V2X And Security: Will Connected Cars Fall Victim To Cyber Attacks?

By Louis Bedigian

Vehicle-to-Everything (V2X) communication is still in its infancy, but a number of companies – including Nissan, Qualcomm Technologies, Ericsson and NTT DOCOMO – will begin testing the technology later this year. They plan to focus on a cellular iteration (C-V2X) that could help connect the cars of tomorrow.

With greater connectivity comes a new challenge for the auto industry. Consumers won't accept a feature that appears to be unsecure or unsafe.

Safety isn't just about ADAS, however. In the future, when cars can accurately drive themselves anywhere, it might be possible to avoid many of the day-to-day collisions. That won't guarantee that roads are any safer, however. Once cars are connected, the battle for safety will shift to something the auto industry has never seen before: cyber threats.

"The more that cars are becoming connected – let alone autonomous, which implies even more connectivity – the more they are becoming a target for hackers," said David Barzilai, co-founder and executive chairman of Karamba Security, an automotive cybersecurity firm. "This is quite consistent of a pattern. When systems become externally connected, then hackers find it as a target and start exploiting vulnerabilities within those systems."

Barzilai said that while hacking initially started as something that was "more for fun," it has transformed into a massive business led by attempts to extract money.

"The business of ransomware is quite significant," said Barzilai. "With cars it's a little different. The risk is not just with data, the risk is also about lives."

Ahead of the curve

Cybersecurity is not a final destination – it is a lifelong journey that begins as soon as a product is released. This is particularly important to the future of automobiles, which must be secured from the moment they leave the assembly line. But that begs an important question: Will connected and self-driving technologies outpace the security solutions needed to protect them?

"By default the answer is yes, but that's not just for autonomous vehicles – it's for every product," said Sam Lauzon, a senior engineer in research at the University of Michigan Transportation Research Institute (UMTRI). "Security is going to have to continually be

refined as the vehicle ages. It's very difficult because cars are on the road for 20 years. You can't upgrade hardware, unfortunately. That means the software security has to be there, and software security is constantly being manipulated and hacked."

Chris Clark, principal security engineer for strategic initiatives at Synopsys, concurred with Lauzon's belief that connectivity and autonomy will advance faster than auto security.

Said Clark: "That's always going to be the case. That's the reality of all industries. Technology advancements are always ahead of security. Until we have a secure development lifecycle of components that are much more capable and much more resilient, we'll continue to be in that cycle. That won't go away for a while."

Automakers might be catching on, however, knowing that if they don't act now they could be in trouble later.

"The industry was really rushing towards autonomy without paying too much attention to the potential Pandora's box that would open," said Yoni Heilbronn, chief marketing officer of Argus Cyber Security. "I think by now there is a good understanding that without cybersecurity you will have no smart mobility, no autonomy. People will not get into cars if they do not know they're safe."

Phil Magney, founder and principal advisor at Vision Systems Intelligence, is hopeful that security will ultimately keep up with new vehicles as they're deployed.

"I think the security folks are really working hard to provide levels of protection that will be in parity with the autonomous vehicle technologies," said Magney. "My biggest concern is if you get to a point when urban environments are 100% automated, and you have the ability to teleoperate these vehicles. That seems like the potential for worst-case scenarios you can imagine if someone were to hack into the fleets and cause them all to go awry."

Message received

One of the key aspects of V2X includes Vehicle-to-Vehicle (V2V) communications. Automobiles could feasibly alert each other to impending issues before they occur. They could also communicate with the infrastructure (V2I) to improve traffic flow and safety at intersections.

These features cannot be implemented without risk, however. Benedikt Brecht, a security professional whose job includes working as a principal investigator for the Crash

Avoidance Metrics Partnership (CAMP), is concerned that a malicious threat actor could intercept and influence V2X communications.

Said Brecht: “If somebody could hack the system in a way that he is able to mimic a different car and force other cars in the infrastructure to react to his messages in a bad way, I think that’s one of the bigger risks. Traditionally, all the OEMs, at least that I know of, were able to control the infrastructure communication to their cars or put strong firewalls in place. But now you want to get data into the car from the outside that’s not in your control, and you want the car to react to that.”

An attack on that level would not come cheap, however. Tim Watson, director of the WMG Cyber Security Centre and a professor at the University of Warwick, said the expense could be used to an automaker’s advantage.

“One thing is to try to make it economically less attractive for criminal groups to be able to hack your system,” said Watson. “It takes a lot of money to develop an exploit that’s going to work identically on every single car of a single make and model, but it could offer a good economic return.”

However, if there’s software and hardware diversity within the same make and model, that could limit an attack’s effectiveness to a subset of those vehicles.

“An attack wouldn’t necessarily work reliably on any single vehicle,” said Watson. “That may well be enough of a disincentive to stop people from exploiting them in the first place.”

