VOL. 1

SAFE TRAVELS IN THE

CAR OF THE FUTURE

WINTER 2017

Trends in Next-Generation Automotive Safety and Security

In This Report

1

The State of Security in the CONNECTED CAR

Driving has never been better. The newest cars on the road are equipped with active safety features that help protect drivers and passengers, heads-up displays that make it easy to read instruments, and in-vehicle infotainment that makes the trip more enjoyable. Once found only in luxury models, these features are making their way to volume brands, much to the delight of drivers everywhere.

However, as vehicles become more connected and automated, security is of greater concern. Vehicles are an attractive target for hackers. Security researchers have already demonstrated exploits on popular vehicle models, while other malicious attacks have remotely disabled door locks and entire vehicles.[1]

Consumers, automakers, and suppliers alike are nervous. Even lawmakers are getting involved. In the United States, the Security and Privacy in Your Car (SPY Car) Act of 2015 would require the National Highway Traffic Safety Administration to issue vehicle cybersecurity regulations to protect against unauthorized access to electronic controls and data.[2]

> "In 2016, one security researcher showed that he could compromise a vehicle's lidar sensor with a device he assembled for just $43 and a laser pointer.[5]"

To secure a vehicle adequately, it must be protected at all levels, from hardware and software to networking and the cloud. In addition to leading research and helping define new standards, Intel is committed to developing security technologies for the new transportation ecosystem.

Three Must-Know Trends in Automotive Security

01: Gartner predicts that by 2019 two automotive companies will be fined for vehicle software design negligence that results in inconsistent technology performance or cybersecurity attacks.[3]

02: Sixty-two percent of consumers worry about connected cars being easily hacked.[4]

03: Forty-four percent of consumers believe a vehicle manufacturer is most responsible for securing a vehicle against hacking.[4] Thirty percent say the makers of mobile software and apps are most responsible.[4]

1. "Hackers Remotely Kill a Jeep on the Highway—with Me in It." Wired, July 2015, wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
2. SPY Car Act of 2015. U.S. Congress, July 2015, congress.gov/bill/114th-congress/senate-bill/1806/all-info.
3. "Staying on Track with Connected Car Security." Gartner, Feb. 2016, gartner.com/smarterwithgartner/staying-on-track-with-connected-car-security/.
4. "Braking the Connected Car: The Future of Vehicle Vulnerabilities." Kelley Blue Book, March 2016, rsaconference.com/writable/presentations/file_upload/ht-t11-hacking-the-connected-car-thetfuturetof-vehicle-vulnerabilities.pdf.
5. "Self-driving cars are prone to hacks—and automakers are barely talking about it." Business Insider, Dec. 2016, businessinsider.com/driverless-cars-hacking-ricks-2016-12.

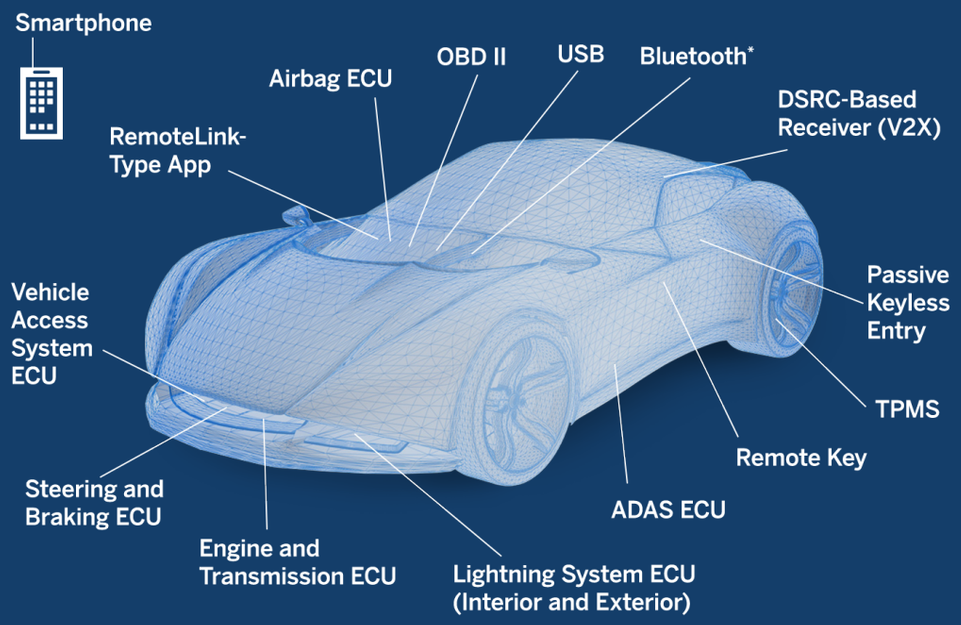
2

15 Main Hackable Points in the Next-Generation Car

(and What to Do about Them)

Smartphone integration. Keyless entry. Blind spot detection. Every cool new feature in a next-generation car brings with it another potential attack surface of an electronic control unit (ECU) and another point of connection.

