End-to-end API Security for the Software Defined Vehicle

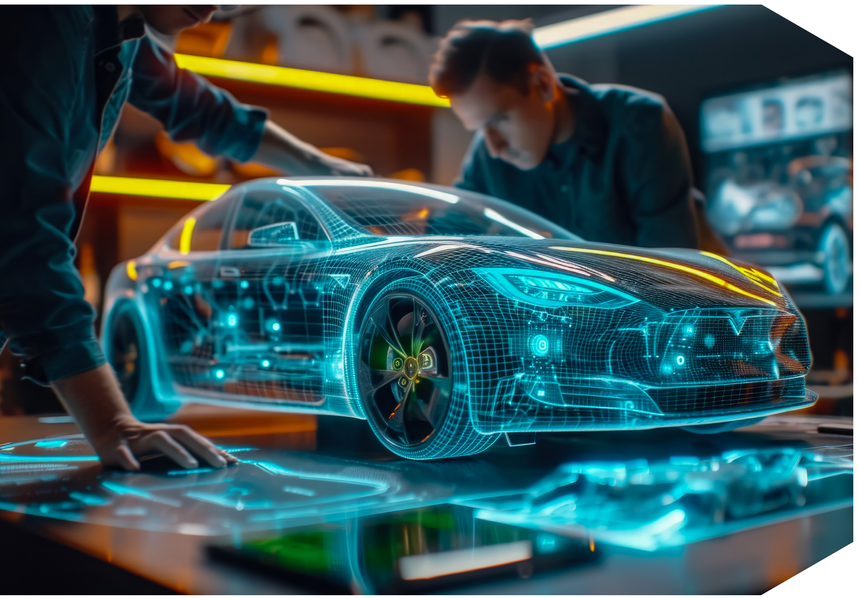
Implementing a DevSecOps Approach for Developing and Protecting APIs

42crunch

Connected services extend beyond the automaker as vehicles consume a wide range of 3rd party services, resulting in billions of API transactions per month traversing the global automotive ecosystem.

Introduction

This paper highlights how to implement a DevSecOps approach for developing and protecting APIs. It identifies what is required to develop and support software defined vehicles and automotive grade APIs at a globally distributed automotive manufacturer. It is important for the reader to understand that software defined vehicles rely heavily on APIs and have extensive safety and security requirements. The security aspects of the automotive API landscape are greatly complicated by the size, scope, and scale of the automotive industry. This paper highlights how 42Crunch is uniquely positioned to address API challenges within the automotive industry and enable an environment where software innovation can flourish globally at scale.



Automotive Grade Software

Software defined vehicles must meet rigorous standards for reliability, safety, and performance. Key attributes include:

Safety: Software must meet high standards for safety, such as ISO 26262, which is focused on the functional safety of automotive systems.

