Insight: Experts hope to shield cars from computer viruses

Jim Finkle, Reuters

(Reuters) - A team of top hackers working for Intel Corp's security division toil away in a West Coast garage searching for electronic bugs that could make automobiles vulnerable to lethal computer viruses.

Intel's McAfee unit, which is best known for software that fights PC viruses, is one of a handful of firms that are looking to protect the dozens of tiny computers and electronic communications systems that are built into every modern car.

It's scary business. Security experts say that automakers have so far failed to adequately protect these systems, leaving them vulnerable to hacks by attackers looking to steal cars, eavesdrop on conversations, or even harm passengers by causing vehicles to crash.

"You can definitely kill people," said John Bumgarner, chief technology officer of the U.S. Cyber Consequences Unit, a non-profit organization that helps companies analyze the potential for targeted computer attacks on their networks and products.

To date there have been no reports of violent attacks on automobiles using a computer virus, according to SAE International, an association of more than 128,000 technical professionals working in the aerospace and the auto industries.

Yet, Ford spokesman Alan Hall said his company had tasked its security engineers with making its Sync in-vehicle communications and entertainment system as resistant as possible to attack.

"Ford is taking the threat very seriously and investing in security solutions that are built into the product from the outset," he said.

And a group of U.S. computer scientists shook the industry in 2010 with a landmark study that showed viruses could damage cars when they were moving at high speeds. Their tests were done at a decommissioned airport.

SAE International charged a committee of more than 40 industry experts with advising manufacturers on preventing, detecting and mitigating cyber attacks.

"Any cyber security breach carries certain risk," said Jack Pokrzywa, SAE's manager of ground vehicle standards. "SAE Vehicle Electrical System Security Committee is working hard to develop specifications which will reduce that risk in the vehicle area."

The group of U.S. computer scientists from California and Washington state issued a

second report last year that identified ways in which computer worms and Trojans could be delivered to automobiles -- via onboard diagnostics systems, wireless connections and even tainted CDs played on radios systems.

They did not say which company manufactured the cars they examined, but did say they believed the issues affected the entire industry, noting that many automakers use common suppliers and development processes.

The three big U.S. automakers declined to say if they knew of any instances in which their vehicles had been attacked with malicious software or if they had recalled cars to fix security vulnerabilities.

Toyota Motor Corp, the world's biggest automaker, said it was not aware of any hacking incidents on its cars.

"They're basically designed to change coding constantly. I won't say it's impossible to hack, but it's pretty close," said Toyota spokesman John Hanson.

Officials with Hyundai Motor Co, Nissan Motor Co and Volkswagen AG said they could not immediately comment on the issue.

A spokesman for Honda Motor Co said that the Japanese automaker was studying the security of on-vehicle computer systems, but declined to discuss those efforts.

A spokesman for the U.S. Department of Homeland Security declined to comment when asked how seriously the agency considers the risk that hackers could launch attacks on vehicles or say whether DHS had learned of any such incidents.

The department helps businesses in the manufacturing and transportation industries secure the technology inside their products and investigates reports of vulnerabilities that could allow attacks.

Bruce Snell, a McAfee executive who oversees his company's research on car security at the Beaverton, Oregon garage, said automakers are fairly concerned about the potential cyber attacks because of the frightening repercussions.

"If your laptop crashes you'll have a bad day, but if your car crashes that could be life threatening," he said. "I don't think people need to panic now. But the future is really scary."

A McAfee spokeswoman said that among those hackers working on pulling apart cars was Barnaby Jack, a well-known researcher who has previously figured out ways that criminals could force ATMs to spit out cash (bit.ly/bqwEbS [1]) and cause medical pumps to release lethal doses of insulin (reut.rs/sCD4Pr [2]). Makers of those products responded by saying they would work to improve security.

COMPUTERS ON WHEELS

White hats are increasingly looking beyond PCs and data centers for security

vulnerabilities that have plagued the computer industry for decades and focusing on products like cars, medical devices and electricity meters that run on tiny computers embedded in those products.

Automobiles are already considered "computers on wheels" by security experts. Vehicles are filled with dozens of tiny computers known as electronic control units, or ECUs, that require tens of millions of lines of computer code to manage interconnected systems including engines, brakes and navigation as well as lighting, ventilation and entertainment.

Cars also use the same wireless technologies that power cell phones and Bluetooth headsets, which makes them vulnerable to remote attacks that are widely known to criminal hackers.

"There is tons of opportunity for attack on car systems," said Stuart McClure, an expert on automobile security who recently stepped down as worldwide chief technology officer of McAfee to start his own firm.

Security analysts fear that criminals, terrorists and spies are gradually turning their attention to embedded computers, many of which can be attacked using some of the same techniques as regular computers.

Automakers are rushing to make it easy to plug portable computers and phones to vehicles and connect them to the Internet, but in many cases they are also exposing critical systems that run their vehicles to potential attackers because those networks are all linked within the car.

"The manufacturers, like those of any other hardware products, are implementing features and technology just because they can and don't fully understand the potential risks of doing so," said Joe Grand, an electrical engineer and independent hardware security expert.

Grand estimates that the average auto maker is about 20 years behind software companies in understanding how to prevent cyber attacks.

Chrysler said it was addressing security issues with industry groups and outside organizations including Battelle Corp, a non-profit company that recently established an auto security research center in Columbia, Maryland known as CAVE, or the Center for Advanced Vehicle Environments.

CAVE, which declined to discuss its research on auto security, has hired hacking expert Tiffany Strauchs Rad, a professor at the University of Southern Maine. Last year, she was part of a team that identified flaws in prison networks which could enable hackers to remotely open or lock cell doors.

'SELF DESTRUCT'

Concerns about such possibilities emerged after a group of computer scientists from the University of California and the University of Washington published two

landmark research papers that showed computer viruses can infect cars and cause them to crash, potentially harming passengers.

The group chose a fairly banal name, the Center for Automotive Embedded Systems Security. Yet their work is as imaginative as that of Q, the fictional scientist who supplies weapons to British secret agent James Bond.

They figured out how to attack vehicles by putting viruses onto compact discs. When unknowing victims try to listen to the CD, it infects the car radio, then makes its way across the network to more critical systems.

For instance, they came up with a combination attack dubbed "Self Destruct". It starts when a 60-second timer pops up on a car's digital dashboard and starts counting down. When it reaches zero the virus can simultaneously shut off the car's lights, lock its doors, kill the engine and release or slam on the brakes.

In addition to designing viruses to harm passengers in infected vehicles, the academics were able to remotely eavesdrop on conversations inside cars, a technique that could be of use to corporate and government spies.

The research group disbanded after publishing two technical papers, in May 2010 and August 2011, that describe multiple types of attacks and ways to infect cars using Bluetooth systems, wireless networks as well as the car's OnBoard Diagnostics port, which is also known as an OBD-II port. (bit.ly/oao8a8 [3])

One issue of concern is fighting ordinary PC viruses that could potentially infect cars when laptops and other devices are plugged into infotainment systems.

"Viruses are something that needs to be addressed directly. How we guard against that transfer to our system is a primary focus of our efforts," said Toyota spokesman John Hanson.

(Additional reporting by Bernie Woodall in Detroit; Editing by Leslie Gevirtz)

Source URL (retrieved on *07/24/2014 - 4:41pm*):
http://www.ecnmag.com/news/2012/08/insight-experts-hope-shield-cars-computer-viruses?qt-video_of_the_day=0

Links:
[1] http://bit.ly/bqwEbS
[2] http://reut.rs/sCD4Pr
[3] http://bit.ly/oao8a8