Tanuja Mohan
ITP 125: Hackers to CEOs
April 12, 2017

ITP 125: Final Paper

We all love the fancy, luxurious car brands we see in commercials such as Lexus, Mercedes, and BMWs. Recently, the hype has switched towards the self-driving automated Teslas. Tesla Motors shocked the automobile industry by introducing its self-driving car model. We are all fascinated by this new technology, but at the same time we have our concerns. What if the car incorrectly calculates the distance between you and the car in front of you? What if the car does not brake fast enough? Another question that security wizards would ask is, *What if someone else, not in the car, take control of my car?* In other words, what if someone hijacks my car remotely? This is a question that I have researched into. I have specifically looked into security breaches that Tesla Motors has already faced and what security measures Tesla Motors has taken to combat these breaches.

One breach that I looked into was a Chinese hack specifically targeting the vehicle's brakes. The hackers were able to take control of the brakes by using Tesla's' Wifi connection allowing them to remotely control when the vehicle would brake or not brake. As soon as Tesla realized that it had this security concern, they immediately went to work by focusing on integrating a security technique called code-signing. Code-signing is the process of digitally signing scripts so that whoever the developed the software can guarantee that their code has not been altered since it was unsigned. Commonly, this process uses a cryptographic hash to validate authenticity and integrity. Tesla took it a step further by not just implementing this security feature to protect the brake system, but also used code-signing to secure all other functionality from steering wheel control to windshield

wiper movement. Now, hackers would not be able to remotely modify any of the vehicle's scripts since they do not have the hash key, which only Tesla has, to authenticate themselves

Code-signing is an interesting technique for Tesla to use because code-signing is known to be used for PCs and smartphones for many years. Some common examples of using code-signing in smartphones consist of checking if the application you are downloading was actually authenticated by the App Store. By using this technique, Tesla is almost saying that their product is not just a piece of hardware with code running it, but rather it is first and foremost designed software with a hardware casing. If we look at the Chinese Hacker example again, the security breach was made possible by tricking the car driver into connecting to a malicious hotspot and then automatically opening up a website that then downloaded the malicious scripts. The entire breach system was done purely through the designed software and also my social engineering the driver into think that the hotspot they were connecting to was safe (the hotspot was purposefully named "Tesla Guest").

This attack is not the only way people have tried to gain access to the vehicle. Another common approach that people have taken involves trying to login as another user on Tesla's website. This can be done by using multiple login attempts to brute force the username and password combination because Tesla does not limit the number of login attempts an attacker can make. Aside from trying to brute force the password, the attacker can also try a technique called phishing. Phishing is the act of requesting confidential information in order to fraudulently obtain access to personal data. Once the attacker has access to the user's credentials, the attacker can then login to the Tesla application and control the vehicle from there by directly changing the car settings. Once in the application, the attacker has full control of the car's settings since there is no second line of security that the attacker needs to get through.

In order to prevent this type of attack from occurring, I propose that Tesla should add a second line of defense to their mobile application. To do this, I propose that Tesla use two step authentication to make their application more secure. We commonly see two step authentication when we create a new email account. We first create a username and password and then are prompted to enter in a phone number that will become associated with that account. In a couple of second the user will receive a text message with a code in it. This code ensures that the user has entered in a valid phone number and that they are indeed the owner of the account. We can apply this same technique to how users access their Tesla mobile application, which then will add a second-layer of security that is missing. With this change users would login to the application and then the application would prompt them to enter in a code. I imagine this code to be generated by using Symantec's VIP access.

What is Symantec VIP access? Symantec VIP access is a dynamic, second factor of authentication. Users would have a Symantec VIP application on their phone, which generates a unique code that changes every 30 seconds. This means that within 30 seconds of entering his or her credentials into the Tesla application, the user would need to switch to the Symantec application and enter in the unique code back into the Tesla application. If the username, password, and Symantec code are all correct only then will the user have access to the vehicle's settings. By including Symantec into the security equation we force any attacker to have to use the owner of the vehicle's phone since the Symantec code associated with the Tesla account can only be accessed on the user's phone. This means that in order for an attacker to get access to someone's car, he or she would need to get the phone of the vehicle owner. This need to get the phone only adds more layers of security.

