The Automotive Cyber Security Industry Overview

By Susan Kuchinskas

The United States Senate will consider the SELF-DRIVE Act that will, among other things, require car makers to develop plans or automotive cyber security, while also directing NHTSA to "consider process and procedure standards for software and cybersecurity as necessary."

Like a lot of legislative initiatives, it's too little and too late. But the automotive industry isn't waiting. The past two years have seen tremendous expansion in the cyber security sector, with auto makers, Tier 1s and startups collaborating to secure connected and autonomous vehicles.

Two years ago, if OEMs talked about cyber security, discussions centered around issues of what was necessary and how much it would cost, says Chris Thomas, a founder and partner in the venture investment firm Fontinalis Partners. "Now, cyber security is not a choice. It's a must-have. There's been a huge paradigm change in how people think about it as an overall component of the system."

Autonomous cars will be even more vulnerable to attack due to their reliance on vehicle-to-vehicle and vehicle-to-infrastructure communications, according to David Barzilai, executive chairman of Karamba Security. While attacks against vehicles usually enter through the infotainment system, he says, an attack against the V2X communications system might compromise safety without being detected in network traffic.

A multi-layered problem

With the complex architectures and complicated supply chains of automotive, even when standards and requirements are delivered to suppliers, it's very difficult to ensure those requirements are being met at the chip level, according to Jonathan Allen, a director of Booz Allen Hamilton.

"Automakers have to assume each one in itself is insecure," he says. The keys are redundancy in design and monitoring to ensure if a part of that system is compromised, it's reported and fixed.

In connected and/or autonomous vehicles, these layers need to be secured:

- Software development among OEMs and suppliers, reducing coding errors that could be exploited and the likelihood of malicious code being introduced
- The factory floor where hardware and software are installed in individual cars
- The transportation system, so that persistently connected cars are not attacked in transit
- The dealership, where software may be installed or updated and connected cars are available for test drives
- The car itself
- Communications to and from the car after it's deployed, including WiFi, cellular, V2V and V2X, and over-the-air updates
- Data produced by the car and stored by OEMs and partners

At the vehicle level, devices, software and communications within the car must be secure:

- The operating system
- Software for different modules and ECUs
- Intra-car networks like the CAN
- Individual control units such as the integrated drive system or telematics control unit

Finally, cyber security should be baked into the company itself—not only in enterprise networks but also into every facet of internal operations.

While awareness of security threats among OEMs is high, McKinsey says that less than half have operational security units.

McKinsey also cites a recent survey finding that only 10 percent of suppliers said cyber security ranked high on top management's agenda, while 45 percent considered the cyber security of external partners to be important.

Having an operational security unit, as well as a chief information security officer (CISO), is necessary because it's not only the car that needs to be secured: Cyber security must extend from enterprise systems through hardware and software design and development, and then include the factory.

Jonathan Allen says, "For many years, companies have had CISOs focused on their own operations but not on products. Now CISOs are demanding security by design upfront."

HARMAN is just one example of a supplier that's doing this. According to Dvir Reznik, senior marketing manager, automotive cybersecurity, HARMAN Connected Services, the company has created a new center of competence for cyber security. Its mandate is to make sure the company's products, processes and solutions are developed to industry standards for security.

Lear's Andre Weimerskirch, vice president of cyber security for E-Systems at Lear, agrees it's essential to test cyber security at every step of the development process. To do this, the company tests software relentlessly and then the security team reviews the entire development process.

Link by link

Automotive cyber security is so complex because of the multitude of suppliers involved in the supply chain. That makes it quite difficult for any entity along the chain to understand how secure a component is.

Says Andre Weimerskirch, "As a supplier, we face the same issue of evaluating vendor claims." When Lear develops a new unit and identifies a particular technology to use, it may have a choice of several vendors. "How do we figure out which is most secure? You can't really measure it. We dig extremely deep to understand what vendors are actually offering. It's a bit like a puzzle."

Lear performs risk assessments and tries to identify attack vectors for each new component, and then selects in-house or third-party solutions to counter each risk it's identified.

