Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller, Chris Valasek

Presented by Hitakshi Annayya

Contents

1. Introduction
2. Network Architecture
3. Evaluation
4. Conclusion
5. References

Introduction

- In 2010, Automotive security research started and found that vehicles are vulnerable to attacks across the country, not just locally.
- If hackers could inject messages into the CAN bus of a vehicle, then they could make physical changes to the car.
- Hackers can remotely control the physical attributes of the vehicle

  a. The display on the speedometer

  b. Kill the engine

  c. Affect the braking system

This paper outlines the research into performing a remote attack against an unaltered 2014 Jeep Cherokee.

Hopefully this remote attack research can pave the road for more secure connected cars in our future by providing this detailed information to security researchers, automotive manufacturers, automotive suppliers, and consumers.

Video

https://www.youtube.com/watch?v=MK0SrxBC1xs

Network Architecture

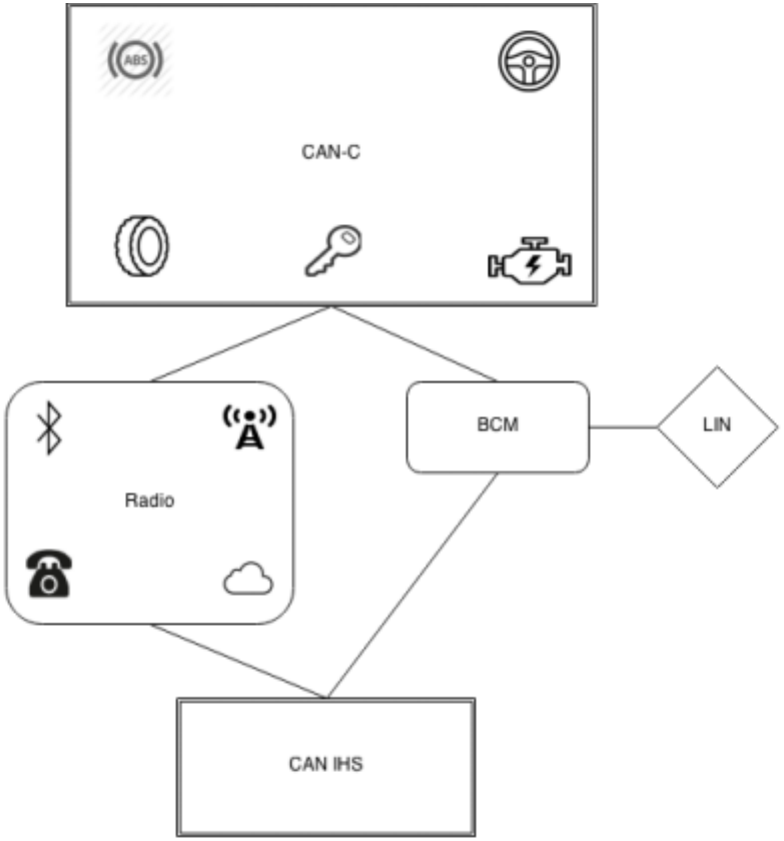


Figure: 2014 Jeep Cherokee architecture diagram

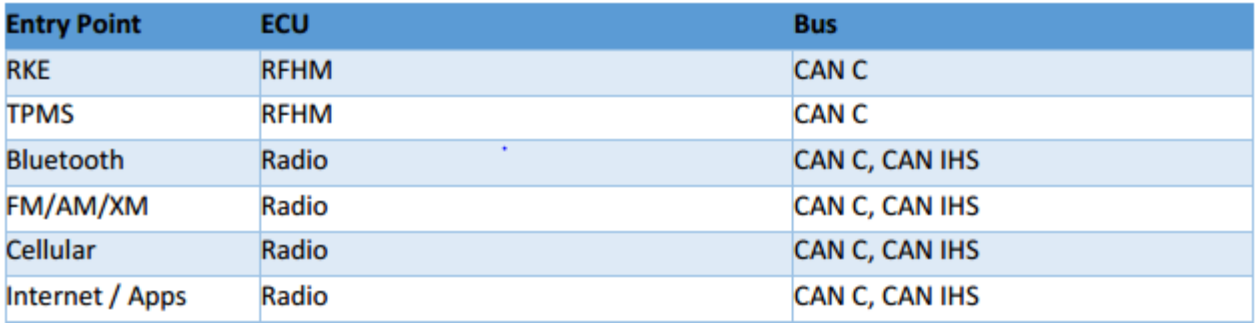
Ref [1] http://illmatics.com/Remote%20Car%20Hacking.pdf