The attacker has to get the phone, know the passcode to the phone, and then also know the username and password to the Tesla application.

All this discussion of the integration of software and hardware in the various Tesla models also brings to the table the security concerns with the Internet of Things (IoT). IoT is commonly used to reference remotely controlled technology gadgets used in a household, such a device to control your house's lighting system or a way to communicate with your laundry system. The IoT have become a popular target for hackers and researchers at the University of Michigan have already found a way to hack into the Samsung SmartThings platform and take control of an entire home automation system. What makes it so easy to do this? IoT are usually all connected by one homehub, which house owners rarely update because it requires them to then reset all of their IoT devices which takes time. Once the attacker has control of this homehub then they have access to all IoT devices. On top of this, there are no security applications out there that allow homeowners to monitor any compromises so an attacker can leave no footprints behind after the attack has already been made making eavesdropping (accessing data with the owner knowing) super easy.

IoT relates to Tesla's vehicles because Tesla can almost be viewed as an IoT. Each Tesla models uses a WiFi connection to allow the driver to communicate with the car just like the relationship between a homeowner and IoT appliances. Both of them are also vulnerable because of how easy their network is to access and the security issues pressing IoT are reflective of the issues that Tesla will need to face in the future.

Aside from the threat of hackers accessing their data, Tesla owners also need to understand how much of their personal data Tesla itself has access to. This is one surprise about IoT that many users do not realize. When users begin the process of using an IoT device they have to agree to its

terms of service and not many users actually read the entire document. Within the terms and services, IoT allows for the distribution of collected data to outside companies. One example, an insurance company can gather insurance on your driving habits from your connected car when calculating your insurance rate and this same process can be used to calculate your health or life insurance. Are we really ok with this? Is this an invasion of our privacy? The data that IoT is collecting should not be distributed to outside companies but because we are not reading our terms of service thoroughly, many IoT owners are not even aware that this is happening. Tesla could be doing the exact same thing by selling the personal data it is accumulating while your drive the vehicle to work and back home. This concern raises the fact that we as consumers need to understand who has access to our personal data and that this information is out there for others to use either positively or negatively.

Tesla is an innovative and progressive company that is striving to build a type of technology not yet been built. With this new technology comes many security concerns that consumers need to know and be educated about. With technology becoming an integral part of our lives, we need to be aware of what is our digital footprint and who has access to our personal information. As Tesla builds new models it will need to figure out more secure ways to authenticate its users and ensure that no one other than the driver has access to the vehicle's control hub. Until the Tesla models become 100% secure, we need to make sure we are alert, aware, and educated on these topics.

Works Cited

Greenberg, Andy. "Tesla Responds to Chinese Hack With a Major Security Upgrade." *Wired*. N.p., 27 Sept. 2016. Web.
https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/

Fisher, Dennis. "Researcher Identifies Potential Security Issues With Tesla S." *ThreatPost*. N.p., 31 Mar. 2014. Web.
https://threatpost.com/researcher-identifies-potential-security-issues-with-tesla-s/105146/

Rouse, Margaret. "Two-factor authentication (2FA)." *TechTarget*. N.p., 4 Mar. 2015. Web.
http://searchsecurity.techtarget.com/definition/two-factor-authentication

Lambert, Fred. "Tesla to release a 'big' mobile app update with version 8.1 next month." *Electrek*. N.p., 18 Nov. 2016. Web.
https://electrek.co/2016/11/18/tesla-big-mobile-app-update-8-1-elon-musk/

Meal, Andrew. "How the Internet of Things will affect security & privacy." *Business Insider*. N.p., 19 Dec. 2016. Web.
http://www.businessinsider.com/internet-of-things-security-privacy-2016-8