Publication date:
March 2023
Author:
Hollie Hennessy

Extending Security Posture to the Connected Vehicle

New regulations and vulnerabilities are increasing the need for new solutions

Commissioned by:
VicOne

Brought to you by Informa Tech

Information Classification: General

Contents

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Summary

More connected cars, more vulnerabilities

According to Omdia's Connected Cars Forecast, in 2021 there were approximately 230 million connected cars around the world, and that figure is expected to reach 571 million by 2025, comprising electric multiple units (EMUs) and a growing number of SIM-enabled cars.

At the same time, according to AV-Test Institute, the number of malicious programs attacking the vehicle ecosystem has grown from 65 million in 2011 to 1.1 billion.

The most dangerous risks include cyber-physical attacks (related to operation of the vehicle) through hijacking of electronic control units (ECUs) to disrupt braking, acceleration, steering, engine operation, and electronics and lighting. Today, cars can contain as many as 150 ECUs that could be vulnerable to attack.

Personal, corporate, and vehicle data may be exposed during vehicle-to-vehicle and vehicle-to-infrastructure communications, including personal data shared with original equipment manufacturers (OEMs), rental companies, car dealers, local infrastructure, and others.

At the enterprise level, hijacking of vehicle fleets (or access to their data) presents serious threats to safety, operations, and revenue. This kind of fleet attack could occur at a central server or at the cloud level, resulting in disastrous outcomes.

Much of the responsibility for securing connected vehicles falls on the OEMs and large suppliers, which have the opportunity to implement security measures in the design and production phases and to establish the operational infrastructure necessary to keep vehicles secure once they are sold.

OEMs are dealing with three problems:

- First, they are primarily aggregators for software content in components. The code for existing software architectures and electronic control systems is developed separately. OEMs need solutions to ensure the software in their supply chain is secure.
- The second problem is how to maintain the security of the vehicle throughout its lifecycle—including the hundreds of millions of lines of code, data integrity, confidentiality, and availability—both inside the car and in transit. They must keep on top of the changing landscape, vulnerabilities, risks, and so on throughout that lifecycle.
- Finally, compliance with new regulations creates a different problem. The rules are evolving in separate geographical regions. While there is some cooperation, as evidenced by the US cooperating with the EU to establish common guidelines, there are conflicting requirements between some regions, such as China and the US.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Fortunately, new solutions are being introduced into the market that conform to emerging regulations while addressing the ecosystem of cyberthreats across the connected vehicle's lifecycle.

Tracking regulations and focusing on what needs to be secured

Regulators, industry groups, and individual companies are working out ways to best identify and address the vulnerabilities. For example the United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (WP.29) created technical rules for automakers that EU manufacturers follow and that are generally followed by Japanese and South Korean companies.

Figure 1: Contracting parties to the UNECE vehicle regulations, which currently apply in 54 countries

Source: Omdia

UN Regulation No. 155, "Cyber security and cyber security management systems," and UN Regulation No. 156, "Software update and software update management system," require manufacturing designs to manage the risk of cyberattacks on vehicle systems and parts, detect and respond to IT security incidents affecting vehicles, and integrate safe and secure software updates.

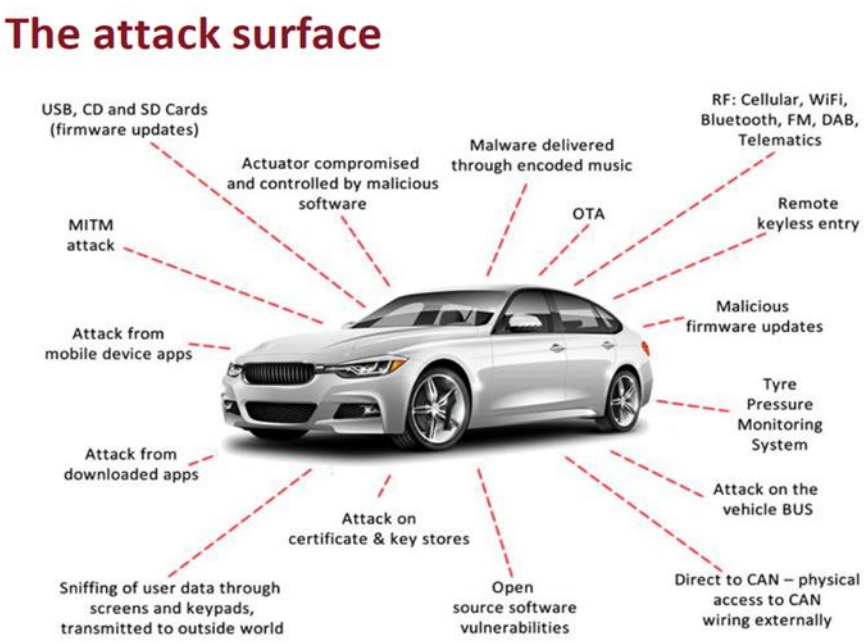
National regulators will check information collected by manufacturers demonstrating that supplier-related risks are identified and are managed, overall IT risks have been tested for and mitigating

