Technology | DOI:10.1145/2018396.2018403

Alex Wright

Hacking Cars

Researchers have discovered important security flaws in modern automobile systems. Will car thieves learn to pick locks with their laptops?

Not so long ago, car thieves plied their trade with little more than a coat hanger and a screwdriver. New anti-theft technologies have made today's cars much harder to steal, but the growing tangle of computer equipment under the modern hood is creating new security risks that carmakers are just beginning to understand.

Ever since Toyota's well-publicized struggles with the computerized braking systems in its 2010 Prius hybrid cars, automotive computer systems have come under increasing scrutiny. In the last few years, researchers have identified a range of new, unexpected security flaws that could potentially affect large numbers of new cars. Given the specialized programming knowledge required to exploit these flaws, however, carmakers are still trying to gauge if these issues present a meaningful risk to ordinary drivers.

Last year, researchers Tadayoshi Kohno of the University of Washington and Stefan Savage of the University of California-San Diego announced the startling results of a two-year investigation into potential vulnerabilities in modern automotive computer systems.

The team initially explored whether they could compromise the onboard computer diagnostics port, a U.S. government-mandated feature in most modern cars. By inserting malicious code into the diagnostic software commonly found in auto repair shops and plugging a computer into the car's diagnostic port, they were able to stop the car's engine, lock the doors, and disable the brakes. More recently, they managed to remotely control a car by means of on-board Bluetooth or cellular services, thus demonstrating that a car could be controlled purely through wireless mechanisms.

Using an undisclosed hack, Kevin Finisterre was able to monitor a police car's video feed in real time.

PHOTOGRAPH BY SERGEI CHUMAKOV / SHUTTERSTOCK.COM

"Our initial goal was to conduct a thorough, comprehensive analysis of a modern automobile," says Kohno. "This meant we wanted to study the brake controller, the engine controller, the light controller, the telematics unit, the media player, and so on. One of the biggest, most labor-intensive challenges was the sheer volume of components within the car."

Today's cars often contain myriad computer systems made by different manufacturers, making it difficult for any single component maker to identify every potential security exposure.

"To improve security one really desires a holistic view of all the components within the automobile," says Kohno, "but because of outsourced components it's hard for even the manufacturer to have that holistic view."

Despite the inherent difficulty of pinpointing security exposures in complex automotive systems, Kohno and Savage's work points to one conspicuous weak link: the onboard computer diagnostics port.

"Manufacturers could take steps to limit what someone might be able to do if they connect to the diagnostics port," says Kohno. He acknowledges, however, that the onboard port plays a crucial role in many cars. "One key challenge is to preserve the benefits but minimize the risks," he says.

Those risks seem destined to multiply as the number of network connections continues to grow, sometimes causing security exposures to crop up in unexpected places.

Take, for example, the humble tire. At the University of South Carolina, assistant professor Wenyuan Xu discovered that she could track the movement of cars by tapping into the RFID data stored in modern tire pressure monitoring systems from up to a distance of 40 meters.

Xu's team explored the proprietary communication protocols typically used to connect tire pressure sensors to onboard computers, and discovered that they could "listen" to the tire pressure sensors and use them to establish a connection with the onboard computers.

By capturing and decoding the tire sensor signals, the team was able to track the car's movements. They also established that they could send fake signals to trick the car computer into lighting up the low tire pressure warning light, regardless of the tire pressure. They were also able to inflict permanent damage to the tire pressure monitoring systems.

"An increasing number of wireless systems are installed in modern cars," notes Xu. "Wireless networks are known to be vulnerable to eavesdropping and packet injection."

Communication Breakdown

Xu's work points to a central problem with many modern automobiles: The Controller Area Network (CAN), which was originally designed to enable microcontrollers to communicate with each other. As additional devices become connected to the CAN, the security exposures are multiplied. "It is a bad idea to trust any commands flowing on the CAN bus," says Xu. "More and more ECUs [Electronic Control Units] with wireless capabilities are added onto the CAN bus, which opens a door for remote attacks."

