Cybersecurity Challenges in the Automotive Industry

SECURITY COMPASS RESEARCH WHITE PAPER

2018

The Current State of Affairs

The automotive industry is undergoing a drastic change. We're at a point, now, where technology has total control over automobiles. With the emergence of connected cars and the complex software that controls them, there's growing concern about the security of the operating technology.

As a part of the Internet of Things (IoT) movement, cars have the potential to host passengers that are more productive and safe during transit. However, the increased connectivity also creates a greater attack surface on the vehicle's controller area network, and just one attack could be detrimental. The connected car future may seem far off, but we're already seeing concrete examples tested in the real world, with self-driving Tesla cars and advanced driver-assistance systems (ADAS) with adaptive cruise control, driver fatigue detection, and collision avoidance. If a malicious hacker gets behind a cyber-physical feature, they have the power to make automotive decisions that have real, and potentially fatal, consequences.

Recognizing the Problem of Lacking Security

Despite the fact that companies struggle with taking the appropriate actions to build security into their technologically-advanced automobiles, it's still a major concern for them. In fact, 89% of those polled agreed that security for connected cars was important.[1] The problem is that, as of yet, security processes and their corresponding application development lifecycles are not integrated across the supply chain in the automotive industry. Of those involved in the building process, 95% believe that this integration will be difficult to accomplish.[2] Amongst the reported barriers, the following stood out: restricted time and budget, limited familiarity with solutions, and a lack of security standards to resort to.[3] Further, connected vehicles come with increased software complexity, so the potential for security vulnerabilities and defects is even greater.

In this article, we will present our research on the challenges facing the automotive industry today, followed by our proposed solutions. First, we'll address the perceived barriers to implementing a security process in the automotive industry. Then, we will elaborate on a security process solution, our policy-to-execution platform, SD Elements, that fits in with time restraints and budget. As part of our ongoing commitment to help the auto industry manage cybersecurity without slowing down, we have recently partnered with Canada's National Research Council through their IRAP program to add new controls in SD Elements. These controls will help Tier 1 and Tier 2 manufacturers and suppliers create secure code for their firmware and software requirements. Finally, we will review relevant automotive security standards.

[1] 2017 Automotive Cyber Survey Results, Automotive IQ
[2] 2017 Automotive Cyber Survey Results, Automotive IQ
[3] 2017 Automotive Cyber Survey Results, Automotive IQ

Our Assumptions about the Auto Industry

Based on our research, we were able to highlight three assumed truths about the auto industry in its current state:

(a) Traditional car manufacturing is becoming more sophisticated.
Connected cars come with various devices that are connected to the Internet. These devices yield a wide range of communication protocols and transmission media, and many new cars are integrating Wi-Fi. This level of technological complexity is unprecedented.

(b) Connected cars are part of the Internet of Things (IoT) movement, and they are here to stay.
Connected cars are part of the new technological frontier. In fact, the automotive industry alone has seen a 32% increased growth rate in adopting machine-to-machine technology.[4] This puts the automotive industry in second place for highest growth rate, behind the energy and utilities industry (37%).[5] Since connected cars are establishing a place in the IoT movement, any potential issues they have will need to be addressed.

(c) A competitive differentiator in cars will be software – and the software will contain vulnerabilities.
Connected car companies will be immersed in the competitive race to release the most advanced software with the most innovative functions. As a result, software will become more complex, and the potential for security vulnerabilities will increase. Even in less complex software, the development process has its limitations due to time constraints and lack of security expertise. As software complexity grows, the potential for vulnerabilities grows as well. This is where 'shifting left,' or implementing security earlier into the software development life cycle (SDLC), through a policy-to-execution platform, becomes important. Ultimately, shifting left produces software with fewer vulnerabilities. Given the general lack of security awareness in the highly competitive automotive industry, however, stringent security considerations may not be a business priority.

---

[4] Yasir Mehmood et al, "M2M Potentials in logistics and transportation industry", Springer, 2016
[5] Yasir Mehmood et al, "M2M Potentials in logistics and transportation industry", Springer, 2016

Auto Industry Security Challenges

Based on our assumptions about the automotive industry, outlined above, we derived 2 major security-related challenges facing the automotive industry today. Given that there is a widespread security skills shortage problem, with 51% of organizations claiming that they were in the midst of a problematic security skills shortage in 2018, and given that the automotive industry is rapidly growing, we outlined the following challenges:

(a) There is a security skills shortage and a policy-to-governance gap.[6]
As previously stated, 95% of those involved in the automotive building process believe that the implementation of a security system will be difficult due to limited familiarity with solutions and a lack of security standards to resort to.[7] Engineers who manage software, cloud services, and vehicle components do not know how to build according to major compliance and secure coding standards. In order to fill this policy-to-governance gap, cybersecurity training is required. Another comprehensive solution is a policy-to-execution program, such as our platform SD Elements, which will be further elaborated below.