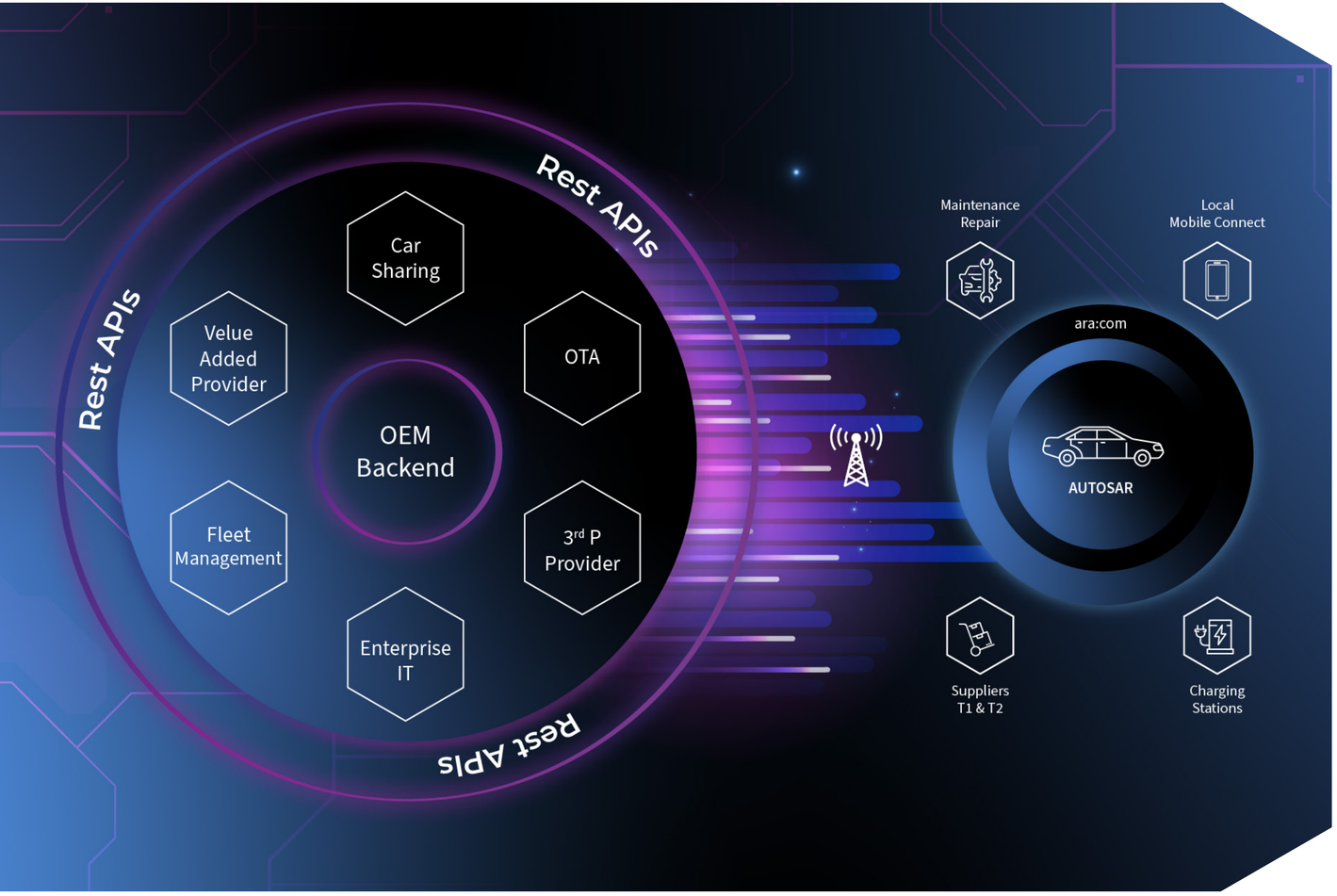
Reliability: Vehicles operate in a wide range of environmental conditions, and the software must perform consistently in varying temperatures, vibrations, altitudes, and humidity levels.

Real-Time Processing: Many automotive applications, such as Advanced Driver Assistance Systems (ADAS), require real-time processing and software must be optimized for low-latency and high-speed data processing.

Security: Software must implement robust security measures to protect against hacking, theft, and unauthorized access, adhering to standards like ISO 21434.

Regulatory Compliance: Software must comply with global industry regulations, such as UNECE R155, and demonstrate that vehicles meet specific technical and safety standards before they can be sold.

Automotive-grade software is foundational for software defined vehicles, and is developed using strict development processes to meet these high standards. This includes not only vehicle software and APIs, but the connected ecosystem APIs and services.



The Connected Vehicle Ecosystem

Vehicles have transformed from stand-alone systems into complex interconnected systems, catapulting APIs to the forefront of automotive design and engineering. APIs are pervasive throughout the automotive ecosystem, and play pivotal roles in ensuring secure operations across the automotive industry. Automotive supply chains are complex and consist of a network of suppliers who provide hardware, software, and infrastructure to automakers.

Automakers rely on tier-1 suppliers to provide many vehicle components and systems. In turn, tier-1 suppliers rely on tier-2 suppliers for many smaller components and subsystems, resulting in an extensive interconnected web of suppliers, software, and connected ecosystems. APIs are the critical gatekeepers in the automotive industry, managing the flow of data between vehicles, customers, and the connected ecosystem. Connected services extend beyond the automaker as vehicles consume a wide range of 3rd party services, resulting in billions of API transactions per month traversing the global automotive ecosystem.

The Automotive Regulatory Environment

Regulatory compliance is paramount in the automotive industry. Cybersecurity regulations require automakers to implement a Cybersecurity Management System (CSMS) to manage all vehicle risks throughout the vehicle lifetime. This includes not only the vehicle itself, but vehicle APIs and the connected ecosystem. The cost of failure is high. As an example, failure to comply with UNECE R155 cybersecurity can result in the inability to sell vehicles in UNECE member countries, and automakers have stopped selling certain vehicle models due to their inability to meet cybersecurity regulations[1]. Automotive APIs must be designed with longevity in mind, as they must exist for the life of a vehicle, which is on average 16.58[2] years.