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

measures taken, and that automakers detect and respond to cybersecurity concerns by logging incidents and providing data for forensic analysis of attempted or successful cyberattacks.

Regulators will conduct ongoing assessment of such IT security capacity and can declare a vehicle is in breach of UNECE standards should cyberprotections lapse. The task of proactively mitigating threats to the attack surface (see **Figure 2**) remain with the manufacturer.

Figure 2: The attack surface of a connected car



Source: Pen Test Partners

Despite the new emphasis, gaining visibility across new software-based end-to-end architectures, IP-addressable ECUs, and new forms of connectivity (5G, etc.) is a daunting challenge. These elements, though they create new vulnerabilities, can also be used as the foundation of an end-to-end security solution. They include

- Lifecycle: design, operations, decommissioning
- Data: what needs to be secured: vehicle system integrity and functionality
- Secure communication and data logging
- IP protection, digital copyright
- Privacy

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

- “Certified” components / spare parts
- System/component tampering
- Software feature activation
- Secure firmware

Real-time data collection and integrated operations

Protecting a connected car throughout its lifecycle requires data collection in real time to identify and analyze vulnerabilities and automotive threats and the maintenance of an effective vehicle security operations center (VSOC) to implement appropriate policies and manage these vulnerabilities and threats. OEMs should establish a vulnerability management process, anchored by the VSOC. In addition to management, the process can help OEMs collect data for a software bill of materials (SBOM) in a centralized location.

However, the tasks of gaining visibility across new software-based end-to-end architectures, IP-addressable ECUs, and new forms of connectivity represent a daunting challenge.

The right data collection method can leverage ECUs that control and monitor a variety of systems, such as chip sets that have their own secure elements. Additional components including intrusion detection systems detecting system integrity at the system level can also be accessed. Finally, telemetry data produced by driver actions that is sent to OEMs via cloud services may be utilized and also needs to be secured.

Correlating the data across these elements is the foundation of the VSOC. VSOCs importantly interpret threats in the context of the vehicle, its complex architecture, and its unique technology ecosystem, helping the OEM’s security teams manage the unique requirements of connected vehicles in a context they are already familiar with. They can be integrated with asset management systems, over-the-air update systems, and security information and event management (SIEM) with telematics data from the vehicle and other sources.

The leveraging of tactics, techniques, and procedures (TTP) in MITRE ATT&CK® VSOCs can be designed to proactively correlate and identify threats, allowing for effective remediation. This solution provides timely analysis of each threat across the organization to identify the impact on other vehicles or components and prevent vulnerabilities from turning into incidents.

One example of this approach is VicOne portfolio, which provides a detection response platform for connected vehicles that applies the MITRE ATT&CK framework to improve the capability of the VSOC. In addition, the platform can integrate data from onboard ECU intrusion detection systems and vulnerability management systems. This results in comprehensive threat and vulnerability detection and can accelerate the root-cause analysis process, thus improving the VSOC’s threat detection, investigation, and response effectiveness as well as its remediation options.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Conclusion

Future vehicles will have centralized high-performing computing with embedded security controlling adjacent electronic modules. Higher bandwidth in in-vehicle networking with multigigabit Ethernet will also enable the implementation of more secure protocols such as TLS and SecOC.

Laying the foundation for effective threat management today will enable automotive firms to grow their security posture alongside advances in vehicle technology and growth in the number of connected cars.

Collecting and integrating onboard ECU intrusion detection and vulnerability management data, and correlating and acting on the data through a VSOC, can help OEMs accelerate threat detection and response.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Appendix

Methodology

Omdia conducted a combination of secondary research and interviews with internal and external automotive security experts to develop this report.

Author

Hollie Hennessy
Senior Analyst, IoT Security
customersuccess@omdia.com

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.