Where digital meets driver, safety is critical. Analysts say that protecting a vehicle starts with integrating security features during the design and production stages.[1] Intel has already developed some of the most advanced in-vehicle security features on the market. In addition, with a growing number of potential attack points in the vehicle (see the illustration below) Intel is addressing three major challenges in automotive security.



Fifteen of the most hackable and exposed attack surfaces on a next-generation car.

CHALLENGE #1

The vehicles of tomorrow may incorporate hundreds of ECUs. This makes assessing the scope of threats an immense job, as just one unprotected attack surface can lead to a serious hack.

The Solution: Intel is working toward greater consolidation, integration, and virtualization of ECUs. But even with consolidation, automotive architectures will continue to grow more complex. That's why Intel is continuing to invest in artificial intelligence, self-adaptation, and, ultimately, self-healing breakthroughs that will significantly increase the level of security in connected and automated vehicles. A range of specific Intel® security technologies are available today that can help protect the vehicle's systems and data.

- Secure boot authenticates firmware components during boot.
- Intel® Trusted Execution Engine provides advanced runtime protection at the hardware level.
- Intel® Virtualization Technology for Directed I/O helps isolate and restrict execution environments to hardware-partitioned sandboxes, ensuring key safety tasks are prioritized over other functions without interruption.

CHALLENGE #2

The attack surface of a next-generation vehicle extends beyond the car itself. It can include external Wi-Fi and cellular networks, as well as connected infrastructure, such as toll roads, drive-through windows, and gas stations.

The Solution: With expertise in network monitoring and enforcement, Intel is working to improve the authenticity and integrity of data transmitted across networks.

- Intel secure storage for key exchange and encryption allows a manufacturer to embed a secure key into the Intel automotive system-on-chip (SoC) to protect against unauthorized software or firmware updates.
- Intel® Enhanced Privacy ID allows cars to connect to smart infrastructure without disclosing personally identifiable information.

CHALLENGE #3

In addition to protecting the vehicle and networks, transportation providers must also protect data as it moves through the cloud and to the data center.

The Solution: Intel is optimizing security technologies forged in the data center to support secure automated driving and connected transportation.

- Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) accelerates the encryption of data in the Intel® Xeon® and Intel® Core™ processor families, keeping data secure from the vehicle to the data center. Intel AES-NI makes pervasive encryption more affordable and feasible in areas where it previously was not.
- Security features are embedded in the hardware of Intel Xeon processor-based servers.

3

KNOW YOUR OPPONENT: The Six Types of Hackers

To confidently secure automated vehicles, it's important to know whom you're up against. By getting inside the brains of potential hackers, you can understand their strategies and motivations.

THIS CAN HELP YOU PLAN THE BEST COUNTERATTACK.

Researchers and hobbyists

Driven either by curiosity or a generous grant, researchers and hobbyists sometimes work alongside universities, government labs, or industry groups. Their main goal is to find vulnerabilities before the market hits critical mass. The good news is that these hackers share their findings with the industry so that exploits can be quickly corrected.

Pranksters and hacktivists

Welcome to the dark side of the hobbyist group. Whether promoting their own cause or just showing off their skills, these hackers are up to no good. Their antics only lead to negative outcomes for the product owner or manufacturer.

Owners and operators

Tech-savvy owners pose a unique challenge. They're not criminals. They simply want to hack their own vehicles for repairs, to remove restrictions, or to improve performance. Of course, tampering with safety-critical systems is almost always bad news for everyone involved.

Organized crime

Where there's money to be made, there's motivation to hack. These criminals exploit vulnerabilities that allow them to steal vehicles, intercept data, or hold individual cars or entire fleets for ransom. The worst part? The sophisticated tools these hackers develop are sold to other criminals as a cybercrime-as-a-service model.

