vehicles to anyone who doesn't need to be involved. In this case, only the car manufacturer should be involved since their cars and customers are affected.

"Professional work" is "a vocation requiring knowledge of some department of learning or science"[5]. The department of science that Charlie Miller has knowledge in is the field of computer security research.

As explained in section 5.2, the public interest is the well-being of drivers, pedestrians, and insurance companies.

5.4.1 Substituted Code: Charlie Miller should only publicly speak, write, or share any information gained from security research on the Jeep car, if it is consistent with the well-being of drivers, pedestrians, and insurance companies.

After their discovery of the vulnerability, on August 10, 2015, Miller and Valasek published a paper titled "Remote Exploitation of an Unaltered Vehicle."[26] This paper outlined the more in depth details of how they managed to bypass the car's TPMs. By providing this information to the public, some Jeep owners were likely left vulnerable, as we will further discuss.

The Jeep hack demonstration happened roughly July 21, 2015[20] and Jeep recalled their affected vehicles only days later.[19] Although Miller and Valasek's official paper wasn't published until a month after the recall, it's very unlikely that every single car on the road who was vulnerable to the security risk reported back to Jeep to have it fixed.

By providing the specifics of the hack, it allowed people to try it on any car they found that wasn't updated, potentially harming drivers, pedestrians, and insurance companies.

The DMCA's anti-circumvention law protects against cases like this by making it illegal to bypass TPMs in the first place.[1] By outlawing this behavior, they can be sure nobody may legally hack into their vehicles, for good or for bad. If nobody finds a vulnerability to exploit, nobody is at risk of being hacked.[27]

SE Code 6.06: Keep private
Charlie Miller: Unethical

6 Conclusion

Yes, Charlie Miller was behaving ethically when he defeated the Jeep's TPM in order to unveil a major security vulnerability. Overall, Miller acted in the interest of the driving community.

Although he violated the anti-circumvention law, he was still acting in the overall interest of the public's well-being. He fulfilled his obligation as a software engineer to detect, correct, and report any flaws in Jeep's security system. The risk that resulted from publishing his findings had far less consequences than if he hadn't found the vulnerability. Additionally, the potential damage that could have resulted to drivers, pedestrians and insurance companies in terms of health, property and money far outweighed the competition concerns of Jeep.

Update on DMCA

As of October 2015, the US Copyright Office added exemptions to Section 1201 of the DMCA. [33]

"Under the new ruling, researchers will finally be able to investigate the software in vehicles for flaws and security vulnerabilities. ... The new ruling will make it easier for researchers to blow the whistle on manufacturers who are programming their vehicles to cheat." [33]

However, the exemptions are only valid for three years, meaning that they must go under review again after that time is up. [33] Additionally, the new laws don't go into effect until a year from when they were first granted. [33]

References

[1] "Copyright law of the united states of america; circumvention of protection systems." [Online]. Available: http://www.copyright.gov/title17/92chap12.html#1201

States the laws of DMCA regarding Anti-Circumvention rules.

[2] "Software engineering code of ethics." [Online]. Available: http://www.acm.org/about/se-code

The Software Engineering Code of Ethics is the basis of my analysis of Miller's actions.

[3] (2015, August). [Online]. Available: https://www.youtube.com/watch?v=OobLb1McxnI

This is the video of Miller and Valasek's DEF CON talk on hacking the Jeep.

[4] (2015, November). [Online]. Available: http://www.driveuconnect.com/features/uconnect_access/

This is the advertising site for the Uconnect system that was hacked into and made the Jeep hack possible.

[5] (2015, October). [Online]. Available: http://dictionary.reference.com/

This is the online dictionary reference used to define terms in the SE Code tenets.

[6] (2015, November). [Online]. Available: http://whatis.techtarget.com/definition/system-software

This offered a good definition of a software system

[7] (2015, November). [Online]. Available: http://www.safespeed.org.uk/killspeed.html

This page illustrates with graphs how fast a car needs to be going and how fatal the hit is at each speed.

[8] S. Almasy, P. Meilhan, and J. Bittermann, "Paris massacre: At least 128 killed in gunfire and blasts, french officials say," November 2015. [Online]. Available: http://www.cnn.com/2015/11/13/world/paris-shooting/

Describes the happenings of the ISIS terrorist attack in Paris

[9] J. Anish, "Why is car insurance mandatory?" January 2012. [Online]. Available: https://coverhound.com/blog/post/why-is-car-insurance-mandatory

This article discusses why car insurance is mandatory and points out that everyone in the US (not counting New Hampshire at the time of writing) requires insurance.

[10] d. . . y. . . u. . h. a. . T. Ayesha Salim, month = July, "Jeep hacker warns auto makers over unhackable claims."

[11] A. Buss, November 2015.

Alanna was the TA for the class and provided many pointers for how to form arguments in my SE code analysis.

