Comprehensive Experimental Analysis of Automotive Attack Surfaces

Checkoway et al

Presented By Lucas Copi

Overview

- Introduction
- Automotive Threat Models
- Vulnerability analysis
- Conclusion

Introduction

- Modern Cars are controlled by ECU's connected by an internal network (CAN)
- Access to CAN has capability to override all computer control systems (demonstrated in previous work)
- Previous research focused on attacks requiring physical access
- New research focuses on new remote threat models
- Paper attempts to investigate entire attack surface of the modern car

Automotive threat model

There are three main ways for an attacker to gain access to the CAN:

- Indirect physical access
- Short-range wireless
- Long range wireless

Indirect physical access

- While the paper investigates the vulnerabilities of physical interfaces the researchers operate under the stipulation attackers may not have direct physical access to the vehicle
- OBDII port
- Entertainment

Short Range Wireless Access

- Bluetooth
- Remote keyless entry
- Tire pressure monitors
- RFID Car Keys
- Emerging short range channels for intercar communication

Long-range wireless

- Broadcast channels: channels not directed toward a car but can be accessed through receivers on the vehicle
- Addressable channels: remote telematics systems

Vulnerability Analysis

- Paper explores one vulnerability in each of the previous segments
- Research assumes attacker has access to similar model vehicle or information allowing them to reverse engineer systems and inspect for vulnerabilities
- For every vulnerability demonstrated, researchers were able to obtain complete control of the vehicle's systems
- Late model economy car was chosen with standard options (specific car unspecified)

Indirect physical channels

- Targeted media player
- Two vulnerabilities
- Latent update capability in media player that can recognize ISO formatted CD's and reflash system with data contained on CD
- Were able to exploit a buffer overflow attack and send can packets embedded in a WMA file to compromise the system

Physical channels continued

- OBD-II port
- Used for vehicle diagnostic and is the standard port on any vehicle older than 2004
- Accessed by passthru devices
- Able to design malware that compromised passthru device and pass malicious can packets to vehicle upon use
- Were able to implement this attack as a worm

Short Range Wireless Channels

- Bluetooth
- Indirect short range wireless attacks: attack requires owner of a vehicle to have a compromised paired Bluetooth device
- Able to implement with a Trojan horse on an Android application
- Direct short range wireless attacks: Were able to obtain MAC address and brute force pairing pin to gain access to the paired channel and carry out an attack

Long range wireless channels

- Telematics connectivity
- Using combined vulnerabilities between the gateway and the authentication attackers were able to gain access through the telematics unit and carry out an attack
- Gateway can be attacked using a buffer overflow attack due to discrepancies between expected packet size
- Authentication can be bypassed by initiating 128 calls
- Attack can also occur by calling the vehicle and playing a “song”

Conclusion

- Cars I/O interfaces are alarmingly open to unsolicited communication creating unnecessary attack surfaces
- Appears code bases for automobiles do not employ same secure coding methods as other software systems
- Research showed almost all vulnerabilities existed in interface boundaries
- More research is necessary

References

Comprehensive Experimental Analyses of Automotive Attack Surfaces. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. In UsenixSecurity'11

Comprehensive Experimental Analyses of Automotive Attack Surfaces.

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno.

In UsenixSecurity'11

Paper Discussion

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

- The paper "Comprehensive Experimental Analyses of Automotive Attack Surfaces" discusses and elaborates on how easily attack or compromise the security of a car and the real threats which one can possibly face from the exploits. The paper also gives some ways in which we can fix the flaws and improve the security till there is a overhaul in the whole system.

- The paper shows various ways in which a attacker can access the system by dividing the threat model based on the distance from the vehicle. The paper denotes three ways of accessing without having physical access to the system and they are Indirect Physical Access, Short Range Physical Access and Long Range Wireless Access.