Nation-states

Industrial espionage. Illicit surveillance. Economic or physical warfare. The motives of nation-states are not easy to pinpoint, but their results can wreak havoc. As cybercrime matures and code is shared, devastating hacks developed by nation-states could make their way into the hands of lower-level criminals, increasing threats.

Transportation infrastructure

Smart vehicles need to do the right thing, even when the instructions given to them are wrong. Imagine, for example, a traffic light set to green in both directions. It's important to remember that next-generation cars aren't just communicating with the cloud, but with each other and the transportation infrastructure. This means smart vehicles must safely navigate through these scenarios to protect everyone inside and around the vehicle.

4

What's Next in Automotive Security?

AN INTEL EXECUTIVE Q&A

Craig Hurst is the executive director of the Future of Automotive Security Technology Research (FASTR) industry consortium and director of industry initiatives and marketing within Intel's Transportation Solutions Division.

Q: At what point in development do automakers and suppliers need to think about security?

From day one. People underestimate how broad a practice area automotive security really is. By starting early and doing a holistic analysis, you're better positioned to identify and mitigate risks. Security should be a nonnegotiable ingredient in the product design life cycle from the start. How will you audit your suppliers, contractors, and internal development teams for security robustness? These are considerations that are needed when defining the system architecture.

Q: How can automakers protect every potential attack surface?

They need a resilient, in-depth security architecture that scales from the lowest electronic building blocks in the vehicle all the way to the data center. This is a critical part of Intel's approach to automotive security.

To use an analogy from modern warfare, there are no front lines. Small units are expected to operate individually to solve tactical goals. In complex systems, such as vehicles, the architecture must be designed using isolated regions of functionality, where failure of one component should not cause catastrophic failure of entire systems. Think about a submarine design. The failure of one compartment should not destroy the entire vessel. Resiliency, self-recovery, predictive failover—all are new aspects of building future secure vehicles.

Q: Can you give an example of how Intel is extending security beyond the vehicle's hardware?

Intel is working closely with the automotive ecosystem, including software providers such as Green Hills Software, QNX, Wind River, and others, to build a security architecture that starts at the silicon level and extends to the operating system. We're also focusing on secure communication—for example, connecting to the cloud for over-the-air software updates. In addition, Intel's enterprise-grade data center security technologies provide the final step for comprehensive security.

Q: How might artificial intelligence (AI) improve security?

We're doing research into new security technologies that can help cyber-physical systems detect or even predict failures and recover from them. This approach incorporates elements of AI to build a high level of resiliency, allowing cyber-physical systems to modify their own behavior to improve efficiency and adaptability in adverse situations.

Q: How can automakers be sure that their vehicles will be secure for as long as they're on the road?

All security technologies need to evolve to address the threats of their time. For example, public key cryptography was invented in the 1970s to secure network communications. Intrusion detection systems came about in the 1980s in response to viruses and worms on personal computers.

Intel is always researching the latest threats, and automakers can stay agile by building on the foundation of a resilient, flexible security architecture. A secure over-the-air update process will extend the ability of automakers to provide security, as well as feature enhancements, for the life of the vehicle.

5

A Closer Look at Technology: Secure Over-the-Air Updates

Think back to the car you first drove. Chances are it was purely mechanical. Today, cars are practically computers—and soon to be data centers on wheels. Software provides more functionality for drivers—infotainment, mapping, web search—and transportation providers, via enhanced diagnostics and telematics.

A vehicle made today may contain

100 million

lines of code.[1]

The reality is that when it comes to software, bugs happen. However, while a buggy smartphone is simply inconvenient, a faulty piece of vehicle software could threaten the safety or security of its passengers.

Automakers can patch these bugs wirelessly by sending software and firmware updates over the air (OTA). This means vehicles can be fixed quickly, without the time or costs involved with taking them to a dealership. The savings to automakers could reach the billions.

Intel® technologies are helping automakers and transportation providers make OTA updates more secure and reliable. For example, Intel secure storage for key exchange and encryption allows a manufacturer to embed a nonrewritable secure key into the ECU. This way, only the OTA updates that are authenticated against the key will make it into the vehicle.

In addition, Wind River, an Intel company, is continually working alongside automakers and suppliers to reduce the complexities developing software-enabled vehicles. In 2016, Wind River added the Arynga software product line to its portfolio, integrating its secure OTA technologies into automotive and cloud offerings.

