Car-hacking researchers hope to wake up auto industry

July 26 2013, by Rob Lever

Computer geeks already knew it was possible to hack into a car's computerized systems and potentially alter some electronic control functions.

But new research to be presented next week shows the vulnerabilities are greater and the potential for mischief worse than believed, in a wake-up call for the automobile industry.

Chris Valasek, director of security intelligence for the security firm IOActive, and Charlie Miller, security engineer for Twitter, found these vulnerabilities in cars' on-board computer, a mandatory feature on US vehicles since 1996.

They found that by accessing this device, which sits under the steering wheel, someone with a brief period of access, like a parking attendant, could hack the car and reprogram key safety features.

"We had full control of braking," Valasek told AFP in a telephone interview.

"We disengaged the brakes so if you were going slow and tried to press the brakes they wouldn't work. We could turn the headlamps on and off, honk the horn. We had control of many aspects of the automobile."

The pair, working with partial funding from the US government's Defense Advanced Research Projects Agency, also manipulated a

vehicle's steering by hijacking the "park assist" feature which was designed only to move slowly in reverse.

"You would need a brief moment of physical access," Valasek said. "You could reprogram and untether from the car and the system."

While some earlier research focused on the potential to wirelessly gain control of some functions, Valasek said his project looked at overwriting the software code in the vehicles, with even more damaging consequences.

The research is to presented next week at Def Con, an annual gathering of hackers and security experts in Las Vegas.

The research is not the first to show the potential for hacking into car computer systems, which are becoming more ubiquitous as more vehicles add services connecting to the Internet or cellular phone networks, and some firms like Google are using self-driving automobiles.

A 2010 study by researchers from the University of Washington and University of California at San Diego demonstrated how an attacker could infiltrate virtually any electronic control unit (ECU) of a car and "leverage this ability to completely circumvent a broad array of safety-critical systems."

That study showed that the engine control devices initially designed for pollution reduction had been integrated into other aspects of a car's functioning and diagnostics.

And the US Department of Homeland Security issued an advisory in May warning of flaws in the wireless Bluetooth systems in some cars which could be exploited by an outsider to take control of some car

functions.

Valasek said most cars on the road have a number of computers and "they all trust each other. As long as they are receiving information, they don't care who is sending it."

This highlights the need for more attention to cybersecurity in vehicle design, he said.

"We want an intelligent discussion on this," he said.

Valasek and Miller will be releasing full technical details of their research at Def Con.

"We hope people enjoy the presentation and take our tools and data and try to reproduce them and do their own research," he said.

"Although there is research on automobile security no one is releasing the data."

Valasek said there have been no real-life exploits of automobile hacking, but added that "we just don't know what could be done with this."

He said it is more complicated than hacking into a personal computer but that his latest research shows that "with a minimal number of people you can have results where you can control the car, and do things that are detrimental to safety."