Wake Up or Crash

Sounding the Alarm on Automotive Cybersecurity

By: Peter Samson, Senior Vice President and General Manager
SI Embedded, Security Innovation

SECURITY INNOVATION

By now, everyone has heard the horror stories of pirates commandeering freighters off the Horn of Africa: small, speedy boats boarding large vessels and holding the crew for ransom . . . or worse.

The threat has waned in recent years, but only after considerable pain and suffering was incurred by the international shipping industry - and after mounting effective, coordinated and system-wide countermeasures.

But piracy isn't for the high seas alone; a newer, more modern variant has emerged that could affect a growing number of the one billion vehicles on the road today.

Imagine a woman putting her kids into a car to go school. When she turns the key to start the engine, a message appears on her navigation screen: "This vehicle has been hacked. Pay 2 Bitcoins to unlock your car."

Farfetched? Maybe not; unlike the ragtag Somalia pirates brandishing small arms who are repelled with vigilance and low-tech countermeasures, these 21st century pirates can strike from anywhere in the world.

When a phone or laptop is hacked, the potential loss of sensitive data represents a real loss of privacy or hypersensitive financial data that can take months, if not years, to recover.

But few—if any—of these kinds of breaches in cybersecurity represent imminent physical danger.

Now imagine a less likely, but even more horrifying, attack that takes over the primary controls of a 5,000-pound full-size SUV with as many as eight passengers. This threat, too, is quite real.

So why are so few imagining it ?

While the motoring public remains largely unaware of the threat, our Federal law enforcement agencies are beginning to get a notion of its danger.

A Public Service Announcement earlier this year from the FBI warned:

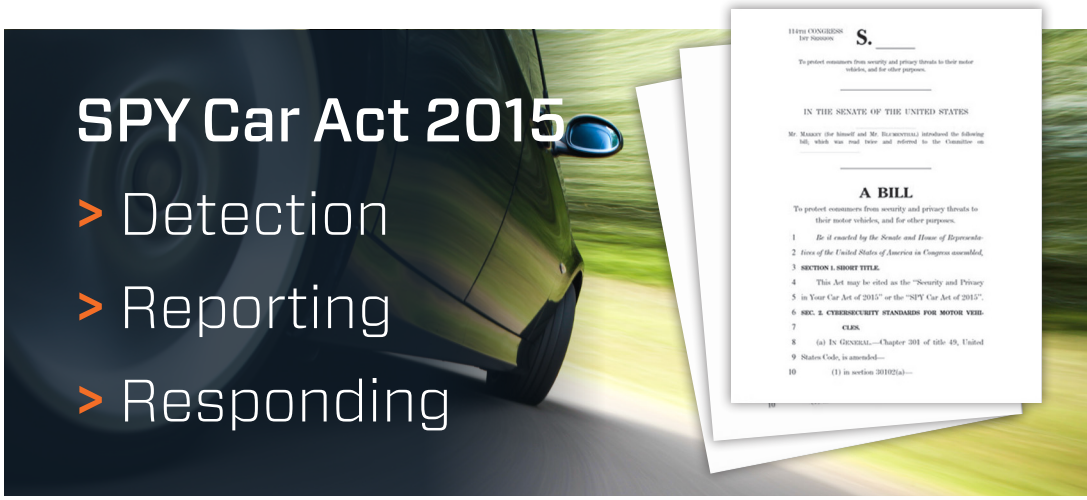
MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

...it is important that consumers and manufacturers are aware of the possible threats and how an attacker may seek to remotely exploit vulnerabilities in the future. Third party aftermarket devices with Internet or cellular access plugged into diagnostics ports could also introduce wireless vulnerabilities.

And despite being one of the most regulated industries in the world, additional government action remains important to stimulate industry collaboration and encourage compliance with new standards within a framework of the emerging consensus on what those security standards should be.

The SPY Car Act of 2015 requires both NHTSA and the FTC to establish new standards for auto cybersecurity. NHTSA has also weighed in with Automated Vehicle Policy guidance as well.

In addition to creating new standards, the SPY Car Act directs automakers to isolate key driving controls from the ECU as well as a "Detection, Reporting, and Responding to hacking" measure.



