SecurityInnovation®

THE NEXT CYBERSECURITY TARGET: Connected Cars

Suddenly, **the vehicle starts accelerating unexpectedly...** The windshield wipers are going off. **The brakes won't work...**You watch as you zoom by other vehicles, hoping you avoid a major collision...

Picture yourself driving along the highway in your brand new car...

Scary, right? Unfortunately, with connected cars becoming more popular among drivers, a scenario such as this one can become a reality for anyone.

With over 50 percent of vehicles sold in the United States in 2014 considered "connected," hackers are turning to vehicles as another form of cybercrime. Gartner predicts a quarter of a billion connected vehicles will be on our roads by the year 2020.

While these connected cars boast of convenient features like blind spot detection, backup sensors, collision avoidance, and voice-activated and handsfree controls, the addition of these features allow hackers another way to take control and access your vehicle data in a number of different ways, leaving drivers to wonder, "*How safe am I using a connected car?*"

AN FAQ ON CONNECTED CAR SECURITY

What is a Connected Car?

Let's start with the basics. The term "connected car" has become a recent buzzword in the media. **A connected car is a car equipped with internet access and usually also with a wireless local area network.** This access allows cars to "talk" with both the driver and other cars surrounding the vehicle. For example, cars with bluetooth capabilities are considered connected vehicles because they use a wireless connection to connect a device to the vehicle. Vehicles with internet radio, navigation, and automotive system diagnostics are also considered connected vehicles and are features many new cars now have.

How Are Hackers Attacking Cars?

Just as a computer connected to the internet can be hacked, so can a vehicle. **In July 2015, hackers remotely cut the transmission of a Jeep on the highway using a smartphone and laptop.** A recent hack shows a $60 laser setup can disable a selfdriving car.[1] Thieves are also controlling radio signals to unlock cars using keyless entry systems. **Attacks do not necessarily need to be malicious and overtake the vehicle. More commonly, hackers could use the navigation system to track where the driver has been and activate the built in microphone to record any conversations.**

What Information is Currently Being Collected from Connected Cars?

Most drivers today are unaware that companies—including automakers, insurance providers, and third party suppliers—are currently collecting data on their driving habits and vehicle performance. Who can access this data is governed by privacy law and the policies of the individual company collecting data. **The data is used to aggregate information about consumers** and provide remarkably accurate predictions of behavior, allowing corporations to categorize individuals by behavioral profile and target them for specific marketing purposes.

How Safe am I in a Connected Vehicle?

Unfortunately, there is little a driver can do at this point in time to protect themselves from being hacked, and there is no reliable way to know whether your vehicle has been hacked. Consumers must rely on automakers to ensure they are doing all they can to provide a safe and secure vehicle. **Consumers can, however, keep an eye out for news on recalls and make sure their vehicle software is up to date.** Also, stay aware of the different wireless networks within the car and what they do. Although little can be done to prevent an attack, **many attacks today are not meant to harm the driver, but are more commonly for spying on and stealing vehicles.**

What Changes are Happening to Make Connected Cars More Secure?

In response to recent news and concerns surrounding connected cars, Senators Ed Markey (D Mass) and Richard Blumenthal (D Conn) established the **SPY Car Act of 2015**, requiring automakers to take vehicle security more seriously.[2] **This Act requires automakers to equip cars with technology that can detect, report, and stop hacking attempts in real time and to have these vehicles fully secure by 2018.**

What are Some of the Challenges Regarding Connected Car Security?

Two of the biggest challenges for automakers are time and resources. With all vehicles needing to comply with the SPY Car Act by 2018, this leaves little time to fully develop and test working solutions. **Technology is constantly changing, and automakers won't be able to reach their objectives and comply with security standards without the help from security partners.** Automakers will also need to work with their partners to solve challenges such as the best way to connect cars to the web, who will pay for connected car services, how will apps integrate within cars, and, eventually, what happens with selfdriving vehicles.

Automakers have been challenged with the task of making a fully secure connected vehicle to keep drivers safe on the road and protect their privacy. Vehicles are designed with driver and passenger safety as a key concern; however, without proper security, there cannot be safety. **The hacker needs to be right only once; automakers need to be right 100% of the time.**

1. http://www.bbc.com/news/technology34185372
2. http://web.securityinnovation.com/automakerspassivecybersecuritywhitepaper