Automotive cybersecurity: Growing technology needs a broader safety net

Joe Kwederis, Deloitte Advisory principal, and Greg Boehmer, Deloitte Advisory senior manager, Deloitte & Touche LLP

The first car radio caught on in the market in 1930. The first car-mounted telephones followed about a decade later. Since then, technology has claimed a greater and greater place in our cars, all in the name of improving customer experience, safety and security. Now, as the "Internet of Things" (IoT) links machines that create, share, and act on data without the need for human intervention, technology is becoming more central to the act of mobility. As connected and driverless cars emerge, technologies like GPS will become less an accessory and more a critical component. Connected vehicle services will play an increasingly greater role. Consumers will expect these components, systems and services to keep us safe. But what protects them?

The increased focus to make vehicles more connected, automated and driverless will transform our vehicles as product innovation, competition, and consumer demand drive integration of the latest technologies and services. The shift from an environment of independent, closed vehicle systems to one that is connected to vehicle ecosystems represents a historic reshaping of the opportunity and risk equation for the marketplace. This is particularly true when you consider the maturity of cybersecurity capabilities and risks.

One hallmark of the IoT is the "Information Value Loop," in which sensors and machines are able to cycle through the stages of creating, communicating, aggregating, analyzing, and acting on data all by themselves. When the sum of those decisions and actions is the safety of human passengers, it becomes critical to make sure any vehicle ecosystem has three mutually reinforcing properties:

- **Secure:** Prevention is worth more than a cure, and effective risk management begins by preventing system breaches or compromises.
- **Vigilant:** Hardware and software can degrade, the nature and intensity of attacks can change, and no level of security is perfect. Security must be complemented by monitoring to determine whether a system is still secure or has been compromised.
- **Resilient**: When a breach occurs, limiting the damage and reestablishing normal operations are much more easily and effectively done when there are processes in place to quickly neutralize threats, prevent further spread, and recover. Remember the definition of "fail-safe"—not safety from failure, but safety *during* failure.

Security, vigilance, and resilience are hallmarks of cyber risk management and information security in more familiar information ecosystems. If the vehicles of the future are leveraging the same technologies we find on our home computers, networks and mobile devices, then are they not subjected to the same vulnerabilities and sensitivities? Companies and consumers need to consider the myriad of cybersecurity risks as the future of mobility takes shape. These risks will only multiply, and they demand attention. According to the World Economic Forum, "Hacking the location data on a car is merely an invasion of privacy, whereas hacking the control system of a car would be a threat to a life."[9] After all, when something goes wrong with your home PC, "crash" is only a metaphor.

Securing vehicles of the future

The importance of securing individual sensors is perhaps most important in today's connected car—a data center on wheels full of Internet-connected features. A typical automobile today contains about 70 computational systems running up to 100 million lines of programming code—twice as many lines of code as the Windows Vista operating system.[10] Along with GPS devices that aid navigation and report on real-time traffic and road conditions, diagnostic devices assess maintenance needs and alert authorities in the event of an accident or breakdown. Many motorists are already familiar with automated theft-retrieval systems, and insurance companies are now promoting safety data transceivers that plug into cars' OBD-II ports. As infrastructure evolves, cars will have the ability to communicate with roadside devices such as traffic lights. Security must inform design from the outset.

IoT-enabled features can help automakers attract early-adopter customers while enhancing safety and convenience. In today's cars, IoT-enabled technologies and services include power and infotainment systems, remote locking and unlocking, and remote engine start, with data flowing between different vendors. Vehicle-to-vehicle communication spans ecosystems as well—for instance, connecting an automobile to the driver's home. Smart cars can communicate with smart home hubs to open garage doors, unlock front doors, and turn on house lights when GPS registers that the driver is nearing home. The *scope* of data communicated between connected vehicles encompasses a wide swath of personal information such as driving habits, real-time location, entertainment preferences, and daily schedules.