Cloud security risks

Moshe Shlisel, CEO of GuardKnox, an auto cybersecurity company, addressed the issue of persistent connectivity in tomorrow’s automobiles. While many have discussed whether AVs will be able to function properly without the Internet, Shlisel is concerned about security solutions that rely on the cloud.

Said Shlisel: “What would happen if I was able to inject a malicious piece of software that would activate itself only when your car is not connected? Then you have a big problem because you’re not always going to be connected. In some cases you don’t have any service at all. You’re just driving and hoping nothing will happen.”

Connectivity risks are not limited to the car alone. Shlisel said that if and when cars are connected to other things – such as the city infrastructure or a power grid for charging – it paves the way for additional vulnerabilities. He warned: “If you are able to hack the

car and start hopping from it to other networks or other nodes, you can dominate the city and create national risk in that way."

As far as specific attacks are concerned, Shlisel speculated about the potential risks for fleets in a connected world. He fears that fleets could be particularly vulnerable to ransomware, which in turn could impact the economy if a large number of fleets are halted.

"It's not a doomsday scenario, it's a realistic one," he said.

From the ground up

Dvir Reznik, senior marketing manager of automotive cybersecurity at Harman Connected Services, is among those who think automakers need to develop connected and autonomous vehicles with security in mind.

"You properly define the security measures in advance instead of trying to play catch up," said Reznik. "Cyber-proof from the foundation, from the ground up."

Not everyone agrees, which concerns Reznik. He spoke about a recent report by Foley & Lardner LLP, which surveyed manufacturers, suppliers and others within the auto space. When asked about the biggest obstacles to the growth of autonomous vehicles, 35% of respondents pointed to safety concerns, but only 1% thought that cybersecurity/privacy would be an obstacle.

Even more troubling, Reznik said that cybersecurity has attracted only 4% of the capital invested in auto-related startups.

New vulnerabilities?

While security experts agree that connected cars will be targeted by cyber threats, opinions vary regarding the potential risks to a smart infrastructure.

Argus' Heilbronn believes that in a world of IoT, everything will eventually be connected. Consequently, this may lead to additional vulnerabilities. He explained: "It's the Internet of Everything. Once you're connected to the outside world, then you can actually reach the outside world. And it goes both ways. It's not only the ability to have a remote connection to influence a vehicle. This could be done the other way around, and we could see vehicles in the end that are potentially infecting other computers related to the infrastructure."

Heilbronn said that a car could be used as a gateway to hacking traffic lights, for example. “Vehicles could be the actual vehicle of infection – or more than that,” he added. “It is already happening in the normal world when you have malware go from one place to another. Why not in cars as well?”

New targets

Andre Weimerskirch, VP of global cybersecurity at Lear, said there could be an incentive to stealing private information stored within a vehicle. Visa, for example, has experimented with a credit card solution that would transform vehicles into the ultimate mobile payment devices. This could make vehicles a new target.

Stronger security could mitigate this risk, however. Weimerskirch said that hackers are not necessarily going after specific industries or devices. Rather, they scan the Internet searching for open computers to attack. He explained: “That might be the same for vehicles where they just stumble on it. They don’t actually care if it’s a vehicle.”

The greatest risks

Between theft, ransomware and malicious intent, V2X security will need to be maintained and monitored around the clock. But while that much is clear, DigiCert’s Mike Ahmadi said it is difficult to quantify which threat will prove to be the most significant.

“Any attack that can generate revenue (such as ransomware) or cause massive destruction (via terrorist-type attacks, for example) are indeed the ones to pay the closest attention to,” said Ahmadi, who serves as DigiCert’s global director of IoT security solutions. “Regardless, all risks should be considered equally, because what may appear low-risk can quickly become high-risk in the right circumstances.”

In order to prevent malicious attacks, Ahmadi recommended that automakers start by building security into the designs of each vehicle.

He added: “Penetration testing should be part of the broader testing that occurs to ensure vehicle safety. OEMs need to make sure all connection points within a vehicle are properly authenticated to ensure only trusted services are able to communicate with the vehicle. Encryption of sensitive data or packages going to or from the devices should always be used. Cyber risks are always evolving, and so must the security solutions to ensure the vehicles of tomorrow are safe.”

The cost of privacy

The price for connected automobiles could be the loss of privacy. Said UMTRI's Lauzon: "Is your privacy guaranteed if you're connected or not? That's still a huge question. From a security research perspective we assume privacy should be guaranteed by using such a system. And creating a system that guarantees your privacy and security and everything else is almost impossible, simply because if I don't know who I'm talking to, how can I verify your identity?"

Lauzon offered another challenge: how will American V2X systems handle vehicles coming over from other jurisdictions, such as Canada and Mexico?

"And then you have the privacy concerns where people might not be maliciously taking advantage but they might be listening to the data to figure out who's driving or what they're doing on the road," Lauzon added. "They might be identifying police vehicles, undercover vehicles, that sort of thing. When you add connectivity you have a really large attack surface simply because you're broadcasting into the air. You have no control over who is actually receiving that data."