ISSEM Week 1 Assignment - Group [illegible]

JEEP CHEROKEE HACK

[illegible]

---

1. How/where it was released

The Jeep Grand Cherokee hack took place in 2015 by Charlie Miller and Chris Valasek. The vulnerability was exploited through Wi-Fi to the Jeeps multimedia unit through an auto generated password based on time. They presented the vulnerability and how it was exploited in depth for the first time at Black Hat 2015, a large security conference.

2. How it was detected

Miller and Valasek began by taking apart the Uconnect (Harman Kardon) system and looked at the hardware it contained. The first step they took was to jailbreak the system and investigate how it worked. Although this was not part of the hack itself, it gave them an understanding of some of the functionality the system had, such as Wi-Fi capabilities. Next, through trial and error, attempting various methods of attack, they discovered that the WPA2 password was seated on time. Using this information, they discovered that leveraging this time dependency they could brute force the system in approximately one hour. Although this was a breakthrough, taking an hour to hack a moving car would be very impractical. Miller and Valasek continued testing and were able to make their hack more efficient by discovering that the Wi-Fi password for Chrysler cars was actually generated before the timestamp is set, and is based on the system's default time plus a couple seconds. With this, they were able to narrow down to a very small pool of password combinations, making it extremely easy to hack.

3. What damage it inflicted

Due to the vulnerability of the Uconnect multimedia infotainment system, it allowed Miller and Valasek to gain access to the electronic control units (ECUs), which practically runs every component of the vehicle. Then by issuing Control Area Network (CAN) protocol commands to the ECUs, it allowed the hackers to control every computer system in the Jeep Cherokee, including the engine, brakes, and steering. In addition, because the Uconnect system is connected to the Sprint network by default, the distance range of attack can now become nationwide. These vulnerabilities can have deadly consequences if it was exploited by malicious attackers anywhere in the country, where the attackers can control every component of the vehicle, not the driver.

Besides technical damage, these vulnerabilities also inflicted financial and reputational damage on Chrysler. As a result of Miller and Valasek's research, Chrysler issued a safety recall of 1.4 million of its vehicles. The recall was a software patch that must be manually implemented via a USB device or a dealership mechanic, instead of wireless or over-the-air updates, which means that many Chrysler vehicles will still be vulnerable to this attack.

4. What remediations were put in and by whom

During the process of investigating and exploiting this attack, Miller and Valasek provided regular information updates to Fiat Chrysler Automobiles (FCA), which allowed FCA to begin working on a security patch shortly before the exploit was made public (Miller & Valasek, 2015). On July 16, 2015, FCA voluntarily recalled 1.4 million vehicles to apply the Uconnect software patch version 15.26.1 (Nagode, 2015). FCA estimated nearly 471,000 cars were vulnerable to the Uconnect hack and those customers should bring in their vehicles as soon as possible (Kovacs. 2015). The Uconnect software patch actively blocked incoming TCP/IP packets for remote access and provided unlisted additional network-level security safeguards (Nagode, 2015). FCA released the Uconnect software out of an abundance of caution and to get ahead of any negative public relations as FCA stressed that this attack was not seen in the wild and was only detected in a controlled environment (Kovacs. 2015).

Shortly after FCA released the Uconnect software patch, Sprint cellular network actively implemented blocks on IRC port 6667 traffic (Miller & Valasek, 2015). Blocking port 6667 essentially prevented the remote-access vulnerability from being exploited through Sprint's cellular network on the vehicles (Miller & Valasek, 2015). Sprint also enabled port blocking on 6667 traffic for users on the same cellular tower (Miller & Valasek, 2015). The Sprint port 6667 blocking effectively prevented remote access to the device even if the vehicle's Uconnect was not patched, as the only method of accessing the vehicle was to be in close proximity of the vehicle (Miller & Valasek, 2015).

The two different vendor solutions improved the security protection and reduced the potential risk of unauthorized and unlawful access to vehicle systems (Kovacs. 2015).

5. What were the crucial enablers for this disaster in retrospective

The vulnerability of hacking into a vehicle was already demonstrated by Miller and Valasek in a wired-in attack back in 2013 at the DefCon conference. However, instead of conducting further research on the vulnerability they exposed, the auto industry downplayed its impact and significance at the time. This lack of security mindset and action was the first crucial enabler that motivated Miller and Valasek for the next attack in 2015. This time they attacked using the wireless network vulnerability.

Another crucial enabler was the weak security from Harman-Kardon's Uconnect multimedia system in the Chrysler cars. From the hardware and software perspective, there is an isolation between the physical and the connected systems in the vehicles. That was why the automakers were confident of the limited damage the exposed vulnerability would cause. However, for the Chrysler cars, this isolation was not as strong as expected. The Uconnect system allowed unauthenticated and unauthorized connection from other access points on the Sprint cellular network to take control of the multimedia system, which was the entry point to control the physical systems of the vehicles.

In addition to the Uconnect system, the V850 controller, which the multimedia system communicates with also bore some responsibility for this attack. After the researchers were able to gain access to the Uconnect system, they were only able to control the accessories of the vehicle at that time, such as radio station, volume control, and digital display. It was not until Miller and Valasek were able to change the firmware of the V850 controller, which Uconnect communicates with, that they were able to access the physical system of the vehicle. The lack of security in the V850 controller that allowed unauthorized change of firmware provided hackers the opportunity to conduct more malicious attacks on the system.