Software, open or closed

Software is another critical part of the supply chain. Sam Lauzon, an automotive cybersecurity software developer in UMTRI's Engineering Systems Group, points out that enterprise software vendors like Microsoft, Apple and Adobe are constantly delivering updates to patch vulnerabilities and fix bugs. If companies like these, which spend billions of dollars on research, can't ship software that's 100 percent he asks, "How can we be certain that a smaller, third-party company that only supplies the auto industry has a secure product?

The majority of software in vehicles is proprietary, making it difficult for customers and third parties to evaluate. Lauzon is a contributor to Uptane, an open-source project that's developed a software update security system for the automotive industry. Because it's open, advocates say, companies and the greater developer community can improve the code and remove vulnerabilities.

Cameron Mott, senior research analyst for Southwest Research Institute and another Uptane contributor, says, "It takes into consideration the needs of all stakeholders and incorporates them in a way that's reasonable for everyone's business model."

Many in the industry advocate for automotive software to be subject to the same kind of crash testing used to provide safety ratings for cars. There might even be a system similar to NHTSA's 5-Star Ratings.

Mott posits that third parties like his organization might use white-hat hacking methods to verify a company's claims for the cyber security of its product. These software-crashworthiness ratings might cover a piece of software, a component or the entire vehicle.

This kind of standardized system is still far off, Mott says. In the meantime, some companies offer bounties to the developer community to encourage them to find vulnerabilities—especially after the legendary Miller and Valasek Jeep Hack.

It's a good approach, Mott thinks. "Then researchers get credit for doing good, ethical security work; the company gets credit for approaching the problem in an honest, transparent method and handling it quickly before putting the vulnerability out in the wild."

Choices vs. market confusion

One area of debate is whether it's better to address the multi-layered cyber security problem with an array of point solutions—the so-called "best of breed" approach—or to use one solution that aims to address every layer—in industry parlance a "holistic" solution.

"Any supplier that says they have it all hasn't understood the whole system," says Steven Tengler, senior director of global automotive cybersecurity for Honeywell.

On Yoni Heilbronn, chief marketing officer of Argus Cyber Security, insists, "There is no one silver bullet to solve the entire problem. Otherwise we wouldn't have a multibillion dollar market for computer security. One should have different layers of solutions to complement each other and make it as hard as possible for perpetrators to attack a vehicle."

That said, Argus has a wide variety of products covering many of the essential—and it was recently acquired by Continental's subsidiary Elektrobit.

According to Martin Schleicher, executive vice president strategy and partnerships at Elektrobit, the acquisition will allow it to offer an overall solution. He says, "We think cyber security and over-the-air updates are becoming essential features of the in-vehicle software platforms, so we will need to provide security as a one-stop solution provider. Companies need to understand cyber security completely in order to be able to offer our customers best possible security approaches going forward."

HARMAN's Reznik provides the opposite argument. He says that focusing on point solutions lets the company shorten the time it takes to deploy or integrate its products. Key to this approach, he says, is partnering with companies that are already entrenched in the automotive ecosystem, including IBM and Airbiquity.

"We're trying to capture on solutions that are already present at the OEM. If you have an existing cloud solution, it's easy for the OEM to extend it with data security." He says this approach is in line with what the company has heard from OEMs.

Karamba Security also proposes the best-of-breed solution, although it says its approach is unique.

David Barzilai, executive chairman of Karamba, says, "Everybody should do what they are good at. Network-based security solutions are pretty good at reporting, but in terms of prevention, they have a major issue of false positives. They are good at reporting what they see. We complement them in prevention and forensics data."

OEMs are starting to move away from outsourcing every piece of the services puzzle, according to Thomas of Fontinalis, whose firm backs Karamba. "We've seen from OEMs a lot more curiosity and a willingness to look at the build-or-buy decision around innovation in new ways."

He sees them being more open to contracting directly with young startups in order to obtain bespoke solutions that the OEM will then validate on its own.

"This doesn't mean they don't want an all-in-one solution," he adds. "It always comes back to ease of use." In some cases, the OEM will identify a point solution and redirect it to its tier 1 or make it a requirement in its specifications.

"It's not a binary decision," he insists, " but there's more creativity and openness about how OEMs best serve their products and their customers.