[12] D. J. Butler. (1999, August) Post-traumatic stress reactions following motor vehicle accidents. [Online]. Available: http://www.aafp.org/afp/1999/0801/p524.html

This article illustrates the risks people have for trauma after car accidents

[13] N. by Symantec. (2015, November) Vulnerabilities. [Online]. Available: http://us.norton.com/security_response/vulnerabilities.jsp

Provides a good definition of 'vulnerability'

[14] R. Chirgwin, July 2015. [Online]. Available: http://www.theregister.co.uk/2015/07/23/jeep_hackers_broke_dmca_says_eff/

Describes how the Jeep hacking broke DMCA and why the author and EFF believe it shouldn't have.

[15] E. Chung, "Carmakers ignore hacking risk, security expert says," October 2014. [Online]. Available: http://www.cbc.ca/news/technology/carmakers-ignore-hacking-risk-security-expert-says-1.2810847

This article has really good information on immediate examples of risks the public faces when manufacturers ignore security risks.

[16] K. Drum. (2015, September). [Online]. Available: http://www.motherjones.com/kevin-drum/2015/09/spreadsheet-day-how-many-people-did-vw-kill

This article illustrates how many potential deaths resulted from the VW scandal.

[17] G. Garcia and R. Lehmann, "Will self-driving cars need hacker insurance?" May 2015. [Online]. Available: http://www.hopesandfears.com/hopes/now/question/213715-will-self-driving-cars-need-hacker-insurance

This was an incredible resource for considering insurance interests in terms of hacked and self-driving cars.

[18] A. Greenberg, “Hackers reveal nasty new car attacks–with me behind the wheel (video),” July 2013. [Online]. Available: http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

This is the original article from their first hack in 2013, the one that car manufacturers dismissed because they had physical access to the car.

[19] ——, July 2015. [Online]. Available: http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

Discusses the results of the remote Jeep hack; 1.4 million vehicles recalled.

[20] ——, “Hackers remotely kill a jeep on the highway - with me in it,” July 2015. [Online]. Available: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

This was the earliest resource I could find on the Jeep hacking and appears to be how Miller and Valasek unveiled their findings.

[21] K. Hill, “Wireds highway jeep-hacking stunt was an amazing story, but a terrible idea,” July 2015. [Online]. Available: http://fusion.net/story/170662/dangerous-jeep-hack/

Hill explains how dangerous the Jeep demonstration was since they were on a freeway with no shoulder.

[22] R. Hotten, September 2015. [Online]. Available: http://www.bbc.com/news/business-34324772

Summarizes the Volkswagen Scandal in which they faked their emission tests for their Clean Diesel technology.

[23] B. R. . B. M. Joseph F. Coughlin, “Driver wellness, safety & the development of an awarecar,” December 2009.

This article touches on the subject of what a driver’s well-being requires

[24] J. Menn, August 2015. [Online]. Available: http://www.reuters.com/article/2015/08/28/us-uber-tech-security-idUSKCN0QX2BQ20150828

News that after the Jeep hack, Uber hired Miller and Valasek to work on security research for their company

[25] C. Miller. (2015, October). [Online]. Available: https://www.linkedin.com/pub/charlie-miller/1/433/260

This is Charlie Miller’s LinkedIn profile which lists all of his former and current employers as well as skills and education.

[26] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” August 2015. [Online]. Available: http://illmatics.com/Remote%20Car%20Hacking.pdf

This is the official paper written by the two hackers on the details of how they did it.

[27] C. Opperwall, October 2015.

This was an interview with Chris Opperwall, who discussed with me the importance and reasoning behind corporations who like the anti-circumvention law.

[28] J. Pan, “Software testing,” Spring 1999. [Online]. Available: http://users.ece.cmu.edu/~koopman/des_s99/sw_testing/

This is a webpage from a professor from Carnegie Mellon who covers the ideals of Software Testing in depth.

[29] A. Press. (2015, July) Fiat chrysler recalls 1.4m vehicles in wake of jeep hacking revelation. [Online]. Available: http://www.theguardian.com/business/2015/jul/24/fiat-chrysler-recall-jeep-hacking

[30] Sifter, “Perfect your testing strategy,” November 2015. [Online]. Available: https://sifterapp.com/academy/essays/testing-strategy/

This source is a good resource for a method of testing that uses phrasing about ”breaking” things

[31] M. Stevenson, November 2015.

Mason was my partner for the peer review lab done in Dr. Turner’s class. He offered many helpful pointers which I used in my paper.

[32] D. C. Turner, October 2015.

This source refers to things Dr. Turner says in class, usually related to the DMCA.

[33] K. Wiens, “We won exemptions for repairing tractors, cars, and tablets,” October 2015. [Online]. Available: http://ifixit.org/blog/7475/repair-coalition-wins-exemptions/

Discusses the new DMCA exemptions that are now active.