Over-the-air software updates could save automakers up to

$35 billion

by 2022.[2]

1. Information Is Beautiful. Accessed Aug. 2016, informationisbeautiful.net/visualizations/million-lines-of-code/.
2. "How automakers will save $35 billion by 2022." Fortune, Sept. 2015, fortune.com/2015/09/04/ihs-auto-software/.

6

Building TRUST for Safer Driving

Advanced driver assistance systems (ADAS), like automatic braking and lane assist, are meant to help drivers keep their eyes on the road and improve safe driving. Self-driving cars will go even further in preventing accidents. But one crucial issue remains: Do people trust automated vehicles?

The actual technology is often not the issue. Instead, it's the implementation that leads to problems with how people interact with automated vehicles. For example:

- Features may be confusing or difficult to use.
- Drivers may misunderstand the limitations of particular features.
- Drivers may mistakenly disengage a feature while believing it's still engaged.
- Missing or confusing indicators, such as lights, icons, words, or audible cues, can exacerbate problems.

Instead of feeling safe and confident when using automated driving features, drivers can feel a kind of anxious vigilance. They may be so unsure of how features are working that they choose not to use them at all.

Earning the trust of drivers and passengers is just as important as the technology that powers automated vehicles. Each year, Intel spends millions on research to reveal insights for better interactions between the vehicle and its occupants—in other words, the human-machine interface (HMI). Here are four capabilities at the heart of these trust interactions.

1. COMPREHENSIVE SENSING

Not only should an automated vehicle be able to sense as close as possible to 360 degrees around itself, but it must also show drivers and passengers what it sees. For example, if a pedestrian or bicyclist is crossing in front of the automated vehicle, the HMI should show passengers a visual display of what is happening so they feel confident in the vehicle's ability to stop or navigate around the obstacle.

Sensing inside the vehicle—knowing the number of passengers, where they are, and what devices they are carrying—is also important, since it can better communicate trip information and whether a passenger has left an item behind in the car. Interior cabin passenger awareness also helps determine the most effective communication methods.

Understanding the context of the cabin, fused with the context of the environment, will allow for safer and more natural interactions. Technologies like Intel® RealSense™ are useful in capturing high-fidelity information to help detect the locations of arms and feet, head orientation, and some biometric data.

2. CLEAR, BIDIRECTIONAL COMMUNICATION

Automated systems must communicate simply and clearly with drivers and passengers. This can be a balancing act. Intel's research has found that in some situations, passengers want more information, such as when the vehicle is rerouting. In other cases, passengers don't want to know every detail, like when the vehicle is stopped at a traffic signal.

3. RESPONDING TO CHANGES

If an automated system is slow to respond to passenger inputs, or if it gives complicated or imprecise responses, it will be seen as unreliable or not working right. Quick, precise, and predictable responses will help drivers and passengers feel comfortable that a system is capable of doing what has been asked of it. In an emergency situation, the system should provide context for what has just happened. For example, if the car needs to pull to the side of the road, it should explain why and what the passengers should do next.

4. MULTIPLE MODES OF INTERACTION

Giving drivers and passengers a variety of ways to communicate—voice interactions, touchscreens, and mobile devices—can help them notice and understand important information. In Intel's research and testing, participants have often started a trip one way (such as by speaking the destination), and then shifted to other modes during the trip (such as using the touchscreen to choose an additional stop).

To achieve these capabilities, active safety and infotainment systems must converge into a unified system architecture. Intel is supporting this approach through hardware virtualization, such as Intel® Virtualization Technology for Directed I/O, and the consolidation of Intel automotive SoCs. With smarter architecture and HMI designs, automakers can help ensure the success of fully autonomous vehicles in the market.

7

Who Wants to Know?

PROTECTING DRIVER AND PASSENGER PRIVACY

The car used to be a closed environment. Today, it's an extension of the smartphone. Entertainment libraries. Even home automation systems.

More consumers are expecting their next vehicle to come with connected features like built-in GPS navigation and compatibility with mobile devices. In addition, transportation providers need to collect data in order to manage fleets and provide value-added services to drivers and passengers. This means a variety of personally identifiable information—location data, address books, and credit card numbers—are now entering and leaving the confines of the vehicle.

Government regulators are already starting to take action to protect the privacy of drivers in connected cars. In 2016, the European Commission adopted new rules to help strengthen data protection for individuals with its General Data Protection Regulation (GDPR).

When it comes to data privacy, there are two main aspects: keeping personal data confidential and preventing data leakage outside the consumer's control.