Connected services extend beyond the automaker as vehicles consume a wide range of 3rd party services, resulting in billions of API transactions per month traversing the global automotive ecosystem.

APIs have emerged as the largest attack vector and are the most attacked assets today in the automotive ecosystem.

Automotive Cyberattacks

In 2015, security researcher Charlie Miller[3] demonstrated the dangers of vehicle hacking. He and his colleague gained remote control over a 2014 Jeep, and this event dawned the era of automotive cyber-security. While significant, his attack took several years of research and impacted only a single vehicle and automaker. Contrast this attack to the exploitation of automotive APIs. In January 2023, a group of security researchers published “Web hackers versus the Auto Industry[4],” which highlighted their work exploring automotive API security. Their research was completed in several months and impacted 19 different automotive companies. The research team uncovered multiple common API vulnerabilities across automakers and suppliers. These vulnerabilities allowed the researchers to remotely control vehicles, connected fleets, access sensitive consumer data, and perform other unauthorized actions.

The extensive use of APIs has made them a prime target for cyberattacks which have evolved from targeting individual vehicles to the connected vehicle ecosystem. This shift in attacks highlights a greater challenge for automotive ecosystem cybersecurity, and that focusing solely on protecting the vehicle and individual APIs is no longer sufficient.

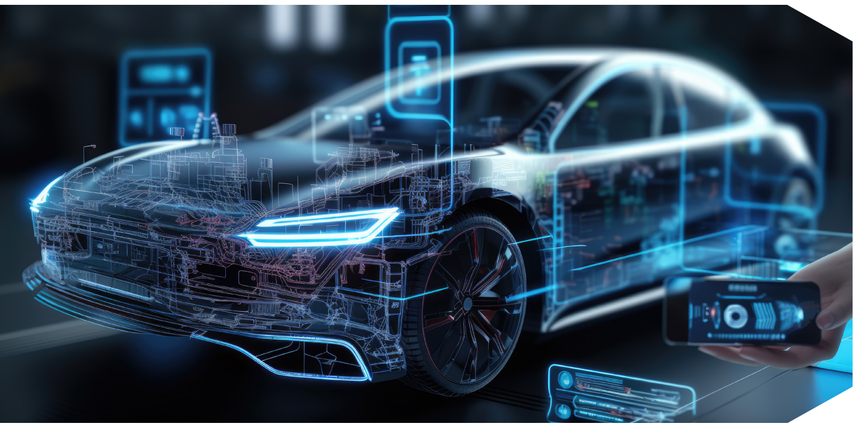
Gartner predicted that by 2022 APIs would be the largest attack vector[5], and this has proven to be true. APIs have emerged as the largest attack vector and are the most attacked assets today in the automotive ecosystem. While the OWASP API Top 10 list identifies categories of vulnerabilities, the majority of API attacks are effectively zero-day novel attacks that exploit recent and unique changes to an automaker’s APIs. When an automotive API is compromised, the implications can range from privacy breaches to safety threats.

Automotive API security is not solely a technological challenge, it is also a safety imperative. Each API's unique attack surface requires a continuous, lifecycle-oriented approach to API security. This approach includes designing security into APIs, conducting API security testing, continuous monitoring, and creating and applying reusable API security policies.

Reactive and Proactive Cybersecurity

Reactive cybersecurity focuses on responding to threats and incidents after they occur. With this approach, security measures are implemented in response to detected threats or incidents, rather than preventing them. Reactive cybersecurity can leave companies vulnerable for extended periods, as threats are only addressed once they are realized. Reactive cybersecurity typically lacks robust preventive measures, such as regular security audits, vulnerability scans, and proactive threat detection. Since damage often occurs before a reactionary response, an organization faces a higher risk of data breaches, financial losses, and reputational damage, as reactive responses tend to be more costly in the long run compared to preventive approaches. Proactive cybersecurity measures, such as security audits, continuous vulnerability scans, and proactive threat monitoring help reduce the likelihood and impact of attacks. A shift from negative reactive cybersecurity to positive proactive cybersecurity allows organizations to maintain a stronger security posture. 42Crunch enables an automaker to shift from a reactive to a proactive approach to API security.

A shift from negative reactive cybersecurity to positive proactive cybersecurity allows organizations to maintain a stronger security posture.