Cyber Physical Features

Advances in technology increase the safety of the driver and its surroundings, and also they present an opportunity for an attacker to use them as a means to control the vehicle.

1. Adaptive Cruise Control (ACC)
2. Forward Collision Warning Plus (FCW+)
3. Lane Departure Warning (LDW+)
4. Park Assist System (PAM)

Remote Attack Surface



Entry Point	ECU	Bus
RKE	RFHM	CAN C
TPMS	RFHM	CAN C
Bluetooth	Radio	CAN C, CAN IHS
FM/AM/XM	Radio	CAN C, CAN IHS
Cellular	Radio	CAN C, CAN IHS
Internet / Apps	Radio	CAN C, CAN IHS

Ref [1] http://illmatics.com/Remote%20Car%20Hacking.pdf

1. Passive Anti-Theft System (PATS) → attack surface is small
2. Tire Pressure Monitoring System (TPMS) → attack surface is small
3. Remote Keyless Entry/Start (RKE) → attack surface is small
4. Bluetooth
5. Radio Data System
6. Wi-Fi
7. Telematics/Internet/Apps

Facts !!!!

Ford, GM and Toyota sued for 'dangerous defects' in hackable cars

Uconnect System

- The 2014 Jeep Cherokee uses the Uconnect 8.4AN/RA4 radio manufactured by Harman Kardon as the sole source for infotainment, Wi-Fi connectivity, navigation, apps, and cellular communications.

- The Uconnect head unit also contains a microcontroller and software that allows it to communicate with other electronic modules in the vehicle over the Controller Area Network - Interior High Speed (CANIHS) data bus.

- Did not get desired results while they tried PPS files to send arbitrary CAN messages.

Uconnect System

Researches discovered open port **6667: D-BUS session bus (in car Wi-Fi)**, vulnerability would be present that could allow remote exploitation.

D-Bus which is essentially an inter-process communication (IPC) and remote procedure call (RPC) mechanism used for communication between processes.

D-Bus permit direct interaction with the head unit, such as adjusting the volume of the radio, accessing PPS data, and others that provide lower levels of access.

Exposing such a robust and comprehensive service like D-Bus over the network poses several security risks from abusing functionality, to code injection, and even memory corruption.

Cellular & CAN connectivity

The Harman Uconnect system in the 2014 Jeep Cherokee also contains the ability to communicate over Sprint's cellular network – termed as telematics.

Telematics system is the backbone for the in-car Wi-Fi, real-time traffic updates, and many other aspects of remote connectivity.

The Uconnect system had the ability to interact with both the outside world, via Wi-Fi, Cellular, and Bluetooth and also with the CAN bus.

Attack payloads - Uconnect

By running arbitrary code on the head unit, within the Uconnect system leads to some attacks

1. GPS
2. HVAC
3. Radio Volume
4. Radio Station (FM)
5. Display

http://users.ece.cmu.edu/~tvidas/papers/ASIACCS14.pdf

Cellular Exploitation

The biggest problem with these hacks is that they require either physical access or the ability for the attacker to join the Wi-Fi hotspot respectively’

Limitations:

1. people don’t pay for the Wi-Fi service – expensive
2. the problem of joining the Wi-Fi network – passwords generate randomly
3. the range of Wi-Fi is quite short for car hacking – 32 meters

Cyber Physical CAN messages

After finding how to send CAN messages via remote exploitation, it is simply a matter of figuring out which ones to send to affect physical systems.

