Cyber threats targeting your car

Who's really driving your car?

Increasing automotive autonomy means increasing risks that your car could be hacked.

By: Eric Tegler on 10/15/2013

There has been a mass-casualty terror attack in Washington, D.C.

Asophisticated, well-funded threat actor has executed the attack. Lives have been lost and more hang in the balance. The pandemonium has been heightened by the force-multiplier used. Hundreds of cars in downtown D.C. made a left turn at the same moment without their drivers turning the wheel. There are numerous accidents. Drivers and pedestrians have been hurt or killed. Vital access routes are blocked. First-responder vehicles can't get through and many refuse to start. It is a grim scene.

The above scenario is highly unlikely. It's also possible. It has been war-gamed. The cars we drive have vulnerabilities. They can be taken from our control remotely. This isn't theory—it's been done.

Related Articles

2013 Mercedes-Benz SL63 AMG review notes

Infiniti planning new global flagship model

Renderings hint at 2015 Ford Mustang appearance

Aston Martin eyes Lagonda comeback

Hackers compromise Prius, seize control of wheel, brakes and more

VW's new modular platform could spark a revolution

Shopping for a **NEW** or **USED VEHICLE**?
Click here to **START YOUR SEARCH.**

Autoweek reader Rodney Joffe brought the issue to our attention after reading a story we wrote on autonomous cars and driving. Joffe is senior VP and technologist at Neustar Inc., a Washington D.C.-based IT firm providing real-time analysis and security services to Fortune 500 companies and federal agencies. Joffe is also one of the commercial Internet's 23 founders and one of a few hundred people watching over Internet security globally. He's also a car guy and he's concerned.

Joffe and a small group, including Dr. Stefan Savage of the Center for Automotive Embedded Systems Security (University of California San Diego/University of Washington), quietly carried out a series of cyber-threat exercises for the Obama Administration. The Department of Homeland Security runs “Cyber Storm” exercises, but Joffe's were different: His included cyber attacks on vehicles.

For example, Joffe and his group demonstrated their ability to unlock, start and drive away a vehicle—from 1,200 miles away. They controlled the car's throttle, brakes and steering. They couldn't guide the vehicle around obstacles but they could take away from the driver control of its steering and systems. They say they can take throttle and brake control away from the driver on 1998 or later cars equipped with OBD-II. Steering can be controlled/disabled on vehicles with autonomous lane-correction or self-parking systems. From dealer service centers to EV charging stations to supplier black boxes to systems inside the automobiles themselves, opportunities to hack your car—and many other cars—exist.

OTHER RECENT ARTICLES


Inside the President's armored limo


2013 Lamborghini Gallardo LP560-2 50th Anniversario Edition drive review


Found on eBay: 1980 Toyota Corolla Tercel


One Lap of the Web: Ferrari renders, Musk is a super villain and '50s Fiat commercials


Anki Drive combines artificial intelligence, remote control and video gaming

POLL OF THE WEEK

Which alternative fuel tech do you think has the most pr

- ◯ Plug-in hybrid
- ◯ Pure EV
- ◯ Hydrogen fuel cell
- ◯ Gas/electric hybrid
- ◯ Diesel/electric hybrid

VOTE

Five presentations on automotive hacking were presented during the August DEF CON Hacking Conference in Las Vegas. While the issue is just beginning to be publicly discussed, governments and automakers have been aware of, and sensitive to it, for years. In fact, a late-July injunction in a U.K. court barred British and Dutch academics from publishing a paper revealing secret codes to bypass the security on vehicles including Porsches and Bentleys. The injunction was sought by Volkswagen.

We attempted to speak with the automakers with limited success. Beyond formal counsel-approved statements, they decline to discuss hacking. Insiders, including a senior IT executive at Ford, say many of the most spectacular mass-hacking scenarios are improbable. They point out that automakers are investing considerable resources to address the problem—hiring IT security staff and working with bodies such as the Society of Automotive Engineers to establish standards to combat cyber intrusions. Still, not one of the original equipment manufacturers (OEMs) we contacted (Ford, General Motors, Chrysler, Toyota, Mercedes-Benz, Nissan and Volkswagen) would agree to an on-the-record interview. Perhaps that speaks for itself. Even supposedly tech-forward Tesla refused to comment.

The reasons have to do with liability, of course, but also the degrees to which each manufacturer has internalized the issue, the absence of a regulatory framework and the scope of the problem.

Professor Savage estimates a modern vehicle has a dozen points open to hacking. They range from Wi-Fi systems and downloadable apps to USB- and SIM-card ports. New radio-enabled collision-avoidance systems in development could be vulnerable and electric-vehicle fast-charging stations already are. There's even an audio file that can corrupt your ECU.

“Everyone has telematics as central to their vehicle plans, positioning their cars to be computing platforms,” Savage adds. “That creates more opportunity.”

Much of this is old news to those who work in IT security both inside and outside the OEMs. The vulnerability of telematic systems like GM's OnStar, for example, was highlighted years ago. Access to OnStar didn't require initial hacking, just identification of each equipped car's OnStar telephone number. That flaw is supposedly fixed.

Safeguards on how apps can interact with ECUs are in place, according to manufacturer sources. Still, informed observers contend they are only as good as the firewalls isolating them and the assumptions of their design. Like their counterparts in the broader IT world, auto manufacturers are playing “whack a mole” with every new tech twist.

For example, there are 16-pin OBD-II ports in every car made from 1996 on. Among the presentations at DEF CON, IOActive researcher Charlie Miller showed “how certain proprietary messages can be replayed by a device hooked to an OBD-II connection to perform critical car functionality, such as braking and steering.”

