It’s Best Not To Get Too Hacked-Off With Cybersecurity

Just what are the main lessons the connected car industry can draw from recent white-hat hacking incidents? Louis Bedigian explores the challenges

Future cars may be smarter but that doesn't mean they will be less vulnerable to attacks that could disrupt or alter their operation. The Jeep Cherokee hack was a strong reminder that connected vehicles can and will suffer the same fate as all other connected devices.

"It's essentially what we're seeing in computers," said Karl Brauer, senior director of insights and senior editor for Kelley Blue Book. "They keep upping the security level of personal computers, phones and tablets, and yet there's always a new way that a hacker finds to go in."

Brauer said that hacks (and the risk of them) are something that consumers will have to get used to over the next several years.

"The scary thing is that cars are going to become more and more autonomous, too, in the next 10 years," Brauer continued. "When you get to a car that's an autonomous vehicle, [hackers] could essentially do everything – lock the doors, start the vehicle driving somewhere and make it impossible for you to do anything about it."

Autonomous vehicles would be primarily run off software, completely relying off data from sensors, mapping, and more, to function. The increasing priority being placed on such technology is causing a huge increase in automotive companies hiring security experts. Harman acquired TowerSec to boost its cybersecurity, which along with RedBend shows it’s betting on putting a strong emphasis on cybersecurity.

Fiat Chrysler Automobiles (FCA) responded to its security vulnerabilities by issuing a recall for 1.4M vehicles. That could solve one problem but where does the industry go from here?

Assume the worst and fight to prevent it

Mark Skilton, a cybersecurity researcher and professor of practice at Warwick Business School, hopes the auto industry will implement proper checking systems to improve security.

This article has been released in the lead-up to the TU-Automotive Cybersecurity USA Conference & Exhibition (March 29-30, Novi, MI).

Find out more at: www.tu-auto.com/cyber-security

"It needs to be taken seriously," said Skilton. "They need to assume that their system will be hacked." According to Skilton, designers often assume their cars are not at risk. "But the truth is, yes it is going to get hacked," he added. "We need to expect standards from our automotive companies whether they're in America, Europe, Asia, or wherever. I think consumers are going to be much more wary. They will want to see proof positive that there [are] security systems protecting them in this car."

SAE's new standard and the automotive ISAC are a strong start for 2016, it remains to be seen how these will be utilized and implemented.

Anything can be hacked

New Scientist recently detailed how future threats could be avoided if tech companies implement an un-hackable kernel device. This idea sounds promising but security experts doubt it will lead to a fool proof system that automakers can adopt.

"It's a matter of how much money you want to put behind it," said Sven Andén, cyber auto security consultant at Sandab. "The hack doesn't come for free. If it's a serious hacker, he's got somebody behind him that's financing him, depending on what he's looking for. Is he looking for data? Is he looking to extort money out of people?" Andén said that "anything" can be hacked. He noted that the investors who bankroll cybersecurity attacks "have it down to the penny how much they are willing to spend".

Robert Neivert, COO of Private.me, thinks that researchers are setting themselves up to fail if they promise a kernel can't be hacked. "As soon as they say it's unhackable, somebody is going to find a way," Neivert warned.

Supply chain lawsuits

Kaiser Wahab, an attorney and partner at Riveles Wahab LLP, expects the auto industry to endure a greater variety of lawsuits if security continues to be an issue. "I think you're going to see [a scenario in which a] car was hacked, and because [of that] you lost your credit card information," said Wahab. "I think you're going to see a lot more of that and increasingly there's going to be tighter scrutiny on the supply chain because a lot of these components come from all over the world."

Automakers might build the drivetrain and chassis in-house but Wahab said the electronics may come from anywhere. As a result, automakers could be forced to absorb the mistakes made by those within its supply chain. "It used to be you just sued the car manufacturer," Wahab explained. "Now you're going to sue a much larger chain of people."

Overblown hysteria

Dave Jevans, founder and chief technology officer of Marble Security, thinks the auto industry has a "very long way to go" in building better security systems.

"We need to improve the security, especially as we get self-driving cars... that are increasingly driven off your iPhone or Android," said Jevans. "I feel like third party research has helped improve security of systems. I think that's provable and you can see it from Windows to the iPhone. Most of the bugs are being found by third parties and they're contributing that and making our platforms more secure. Car companies need to be open to that."

Regardless, Jevans believes the "attack hysteria" has been "overblown." Instead of hacking a car remotely, he said it would be "a lot easier to come over with a pair of pliers and just pull the brake lines."

In any case, automakers and their suppliers do not want to take the risk.

Connected cars are here to stay

Skilton does not expect automakers to abandon smart technology, even if it could lead to safer (less hackable) vehicles. "I prefer to believe another vision, which is where we want this because we need to reduce costs of travel," said Skilton. "If you look at pollution, there are a million and one reasons why we want to get a better, more efficient transport system for just the volume of cars."

As long as the automakers continue to invest time and money into cybersecurity, they can mitigate the risks of these technologies.

Catch up with all the latest in auto security at TU-Automotive Cybersecurity USA 2016 this March 29-30.