A Diamond in the Rough

Taylor Broach

East Carolina University

Abstract:

Auto markets today are flooded with new cars equipped with features harnessing cutting edge technology. Tesla Motors leads this wave of technologically advanced cars; however, their cars not only boast the best features but they offer security in their products like none other. Many other auto makers have joined the smart car revolution and displayed various attempts at a marriage of technology and the driver. Jeep has struggled greatly with their vehicle intelligence features because they have been shown to have various security vulnerabilities and dangers. Tesla offers a refined, secure and reasonably priced electric platform for drivers to feel safe carrying their families in.

Keywords: Tesla Motors, Jeep, hacking, auto market, technology, cars, electric cars, safety

A Diamond in the Rough

Information Security is the protection of data against the dangers of unauthorized access. One of these dangers lies within the world's largest and most innovative advancements, the automobile. Tesla has recently created a new genre of vehicles, electric smart-cars. As the industry begins to adopt these new electric cars people are beginning to witness "…a new age of motor vehicles…" (McCarthy, 2013). Even so Tesla's vehicles are not the only smart cars on the market. A new 2015 Jeep Cherokee was remotely hacked and then hijacked through its smart system called Uconnect. This hack was achieved by a pair of technicians sitting on a couch over 10 miles away (Greenberg, 2015). Technology is remarkably vital in people's lives today, so much so that the impending dangers have become trivial. A vulnerability in a trusted and largely established name in the auto industry, like Jeep, is not only startling to the owner; it begs the question of if this could happen to one's own vehicle. Although, among this strife there is one company, Tesla Motors, who presents itself above the rest alleviating the valid concerns surrounding this new concept. Tesla takes security personally with their products by incorporating security, protection, and responsibility into the vehicle's mechanical and technical core. As security is consistently pushed in technology, the risks have been acknowledged and conquered by Tesla through their commitment to their vehicle's security and technological advances.

Car Security

With the new age of cars comes more than just security; the industry is seemingly in the midst of the eradication of the combustion engine. When looking towards the future of modern vehicles, information safety is the number one revolution taking place, especially

within electric vehicles. This evolution in information security is the most prevalent change, but while looking even closer, one can find other major benefits as well. Tesla's "intelligent" or "smart" vehicles, have information systems capable of seamless smart phone integration, blind spot detection, and also intelligent braking. One may recognize these features because they are not Tesla exclusive. Where Tesla begins to raise the modern vehicle standards is with their features such as "Autosteer, Lane Change, Autopark, and Summon" (Tesla, 2016). The two features with the highest risks are Autosteer and Summon. Autosteer keeps the car in its lane at speed, as long as the car can detect the road lines. This feature is mostly used on the highways for reasons of the longer roads and lack of sharp turns. Summon on the other hand, is a feature in which the car can be told to back out of either a garage or a parking spot for a distance up to 39 feet (Gitien, 2016). Tesla truly has developed software like no other, but it is how the software is implemented that makes the difference. Due to the sophistication of these features and the potential mayhem that could occur if these systems were hijacked, security protection is requisite.

Feature Security

Tesla has topped the charts with their incredible software advancements, but it is their overall security that is an even greater achievement. When software is created, there are many components that come together to make a whole. Like most cars, in any Tesla there is a local network spread through the car, this network is called the controller area network or CAN (Gandini & Anzoino, 2010). This specific network is compromised of each and every part of the car and the CAN is both the connection and protection between the cars software and hardware. The instruction of any program is the primary goal, however, often times the more

crucial objective is the security of that program. If in some way the central area network is compromised and new malicious hardware introduced to the network, that malicious hardware could force the software to send its instructions to it instead of the rest of the car. If this interruption were to happen, the car would not only lose connectivity, but the new malicious hardware could start sending out its own instructions, acting as the new software. In turn this new malicious hardware would cause major issues unless preventative measures were taken to avoid such an attack.