Much of this communication uses existing tools repurposed for the IoT, including mobile apps, cellular networks, and SMS technologies not originally designed for secure communications. These extended functionalities leave networks vulnerable to breaches. A recent survey found that nearly 100 percent of today's cars include wireless technologies that may be inadequately secure, and most manufacturers may not be able to easily determine whether their vehicles have been hacked.[11] Hackers, on the other hand, have demonstrated the ability to infiltrate vehicular systems by using SMS texting.[12] Physical attacks via onboard diagnostic devices have shown it could be possible to manipulate some systems even while cars are moving.[13]

Another complication: Those managing the secure development and deployment of these technologies often have less experience doing so—particularly for automotive. Coupled with the newness of the technology, that may mean fewer precautions to secure data at the component level. IoT manufacturers have yet to implement common security standards. Data transmission between multiple vendors—the automaker, dealership, third-party data centers, GPS and onboard diagnostics systems, smart home devices, and others—creates multiple vulnerable points that should be monitored.[14] Hardening the current systems and components with tougher security measures will be crucial to safeguarding the connected automobile.

How is the risk and regulatory environment adjusting?

We have seen a broad set of responses to the risks. Senator Markey introduced the Security and Privacy in Your Car Act of 2015, which would begin the process of developing motor vehicle cybersecurity regulations. Additionally, with Defense Department backing, Mission Secure of Charlottesville, VA, and the University of Virginia are developing a proprietary methodology for identifying the most effective and easiest ways to launch cyberattacks on autonomous systems.[15] They are continuing to explore security vulnerabilities and solutions at events such as the Defense Advanced Research Project Agency's (DARPA's) automated vehicles challenges.

The National Highway Traffic Safety Administration (NHTSA) meets regularly with the technical leads at OEMs and Tier 1 suppliers regarding their cybersecurity initiatives, processes, risk assessment and product/process plans to design security into their products.[16] NHTSA also works closely with other federal organizations with interests in automotive cybersecurity like DARPA, the U.S. Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST). These activities and partnerships reflect the broader acknowledgement of the changing risk, cybersecurity, privacy and regulatory environment, but there is a lot of work to be done. Cybersecurity is becoming a regular agenda item on many boards as companies seek to understand and manage strategic, reputational and cyber risk.

Next steps

As vehicles continue to expand in complexity, the attack surface of an automobile expands. A single vulnerable device can leave an entire automotive ecosystem open to attack, and the potential exposure ranges from inconvenience to massive safety breakdowns. In the face of such challenges, automakers can remain secure, vigilant, and resilient by taking several steps to safeguard their ecosystems and the data they create. Stakeholders in the new mobility landscape need to be active in shaping a secure future by:

- **Expanding the dialogue:** Continuing to engage in the regulatory, risk and cybersecurity dialogue to enhance overall vehicle safety, security and privacy.
- **Developing talent:** Cultivating the industry's cybersecurity talent, methodologies, expertise and awareness to improve overall vehicle safety and security.
- **Securing the product:** Building secure product development and software coding regimens to create, maintain and operate critical hardware and software components—with heavy involvement from security professionals.
- **Monitoring for threats:** Creating robust technology and monitoring capabilities to manage security events and responses—sharing information across the industry on evolving threats and responses.
- **Building for resilience:** Establishing capabilities within the vehicle, its ecosystem and supply chain for avoiding attacks, repairing vulnerabilities and responding to attacks.

High stakes

In the IoT, the many data-driven components of a car will form a rolling ecosystem. The car itself will be one component in a larger ecosystem. And the whole thing will be moving at highway speed, with people's lives and their personal information as the cargo. Cyber threats and cybersecurity have paced each other in an arms race for many years. But now, those dual forces have a new field of battle.

The prospects for creating and operating within a seamless, secure network—with or without external partners—may seem daunting. Vulnerabilities exist on all sides. Security cannot be an afterthought—it must be integral throughout the design process. Connected product and services that blend a deep understanding of the myriad of use cases with knowledge of multilayered cyber risk management techniques can create customer experiences that are secure, vigilant, and resilient.