Organizing Automotive for Intentional API Design

The API industry champions the idea of Intentional Design, which is an approach for designing APIs with a focus on customer requirements, security, and customer experience. Intentional API design contrasts the approach used when companies expose APIs with little regard to how they will be used and secured. Intentional design is about making deliberate, user-centered choices throughout the API lifecycle. Intentional design is fundamental to automotive software development, including automotive APIs, as the public would not tolerate a vehicle or APIs which are developed without an explicit design or focus on safety. APIs operating safely while driving at 70mph down the road is the norm for automotive engineers. 42Crunch's shift-left approach to API security aligns directly with intentional design practices.

Automakers view vehicles through 3 different lenses.

1. **As Designed** is the vehicle blueprint, the design intent
2. **As Built** is the final product including any changes made during the vehicle development process
3. **As Consumed** is how a vehicle is utilized by its consumers, and is essentially the real-world application of the design.

Automakers follow a simple equation *As Designed = As Built = As Consumed*. When this equation gets out of balance, and the vehicle design no longer represents the source of truth, then what usually results are quality, safety, security, and reliability problems. 42Crunch's approach of defining and using a well-written API contract, the design intent, helps ensure that this fundamental equation is in balance and enforced for automotive APIs.

The Single Source of Truth

With automotive APIs, the OpenAPI document is the single source of truth. The OpenAPI document is similar to a well-written business contract, and enumerates the shared understanding between API producers, consumers, and cybersecurity. When a business contract is not enforced, it often results in financial losses, operational disruptions, and damage to a business. An automaker that fails to consistently enforce contracts risks long-term harm to their reputation as well as financial and legal complications. In a similar manner, when an API contract is not well written or enforced, damage occurs to the business. The 42Crunch API security audit performs 300+ security checks and provides the means to automatically and securely enforce well-written API contracts.

With automotive APIs, the OpenAPI document is the single source of truth.

The 42Crunch API firewall uses the OpenAPI document to identify, block, and alert on undocumented and shadow API designs, and ensures that the API contract is enforced at runtime.

During software development, API contracts are consumed by source control and CI/CD pipelines to automate the delivery and testing of APIs. The 42Crunch conformance scan serves as a rapid API pen test that can be run continuously during the development cycle. The conformance scan utilizes the OpenAPI document, the single source of truth, to ensure that the actual API implementation conforms to the design intention, addresses OWASP API Security Top 10 vulnerabilities, and can safely handle unexpected and malicious requests.

During runtime, the OpenAPI document is used to monitor and enforce secure API consumption. This is important as shadow APIs often exist in organizations. A shadow API is any undocumented, unapproved, or unmanaged API within an organization's ecosystem. These APIs often lack security oversight, making them vulnerable to misuse, breaches, or other security risks. As an example, in many buildings, safe rooms are often omitted from the blueprints. This security by obscurity is believed to ensure the room's secrecy and security. Unfortunately, this practice of omission, either intentional or accidental, sometimes happens with API contracts. Undocumented API endpoints and parameters provide a path for bad actors to exploit. The 42Crunch API firewall uses the OpenAPI document to identify, block, and alert on undocumented and shadow API designs, and ensures that the API contract is enforced at runtime.

This integrated approach allows engineers to meet the demand for speed and innovation without sacrificing the safety and security of the final product.

Automation - Enabling Innovation at Scale & Speed

The growing need for software speed and innovation is reshaping automotive industry development practices. Rapid software development allows automakers to quickly release new products and features, gaining a competitive edge. Automakers have adopted Agile methodologies and DevOps practices, which emphasize collaboration, automation, and continuous delivery. Software engineers are pivotal in these processes, as they work in cycles that allow for rapid feedback and continuous improvement. To enable faster innovation, a wide range of tools, platforms, and frameworks are used, streamlining coding, testing, and deployment. These tools, when used properly, make it easier to iterate and quickly release safe and secure software. Effective tools reduce developer friction and empower engineers to focus on innovation, without being bogged down by cumbersome processes. In short, automation must make the right thing the easiest thing to do or it will be bypassed by software engineers.

While speed is important, it introduces security challenges as fast releases can sometimes lead to overlooked vulnerabilities. Balancing speed with security requires embedding security into each development phase and creating a culture that values both rapid delivery and safe and secure software. This integrated approach allows engineers to meet the demand for speed and innovation without sacrificing the safety and security of the final product.

