Automotive News

Current Issue | Video

Blogs New Product Photo Galleries Automakers and Suppliers Dealers Access F&I

Opinion Jobs

Originally Published: March 21, 2016 3:49 PM
Modified: March 22, 2016 6:31 AM

TECHNOLOGY GOVERNMENT REGULATIONS AND OTHER ACTIONS

Auto industry turns to 'bug bounties' to find security holes

Chad Halcom

Cybersecurity researchers Charlie Miller, left, and Chris Valasek helped Jeep identify security weaknesses in its software.

"Bug bounty" reward programs, for hackers to responsibly identify and help correct automotive software weaknesses, may be on their way for the top automakers, much as they have been adopted already in other industries.

General Motors has had an internal "Collaborative Disclosures" program running since January to interact with software researchers, or "white hat" hackers, and could soon expand the program to offer financial rewards or incentives for finding vulnerabilities before they create problems.

Tesla Motors Inc., the California-based electric car maker headed by CEO Elon Musk, has sponsored a bug bounty program since last June offering rewards of $100 to $10,000 per error or software flaw. That program has issued 106 awards as of March, according to Tesla's website.

Ford Motor Co. and Fiat Chrysler Automobiles have yet to announce any internal collaboration with hackers, but both companies are part of a new automotive Information Sharing and Analysis Center, or a collaborative industry program to share intelligence on software attacks and bolster cybersecurity, also launched in January.

Ford spokesman Alan Hall said the automaker "routinely monitors the security environment" and is reviewing possible strategies like a software bug disclosure program in the future, to mitigate threats. FCA spokesman Michael Palese said the automaker would not discuss its future plans for software disclosures.

But industry experts told *Crain's Detroit Business*, an affiliate of *Automotive News*, that other automakers are likely to follow GM and Tesla, with new cybersecurity initiatives of their own.

Automotive security executives and others are expected to attend the third annual Automotive Cyber Security Summit this week at the Baronette Renaissance Detroit-Novi Hotel, hosted by New York-based Penton Learning Systems LLC or International Quality & Productivity Center.

GM program

Jeff Massimilla, chief product cybersecurity officer at GM who sits on the board of directors at the new ISAC, said earlier this month that the internal GM program has been primarily vetting and talking with researchers for sharing findings on auto vulnerabilities, since it launched at the start of the year.

A rewards program is likely to follow, but he declined to estimate when that might be.

"I don't think it is ready for that yet, because right now we're in a "crawl' program phase. That would be more of a "run' phase -- to have a bug bounty, or be sponsoring a participatory and reward program for researchers," he said.

But Scott McCormick, president of the Connected Vehicle Trade Association, said he expects bug bounties and open collaboration with white hat hackers to become a standard industry practice.

Saving millions

If FCA had already had a bug bounty or collaborative program up in place when researchers hacked a Jeep Cherokee using Uconnect software in its entertainment system last summer, it likely could have saved millions in software fixes, he said.

Tesla's program was pretty restrictive on researchers, and GM will probably work in a similar way, McCormick said. "There are often ground rules like the research can't harm GM or its customers, you can't risk the safety of others, and researchers have to keep private the details of their findings until an automakers has a period of time to review and confirm it. I'm expecting the other companies will model that," he added.

Barbara Ciaramitaro, professor of information technology and cybersecurity and director of the newly-formed Decision Science program at Walsh College, said administrators at the school have been meeting with Ford and other local automakers in recent months about possible ways to collaborate on training new professionals in cybersecurity. But those talks are still preliminary.

The college added a new cybersecurity concentration within its master of science in information technology degree program, also in January.

"The automotive engineer community has to interact with the hacker and software engineer community to understand the whole mindset that goes into cyber attacks, and building your program to withstand attacks. There are cultural differences between" the software and auto industries, she said.

"It's a learning process for everyone, and even though there's progress this is still going to take a couple more years."

Talent competition

Even when automakers do understand the world of hackers and cyber threats, they are often competing for the top software talent with Silicon Valley firms and other industries, so collaborating with specialists outside the industry might be more convenient than building and training a workforce to tackle the challenges of cybersecurity, she said.

The new ISAC for auto cyber defense is one of about two dozen such centers nationwide, some industry-specific and others that cross industries but focus on specific infrastructure or threats that various businesses have in common, as part of the National Council of ISACs.

President Barack Obama three years ago signed new executive orders to direct the U.S. Department of Homeland Security to encourage and cooperate with ISACs to address cyber threats affecting critical infrastructure.

Experts expect automotive cyber defense is going to be a priority focus for at least the next year or two. Ciaramitaro and McCormick both said connected vehicles can have as much as 100 million lines of code across their various systems -- more than some airplanes -- and if even one in 4,000 lines contains a code error or vulnerability that could be 25,000 points of potential access.

Legislation and executive orders to facilitate ISACs or information exchange can be vital for automakers and suppliers, who might otherwise run afoul of federal antitrust laws on collusion or conspiracy by sharing too much, said Claudia Rast, an attorney at Detroit law firm Butzel Long. She also said ground rules can be important in working with white hats.

She said: "In a sense, working with one is not too dissimilar from hiring an external consultant or an expert, they would all be an outside party, and there are a couple of entrance legal issues to settle like confidentiality, and the aspect of whether there's an existing agreement in procurement for the service."

Tags: SECURITY INFORMATION TECHNOLOGY TECHNOLOGY SOFTWARE FORD GENERAL MOTORS VEHICLE TECHNOLOGY JEEP MICHIGAN

Search AutoNews.com SEARCH

Home [Breaking News]

Automotive News Europe

Digital Issue

Industry Events

Webinars

Subscribe

Register

Log In

Log Out

Contact Us

Find us on Facebook

Follow us on Twitter