Smart gadgets from guns to cars ripe for hacking

August 2 2015, by Glenn Chapman

Hackers are not just after your computer: connected devices from cars to home security systems to sniper rifles are now targets for actors looking to steal or cause mischief

Hackers are not just after your computer: connected devices from cars to home security systems to sniper rifles are now targets for actors looking to steal or cause mischief.

The rapid growth in the "Internet of Things" has opened up new opportunities for cyber attacks and new markets for cyber defenders.

This is among the hot topics at a Black Hat computer security conference that kicks off in Las Vegas on Sunday and an infamous Def Con hacker gathering that follows.

Early glimpses have been provided of scheduled presentations about how to commandeer control of some Chrysler Fiat vehicles or accurately retarget self-aiming sniper rifles.

"The Internet of Things is definitely one of the big new frontiers," said Christopher Kruegel, co-founder of cyber security firm Lastline and a professor of computer science at a state university in Southern California.

Fiat Chrysler Automobiles issued a safety recall for 1.4 million US cars and trucks in July after hackers demonstrated that they could take control of their systems while they are in operation.

The recall came after cybersecurity experts Charlie Miller and Chris Valasek of the firm IOActive Labs remotely commandeered a Jeep Cherokee, made by Chrysler, to demonstrate the vulnerability of the vehicles' electronic systems.

As reported in Wired magazine and elsewhere, working from laptop computers at home, the two men were able to enter the Jeep's electronics via its online entertainment system, changing its speed and braking capability and manipulating the radio and windshield wipers.

After the report, Chrysler issued a free software patch for vulnerable vehicles even while saying it had no first-hand knowledge of hacking incidents.

Miller and Valasek are to reveal more about their Jeep hack at Black Hat.

"The ambiguous nature of automotive security leads to narratives that are polar opposites: either we're all going to die or our cars are perfectly safe," read a description of a scheduled briefing by the researchers.

"In this talk, we will show the reality of car hacking by demonstrating exactly how a remote attack works against an unaltered, factory vehicle."

Intel security vice president Raj Samani told AFP of an earlier demonstration of using hacks to take control of accelerators of cars, one of which was crashed into a wall.

"Cyber threats have been real threats for a while," Samani told AFP.

"Stuxnet should have been the wake-up."

Fiat Chrysler Automobiles issued a safety recall for 1.4 million US cars and trucks in July after hackers demonstrated that they could take control of their systems while they are in operation

Low-hanging fruit

Iran was hit in 2010 by several computer attacks including the Stuxnet virus—widely believed to be developed by the US government—targeting Tehran's nuclear program

Most Stuxnet infections were discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there to derail efforts to make a nuclear bomb.

"The idea of bridging the gap between the cyber world and the physical world has been around for a while," Kruegel said, referring to long-standing fears of possible cyber attacks on power grids, water plants, and other infrastructure targets.

"Now, these proof-of-concepts show that it is a real threat. All these devices are out there and reachable, and security is terrible."

Stuxnet-type attacks were seen as the work of sophisticated, state-sponsored actors with ample resources and time. The explosion of connected devices in the booming Internet of Things has created easy targets for independent hackers motivated by greed or malice, according to security researchers.

"It's hard to find a way into Windows 10, but now you have these devices that are not hard to get into," Kruegel said, referring to latest

generation Microsoft computer operating system.

"It is low-hanging fruit, in a way."

Hacking smart watches, door locks, fitness bands, power meters, or other devices woven into the Internet of Things also carries the risk of villains tapping into rich troves of data gathered by sensors monitoring many aspects of people's lives.

Samani told of shopping for a kettle recently only to find he could buy one with Wi-Fi connectivity.

Data from a home smart meter could reveal what types of devices are being powered inside as well as "when you have a cup of tea, make toast, or in most cases what TV show you are watching," he said.

Smart but not secure

Protecting gadgets in the Internet of Things is possible, but increases costs of smart gadgets while manufacturers prefer to keep prices low.

"Given the insecurity we see regularly, it's evident that for most makers that it isn't a priority," IOActive chief technology officer Cesar Cerrudo told AFP.

Samani joked that as the only computer security person presenting at a recent sensor conference in Germany, he was the "most unpopular guy" there.

"We haven't seen planes drop out of the sky or cars run off the road, that we know of, but these are the issues we face," he said. "Real world hacks are coming."

Lack of a profit motive for hackers with the right skills to commandeer control of planes, cars, or rifles was considered a prime factor for the lack of trouble so far.

"The guys who can do it don't have an interest now," Kruegel said.

"But, when you get the bored kid or the person who like to create havoc you will have a problem."