2 types of CAN messages

Normal - Normal messages are seen all the time on the bus during normal operation.

Diagnostic -Diagnostic messages typically are only seen when a mechanic is testing or working on an ECU

Cyber Physical CAN messages

Turn Signal → blinker is controlled via CAN message on the CAN-C network.
If the first byte is 01, it makes the left signal come on, if it is 02, it makes the right signal come on.

Locks → CAN message on the CAN IHS Bus.

Diagnostic CAN messages

Jeep diagnostic messages are 29-bit CAN messages.

1. Kill engine
2. No brakes
3. Steering

Patching & Mitigations

A fix was made by Chrysler.

→ the vehicle now no longer accepts incoming TCP/IP packets.

Additionally, the Sprint network was reconfigured to block (at least) port 6667 traffic even within the same cellular tower.

Conclusion

- Remote attack that can be performed against many Fiat-Chrysler vehicles.
- The number of vehicles that were vulnerable were in the hundreds of thousands
- Remote attacks physical systems of the vehicle such as steering and braking are affected.
- Research in the hopes that we can learn to build more secure vehicles in the future so that drivers can trust they are safe from a cyber attack while driving.

References

http://illmatics.com/Remote%20Car%20Hacking.pdf

http://illmatics.com/Remote%20Car%20Hacking.pdf

http://www.consumerreports.org/cro/news/2015/05/keeping-your-car-safe-fromhacking/index.htm

THANK YOU!

Remote Exploitation of an Unaltered Passenger Vehicle.

Charlie Miller and Chris Valasek.
In BlackHat USA'15

Paper Discussion

- Zhenyu Ning,
- CSC 6991 – Advanced Computer System Security

- After vulnerability found through previous research been quibbled by automotive industry, the authors present several approaches to attack unaltered vehicles remotely to draw more attention to the car security.
- This paper chooses 2014 Jeep Cherokee as attack target and generally introduced important components and software environment of this car at the very beginning. It then describes how to access the vehicle's network with a clever brute forced way and also how to jailbreak the Uconnect system just with a few steps associating with self-update mechanism. After that, the author illustrates how to injection arbitrary codes to the D-Bus both through command injection and through some scripts, while the later approach even does not need jailbreaking. And with these efforts, some examples are given to show how to read information from the components and how to arbitrarily modify the component configurations.
- More horrifically, the paper then demonstrates that though a custom cell tower, the attacker could communicate with the vehicle via cellular network, which means that the attacker even need neither connecting to the in-car wifi nor jailbreaking the system. And as a final harvest, the author finds an approach to spread the attack from one to anther using an in-car chip named V850, i.e., maybe millions of vehicles will suffer from this if someone perform this kind of remote attack.
- Though some parts of the vulnerability have been fixed by the manufacturer, we can predict that there may still exist the other vulnerabilities which have not been revealed yet and the security of vehicles is really not something trivial.

Paper Discussion

- Sai Tej Kancharla,
- CSC 6991 – Advanced Computer System Security

- The paper draws our attention towards how cyber security could effect everyday lives and things we depend on daily. The paper briefly discusses on how easy it would be to compromise the security of a car and how easily one can put the driver in harms way with very little research

- The paper executed various ways of attacking the security of car, they used the 2014 Jeep Cherokee but the same mechanism can be followed on other Chrysler produced cars and much more. The paper discusses in length how the hacker can make use of the Uconnect system by accessing it with a WiFi connection or physically through USB with a compromised update firmware. With this the author shows they can find the GPS location of car, disable HVAC systems and much more. But for this to happen the hacker needs to be physically near the car.

- The paper also discusses about how any Sprint device from anywhere in the country can remotely communicate with the D-Bus on board the car. This is worrisome cause the hacker can remotely disable the Anti Collision control or more from anywhere and cause serious harm. Though most of the functions that tested were not executed in high speeds and only at lower speeds it is still a sign for need of better security.

