John Zeiders

Chi So

ITP 125

April 25th, 2017

DEFCON 23: Jeep Hacking

One of the highlights of DEFCON 23 was an analysis on the hacking of Chrysler vehicles. This was done by two security researchers Charlie Miller and Chris Valasek. They were able to successfully gain control of a 2014 Jeep Cherokee and remotely control all components of the car: including steering and braking. The presentation centered around their four step process to hacking the car that took several months. The first was to figure out a way to gain entry to the vehicle, in terms of digital control. The second was to then go from there to the CAN network, which interfaced the central computer to the electronics and hardware on the car. They then had to figure out the CAN messages themselves and what signals they would need to send to control the car’s behavior. Then lastly, they had to inject these CAN messages into the system. This was a fairly standard process for seizing control of digitally interfaced hardware and was only slightly complicated by Chrysler’s security measures.

Wirelessly connecting to the car’s computer was the first challenge that was presented to Charlie and Chris. They did this through the UConnect system, which is Chrysler's digital entertainment hub for all of their vehicles. It exposed two primary mediums of entry, the first was WiFi and the 2nd was the cellular service. The Wifi was seen as the simpler form of connection and they tried it first. The car contained a hotspot service that generated its own random password. Conveniently though, after evaluating the source code, obtained through jailbreaking the console, they found that the password was generated from a seed when the cars ECU was first turned on. Since the car was only produced over a 12-month span, they were able to brute force the password within an hour. Further analysis was able to reduce it to roughly 30 passwords as if the car was unable to receive a time from the GPS unit, it defaulted to a new password seeded from a default time. Wifi, however, posed two difficulties, the first was the range, it was necessary to be within roughly 20ft of the car, the 2nd was that WiFi has to be enabled for the car, which approximately costs $30 per month. This price meant that few people had it enabled.

Therefore they moved to the 2nd medium of entry through the cellular service that provided the internet service for the car's internal Wifi. They found that there was a port that was left open for IRC chat that enabled them to access the computer. Not just that but they could do it for any car in the entire United States or Canada that was on the cellular network. A quick query for this port, returned roughly 380,000 vulnerable vehicles, across several different makes and models. This exploit was crucial to gaining effective access to the car and was also the most frightening, given that it meant that the attacked did not need to be near the car. To show the risk, they demoed a system they quickly whipped up that allowed them to theoretically track every Chrysler in the nation.

Once inside the car, they then had to get to the CAN network. This ended up being one of the easiest parts of the hack. A quick google found several ways of injecting Command Line functions to the ECU. In fact, they eventually found that there was an exposed public function that was designed to explicitly expose the Command Line for development and debugging purposes. Using only the exploits that they had achieved so far they were able to control the radio and lighting systems within the car.

However, one of the security measures that Chrysler had taken was the separation of the driving and hardware control unit from the digital entertainment system. In fact, this was not just a software separation there were two separate chips that were supposedly air gapped. However, for some features of the car to work they aren't actually air gapped, there was a single serial connection between the two. The trick was that the car’s control chip, a V850, was programmed to only accept certain commands from the main chip, meaning that they would be unable to send malicious or invalid messages to it. Solving this problem took the majority of the several months they spent cracking this problem. Eventually though, after reading through 1000’s of data sheets they were able to find an exploit that let them reflash the V850 chip. This lets them do effectively anything they wanted to it.

From here it was a simple matter of tracing the CAN signals used to induce certain actions within the car. They started small and spoofed the speedometer readings, convincing the car into showing that it was traveling 40 when in fact it was traveling 70+. This was important as their primary goal was to seize control of the steering, power, and braking systems, which they planned to do through simulating signals from the auto parking feature. However, this system locked out if the car was traveling greater than 5 Miles per hour. Circumventing the real speed readings allowed them to utilize this system whenever they desired. This allowed them to achieve their goal and they were able to remotely drive their Jeep 2014 Cherokee. They then went public were their findings in a WIRED magazine article that explained what they had done and what they are capable of doing.

Since then, their findings have profound implications across the entire automobile industry. The first was a massive recall by Chrysler, that ended up affecting approximately 1.4 Million vehicles. Chryslers stock also tanked in the short term, showing the fears that investors have about the dangers of these exploits. Charlie and Chris had predicted this would happen and we're glad that it did, as it will push corporate boardroom to care more about software security. They also took pride in noting that they did not short the stock, stating that they had done this for the greater good rather than any personal gain. Intriguingly, the recall did not solve the serial exploit that they had used to gain control of the V850 chip but rather closed the ports by which they entered the car. It shut both the exposed mobile port and enabled better password generation for the Wifi network. This means that their exploits still work when entry is gained to the car system, which they can still do now by plugging into the “mechanics” aux port. This is a port intended for use by dealer mechanics for receiving status codes and manually overriding error codes. While this exploit does not pose a particular risk to consumers, as it is rather infeasible, requiring physical access to the interior of the car, it is only a matter of time before another vulnerability allowing entry is found. Therefore this is an issue that they expect to plague the automobile industry for years to come. Chris and Charlie have set out to solve this problem for Uber and are working on securing their autonomous cars, which are exposed to an even greater vulnerability to hacking.

Works Cited

DEFCON 23. Perf. Charlie Miller and Chris Valasek. Youtube, 21 Aug. 2015. Web. 25 Apr. 2017.