No doubt, the need for cybersecurity in the automotive industry is real. According to a recent Frost and Sullivan study, it is expected that by 2020 there will be more than 220 million connected vehicles on the road. And, the demand from consumers and fleets for connected infotainment and vehicle systems, as well as a shift from mechanical controls to electromechanical controls to purely electronic controls ("drive-by-wire" etc.), will combine to expose automakers and drivers alike to electronic hijacking.

But even without actual hijacking events, will customers become aware of the dangers? And what could this awareness do to the auto business?

A recent KPMG survey study shows consumer's buying habits will be affected by security threats; while stolen IDs for personal banking and credit cards are more top of mind with consumers, they've only really begun to become aware of the more serious hacking scenarios. We can only imagine their reaction when they learn the implications for their connected car.

And while no large scale attack on passenger vehicles has happened thus far, it's only a matter of time as the number of hackers climbs to more than 150,000 in 2018, according to industry analysts Frost and Sullivan.

150,000 hackers globally by 2018

A Giant Awakes

The good news is that the auto industry is making meaningful progress in recognizing the potential severity and scale of the threats against vehicle and data security.

The industry is trying to get out ahead of the problem through pre-competitive cooperation; last year, automakers working through their Auto Alliance group launched the Automotive Information Sharing and Analysis Center (Auto-ISAC). Its purpose is to act as a "central hub for gathering intelligence that allows automakers to analyze, share and track cyber threats and spot potential weaknesses in vehicle electronics."

> The auto industry is making meaningful progress in vehicle and data security.

Just this year the Auto-ISAC announced a "Framework for Automotive Cybersecurity Best Practices" and "Automotive Cybersecurity Best Practices." The idea is that threats are flagged among members to react and respond adequately…across and among industry participants.

Culture Change: Imaging the Idea of a "Safe" Car

50 years ago, a young lawyer named Ralph Nader took on the auto industry and prompted a now well-known series of changes at both the industry and regulatory levels; the result of which is that automobiles became much safer.

Now, safety is at the heart of every automaker; some car companies—Volvo and Mercedes-Benz most notably—even market their vehicles by appealing to the ideas of crash avoidance and survivability. Volvo even claims that by 2020, no one will be killed or seriously injured in a new Volvo car or SUV.

The question facing the industry and regulators is will we—as a driving society—require the cybersecurity breach equivalent of exploding fuel tanks to change the culture? Or will we remain, in Nader's words, Unsafe at Any Speed?

In the past, engineers fundamentally re-worked their vehicles from the ground up to address the safety threats presented to modern drivers and their passengers; today, we need to do the same thing to address the multiple entry points (tire pressure monitors, OBD-II ports, Wi-Fi connections, etc.) for data breaches in the modern, connected car.

Security needs to be a priority, but a recent survey by the Poneman Institute, a leading independent security research organization, found that 52 percent of OEM and auto supplier survey respondents believed that hackers are actively targeting automobiles; worse, the suppliers who will build the hardware and software show less concern than the automotive manufacturers (by 10 percent).

In short, half now believe new vehicles are at risk and the number is growing. However, across the industry only 54 percent feel security is a priority for their company. This ranks among the lowest compared to other industries like financial services (73 percent) or healthcare (67 percent). And what's even more worrisome is that a far greater percentage of senior managers believe that security is a priority than do their development teams (61 percent to 45 percent), indicating a leadership and communication challenge.

> 52 percent of OEM and auto supplier survey respondents believed that hackers are actively targeting automobiles.

Although the numbers look better than last year, less than half (47 percent) of all respondents have security processes, less than half (47 percent) are trained on security and only 46 percent have the necessary enabling security technology.

Next Steps: A Framework for Action

Security needs to be considered at every step of product development. The industry needs to take a holistic approach.

Cybersecurity and the protection of new vehicles and the consumers driving them should be thought of as designing a castle with multiple layers of defense . . . and that defense should be throughout the entire vehicle development lifecycle.

First, the industry needs to define the totality of automotive cybersecurity for OEMs and suppliers. This needs to include design, development and the full rigors of testing that the industry already has in its DNA for physical safety.

> Security needs to be considered at every step of product development.

