digitalcitizens alliance

A DIGITAL CITIZENS ALLIANCE REPORT
BY GARTH BRUEN

OUT OF CONTROL: THE THREAT OF CAR HACKING

HOW CYBERCRIMINALS CAN TARGET DRIVERS

OUT OF CONTROL: THE THREAT OF CAR HACKING

To many Americans, automobiles are a critical component of daily life. Taking the keys to your first car is a huge step toward personal and financial independence. Getting into the driver's seat, people can't help but dream of open highway, traveling from coast to coast. Many stylize their cars' chassis to reflect their personalities. Others enjoy the sanctuary they find inside – privately listening to music from Britney Spears, commentary on NPR, or anything a friend or family member might not normally allow them to enjoy.

However, we must accept that the same technology that has made cars safer, faster, and more pleasurable also poses a threat. Cars can now contain dozens of processors depending on how expensive or recent the car. In general, any car built in the last ten years has a computer in it. This has opened the door to cyber-attacks on automobiles which is the one place many people feel in control. While there are virtually no proven examples of an attack in the real world, it is not farfetched or unfounded. The University of Washington has created a special Center for Automotive Embedded Systems Security[1] (CAESS) which is studying these threats. Researchers at the center have tested a number of attacks on car systems successfully taking control over them. Their overall goal is to study these vulnerabilities to protect against them.

Controversial journalist Michael Hastings died in a fiery car wreck after making comments about a big story he was working on.[2] It is entirely possible the accident was due to driving too fast late at night, but conspiracy theorists have speculated

[1] http://autosec.org/index.html

[2] http://nym.ag/1cQX3IM

RPM

that Hastings may have been a car hacking victim.[3] The arguments in some corners about Hastings's death will go on, but there is no debate that some hackers have the knowledge and skill to infiltrate a car's computer and take control of the vehicle.

What do car computers do?

Most of the devices included in cars are harmless in terms of hacking. These computers are completely passive, informational devices measuring the output of performance sensors and converting the analog data from these sensors to digital. For example, embedded sensors measure fumes inside the car to comply with emissions standards, regulating the catalytic converter, which modifies the fumes inside the car before it goes into the air. Besides gas and oil, cars use a variety of chemicals which need tracking, some benign and others vital. The computers also make mechanic diagnostics much easier by collecting information about component performance. The only conceivable hacking threat for these components is in their potential misreading or faulty diagnostic which would fail to note a serious problem. Less harmful, but still a concern for hacking is the issue of the computer data being used to violate ones privacy. So-called black boxes record everywhere the car goes and how fast it travels. Built-in phone conversations can be intercepted or simply have the microphone activated to passively listen to conversations in the car. There is even a more annoying possibility of advertisers remotely scanning diagnostic data and sending spam to your phone, GPS output or even the radio Truman-show-style. "YOU NEED NEW TIRES! PULL OFF EXIT 24 AND COME TO OUR SHOP!" Laugh now, but if someone can figure out how to do it, they will. "WE SEE YOU STOPPED AT BURGER KING YESTERDAY. THERE IS A BETTER BURGER 2 MILES UP ON THE LEFT." However, this type of situation is not the focus of our concern.

[3] http://huff.to/1ji2vty

What computers are of concern?

Any processors which regulate the speed, steering or breaking of the car are what we are worried about. Taking remote control over a car may seem like science fiction, but it has already become trivial and normal. Consider that standard auto security and navigational systems are equipped with remote engine termination. If a car is stolen or is otherwise out of the owner's control, the police may shut off the engine with a special code. Stopping an engine while in hot pursuit has become a routine part of the law enforcement tool kit. Now, consider this procedure is imbedded in the car system itself and is accessed from outside the car. Think about basic remote control for unlocking, engine starting, and temperature control. Technology added for convenience can be a pathway for malicious activity. Car and Driver, a magazine not known for conspiracy theories, has reported on the ability to infect a car computer through the MP3 player[4] and maybe even WIFI if the device is enabled to accept this input. Controlling the car is possible through the common Controller Area Network (CAN) in all modern vehicles which allows messaging between different components. Because the sound system is connected to the CAN it is ultimately connected to the brakes, cruise control, passive restraints (airbags), steering, power windows, locks, etc. CAN has no security built into it, rather security is expected to be deployed in the systems that access it. Because of the number of potential sources for car parts, it is easier for the CAN to be passive, meaning it does not dictate how instructions are fed to it. The CAN does not inherently concern itself with where instructions are coming from; rather it depends on the other devices sending correct data. The simplicity of the design is for practical purposes but it makes rogue instructions easier to deliver.

[4] http://caranddriver.com/features/can-your-car-be-hacked-feature

180
200
220
240
260
280
300
320
340
360
400
km/h
20
0

Is the threat serious?

Car and Driver references the work of CAESS who try to allay public fears by saying that car hacking is not easy, requiring lots of effort and technical knowledge. Each make and model is slightly different so attackers must have detailed knowledge of a specific vehicle. However, the idea that car hacking is difficult should not make us feel safe for long since this was the same situation with remote PC hacking at one time. Downloadable malware and intrusion kits made hacking available to people who knew nothing about systems engineering. Hacking kits for computers and other devices are already sold on the dark web. Deployable car hacking modules will appear sooner or later extending these complex attacks to any reckless moron. The scenarios generally discussed focus on specific targeting of an individual's car to make a murder "look like an accident" in the time-old vernacular.

The attack could be as subtle as flashing high-beams on another driver at an inconvenient moment or as specific as revving the engine to run the other car into a spin. The attacker does not have to control the entire car, just make certain functions fail.

So what can consumers do?

This is a tough one. Cars and car purchases are already complex enough. One thing consumers can be sure of is that manufactures and dealerships invest considerable time and money into ensuring that drivers feel safe. The last thing they will allow to happen is a lingering fear of car hacking. Manufactures are taking heed of these stories and engaging the experts for protections. The government also pours enforcement in this area because of the automobile's importance in interstate commerce. However, it is still up to the car owner to stay informed. Ironically, drivers seem to know less and less about how an automobile works as this threat grows. This is directly attributable to the technology as do-it-yourself car maintenance is made more complex by these embedded computers. Regardless consumers need to stay informed and, believe it or not, ask about cybersecurity when they buy a new car. But consider this a new bargaining chip when negotiating price, if the dealer can't guarantee some level of protection go somewhere else. Unfortunately, consumers will also have to take more care of who and what interfaces with their car. Since researchers have indicated that an exploit could be embedded in a compact disk or USB drive.[5] Who your keys are loaned to now has an additional concern. As if we were not already paranoid enough.

[5] http://onforb.es/19MPsXj

digitalcitizens alliance

www.digitalcitizensalliance.org