Devices connecting your OBD-II port are available to everyone and range from code readers to ECU monitors/tuners to portable GPS timers. Insurance companies offer discounts to drivers who will share data via their data-loggers. All of these devices can be hacked and implanted with “proprietary messages” or bugs. Pick a device, hack it, develop an exploit of the dealer service system it connects to, load your malware (malicious software) onto your car's ECU and drive it to the dealer for service. Once a tech plugs in a scan tool or laptop and downloads data, his devices can be contaminated and every successive vehicle that uses those devices gets the worm.

Then, if the same devices connect to an OEM tech website via the Internet (say, to look up a part number or download software updates), that portal is potentially infected. Implanted bugs can be set to go off like time bombs. Months after a dealership is compromised, all the infected cars that have been through could be commanded to simultaneously shut down or speed up at an appointed date and time.

Proximity is not needed to spread malware. Dealer systems can potentially be affected via their wireless local networks. Manufacturer Web portals providing information and software updates can be hacked. Access to compromised computers within the OEMs and their suppliers (also Fortune 500 firms and the government) can be purchased on the Internet black market.

Know that the above avenues are truly difficult to exploit, and manufacturers have been (and are) working hard and as quickly as possible to close them. While no one can guarantee secure systems inside or outside the auto industry, another source maintains the OEMs “have got the security religion.”

They also have weighty commercial partnerships. Ford and Toyota have partnered with Microsoft for their in-vehicle systems. Ford uses programmers to write apps for its Microsoft-based SYNC system. Microsoft's platform is undoubtedly cost effective but also perhaps the most frequently hacked in the world. As Joffe puts it, “There are zero-day exploits [attacks] in Windows every day. They are patched, but when was the last time you saw someone patching your ECU?”

Manufacturers are quietly doing just that as part of routine maintenance in dealerships. Still, they will need new recall/software update strategies. Earlier this year Ford released an update to owners with the SYNC system via 30,000 USB sticks, encouraging them to have a unique, non-password protected USB for each Ford they own. The update was downloadable online, as well.

That could be a risky proposition, but not more than the security flaws emanating from software/hardware that OEM vendors provide. That's because automakers buy an array of subsystems and have varying degrees of quality and security.

“All of the vulnerabilities we found,” says Savage, “were precisely at the intersection of code written by different vendors. That's what we were always able to exploit.”

Countermeasures are difficult to apply, he says, because OEMs often have no access to vendor source code. In

fact, a semi-adversarial relationship exists: Suppliers are concerned about giving away intellectual property and/or having OEMs take their competencies in-house. “Figuring out how to embed security into the contract language which goes with this is a big challenge,” Savage adds.

Embedding vehicle security is the business of Escrypt, a subsidiary of German electronics firm Bosch. Many view Europe's auto sector as having an edge in combating hacking, and Escrypt is regarded as a leader. The firm's Dr. Marko Wolf agrees that standardizing vendor/OEM software/hardware at the interface/design junction is critical to securing in-vehicle systems.

Based on probability and the media hysteria it would generate, a successful single cyber attack with a minor safety impact is of greater concern to Escrypt than a large-scale attack. Escrypt views smartphone and Wi-Fi interfaces as the most vulnerable access points for exploits, including personal data theft and the stealing of subscriber services.

But Wolf cautions: Car-control takeover cannot be precluded. He points to a potential example Americans seem unwilling to discuss, the case of Rolling Stone journalist Michael Hastings, who died in a fiery accident in June (reportedly in a new Mercedes C250). Some theorize a cyber attack caused the accident.

The National Highway Traffic Safety Administration does not share that view. NHTSA would only discuss vehicle hacking briefly on background and referred to a statement it issued in late July. The agency says it “is not aware of any consumer incidents where any vehicle-control system has been hacked.”

NHTSA has established an Electronic Systems Safety Division to focus on electronics, automated vehicles and cyber security. It maintains that months of physical proximity to a vehicle are needed to access its vehicle-control functions. Further, it asserts it has not seen a case in which vehicle control can be exploited via Bluetooth or wirelessly without extended physical access.

The Department of Homeland Security is actively working on the problem within its National Cyber Security Division. It refuses to comment. Like automakers, Uncle Sam has legitimate concerns about discussing cyber threats publicly. Devising a regulatory response will be difficult. Bottom line: Malicious vehicle hacking is now a public issue. So overall, how concerned should we really be? “This stuff is feasible,” Savage allows. “Do I think the average driver should worry that their car might be taken over? I'd say, over the next five years, this would not be high on my list of things to worry about. Longer term, it would be on my list.”

The most likely, if improbable, large-scale attacks are analogous to the Distributed Denial of Service (DDoS) attacks common on the Internet, Savage agrees.

“Making something not work is a hell of a lot easier than making it work in a particular way. … Controlling a car requires substantial investment. On the other hand, I can completely see some group of hackers thinking it would be funny to disable all the Mercedes in San Francisco.”

Joffe worries more about an “inadvertent catastrophic event.” Young hackers could mount an exploit for fun, he notes, say flashing 500 cars' headlights in snyc with a song. Because they're experimenting, something can go wrong with the code. Likewise, a motivated, talented individual hacker with a random grudge could be a problem. Both risks have manifested themselves in the past, Joffe assures.

The potential of the car-hacking threat is roughly proportional to the interests and positions of the expert you ask. That threat is also continually evolving. Today, with industry leaders and the government mum, it's difficult to assess whether senior leadership really “gets it.”

Over the last few years, the phrase “war on cars” has been bandied about in cities from Seattle to Toronto to Boston, where bicycle/mass transit proposals clash with automotive interests. That could be a sideshow. The real war on cars is being fought through the software they run on; and we can't be completely sure who's driving.

Filed Under: