EDUNET FOUNDATION - Case Studies: IoT Security

Case Study 4 - The Jeep Hack

Introduction:

In 2015, a groundbreaking case emerged that exposed the vulnerabilities of connected vehicles. This case study delves into the "Jeep Hack," an incident that demonstrated the potential risks associated with the convergence of automotive technology and the Internet of Things (IoT), uncovering critical insights into the security challenges facing modern automobiles.

Attack Overview:

The Jeep Hack, which occurred in July 2015, involved the remote takeover of a Jeep Cherokee's control systems, leaving the driver virtually powerless over their own vehicle. This incident brought to light the susceptibility of connected cars to cyberattacks and underscored the need for robust cybersecurity measures within the automotive industry.

https://pbs.twimg.com/media/CKnuHigXAAAnyFV?format=jpg&name=small

At the start of their research Miller and Valasek tried to hack the multimedia system of Jeep through Wi-Fi connection Chrysler, the manufacturer of the vehicle, offers this option by subscription. It turned out, that it isn't that hard to hack this Wi-Fi due to the fact that the Wi-Fi password is generated automatically, based on the time when the car and its multimedia system the head unit is turned on for the very first time.

In theory, considering the second precision of the date/time, it's a rather secure method which gets you lots of possible combinations. But if you know the year when the car in question was manufactured and if you successfully guess the month, you can bring the count down to just 15 million combinations. If you suppose the time was during the day, it gets you to about 7 million combinations. For a hacker, this number is pretty workable you can brute force it within an hour. The problem is, that you need to follow that very Jeep for that hour to stay in touch with its Wi-Fi connection. The researchers tried to find another way. And *surprise, surprise!* they found one: it turned out, that the Wi-Fi password for Chrysler's cars is generated before the actual time and date is set and is based on default system time plus a few seconds during which the head unit boots up.

So, the January 01 2013 00.00 GMT it was, or more precisely 00.00.32 GMT in this very case. The number of combinations is very small, and it's a piece of cake even for amateur hacker to guess the right one.

Attack Method:

Cybersecurity researchers successfully exploited vulnerabilities in the vehicle's infotainment system, which was connected to the internet through the cellular network. By leveraging these vulnerabilities, the researchers gained access to critical vehicle functions, including steering, braking, and acceleration, all from a remote location.

Impact:

1. **Driver Vulnerability:** The attack showcased the potential for attackers to remotely control a vehicle, endangering the driver's safety and potentially leading to accidents.

2. **Public Alarm:** The incident raised public awareness about the security risks of connected cars and eroded public trust in the safety of modern vehicles.

3. **Automaker Reputation:** The automaker's reputation suffered due to the perception that its vehicles were susceptible to remote manipulation, damaging brand credibility and sales.

Response and Mitigation:

1. **Immediate Recall:** The automaker issued a voluntary recall of over a million vehicles to address the security vulnerabilities and released a software patch to fix the affected systems.

2. **Collaboration with Researchers:** The automaker collaborated with the cybersecurity researchers who exposed the vulnerability, using their findings to strengthen the vehicle's security systems.

3. **Regulatory Scrutiny:** Regulatory agencies began to scrutinize the cybersecurity practices of automakers, leading to discussions on establishing industry-wide standards for connected vehicle security.

Lessons Learned:

1. **Prioritize Cybersecurity:** The Jeep Hack highlighted the necessity of integrating robust cybersecurity measures into the design and manufacturing of connected vehicles.

2. **Continuous Monitoring:** Automakers must continuously monitor and update the software in connected cars to address vulnerabilities and mitigate risks.

3. **Collaboration is Key:** Collaboration between automakers, cybersecurity researchers, and regulatory bodies is essential to ensure that vehicles remain secure against emerging threats.

4. **Regulatory Oversight:** Regulatory agencies should establish clear cybersecurity standards for connected vehicles, encouraging automakers to meet minimum security requirements.

Conclusion:

The Jeep Hack demonstrated that the era of connected cars brings both innovation and risks. As vehicles become more integrated with IoT technology, the need for robust cybersecurity measures becomes paramount. This incident serves as a wakeup call for the automotive industry, urging automakers to take proactive steps to secure their vehicles and collaborate with experts to stay ahead of evolving cyber threats. By learning from the Jeep Hack, the industry can pave the way for safer and more secure connected transportation systems in the future.

Reference

https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

https://chat.openai.com/