Poneman... Go

As the Ponemon Institute's recent Automotive Cybersecurity survey discovered, at present, many car companies leave cybersecurity to the quality assurance teams (18%), who often have insufficient training in the identification and remediation of vulnerabilities.

Others from the survey named the Chief Information Officer (22 percent) followed by Chief Information Security Officer (17 percent), developers (12 percent) and partners (11 percent) as having the ultimate responsibility for cybersecurity. And, 19 percent report that no one has the overall responsibility in their organization.

Today, it's clear that most automakers are only dabbling with the notion of an existential threat; but General Motors' hiring a Chief Product Cybersecurity Officer was a profound signal sent to the industry that the threat is in

fact real and that they are beginning to take this seriously at the executive level.

We, as an industry, should be assured that the trial lawyers will argue that pushing down the responsibility for vehicle cybersecurity to the ranks of middle managers is gross negligence and dereliction of duty by the heads of product development.

This needs to change immediately.

As we begin to recognize the importance of having in-house cybersecurity experts throughout the product development organizations of the car companies, we need to find the right people with the right skills and training as soon as possible. Also, credible and skilled third-party experts can and should fill the gap.

Finally, security requires an immediate need for encryption specialists to secure vehicle and customer data.

This leads to the bigger questions of who actually owns the vehicle data and who will be responsible for ensuring security and privacy? The answer isn't always obvious.

If a customer uses their phone to access infotainment features in their vehicle—and that phone data is breached through the car—who is responsible? The handset maker or the automaker? Where is that handoff in responsibility? Is there any shift ever in responsibility if the phone interfaces with the vehicle?

It's understood at this point, as was mentioned earlier in this paper, that a mass data breach is a question of when, not if. To that end, OEMs and suppliers must focus on preparedness, beginning with square one.

Teams throughout the organization, including purchasing, will require training. And, unfortunately, this is not currently happening within the industry with just under half (49%) of those asked in the Ponemon survey saying they have proper training.

At the systems level, standards will need to be established, not only within the company, but likely between companies (both OEMs and suppliers). Security practices, once established, will themselves require continuous validation and updating.

The necessary industry-wide next steps include on-going collaboration to establish standards for the industry (in our view, the Auto-ISAC materials and framework constitute a meaningful first step in this direction).

With 39 percent of respondents in the Ponemon research believing the automotive industry is not sufficiently knowledgeable about secure platform development, we also need to aggressively learn from the experience of other industries, most notably banking and retail, to avoid the mistakes of the recent past.

We, as an industry, need to imagine and engineer a holistic solution. Just as traditional industries now know there is no silver bullet, the automakers should leverage firewalls, hardware roots of trust, network segmentation, intrusion detection and other tools at their disposal. They also need to perform detailed threat modeling early in the development process to prioritize security and privacy investments.

> A mass data breach is a question of when, not if. To that end, OEMs and suppliers must focus on preparedness, beginning with square one.

This broad view of security must also include the dealer network. There are more than 90 million dealer communication system transactions per month. These serve as easy points of access for hackers and need to be addressed.

Finally, the industry should recognize that cybersecurity is currently not one of their core competencies and seek out established third-parties to help them navigate unchartered waters and chart a course for avoiding the mines floating just below the water's surface in the near and long term.

In conclusion

The industry is beginning, but just beginning, to recognize the threat. Some major players have begun to act in significant ways. But the risks are too great and the threats are too pervasive to treat cybersecurity as an afterthought.

The auto industry has a long history of being beset by great, highly visible crises that eventually lead to great change—typically after a barrage of lawsuits, Congressional hearings and loss of life and property. Time and time again, the industry has fallen hard to the risk of acting "pennywise and pound foolish."

This time – on cybersecurity – it doesn't have to be that way.

About Security Innovation

Since 2002, Security Innovation has been the trusted partner for cybersecurity risk analysis and mitigation for the world's leading companies, including Microsoft, Sony, GM, Disney, Google and Dell. Recognized as a Leader in the Gartner Magic Quadrant for Security Awareness Computer-Based Training for the second year in a row, Security Innovation is dedicated to securing and protecting sensitive data in the most challenging environments - automobiles, desktops, web applications, mobile devices and in the cloud. Security Innovation is privately held and headquartered in Wilmington, MA USA.

www.securityinnovation.com

SECURITY INNOVATION