the Availability Digest

www.availabilitydigest.com
@availabilitydig

My Jeep Wasn't Hacked!

August 2015

Jeeps are being hacked! A pair of security researchers has demonstrated remote control of a Jeep by turning on its air conditioner and its radio, activating its windshield wipers, and putting it in neutral while it is moving. They also can disable the brakes and control the steering and the accelerator. Fortunately, my Jeep is not one of those affected – it is just a couple of years too old.

In a recent *Availability Digest* article,[1] we described a security researcher who was able to access a plane's flight controls via the in-flight entertainment system in the cabin. It turns out that the cabin Intranet network and the flight-control avionics Intranet network were linked by a firewall, which he was able to breach.

Now this malicious technology has been extended to automobiles. Security researchers have demonstrated that they can take control of a car's computers by accessing them via the car's infotainment (information and entertainment) center using a cell phone from hundreds of miles away. The infotainment center's Intranet and the Intranet connecting the car's computers are separated only by a firewall, which they were able to breach.

The Jeep Grand Cherokee Hack

Chris Valasek and Charlie Miller have spent several years developing their car-hacking abilities. Today's cars often contain over fifty computers running 50 million lines of code. The hacker's attack relies on the car's infotainment center that controls the car's radio, music, navigation, and telephone capabilities. The elements of the infotainment center are interconnected by an Intranet. This is the same Intranet that is used by the car's computers to communicate, though the Intranets of the infotainment system and the car's computers are separated by a firewall.

The researchers focused particularly on the Uconnect entertainment system used by Fiat Chrysler in hundreds of thousands of their automobiles. After studying mechanical diagrams of a number of cars, they settled on Jeep Grand Cherokees as a particularly vulnerable vehicle.

Uconnect receives information over Sprint's 3G network. Uconnect controls the vehicle's entertainment and GPS navigation systems. It enables phone calls and even offers a Wi-Fi hot spot. It allows control of all of these services by voice commands.

The Uconnect cellular connection to Sprint allows anyone who knows the car's IP address to gain access to the vehicle from anywhere in the country. The hackers were able to communicate with the Uconnect system via a 3G cell phone. They discovered a service in Uconnect that enabled them to exploit a vulnerability that let them put their code into the firmware of the entertainment system.

[1] Can An Airliner Be Hacked? *Availability Digest*; May 2015.
http://www.availabilitydigest.com/digests/v10_i05/1005_digest.htm#Can_An_Airliner_Be_Hacked

From there, Valasek and Miller were able to communicate with and reprogram another chip that was responsible for in-vehicle communications. They could then forge messages and send them to the car to cause its computers to execute any number of actions. They could interact with the engine, steering, transmission, or braking systems. They could control the air conditioner, the windshield wipers, the turn signals, and the radio. In short, they could control the car from hundreds of miles away with a cell phone.

Of course, to do this, they needed to know the IP address of the car. To address this challenge, they created a laptop program that can scan Sprint's 3G network for cars with Uconnect systems. They realized that they could identify cars with a Uconnect system anywhere in the country. They could read a car's GPS coordinates, its vehicle identification number, its make and model, and its IP address. With this information, they could select a car and control it.

A Wild Ride

To demonstrate that their work was real, Valasek and Miller subjected a journalist from Wired magazine to a wild ride (see the article referenced below and entitled "Hackers Remotely Kill a Jeep on the Highway – With Me In It").

They let him drive a Jeep down a local highway. All of a sudden, without his touching the dashboard, cold air started blasting from the air-conditioning vents. The radio started playing, and the windshield wipers switched on. The journalist couldn't control any of this. His transmission then went into neutral and he coasted to a stop.

He was able to recover only by switching off the engine and restarting. This reset the computers.

Working with the Manufacturers

Valasek and Miller worked closely with Fiat Chrysler while they were perfecting their hacking technique. They also involved other manufacturers by sending them questionnaires about their security practices. Of the sixteen automakers who responded, all confirmed that virtually all of their vehicles have some sort of wireless connection. Only seven of the companies said they hired independent security firms to test their vehicles' digital security. Only two said that their vehicles had monitoring systems that checked their computer networks for malicious digital commands.

Chrysler's Recall

In response to this vulnerability, Fiat Chrysler has issued a safety recall affecting 1.4 million vehicles in the United States. It issued a statement saying that exploiting the flaw "required unique and extensive technical knowledge, prolonged access to a subject vehicle and extended periods of time to write code." They declared any such attack to be a criminal action.

The affected vehicles are generally two to three years old and include:

- 2013-2015 MY Dodge Viper specialty vehicles
- 2013-2015 Ram 1500, 2500, and 3500 pickups
- 2013-2015 Ram 3500, 4500, and 5500 Chassis Cabs
- 2014-2015 Jeep Grand Cherokee and Cherokee SUVs
- 2014-2015 Dodge Durango SUVs
- 2015 MY Chrysler 200, Chrysler 300, and Dodge Charger sedans
- 2015 Dodge Challenger sports coupes

The safety upgrade requires the installation of new code via a USB that must be installed by a dealer.

Chrysler Fined for Inadequate Recalls

This is not the first recall by Fiat Chrysler. In fact, the U.S. National Highway Traffic Safety Administration (NHTSA) has criticized the company for its handling of 23 recalls involving 11 million vehicles. It points to shortcomings in reporting defects and in inadequate recall procedures. As a consequence, Fiat Chrysler has been fined USD $105 million.

The company has acknowledged violations of the Motor Vehicle Safety Act's requirements to repair safety defects, and it has agreed to submit to rigorous federal oversight. The fine could be reduced if the company shows good faith in correcting its recall issues.

Summary

The NHTSA is trying to determine how many car makers have received wireless components from the same company that supplied Fiat Chrysler with Uconnect. They are making tests to determine how wide this vulnerability might be.

Furthermore, many other infotainment systems currently in use might present a similar vulnerability. Among them are GM Onstar, Lexus Enform, Toyota Safety Connect, Hyundai Bluelink, and Infiniti Connection.

Two U.S. senators have introduced a bill in Congress to call on the U.S. Federal Trade Commission and the NHTSA to set standards on vehicle safety. Included would be a security rating system for cars so consumers would know which ones worked the hardest to make unhackable automobiles.

Of course, the ultimate protection is to drop the use of the firewall and to use an air gap instead. Provide two Intranets, one for the infotainment system and one for the vehicles' computers, that have no common connection.

Acknowledgements

Information for this article came from the following sources:

Jeep hacker explains why he did it, *BBC*; July 13, 2015.
Hackers Remotely Kill a Jeep on the Highway – With Me In It, *Wired*; July 21, 2015.
Car hack used digital-radio broadcasts to seize control, *BBC*; July 22, 2015.
Fiat Chrysler recalls 1.4 million cars after Jeep hack, *BBC*; July 24, 2015.
Car hackers use laptop to control standard car, *BBC*; July 26, 2015.
Chrysler is fined record $105M, *USA Today*; July 27, 2015.
Car hacking risk may be broader than Fiat Chrysler – U.S. regulator, *Yahoo Finance*; July 31, 2015.