Hackers find weaknesses in car computer systems

TOM KRISHER, AP Auto Writer

DETROIT (AP) — As cars become more like PCs on wheels, what's to stop a hacker from taking over yours?

In recent demonstrations, hackers have shown they can slam a car's brakes at freeway speeds, jerk the steering wheel and even shut down the engine — all from their laptop computers.

The hackers are publicizing their work to reveal vulnerabilities present in a growing number of car computers. All cars and trucks contain anywhere from 20 to 70 computers. They control everything from the brakes to acceleration to the windows, and are connected to an internal network. A few hackers have recently managed to find their way into these intricate networks.

In one case, a pair of hackers manipulated two cars by plugging a laptop into a port beneath the dashboard where mechanics connect their computers to search for problems. Scarier yet, another group took control of a car's computers through cellular telephone and Bluetooth connections, the compact disc player and even the tire pressure monitoring system.

To be sure, the "hackers" involved were well-intentioned computer security experts, and it took both groups months to break into the computers. And there have been no real-world cases of a hacker remotely taking over a car. But experts say high-tech hijackings will get easier as automakers give them full Internet access and add

computer-controlled safety devices that take over driving duties, such as braking or steering, in emergencies. Another possibility: A tech-savvy thief could unlock the doors and drive off with your vehicle.

"The more technology they add to the vehicle, the more opportunities there are for that to be abused for nefarious purposes," says Rich Mogull, CEO of Phoenix-based Securosis, a security research firm. "Anything with a computer chip in it is vulnerable, history keeps showing us."

In the last 25 years, automakers have gradually computerized functions such as steering, braking, accelerating and shifting. Electronic gas pedal position sensors, for instance, are more reliable than the old throttle cables. Electronic parts also reduce weight and help cars use less gasoline.

The networks of little computers inside today's cars are fertile ground for hackers.

Charlie Miller, a St. Louis-based security engineer for Twitter, and fellow hacker Chris Valasek, director of intelligence at a Pittsburgh computer security consulting firm, maneuvered their way into the computer systems of a 2010 Toyota Prius and 2010 Ford Escape through a port used by mechanics.

"We could control steering, braking, acceleration to a certain extent, seat belts, lights, horn, speedometer, gas gauge," said Valasek. The two used a federal grant to expose the vulnerability of car computers. Even with their expertise, it took them nine months to get in.

Valasek and Miller released a report, including instructions on how to break into the cars' networks, at a hacker convention in August. They said they did so to draw attention to the problems and get automakers to fix them. The pair say automakers haven't added security to the ports.

Ford wouldn't comment other than a statement saying it takes security seriously, and that Miller and Valasek needed physical access to the cars to hack in.

Toyota said it has added security and continually tests it to stay ahead of hackers. The company said its computers are programmed to recognize rogue commands and reject them.

Two years ago, researchers at the University of Washington and University of California, San Diego did more extensive work, hacking their way into a 2009 midsize car through its cellular, Bluetooth and other wireless connections — even the CD player.

Stefan Savage, a UCSD computer science professor, said he and other researchers could control nearly everything but the car's steering. "We could have turned the brakes off. We could have killed the engine. We could have engaged the brakes," he said.

Savage wouldn't identify which manufacturer made the car they hacked into. But

two people with knowledge of the work said the car was from General Motors and the researchers compromised the OnStar safety system, best known for using cellular technology to check on customers and call for help in a crash. The people didn't want to be identified because they were not authorized to speak publicly on the matter.

GM wouldn't comment on the research, but the company issued a statement saying it takes security seriously and is putting strategies in place to reduce risk.

One of the people said GM engineers initially dismissed the researchers' work, but after reading the report, quickly moved to close holes that allowed access to the car's computers.

Savage doesn't think common criminals will be able to electronically seize control of cars anytime soon. Currently it would take too much time, expertise, money and hard work to hack into the multitude of computer systems.

"You're talking about a rarefied group who has the resources and wherewithal," he said.

Instead, he believes basic theft is a more likely consequence of computerization, with criminals being able to unlock doors remotely and then start and drive the car by hacking through the diagnostic port. Remote door unlocking could also lead to theft of packages, phones and other items that are stored in a car.