CSCI3403 Project 1 - Jeep Cherokee Cyber Attack

Jason Lubrano, Teagan Peters, Andrew Gitlin, Darian Valdez, Milan Formanek

Main Objective of the Attack

As technology advances, cars are becoming more electronically and wirelessly connected through dashboards and features such as UConnect. With these advancements, cars are becoming increasingly vulnerable. Hackers are starting to discover ways of breaching into these cars' software and taking complete control of the system remotely. Thousands of cars on the road today such as the 2014 Jeep Cherokee are vulnerable to remote access attacks. Since 2011, major security flaws have been found in the computerized systems of cars. In 2015 a team of hackers consisting of Charlie Miller and Chris Valasek sought to make notice of these vulnerabilities. In the infamous Jeep Cherokee cyber-attack, the main objective was to show the public that cars that are using a feature called Uconnect are vulnerable to a cyber-attack. By releasing a white paper and making a video of the team hacking into a Jeep while someone was in it on the highway, they demonstrated the dangers and impact of a breach. The risks and potential impact is huge, illustrating why research like this is important to keep us safe.

Details of the Attack

In 2011, four years prior to the publication of the Jeep Cherokee exploit, a group of researchers at the University of California succeed in disabling the breaks and locks of an unidentified vehicle. Following this attack, in 2015 Charlie Miller and Chris Valasek dove deeper into researching vulnerabilities in modern cars. By exploiting a feature marketed as Uconnect, the Chrysler-Jeep's internet connected computer functionality, the team was able to take control of all the major systems of the car. Uconnect is originally designed to allow the driver to answer calls using Bluetooth, control the navigation and even use the car as a mobile Wi-Fi hotspot connected through the Sprint mobile network. Through Uconnect, the researchers were able to remotely control the steering, transmission, and brakes of the victim car. This is very dangerous when taken ahold of malignantly. By gaining remote access through Uconnect, a hacker can exploit the car in many ways such as dialing the volume to the car's highest setting, using signals such as blinkers and hazards, turning off and reving the accelerator, and even shutting down the car completely. Surprisingly, the researchers did not install any physical equipment in the car and the entire attack took place remotely. Fortunately, these researchers didn't exploit this flaw in the Jeep maliciously; however, the team was very unsafe when demonstrating the flaw. In the demonstration video the car was on a busy highway public in normal traffic. Secondly, the driver was very distracted throughout the entire demonstration. Lastly, the car completely was shut down in the highway. Not only is this unsafe, in some states it is illegal to have a stopped vehicle not pulled over on the shoulder. Many people's lives were put at risk due to this reckless behaviour. The attack could have the same effect had the team worked in an empty parking lot or a track.

NIST Framework

Identification is the first aspect to the NIST framework. Identification is the understanding of which risks and assets are at stake in an organization for a cyber attack. Under identification falls risk management. Jeep's biggest understanding should be which risks are at stake for a remote access cyber attack. Due to the UConnect service being exposed to the internet, there is the threat of a remote accessed attack. The UConnect has a vulnerability where inter-vehicular messages are not encrypted. The driver, passenger(s), and other people and things around such as pedestrians, bikers, other cars, and buildings are all affected by a runaway car being breached. By identifying these vulnerabilities and managing these risks, it is a general understanding that a cyber attack could be fatal and many lives could be lost.

Both mechanical and software components of a vehicle require maintenance. As part of a scheduled maintenance, car manufacturers can include software update packages and software integrity diagnostics. These updates will include patches for vulnerabilities that are discovered and fixed by the manufacturer. Integrity checks for the various systems can ensure attacks similar to the one on the Jeep Cherokee have not happened. Having this maintenance would fulfill the protection aspect of NIST Framework.

Detection is important for the car to be resilient to attacks as they are happening. Modern vehicles can have the capability to detect strange command behavior. Detecting these anomalies and events shows the system that something is taking control or sending commands to another part that it shouldn't. For example, the radio sending a command to the transmission saying to shift gears is an anomaly. This would be detected in this stage.

Response to the anomalies would involve the central ECU in the car to make decisions about the detected behavior. An update to the CAN bus protocol could allow for the source of messages to be determined. The system can lock out non-essential components. When this happens, the messages and commands can be ignored and the car will notify the driver to take the vehicle into a mechanic or technician.

Last on the NIST framework is improvements. One improvement the group discussed was regular integrity checks using checksums, online connection updates, or mechanic visits. For example, everytime the car turns on it can run a basic integrity check on its essential software. Current cars on the road could release a patch through online updates to the UConnect system. The companies should also make note to the owners to bring the vehicles into a mechanic or technician to ensure the integrity of the software. Car manufacturers can reduce the number of attack vectors significantly if a few changes are implemented as standard. These changes can include disabling reprogramming functionality for various controllers and blocking communication from non-authorized sources. This would significantly limit the effectiveness of the remote attack as it would be much harder for the attacker to modify the firmware on the onboard computers in order to run arbitrary commands.

Sources:

Jeep Cherokee Cyber Attack - Due Friday, February 1st
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Wikipedia page on NIST Framework
https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

CANtact
https://linklayer.github.io/cantact/

Remote Exploitation of an Unaltered Passenger Vehicle
http://illmatics.com/Remote%20Car%20Hacking.pdf