1. CONFIDENTIALITY

To maintain confidentiality, data needs to be encrypted inside and outside the vehicle when stored, transmitted, and processed. This includes not only stored personal information, but also styles of driving, locations visited, and other metadata. Intel helps keep data encrypted from the car to the cloud with Intel® AES-NI.

2. PREVENTING LEAKAGE

One important step in preventing leakage is minimizing the amount of data shared with third parties. Vehicles must share some data in order to communicate with smart city infrastructure, such as traffic signals. Intel® Enhanced Privacy ID (Intel® EPID) enables vehicles to connect with smart infrastructure without disclosing any personally identifiable information—only verification that it's part of a group of vehicles approved to access certain alerts, such as light changes and approaching emergency vehicles.

8

Bringing It All Together

Creating a More Secure Ecosystem

Vehicle security goes beyond the door lock. That's why Intel takes an approach that starts well in advance of product design. Here are six ways Intel is building security technologies into every point across the new transportation ecosystem.

1 Rigorous design life cycles

Like the systems they target, hackers' techniques evolve over time. Intel's design cycle includes ongoing internal and external security audits to evaluate and swiftly respond to new potential threats. In addition, to help minimize the attack surface, Intel is exploring designs that drive the consolidation and virtualization of ECUs in the vehicle.

2 Talent and corporate acquisition

By adding focused expertise, Intel is accelerating the development of functionally safe products. In 2016, Intel acquired YOGITECH, an expert in semiconductor functional safety and methodologies. This reinforces Intel's already rigorous manufacturing methodologies and quality systems. In addition, Wind River, an Intel company, acquired the Arynga software product line for secure OTA updates.

3 5G network development

Get ready for breakneck speeds. 5G will deliver incredibly high bandwidth and low latency, opening the doors for fast and secure vehicle-to-everything (V2X) applications, OTA updates, and entertainment services. Intel is paving a path forward with expertise in network monitoring and enforcement to improve the authenticity and integrity of data transmitted across 5G networks. And by partnering with leaders in the telecom industry, Intel is ensuring that secure connectivity solutions for the automotive industry will be ready when 5G arrives.

Analysts say that technologies like message encryption and authentication can't be incorporated into existing vehicles, but must be integrated during the design and production process.[1]

4 Heterogeneous architecture

Rather than relying on a single compute architecture to handle everything, Intel®-based platforms harness a flexible architecture of CPUs and integrated accelerators. With multiple domains of overlapping compute and sensor fusion, workloads can be distributed with greater safety and security. These designs are ideal for level 3, 4, and 5 automated vehicles.

5 Trusted Analytics Platform

It's easy to collect data. The real challenge is extracting value from it. Intel developed the Trusted Analytics Platform (TAP), an open source software optimized for performance and security, to help developers securely connect big data with applications. This simplifies solution development so that transportation providers can derive value from data faster.

6 Ecosystem collaboration

Intel is investing in partnerships with hardware vendors, software vendors, and integrators to develop secure solutions for the automotive industry. To accelerate collaboration, in 2016 Intel announced a USD 250 million Intel Capital investment fund for the automotive ecosystem.

1. Report to Congressional Requesters. GAO, March 2016, gao.gov/assets/680/676064.pdf.

9

INTEL: PROTECTING VEHICLES

FROM CAR TO CLOUD

When it comes to building the next-generation vehicle, nothing is more important than protecting its drivers and passengers. Backed by 30 years of embedded security and IT expertise, Intel is developing solutions that help protect people and data, from car to cloud.

Intel is leading an industry of community thought leaders—in hardware, software, networking, and the cloud—to solve the toughest challenges in transportation safety. With an eye on comprehensive security, Intel is making investments in talent and corporate acquisitions to strengthen product offerings in functional safety and security. By partnering with a wide range of academic research labs, conducting research workshops, and defining reference architectures and technologies, Intel is setting new standards for safe, secure transportation.

With technology and product leadership that span the vehicle, communications, and the data center, Intel is uniquely positioned to prepare transportation providers for the amazing future of transportation. And with a continued commitment to security and safety, Intel is providing layered protection with features rooted in the hardware and trusted cloud services.

To learn more, visit **intel.com/automotive.**

10

Resources

Intel Automotive Security Best Practices
Read the white paper ›

Intel®-Powered Automated Driving
View the infographic ›

Advanced Driver Assistant System Threats, Requirements, Security Solutions
Read the technical white paper ›

Future of Automotive Security Technology Research (FASTR): **fastr.org**

SPONSORED BY intel®