(b) Lack of security controls can have severe consequences.
Building automotive software without a security system in place can result in serious negative consequences for drivers as well as those involved in the automotive building process. Premium connected cars are built with an average of 100 million lines of code, creating great potential for vulnerabilities to arise. Vulnerabilities may be found within a vehicle's wireless communications functions, within the associated driver's mobile device, or within a 3rd party's device that is connected through a vehicle diagnostic port. These vulnerable areas are open to remote attacks in which the hacker can access the vehicle's controller network or its data storage. In a 2014 study, researchers testing a connected car were able to shut down its engine while it moved at a speed between 5 and 10 mph. They were also able to interfere with the brakes and steering at this speed. When they tested the car at any speed, these researchers were still able to manipulate door locks, turning signals, the car's HVAC, GPS, and its radio. In a 2016 study, researchers demonstrated the multiple ways in which a connected car could be attacked, including the attack of ultrasonic sensors that created a Denial of Service, distance alterations, and obstacle obfuscations. They also found that they could conduct blinding attacks on automotive cameras, which interfered with lane departure warnings, traffic sign recognition, lane keeping, and parking assistance.

In addition to the serious safety issues that software security vulnerabilities create for drivers, automotive manufacturers could potentially face serious revenue loss and reputation damage in the case of a data breach. Chrysler, for instance, had to contend with recall costs over 600 million dollars when vulnerabilities were found in their connected vehicles.

[6] 2017 CIO Agenda: An Automotive Perspective
[7] 2017 Automotive Cyber Survey Results, Automotive IQ

The Other Major Challenge in the Auto Industry: Compliance

As connected cars become more prevalent, it's critical that best practices in the auto industry are followed. Outlined below are notable secure coding best practices, regulations, and compliance frameworks that pertain to the auto industry.

MISRA C: The Motor Industry Software Reliability Association (MISRA) focuses on remediating vulnerabilities commonly found in the C language, and they focus primarily on safety-related applications. Their guidelines are divided into three individual classifications, where a guideline is either 'mandatory,' 'required,' or 'advisory.' In order for software to comply with MISRA C, all mandatory rules must be met, all required rules must be met unless formally approved, and advisory rules should generally be followed or else formally documented if not followed.[8]

AUTOSAR Coding Guidelines: Automotive Open System Architecture (AUTOSAR)'s goal is to standardize software so that vehicle manufacturers can better manage growing system complexity. AUTOSAR recently developed an 'Adaptive Platform' for connected and autonomous vehicles.[9]

ISO 26262 Functional Safety: The ISO 26262 is an international standard for the functional safety of electrical or electronic systems in automobiles, defined by the International Organization for Standardization. This standard outlines the 'safety lifecycle' for automobiles, from management and development, to production, operation, and service. It considers safety management concepts including hazardous events, safety goals, and automotive safety integrity levels. It also addresses the functional safety of development, from design, implementation and integration, to verification, validation, and configuration.[10]

SAE J3061 Process Suggestions: The Society of Automotive Engineers (SAE) J3061 process framework offers an engineering process outline that instructs how to design and build cybersecurity into vehicles. These instructions account for the detection of incidents as well as the response to these incidents, and they also cover vulnerabilities related to service and operation. J3061 can be tailored to any given organization's existing development process, so that developers can build according to their original process.[11]

There are plans with SD Elements to improve our audit report capabilities related to major compliance regulations and standards for connected cars. These include NIST 800-53, ISO 26262, and SAE J3061. Our current objective is to add at least one major compliance regulation to the generated report. There are also plans to add a process-level report based on a major security management framework, such as Building Security In Maturity Model (BSIMM).