Organizing for Success

To deliver a robust API security program, automakers must structure their organizations with a focus on cross-functional collaboration, shared cybersecurity responsibility, and specialized API security expertise. Companies must establish a cross-functional product cybersecurity governance board that has representatives from cybersecurity, compliance, legal, marketing, and engineering to oversee compliance with regulatory requirements, such as those related to data privacy and vehicle safety, and ensure consistency in product cybersecurity practices.

A dedicated API security team should also be established which focuses exclusively on API security for vehicle products and services. Organizations should also adopt DevSecOps practices, where security validation is automated and seamlessly integrated into the CI/CD pipelines.

By adopting 42Crunch, not only will automotive APIs be more secure, but automakers can demonstrate API compliance with industry standards and cybersecurity regulations.

This approach helps ensure that security becomes a core, shared responsibility across the organization, which quickly addresses threats in the rapidly evolving automotive landscape. By structuring their organization to foster collaboration and integrate cybersecurity into product development, automakers can more effectively address API security challenges.

In 2015, automakers established the Automotive Information Sharing and Analysis Center (Auto-ISAC) to enhance automotive industry cybersecurity and enable a proactive, industry-wide approach to cybersecurity. Auto-ISAC facilitates the sharing of cybersecurity threats and vulnerabilities specific to the automotive industry. The viewpoint of Auto-ISAC members is that the automotive industry competes on product and not on cybersecurity, and that an attack on one is an attack on all.

By sharing information and collaborating, the automotive industry seeks to better defend against the complex and evolving threats that target software defined vehicles and their connected ecosystems. Auto-ISAC offers training programs, webinars, and workshops, including APIs, to educate members on security trends, regulatory requirements, and innovative technologies.

Governance Across Ecosystem

In summary, 42Crunch is crucial for safeguarding automotive APIs against common vulnerabilities, meeting regulatory compliance standards, and preventing costly security incidents, while providing a seamless developer experience. The platform empowers software engineers to identify and rectify API vulnerabilities early in the development process, while also providing security teams with governance across their API ecosystem. By adopting 42Crunch, not only will automotive APIs be more secure, but automakers can demonstrate API compliance with industry standards and cybersecurity regulations.

About the Author

Darren Shelcusky

Darren Shelcusky is a senior consultant, working in the automotive industry. He recently retired from Ford where he held the position of Manager Vehicle and Connectivity Cybersecurity. His areas of expertise encompass cybersecurity for the vehicle connectivity ecosystem and vehicle tech stack including clients, cloud, APIs, VSOC, software engineering, and cyber-physical systems. Darren earned a BS in Systems Engineering from General Motors Institute and an MBA from Penn State University. He is a 43-year veteran in the automotive industry, where he has led software-based initiatives in manufacturing, product development, product testing, in-vehicle, connected vehicles, and cybersecurity. He has first-hand experience implementing the 42Crunch API security platform as part of an overall API security governance program for a leading global automotive manufacturer. Darren has 12 patents for various connected vehicle and telematics innovations globally.

References

1. EU Cybersecurity Laws Kill Porsche's 718 Boxster And Cayman Early: https://www.forbes.com/sites/michaelharley/2024/03/28/eu-cybersecurity-laws-kill-porsches-718-boxster-and-cayman-early/
2. What Is The Lifespan Of A Vehicle In The USA: https://autorecyclingworld.com/what-is-the-lifespan-of-a-vehicle-in-the-usa/
3. Charlie Miller: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
4. Sam Curry: Web Hackers Vs The Auto-Industry: https://samcurry.net/web-hackers-vs-the-auto-industry
5. Gartner Quote Reference From Mark O'Neill's First Pronouncement: https://www.forbes.com/councils/forbestechcouncil/2022/07/25/how-to-address-growing-api-security-vulnerabilities-in-2022/

About 42Crunch

42Crunch enables a standardized approach to API security that automates the enforcement of security compliance across distributed development and security ecosystems. Our API security testing and runtime threat protection services are used by Fortune 500 enterprises, mid-sized firms and more than 1.5 million developers worldwide. The 42Crunch API DevSecOps platform empowers developers to build security from the IDE into the API pipeline and gives application security teams full governance from the CI/CD pipeline across the entire API lifecycle. This seamless DevSecOps approach to API security reduces governance costs and accelerates the delivery of secure APIs.

Contact us

sales@42crunch.com

42crunch.com