To CEO

Security Operation Center

Global Comm

Jeep Hacking – Security Advisory

Summary

Researchers have found out the vulnerabilities in the smart systems in cars that can be exploited remotely. If exploited, attackers will be able to gain control over the car from the remote point. There are various attack vectors involved which makes its possible. There exist the common head unit in the car which communicates with both of the CAN Buses which are installed in the vehicle. The CAN buses are the interfaces which is used by the different micro-controllers and the devices to communicate with each other through CAN messages.

Through the attack vectors mentioned in the paper, attackers can have the access to the ECUs on both CAN-HIS and CAN-C networks. This would enable an attacker to control all the physical systems in the car which are connected to these ECUs. The network architecture of the car is designed in the way that almost all the physical attributes in the car are directly connected to these ECUs.

In the given case study, the head unit being used is a Uconnect System which is manufactured by the Harman Kardon. It controls and manages the infotainment system, Wi-Fi connectivity, navigation, apps and other cellular communications. It is comprised of QNX operating system running on the 32-bit ARM processor. It is also responsible for the managing the micro-controllers and softwares for communicating with CAN-IHS data bus and CAN-C networks. That's, why this head unit becomes the critical point for the study to find the vulnerabilities and exploit it.

Through this attack, attackers will be able to control many physical attributes of the car remotely. It becomes even easier when the attacks have the physical access to the car and can make much more damage. The impact includes code execution on the physical systems to control or the physical features of the car like music, gates, steering, display, speed or GPS.

Technical Details:

Network Architecture: The network Architecture of the car is such that there is one head unit which communicates with both of the CAN Buses: CAN-IHS and CAN-C networks. These Can buses are responsible for sending and receiving the CAN messages to/from ECUs which handles almost all the physical attributes of the car. Head Unit becomes most important for the vulnerability research on the cars with this type of architecture. Though there are several stages involved in the process to make head unit send and receive messages from the CAN Buses though the control of an attacker.

Uconnect Head Unit System: The head unit in this case study is Uconnect System. The system is manufactured by the Harman Kardon and serve as to the purpose to manage the infotainment system, navigation system, WI\i-Fi connectivity, apps and cellular communication. It is hardwired onto OMAP-DM3730 chip with the operating system QNX running on the 32-bit ARM processor. It is responsible for managing the micro-controller and software communicates with ECUs in the vehicle. But, still there is no direct communication from the head unit to CAN Buses. The CAN communications are handled by the Renesas v850ES/FJ3 chip.

The Potential attack entry points are:

1. **PATS(Passive Anti-Theft System):** Not critical as exploiting this attack surface is difficult. The sensors generate RFHM signal to transponder which in returns send another RFHM signal to computer for confirmation to start the engine.
2. **TPMS:** Not critical. Attack surface is small. Transmitts real time data to ECU for the pressure on the tire. Remote bricking is possible by crashing the ECU completely.
3. **Bluetooth:** Bluetooth is managed by the head unit and the signals are received and sent by this unit itself. All the things of the user are in sync through the Bluetooth. Two attack scenarios are possible: after pairing device or before pairing a device. This a large attack surface and in the past researchers have already shown the compromise using Bluetooth.
4. **Radio Data System:** A built in system used not only to send and receive audio signals from the radio stations but also send and receive data. There must be some mechanism to read and parse this data. Thus, making it a potential attack surface for security vulnerability.
5. **Wi-Fi:** It's a paying service. We assume that the target has it. Accessible from the Uconnect Interface.
    a. WPA2 Encryption: Randomly generated password is being used. Hard to brute force. Not practical. But looking that WiFiSVc binary file, attacker can figure out the algorithm being used to generate the random password. In this case study, it is found that random password is generated from the epoch time function(). It was found out by the attackers that it is practically possible to brute force.
    b. WEP or no encryption: Very easy to compromise. Not a big problem for an attacker.

   c. Compromise the user device which uses the WiFi hotspot of car and then too many pre-requisites to take in consideration.

6. **Telematics/Internet/Apps**: This serves as a very large attack surface as it contains a cellular radio which connects to the cellular networkof the car. There must be some way these communicates with the CAN buses, if not directly, maybe through some other interaction. That's where the Head unit UConnect comes in.
7. **USB Stick Attack:** Valid for any version of the head unit. While updating the system through the USB stick the system reboots and ISO is responsible for the verification and integrity check of the USB. But the bug in the Version 14_05_03 allows an attacker to bypass the verification process from ISO.
   a. Update Mode: running malicious code during update mode, achieves the persistence of the attack across the reboot cycle of vehicle.
   b. Normal Mode: Altering boot.sh allows an attacker to run code and cmds.sh file can give SSH back for remote control.
8. **D-Bus Services:** Provides inter-process communication and remote procedure call mechanism for communication between processes. Two types of buses are involve din the D-Bus: System Bus(daemons and registers) and session Bus (user applications). It requires authentication but set to anonymous from the head unit.

   There are many services thatrun under D-Bus Service but the most important from the vulnerability standpoint is NavTrailService. It was found out that the command injection vulnerability exists in 'rmTrack' method. The service also provides another method "execute" which facilitates the command injection vulnerability. Thus, it is very easy to execute any code as a root on the head unit.

9. **Cellular Exploitation:** The above presented attack vectors requires some kind of physical access. Among all the network interfaces of the Uconnect, there is a ppp0 interface for cellular communication with outside world through Sprint's 3G services. Using a Airwave Femtocell, it is possible to ping the Jeep and communicate with D-Bus over cellular network through Telnet. This is a remote exploit with good range.
10. **Renesas V850 processor:** This is the processor which is mainly responsible for the communication between the head unit and the CAN Buses. The type of communctaion is reffered as IOC. It has three modes: bootloader Mode, application mode and bootloader updater mode.
    a. Researchers tried to reprogram the application firmware of the IOC so that it could modify the program in a way which accepts and forwards the command to the CAN buses. Took them a while but they figured out a way to do that.
    b. SPI Communication: Serial peripheral Interface used for communication between the OMAP chip and V850 processor. If we can modify the firmware, as already done by the researchers, there are any ways to send CAN data from the OMAP chip but the safest and easiest way is the SIP messages.

Lacking points of Vulnerable Controls:

There is always a trade-off between providing the more rich user experience and the security measures. In this case study we have seen some of the examples proving the former statement true. The controls that left the Jeep vulnerable can be:

1. Cellular Communication: The communication with the outside world though sprint service enables an attacker to attack remotely. Use more secure cellular communication.

2. USB Stick attack is possible because of the vulnerability in the ISO service. So, in a way the flaw in the updating system of Uconnect system can expose to the jeep to serious attacks. Update the system and use the updated version of the ISO.
3. Segmentation of the network architecture should be there to avoid exposing the physical access of controls like steering to either of the CAN Buses.
4. Since the device is connected to the internet, a simple scan can show all the vulnerable vehicles. Attackers were able to achieve that. Avoid using default ports for the D-Bus.

Remediation and Mitigation at hand:

1. Unsubscribe the Wi-Fi Service if using.
2. Look for valid and trusted sources for the software updates.
3. Block the open port 6667 and any traffic coming on this port through cellular tower.
4. Put filters on the CAN messages and provide a way to correctly verify the source of these messages.
5. Integrity checking should be done
6. Segmented Updates: update the system and the devices in different phases.

References:

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