In a similar vein, researcher Kevin Finisterre of security consultancy Digital Munition recently drew headlines when he managed to compromise a police cruiser by taking advantage of security holes in the onboard networking system.

"I was working to help a police department vet its technology choices," recalls Finisterre, who has declined to identify the municipality that hired him. "The staff had several concerns with regard to the resiliency of their network to withstand an attack from a hacker."

Finisterre soon proved his client's hunch correct. After scanning several IP addresses known to be used by the city, he traced one of them back to a Linux machine installed inside one of the city's police cruisers. Using simple Telnet and FTP connections, he was able to access a streaming live video feed from the cruiser's onboard camera, as well as stored footage on a digital video recording device, and could upload, download, and delete footage stored on the car's onboard computer. At one point, Finisterre found himself monitoring the cruiser's video and audio feeds in real time as an officer responded to an incident.

Demonstrations like this may highlight potentially troubling flaws in modern automotive security, but how likely is it that ordinary car thieves will master these advanced computer science techniques in sufficient numbers to present a real threat to the average driver?

"To me, expertise is never a factor in determining threat level," says Finisterre. "Expertise can be gained either through rapid prototyping in a test environment or via simply social engineering someone who already has said experience. I think at this point in the game more targeted attacks may be occurring and being kept under wraps."

Finisterre acknowledges, however, that most of the threats remain largely hypothetical. "The general population is most likely not currently exposed to much risk. If you, on the other hand, were in a position in which sensitive conversations are had in your vehicle I may be more concerned about the built-in system and its various data ingress points."

U.S. researchers have remotely controlled a car by means of on-board Bluetooth or cellular services, thus demonstrating that motor vehicles could be controlled purely through wireless mechanisms.

Xu agrees that the real threat to drivers is probably limited. Replicating her team's tire-hacking exercise would be expensive for most car thieves; each of her vehicle-tracking tools costs $1,500 to make. "It requires higher commitment, and thus imposes less risk," she explains. "Of course, the unit price can be further reduced, but it's still not a small number for regular consumers."

However, Xu isn't taking any chances. Her team won't release its tools to the public. "It is not impossible that some people driven by profit incentive could make and sell commodity products on eBay to unlock others' cars," she says.

While the practical risks may seem limited, nonetheless the automotive industry bears the ultimate responsibility—and potential legal liability—for ensuring the safety and security of its vehicles.

To date, computer security has lagged far down the list of automakers' business priorities. That may be starting to change, however, thanks to Toyota's 2010 Prius problems and a growing awareness of automotive security issues in the computer science community.

"Traditional computer security stra-tegies can drastically improve the computer security of modern automobiles," says Kohno. "I think at least some major industry players are now very aware of potential computer security concerns, and they are working very hard to try to mitigate those concerns."

To that end, a group of scientists from academia and industrial labs recently formed the Embedded Vehicle Safety Committee in an effort to set standards for computer security for future automobiles.

Not all researchers agree that the automotive industry is doing enough to address security issues, however. "There is some work going on," says Xu, "but not enough."

Finisterre agrees. "Bells and whistles often take precedence over security concerns," he says. In this respect, the automotive industry is no different from many other consumer-oriented industries, where marketing considerations and cosmetic features frequently take first priority. Until automakers see a meaningful impact on their bottom lines, computer security may continue to take a proverbial backseat.

Further Reading

Checkoway, S., et al.
Comprehensive Experimental Analyses of Automotive Attack Surfaces, National Academy of Sciences Committee on Electronic Vehicle Controls and Unintended Acceleration, Washington, D.C., March 3–4, 2011.

Francillon, A., Danev, B., and Capkun, S.
Relay attacks on passive keyless entry and start systems in modern cars, *Proceedings of the 19th USENIX Security Symposium*, Washington, D.C., August 11–13, 2010.

Koscher, K., et al.
Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, Oakland, CA, May 16–19, 2010.

Rouf, I., et al.
Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study, *Proceedings of the 19th USENIX Security Symposium*, Washington, D.C., August 11–13, 2010.

Alex Wright is a writer and information architect based in Brooklyn, NY.