Tesla has addressed security very differently then automakers in the past, instead of a total lock down of the car, certain unimportant features are intentionally left unprotected. This surprisingly does not make the car susceptible to a breach in security. Instead, it focuses the car's resources on functions of high importance such a power regulation, steering sensitivity, surrounding sensors, and other crucial processes to get the car rolling safely. Once the car tops five miles per hour, the unprotected and nonessential features are then resecured; the cars computer resources are distributed back among the cars processes accordingly using the controller area network or CAN. Tesla is incredibly confident in their systems security, yet even so they have built in several components in case of an emergency. In a very intelligent way, protocols are in place to ward off phony or trick commands inside their software (Ward, 2015). Also if the car was to lose power or stop for any reason, there is a small power supply that would allow the car to gently stop while allowing the driver full control of the steering wheel until the car comes to a complete stop. This gentle stop along with the many other security features all combine resulting in the most secure automobile platform in the industry.

Importance of Security

Security plays a major role in all aspects of the world, especially in human life. The internet of things or IoT, is a component that joins many of these aspects together. "In the IoT, environmental and daily life items, also named "things", "objects", or "machines" are enhanced with computing and communication technology and join the communication framework" (Chaouchi, 2013). The IoT is one of the largest growing security risks todays because it is ever expanding and involves so many pieces of technology, smart cars included. An intelligent Jeep Cherokee was recently exploited revealing a number of severe security inconstancies within its CAN system. The primary entertainment and control system in all new 2015 Jeeps is called Uconnect. This system runs off of Sprint cell towers to allow constant internet access for both the car and the user. Recently an article, from Wired Magazine followed two men, Charlie Miller and Chris Valasek, who demonstrated the vulnerability they found in this system (Greenberg, 2015). Miller, a security researcher for Twitter, and Valasek, former NSA hacker, were able to modify how the Jeeps phone application connected to the Jeep. With this tweak they could see all other vehicles using the Uconnect system anywhere in the US. "Seeing the actual, mapped locations of these unwitting strangers' vehicles—and knowing that each one is vulnerable to their remote attack…" wrote Andy Greenberg in the Wired article (2015). The phone was then converted to a hotspot and using Sprint mobile connection to the Uconnect the Jeep's location was pin pointed and the team was able to log into the Jeep. Access was gained into the Jeep's CAN using the assigned IP address (Greenberg, 2015) of the exploited network port. Once inside the system, the flaws are based on the lack of protection against any sort of man in the middle attack or MiTH.

The information security world is familiar with these sort of attacks within regular networks, however in this case the network was the vehicle's CAN. If a MiTM attack was deployed it could poison the CAN's ARP table which in part is how the software commands are manipulated and then spoofed (Agarwal, Biswas, & Nandi, 2015). As the commands from the main computer in the car are transmitted, they are intercepted by the MiTM attack. The MiTM then generates its own bogus commands, which are then sent in place of the originals. Using the bogus commands, Miller and Valasek's attack granted them not only access to technical systems of the car but also physical control, allowing them to manipulate the engine, braking, lights and various other elements (Greenberg, 2015). With Miller and Valasek's findings, this vulnerability within Uconnect shows just how far beyond information security that hacking has gone.

A Lack of Protection

History has repeated itself through the Jeep, and habits have been broken with Tesla. The Ford Pinto was the start of a revolution in 1970 for reasons both good and bad. The Pinot was quickly nicknamed, a firetrap, due to a major defect in the gas tank that could result in a rupture if rear ended at a fairly low speed (Lee, 1998). Even with this defect, the well know the car was still produced and sold even though the fix would have cost only 11 dollars per Pinto (Lee, 1998). As the vehicle industry enters the most recent revolution, the 2015 Jeep Cherokee resulted in major security flaws with Jeeps Uconnect system. This technical vulnerably was announced to Fiat Chrysler resulting in a recall of almost 1.5 million vehicles (Ward, 2015). The Jeep Cherokee plays the role of Tesla's foil character as it's downfall of the Uconnect system is an undeniable security risk. If Fiat Chrysler had not recalled those vehicles to install a software

patch supposedly fixing the vulnerability it was likely issues of severity could have followed, as they did with the Pinto. With all these faults and failures in other vehicles, Tesla and its features have continued to stay safe and secure.