- In Indirect Physical Access, the authors exploit OBD-II which is federally mandated by the U.S government and this provides direct access to CAN buses. The author uses a laptop with 'PassThru' device(mostly via USB or WiFi) to gain access to the OBD-II port. We can compromise the whole system this way and can possibly infect other PassThru devices nearby by writing a worm to infect other systems. The author also tells how by using a malicious CD or iPod we can infect the media unit and then slowly work our way in compromising the whole system

- The Short Range Attacks are though complex and lack accuracy, there are wide range of exploits to be used like the Bluetooth, Remote Key Entry, Tire Pressure Monitoring Systems(TPMS), RFID tags and also Wifi Hotspots in the car. The most preferred being Bluetooth, the authors discuss 2 ways: 'Indirect' way where the vulnerability can be exploited by using a Paired Bluetooth Device, or the 'Direct" way where the attacker needs to know the Bluetooth MAC address and also the secret shared key which allows access to the Bluetooth pairing. This process is very long and also needs the car to be running all the time which is highly unlikely.

- The Long Range Attack is the most convinent one and most dangerous as it can be done through the access of cellular capable device on the car and this can be done from anywhere without any physical distance constraint. The manufacures use Airbiquity's aqLink software modem to covert between analog waveforms and digital bits and synthesizing a digital channel. The authors reverse engineer the aqLink protocol to gain access to the system. The authors also discovered a code parsing authentication response bug which blindly satisfies the authentication challenge after 128 calls and enables the exploit.

- The paper assess that Cyber War is a possibility where large number of cars are affected and are put in harms way. The main scenarios identified are Theft and Surveillance which would be really problematic. The authors suggest various ways in which the exploits can be fixed and strongly suggest an overhaul in the existing system from ground up to increase the safety.

Paper Discussion

- Zhenyu Ning
- CSC 6991 – Advanced Computer System Security

- The paper generally discusses the attack surfaces that may be leveraged while someone try to compromise a vehicle remotely and what could happen after the vehicle is exploited in that way.

- The attack channels are classified to 3 categories: indirect physical access, short-range wireless access and long-range wireless access. For each category, the author firstly lists some components that may be leveraged by the attacker, such as OBD-II port and CD player during indirect physical access, Bluetooth, RKE and RFID key cards in short-range wireless access and cellular channels in long-range wireless access.

- After that, some vulnerabilities in these components are analyzed. For example, a “crafted” WMA audio file may give the attack ability to execute arbitrary code, OBD-II could be used to achieve shell injection if the attach can connect into the same wireless network with PassThru devices, Bluetooth device in the vehicle could be connected after brute forced the PIN, the telematics unit could be made to download some additional payload after reset the call timeout with some complicated hack way. Through any of these compromised components, the attacker then can communicate with CAN to perform some malicious behaviors.

- Though some fixes and suggestion are given in the paper, it seems that the industry didn’t pay enough attention about there issues, as the attack we discussed in the last class used some similar approaches to achieve their target.

Paper Discussion

- Hitakshi Annayya

- The paper 'Comprehensive Experimental Analyses of Automotive Attack Surfaces' states modern automobiles provide several physical interfaces that either directly or indirectly access the car's internal networks. The paper talks about the four contributions. Firstly, **threat model characterization:** synthesize a set of possible external attack vectors as a function of the attacker's ability to deliver malicious input via: indirect physical access (CDs), short-range wireless access (Bluetooth), and long-range wireless access (cellular). OBD-II port provides direct access to the automobile's key CAN buses and can provide sufficient access to compromise the full range of automotive systems.
- Secondly, **analyzing the Vulnerability** on the attack surface, thus there were able to gain complete control over the vehicle's system. Thirdly, **threat assessment** talks about the real threats which creates practical risks by two means financially motivated theft and third-party surveillance. By simple to command a car to unlock its doors on demand, thus enabling theft. An attacker who has compromised our car's telematics unit can record data from the in-cabin microphone, to capture the location of the car and track where the driver goes. Lastly, **Synthesis** by finding out the loopholes in the "glue"code and software modem and also some pragmatic recommendations for future automotive security, as well as identify fundamental challenges.