[8] https://www.embedded.com/electronics-blogs/beginner-s-corner/4023981/Introduction-to-MISRA-C
[9] https://www.autosar.org/fileadmin/user_upload/standards/adaptive/17-03/AUTOSAR_RS_CPP14Guidelines.pdf
[10] http://www.ni.com/white-paper/13647/en/
[11] https://www.sae.org/learn/content/c1730/

Our Solution to the Challenges: a Policy-to-Execution Platform

Our policy-to-execution platform, SD Elements, stands as a potential solution to security challenges faced by the automotive industry. First, it fills in the policy-to-governance gap by translating policies to actionable tasks that can be used by IT and engineering teams to meet security and compliance objectives. SD Elements also succeeds in creating a simple method for implementing security measures by offering an automated security process. Our platform has an expansive knowledge-base that is upkept by Ph.D. researchers and subject matter experts, covering all relevant security and compliance needs. SD Elements operationalizes its robust security knowledge-base on any software, and it allows you to customize its content so that it's specific to your organization and industry. It also integrates Just-in-time Training (JITT) modules with your organization's native ALM so that your developers can learn secure coding on the job.

How It Works

SD Elements has four distinct phases including Identification, Implementation, Validation, and Auditing. The process starts with a 15 minute questionnaire, where information is gathered about the relevant software language, platform, features, compliance, and tools. This information is then used to determine the relevant threats and countermeasures. Once the questionnaire is completed, the appropriate security controls are automatically generated, and tickets including secure coding instructions are delivered directly to the developer. The expert database in SD Elements is regularly updated with new content, and clients are able to custom create their own policies in the platform.

SD Elements effortlessly fits into existing development processes in the user's organization. It synchronizes with virtually all ALM tools, including HP ALM, IBM Rational CLM, JIRA, and Microsoft TFS. It also comes equipped with eLearning and Just-in-Time Training (JITT) modules to address the security skills and knowledge gap in organizations. The JITT modules and relevant code samples are delivered to developers through an ALM synchronization. This training also offers task prioritization, guiding engineering teams on which tasks to address first.

The code samples offered help the developers to understand the 'how' and 'why' of security controls. The test results from SD Elements are imported from HP Fortify, HP Webinspect, IBM AppScan, Veracode, Checkmarx, WhiteHat, and other popular scanning tools. Imported data is matched to controls for validation and compliance reporting. SD Elements offers reports to track progress, risk profile, and compliance. It also offers detailed activity logs for audits and has a custom reporting capability, saving time during regulatory audits and security reviews.

How Your Automotive Organization Can Use SD Elements

In the future, automotive industry content (e.g., compliance) will be added to SD Elements. Organizations can also create custom content capabilities, specific to their automotive company. The SD Elements risk policy compliance feature can be leveraged to mirror organizations' internal policies.

Summary

The automotive industry is transitioning into a new technological space, and the need for systematic security is more critical than ever before. Given that connected cars are in growing demand and new to the market, there's a lot of incentive for companies to compete with one another to put out the most innovative and advanced technology, so that they can differentiate themselves from their competitors. With these pressures added to the increasing complexity of functional software, there's potential for security vulnerabilities to arise in software also increases. Though many people recognize that security is a growing concern for the automotive industry, several perceived barriers–including budget and time constraints, as well as a lack of security implementation processes–stop them from taking the necessary measures to secure their software. In order to overcome these barriers, people need to improve their security skills and knowledge, they need to educate organizations about the negative consequences of lacking security, and they need to establish a simple method for implementing security. As an all-in-one solution, we proposed our own policy-to-execution platform, SD Elements. This advanced platform fills the policy-to-governance gap and provides a simple, automated security implementation method for organizations, while educating developers on security practices.

About Security Compass

Security Compass is a leader in helping customers proactively manage cybersecurity risk, without slowing down their business. Offering SD Elements, Just-in-Time Training, and Enterprise Delivery Services, as well as Verification Services, our first priority is to help your organization efficiently deliver technology that's secure by design. Our solution is tailored to your organization's unique needs, equipping you with the right resources and tools. At its core is our award-winning policy-to-execution software platform, SD Elements, which translates policies into actionable tasks for technical teams. Our Verification Services help to improve your organization's security posture, through penetration testing, Red Teaming, and Cloud Security Services. Security Compass serves some of the world's largest enterprises, including 16 of the largest financial institutions in North America, South America, and Asia, as well as 4 of the largest tech companies in the world. Our privately held company is headquartered in Toronto, Canada with global offices in the United States and India. Follow Security Compass on Twitter @securitycompass or visit https://www.securitycompass.com/

Security Compass

Making Software Secure

www.securitycompass.com

info@securitycompass.com

+1 (800) 777-2211