Protection Breakthrough: Tesla

Tesla has prevailed through many security issues where as other comparable vehicles have not. Nevertheless, this does not mean Tesla has been perfect. Very few attacks have proven successful other then one which forced the Tesla to stop and shut off briefly (Kovacs, 2015). Since this vulnerability was announced, Tesla released an over the air or OTA update, to patch the car within a week (Kovacs, 2015). All Tesla's can receive OTA updates regularly to keep up with security and features updates. This attack was preformed on the Tesla by Marc Rogers from web security provider Cloudflare and Kevin Mahaffey from Lookout the phone security application (Kovacs, 2015). The work around was only achieved because the attackers were physically connected into the Tesla's CAN system, but even when the car was shut down it did so gracefully and slowly with the driver still in total control of the steering. The reason this graceful shut down is so important is when any of a vehicles systems fail or shut off the car is reactive to that failure. On the other hand, Tesla's systems are proactive for regarding failures. If a Tesla system were to fail, the car would simply glide to a stop and not be a safety risk.

In a statement made to BBC, Tesla stated, "Our well-developed safeguards protect every layer of our vehicle and network security system, including for the mobile app, Tesla's servers, and the car itself. "(Ward, 2015). Tesla has received many accolades for their past and on going security work to make their cars and software the safest and most secure available. Hackers look for ways to compromise anything through any means possible; data is stored many places

in technology and there are often times there are many ways to get to that information. Tesla actively keeps attackers guessing by cycling all onboard passwords every 24 hours; systems are also kept secure by using a virtual private network or VPN to connect directly back to Tesla's servers keeping data streams encrypted (Kovacs, 2015). The largest security standard for all Tesla's models is that the infotainment system is set apart from the CAN of the the car (Kovacs, 2015). This means that unlike Jeep, the critical systems of the car are not directly tied into internet connected systems of the car. Whether through a specific system or the car in general, Tesla has managed to secure their vehicles and systems to the best of their abilities.

Since the creation of the automobile human life has not been the same; the need for quick effective and efficient transportation has become a necessity rather then a luxury. When there is a necessity there is a demand; to keep up with that demand the auto industry is continually creating vehicles offering new options and technical features. Among all the technical growth in the auto industry, Tesla Motors is the company making great strides in the electric car arena, producing the most secure and advanced vehicle on the road. Tesla is not the only company trying to introduce smarter cars; Jeep has started to equip their vehicles with a smart system call Uconnect. Unfortunately, this Uconnect system is poorly secured, creating major safety problems as physical control was granted to a group of hackers once they successfully deployed their exploit. This vulnerability found in Jeeps goes up and beyond any information security risk, this is about the safety of motor vehicle transportation and over all, human life. Tesla Motors has been tried and tested, revealing intuitive and active security measures against all attacks to the vehicle. Tesla is definitely a diamond that shines through the rough when put next to other competitors. When looking towards a future of more

advanced technologies, especially in vehicles, one must consider what car they want in control of their personal data and most importantly the safety of their family.

References

Agarwal, M., Biswas, S., & Nandi, S. (2015). Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks. *IEEE Communications Letters, 19(4)*, 581–584.

Chaouchi, H. (Ed.). (2013). Iste : The Internet of Things : Connecting Objects (1). Somerset, US: Wiley-ISTE. Retrieved from http://www.ebrary.com

*Gandini, F., & Anzoino, N. (2010). Car crash: Accident or … computer-hacking? *Journal of Science & Justice*, *50(1)*, 43-44. http://dx.doi.org/10.1016/j.scijus.2009.11.065.

Greenberg, A. (2015). Hackers Remotely Kill a Jeep on the Highway-With Me in It. Retrieved April 10, 2016, from http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Gitlin, J. M. (2016). Tesla's new firmware improves autosteer, adds remote parking--of a sort. New York: Condé Nast Publications, Inc. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1755352277?accountid=10639

Kovacs, E. (2015). Tesla Increases Bug Bounty Payout After Experts Hack Model S SecurityWeek.Com. Retrieved April 10, 2016, from http://www.securityweek.com/tesla-increases-bug-bounty-payout-after-experts-hack-model-s

*Lee, M. T. (1998). The ford pinto case and the development of auto safety regulations, 1893-1978. *Business and Economic History*, 27(2), 390-401. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/220064181?accountid=10639

McCarthy, M. (2013). Tesla generates small sales, huge buzz without paid ads. Advertising Age, 84(23), 9. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1367101121?accountid=10639

Ward, M. (2015). Warning after security experts hack Tesla car - BBC News. Retrieved April 10, 2016, from http://www.bbc.com/news/technology-33802344

Tesla. (2016). Model S. Retrieved from from https://www.teslamotors.com/models