Continuous monitoring, continual learning

Network monitoring and threat detection, a standard in conventional IT security, has come to the automotive sector. It requires a security operations center to receive and analyze data from connected cars. Lear has partnered with Honeywell to deliver this, while it's also part of HARMAN's offering.

Honeywell's cyber security offering is the Intrusion Detection and Prevention System that detects anomalies in the messages received by the car's computing systems. The embedded software communicates with a security operations center where messages are analyzed for violations of rules or abnormalities. Reports go to the automotive OEM so that it can fix software errors and apply patches.

There will be a learning process for the software tools and for the OEM itself, Tengler says. While the software can be set up to immediately block an anomalous message, he thinks it's likely that, at first, it would be configured to only detect anomalies. That learning process might take place in preproduction vehicles.

"This is one part of layered protection," Tengler says, "another level of monitoring of the system."

Best practices and the Auto-ISAC

The Auto-ISAC has also been working its way through the creation of its set of best practices for cyber security:

- Governance
- Risk management
- Security by design,
- Threat detection and protection
- Incident response and recovery
- Training and awareness
- Collaboration and engagement with appropriate third parties

One they are done, executive director Faye Francy thinks that the organization will likely revisit and mature each one. "This is an iterative process," she says.

There are very many standards bodies involved in creating or modifying standards to apply to automotive cyber security: crypto algorithms including AES, RSA and ECC; the OneM2M standards initiative for the Internet of Things; and the SAE has at least five committees working on it, including the Vehicle Electrical Systems Security Committee.

The Auto-ISAC's work is different. " Best practices are a living document, tend to be more aspirational than prescriptive," Francy says.

Booz Allen Hamilton was asked in 2015 by the Auto Alliance to lead the formation of an Auto-ISAC. Jonathan Allen says the best practices approach allows stakeholders to be more open and collaborative.

"If we were writing standards, people would try to figure out how to meet that standard easiest way. Best practices drive people to share among themselves what they're doing. You can have a lot more frank conversations with best practices."

He also notes that a company that's compliant with a standard is not necessarily secure.

Membership in the organization is growing, and smaller companies are starting to join, although Francy notes that participation can be a challenge for startups.

"Cybersecurity is a global team sport," she says."

Looming issues

Finally, our experts identified a couple of issues that aren't currently being addressed: forced over-the-air updates and aftermarket devices and alterations.

Elektrobit's Schleicher believes that forced OTA to patch vulnerabilities are inevitable. In order to prevent hacking, an OEM might need to provide a security update very quickly. But what happens if someone is driving? "Do you want to stop driving for an hour or two?"

He thinks such updates must be done in such a way that it's convenient for the car owner, ideally even while the car is being operated. Moreover, the OEM will need to find a way to communicate to the driver why a forced update is necessary.

Krish Inbarajan, global head of connected car at Cisco Jasper, says that aftermarket devices pose their own security challenges, ones that OEMs are in no position to address.

While OEMs put controls in place to secure communications within and exterior to the vehicle, he notes, "There are no rules that govern who can put a device in." While providers of aftermarket devices may be moved to secure their products in order to protect their brand equity, devices may not have been validated within the overall cyber security of the OEM's product.

Moreover, Inbarajan says, with hundreds or even thousands of aftermarket vendors in the United States alone, "Security has not necessarily been the focus of the aftermarket, where competition is intense."

While some automakers have expressed the desire to limit access to the OBD port, Inbarajan doesn't think this is feasible because the repair industry needs that access. "That means the OBD port cannot be closed out to reading and potentially writing some information," he says. "If that's the same pipe thru which aftermarket devices get access, how do you make sure you can't read and write to it?"

Cyber security as a differentiator

Consumers are also waking up to the security threats to autonomous cars—and the resultant physical threats to themselves.

Tengler says that many OEMs still don't understand how to implement full cyber security; the ones that do are the ones that will thrive. He says, "It's going to require the understanding that cyber security is no longer a build and forget. It's a build and remember. They must continue to oversee and update and protect."

When it comes to vendors, Fontinalis' Thomas says, " I think we'll see solutions that are bespoke and siloed, as well as holistic or incredibly broad in their application. We'll also see security solutions coming from industrial IoT and a variety of different venues. We'll see lot of winners that surprise people in terms of owning market where they are now and where they go from there."