- Though the paper helped disclose the vulnerabilities and help the manufacturing companies fix the loopholes with patch works.There might be many more exploits which can cause harm, so there is a need for the Automobile companies to take the threats and also system security very seriously.

Paper Discussion

- Hitakshi Annayya

- The paper "Remote exploitation of an unaltered vehicle" states that the modern technologically advanced automobile vehicles are more prone to vulnerable to attacks remotely as well locally. Hackers can gain entry into the head unit to inject the CAN messages and attack the physical attributes of the vehicle such as controlling the speedometer, steering, kill the engine, affect the braking system of the vehicle.

- The advanced technology used for driving the vehicle and for the safety driver has made road to the hackers to attack any attribute of the vehicle very easily. The researchers has demonstrated the attacks on the 2014 jeep cherokee. The entry points to attack the vehicle would be bluetooth, mp3 parser radio, and through telemantic units. The 2014 Jeep Cherokee uses the Uconnect 8.4AN/RA4 radio manufactured by Harman Kardon as the sole source for infotainment, Wi-Fi connectivity, navigation, apps, and cellular communications.Examining and categorizing all the D-Bus services and method calls over TCP is an exercise left up to the reader, but we've found several that permit direct interaction with the head unit, such as adjusting the volume of the radio, accessing PPS data, and others that provide lower levels of access.

- Once the researchers found the way to inject messages into the CAN bus in either way normal or diagnostic , then they demonstrated kill engine, no brakes, steering disabled while parking. A fix was made by Chrysler for this issue. we can conclude by the research made in automotive security, the number of vehicles that were vulnerable were in the hundreds of thousands and it forced a 1.4 million vehicle recall by FCA as well as changes to the Sprint carrier network and also we hopes that we can learn to build more secure vehicles in the future so that drivers can trust they are safe from a cyber attack while driving.

Paper Discussion

- Lucas Copi
- CSC 6991
- 28 September 2015
- Car Hacking
- The paper *Remote Exploitation of Unaltered Passenger Vehicle* details the many vulnerabilities of vehicles with technically advanced infotainment systems, specifically targeting a 2014 Jeep Cherokee. Although previous research has shown the capabilities of an attacker to send messages to the CAN bus and control physical attributes of the vehicle, these attacks required physical access to the vehicle. This paper focused research on attacks that could be exploited remotely.
- The authors focused their attacks on a Jeep Cherokee due to the large attack surface area and the ability for the radio head unit to interact with both CAN busses. The paper details the many areas that could provide an attacker access to the vehicle including: Bluetooth connectivity, Wifi hotspot sharing, jail breaking the head unit, cellular exploitation and exploiting the D-bus. Due to the papers focus on remote attacks, cellular exploitation was utilized to compromise the Jeep's UConnect system.
- Researchers were able to directly communicate with the UConnect system from Sprint's wireless cellular network and exploit vulnerabilities in the D-bus system to interact with and compromise the system. Once the system was entered through the D-bus port 6667, attackers were able to modify the firmware of the UConnect system to allow them to send commands to the CAN bus and control the physical elements of the car such as braking and steering.
- The paper prompted a 1.4 million vehicle recall by Fiat-Chrysler and modification to Sprint's cellular network to eliminate some vulnerabilities.

ECE Seminar

Speaker: K. Venkatesh Prasad.

Senior Technical Leader, Open Innovation, Ford Motor Company

https://media.ford.com/content/fordmedia/fna/us/en/people/k-venkatesh-prasad.html

Date: Wednesday, October 14, 2015.

Venue: 1200 Engineering, Hall of Fame.

Time: 1:30 PM – 2:30 PM.

Topic: Automobiles as Platforms for Open and User-Innovation.

Reminders

- Term project proposal is due a week from today (firm deadline)
- Paper summaries