From Car Jacking to Car Hacking

Peter Silva, 2012-23-08

With the promise of self-driving cars just around the corner of the next decade and with researchers already able to remotely apply the brakes and listen to conversations, a new security threat vector is emerging. Computers in cars have been around for a while and today with as many as 50 microprocessors, it controls engine emissions, fuel injectors, spark plugs, anti-lock brakes, cruise control, idle speed, air bags and more recently, navigation systems, satellite radio, climate control, keyless entry, and much more.

In 2010, a former employee of Texas Auto Center hacked into the dealer's computer system and remotely activated the vehicle-immobilization system which engaged the horn and disabled the ignition system of around 100 cars. In many cases, the only way to stop the horns (going off in the middle of the night) was to disconnect the battery. Initially, the organization dismissed it as a mechanical failure but when they started getting calls from customers, they knew something was wrong. This particular web based system was used to get the attention of those who were late on payments but obviously, it was used for something completely different. After a quick investigation, police were able to arrest the man and charge him with unauthorized use of a computer system.

University of California - San Diego researchers, in 2011, published a report (pdf) identifying numerous attack vectors like CD radios, Bluetooth (we already knew that) and cellular radio as potential targets. In addition, there are concerns that, in theory, a malicious individual could disable the vehicle or re-route GPS signals putting transportation (fleet, delivery, rental, law enforcement) employees and customers at risk. Many of these electronic control units (ECUs) can connect to each other and the internet and so they are vulnerable to the same internet dangers like malware, trojans and even DoS attacks. Those with physical access to your vehicle like mechanics, valets or others can access the On-Board Diagnostic System (OBD-II) usually located right under the dash. Plug in, and upload your favorite car virus. Tests have shown that if you can infect the diagnostics tools at a dealership, when cars were connected to the system, they were also infected. Once infected, the car would contact the researcher's servers asking for more instructions. At that point, they could activate the brakes, disable the car and even listen to conversations in the car. Imagine driving down a highway, hearing a voice over the speakers and then someone remotely explodes your airbags. They've also been able to insert a CD with a malicious file to compromise a radio vulnerability.

Most experts agree that right now, it is not something to overly worry about since many of the previously compromised systems are after-market equipment, it takes a lot of time/money and car manufactures are already looking into protection mechanisms. But as I'm thinking about current trends like BYOD, it is not far fetched to imagine a time when your car is VPN'd to the corporate network and you are able to access sensitive info right from the navigation/entertainment/climate control/etc screen. Many new cars today have USB ports that recognize your mobile device as an AUX and allow you to talk, play music and other mobile activities right through the car's system. I'm sure within the next 5 years (or sooner), someone will distribute a malicious mobile app that will infect the vehicle as soon as you connect the USB.

Suddenly, buying that ‘84 rust bucket of a Corvette that my neighbor is selling doesn’t seem like that bad of an idea even with all the C4 issues.

ps

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com