Here's how hackers are making your Tesla, GM and Chrysler less vulnerable to attack

July 5 2019, by Dalvin Brown, Usa Today

In March, a Tesla Model 3 was hacked.

The duo responsible for uncovering the vulnerability accessed the car's web browser, executed code on its firmware and displayed a message on the infotainment system before making off with the Model 3 and

$375,000.

The hackers didn't remotely take total control of the car or wreak havoc on its door locks or brakes while an innocent driver sat inside. In fact, they weren't able to break into any other systems in the electric vehicle, and the cash they collected came in the form of a check from Tesla.

It was all part of a three-day cybersecurity contest called Pwn2Own, an event where Tesla pays top dollar to anyone masterful enough to find previously unknown bugs. Correcting any weakness helps the electric car company protect the people who drive its vehicles, it hopes.

As an increasing number of cars become hi-tech computers on wheels, experts say that vehicles—like everything else that connects to the internet—are inherently hackable. That means every smart car could theoretically be broken into and controlled on some level by savvy hackers, criminals or worse.

While unrealized threats exist, automakers' efforts to protect motorists are extending beyond hiring experienced internal security teams.

For companies like Tesla, that means entering cars in rigorous third-party testing competitions or implementing other so-called "bug bounty programs" to encourage security researchers to actively locate and report any hot spots on the company's hardware.

At face value, encouraging outsiders to search for flaws may appear counter-intuitive. However, not only does the move give skilled hackers a chance to flex their muscle, but it also helps companies like Tesla, GM and others strengthen car security.

"We believe that in order to design and build inherently secure systems, manufacturers must work closely with the security research community to benefit from their collective expertise," Tesla said in a statement to U.S. TODAY.

Tesla used a software update to fix the vulnerability found by the "white hat," or ethical, hackers, which is a benefit as drivers don't have to visit a repair shop or pay fees to get an car's software updated.

Bug bounty programs

Tesla's approach toward plugging access holes began with its bug bounty program in 2014, however, it's not the only automaker that invites hackers to test systems.

Fiat Chrysler has had a bug bounty program in place since 2016 and it pays hackers up to $1,500 each time they discover a previously unknown vulnerability. GM officially rolled out its bug bounty program in 2018 after establishing what it calls the Security Vulnerability Disclosure Program in 2016.

More than 500 researchers have participated in GM's program to identify and resolve more than 700 vulnerabilities.

Ford announced in January that it's selecting top researchers to participate in future special hacking projects.

In order to thwart hackers, automakers and their suppliers are taking multiple approaches to protect cars from all sides, according to Asaf Ashkenazi, chief strategy officer at Verimatrix, a security and analytics software firm.

He said that cars today are in the beginning stages of what he called a three-prong approach to smart car security.

"They are filtering away the obvious attacks from the outside by trying to create firewalls between subsystems," he said. "If one is compromised, the hacker can't move to other systems."

This approach was shown during the Tesla hack as the Palo Alto-based company managed to contain the damage to just the browser while protecting all other vehicle functions.

Remote updates

The next level of protection from automakers is the ability to upgrade and fix issues via the airwaves, Ashkenazi said.

Legacy car companies have lagged behind Tesla's ability to send these smartphone-style refreshes to its customers. The Palo Alto-based company uses the feature to update everything from semi-autonomous driving modes to cheeky Easter eggs or hidden gems.

When responding to bugs, the company has fixed issues through software updates within a few days of discovering vulnerabilities.

Alongside Tesla, some of Ford and General Motor's 2020 models will allow over-the-air updates that can upgrade a vehicle with new features and remotely fix problematic software. GM's 2020 Cadillac CT5 will come with a new "digital nerve system" that makes the updates possible.

In May, GM announced that most of its global models will be capable of over-the-air software upgrades by 2023.

Constant monitoring

The third level of consumer vehicle protection involves having AI detect that a car is behaving differently. That gives automakers a better chance to identify attacks early on, Ashkenazi said.

Third-party software companies like Argus Cyber Security are stepping in help car companies develop and bake-in these types of remote diagnostics capabilities during the production process.

"Even if you have real-time protection inside the vehicle, you still need to know that one of your cars is being targeted," said Monique Lance, director of marketing at Argus Cyber Security.

That's where monitoring technology steps in, allowing auto companies to perform cross data analysis and identify suspicious behavior that could otherwise be missed.

"You need the ability to have visibility of your entire fleet because there may be other affected vehicles," Lance said. "It's paramount that you know what's happening within the network. It's much cheaper for automakers to be able to prevent attacks than to respond to them once they've happened so that service is vital."

Worst case scenario

Lance said without a layered approach to security, catastrophes await.

One example of what this could look like happened in 2015 when data security researchers successfully took remote control of a Jeep Cherokee. Fiat Chrysler responded by recalling 1.4 million cars and trucks and sending UBS sticks with software patches to owners.

That same year, another hacker revealed that he placed a small electronic box on a car to steal information from GM's OnStar system so he could open doors and start the vehicle. GM said the hack was isolated to one car and it has since closed the loopholes.

A fleet-wide vehicle hacking that results in death and destruction has yet to happen but as Tesla CEO Elon Musk said in 2017, it's "one of the biggest risks for autonomous vehicles." He added that a fleetwide hack of Tesla is "basically impossible."

Partnerships

Automakers are collaborating to prevent these types of scenarios from happening.

Established in 2015, the industry's information-sharing and analysis group called Auto ISAC is dedicated to research and creating best practices for cybersecurity. Mitsubishi Electric, PACCAR, Volvo Group North America and American Trucking Associations joined the pact in 2018.

The non-profit says that 98% of vehicles on the road in the United States are represented by member companies. A collaborative approach is a step in the right direction, Ashkenazi, the cybersecurity expert, said.

"But forming groups and creating guidelines may not necessarily work in all situations, to all cars. Getting to that point is very difficult and will take a long time."

Citation: Here's how hackers are making your Tesla, GM and Chrysler less vulnerable to attack (2019, July 5) retrieved 25 April 2024 from https://phys.org/news/2019-07-hackers-tesla-gm-chrysler-vulnerable.html