6. What could have been done better

Based on Miller and Valasek's white paper, which systematically outlines the attack vectors that were successful and failed, the trend we see most often is inadequate authentication between the various modules/components within modern vehicles (Miller & Valasek, 2015). Miller and Valasek were able to successfully access the Jeep's internal D-Bus message daemon on the Uconnect system on port 6667 due to the message daemon accepting anonymous connections through telnet (Miller & Valasek, 2015).

Another attack vector the team found was that the Serial Peripheral Interface (SPI) directly communicates with the V850, which can allow an attacker to send CAN messages to manipulate the vehicle (Miller & Valasek, 2015). An attacker could also directly interface with the OMAP chip via the internal D-Bus system (Miller & Valasek, 2015). The most significant attack vector seen was the Wi-Fi default password generation mechanism, which allowed the team to easily guess the Wi-Fi password (Miller & Valasek, 2015).

While Miller and Valasek pointed out that the tools and applications they used to exploit this vulnerability were more expensive for lower-level attackers, an attacker that is motivated could easily acquire these same tools and develop a similar solution as the team did.
If FCA implemented a form of authentication on the D-Bus, or even disabled anonymous login, randomly generated Wi-Fi passwords not based on the vehicle's manufacturing date and required

authentication when crossing modules/components the team could have seen different, unsuccessful results. Having a large attack surface such as modern vehicles should trigger more secure coding and software development processes to ensure that unauthorized users can not access the main components of the systems and laterally pivot into areas of the components which could cause serious bodily harm if tampered with.

7. How do we prevent this in the future or is likely to recur

So long as there is some form of motivation, attacks like the one used on the Jeep Cherokee will continue to be developed. The likelihood for this kind of hack to occur in the future is dependent on the hacker's skill, funds, and time.

Prevention measures could be addressed by first revamping communication between collaborating businesses. In the case of this hack, products most notably from Harmon-Kardon and Sprint were used to exploit multiple vulnerabilities in the Jeep Cherokee. One of these included connecting through Sprint's network port 6667 to access the D-Bus service from the Jeep Cherokee's Uconnect system. The port did not filter its connections and was used to access the vehicle's computers from a remote location. To prevent attacks like this, applicable companies involved with developing the product need to make sure they are communicating the intricacies of their product design not only with product engineers but also with security personnel. This way vulnerabilities like the one mentioned above are less likely to be overlooked, and appropriate security measures can be put in place.

Additionally, greater feedback from security personnel should be utilized during the design phase of the product. When Miller and Valasek searched for a vehicle to exploit, they researched which vehicle had "a combination of a large attack surface, simple architecture, and many advanced physical features" (Miller & Valasek, 2015). To start, the system architecture of the Jeep's radio head unit was physically attached to both CAN buses. To Miller and Valasek, this meant that if they could compromise the radio, they would be able to have "control of physical attributes of the vehicle" (Miller & Valasek, 2015). While software can be patched to make compromising the radio system harder, it will still have a physical link and be inherently vulnerable. In addition, Miller and Valasek were looking for vehicles with many advanced physical features like adaptive cruise control, forward collision warning, and lane departure warning, among others. These additional features, if compromised, could give a hacker physical control of the vehicle. By contributing more closely with the development team, security can be built into the product; in this case, by creating a more isolated systems architecture. This can secure critical physical components of the vehicle if other internet-connected systems become compromised, preventing a hack of this scope from occurring.

Legislation can also be considered. At this point, legislation varies between each country. The United States has standards for vehicle safety (e.g., Federal Motor Vehicle Safety

Standards), but is lacking federal regulations related to cybersecurity in automotive applications. The closest options include guidelines by the National Institute of Standards and Technology (NIST) and the National Highway Traffic Safety Administration (NHTSA) that are designed to assist companies in mitigating safety risks due to cybersecurity problems (National Highway Traffic Safety Administration, n.d.). Since cybersecurity is an international problem, unified legislation could make it easier for organizations to create appropriate security protocols and stay compliant with the latest standards. One current example that follows this line of thinking is the United Nation Economic Commission (UNECE) for Europe WP.29's recent additions on automotive regulations in cybersecurity and software updates. This regulation was introduced in 2020 and addresses: setting standards in managing cyber risk, securing vehicles by design, detecting and responding to security incidents across a vehicle fleet, and providing safe and secure software updates to ensure vehicle safety is not compromised (UNECE, 2020). While this a good start, for legislation of this nature to be more effective UNECE would need to have greater worldwide participation, as notable players in the automotive market like China and the United States are absent from this agreement.

References:

Kovacs, E. (2015, July 24). Fiat Chrysler Recalls 1.4 Million Cars Following Jeep Hack. SecurityWeek. https://www.securityweek.com/fiat-chrysler-recalls-14-million-cars-following-jeep-hack.

Miller, C., &; Valasek, C. (2015, August 10). Remote Exploitation of an Unaltered Passenger Vehicle. http://www.illmatics.com/Remote%20Car%20Hacking.pdf.

Nagode, A. (2015, July 24). Stellantis Media - Statement: Software Update. https://media.stellantisnorthamerica.com. https://media.stellantisnorthamerica.com/newsrelease.do;jsessionid=5DF0319DEE00F047387014495E69A518?&id=16849&mid=

National Highway Traffic Safety Administration. (n.d.). *Vehicle Cybersecurity*. https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

UNECE. (2020, June 24). *UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles*. https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll.