VicOne, NXP, AWS, and Inventec Collaborate on Pre-Integrated and Comprehensive Cybersecurity Solution for Software-Defined Vehicles

Cybersecurity Risks of Software-Defined Vehicles

The automotive industry has entered a new era marked by connected, software-driven, and personalized experiences. With the clear trend toward software-defined vehicles (SDVs), the ability to rapidly evolve software can garner decisive competitive advantages. However, these advancements also bring heightened susceptibility to cyberattacks.

The complex and interconnected nature of modern vehicles has raised the stakes for OEMs and Tier 1 suppliers, compelling them to rethink their cybersecurity capabilities. As the automotive landscape becomes more connected and software-oriented, it inevitably becomes a target for malicious actors, amplifying the need for robust security measures. What was once a concern primarily for financial implications has now evolved into a potential threat to human lives. It is imperative for industry leaders to prioritize and enhance their cybersecurity efforts to safeguard the automotive industry against the emerging risks:

- **More motivation for attackers.** Connected cars gather enormous amounts of valuable data, such as driving behavior, personally identifiable information (PII), vehicle identification numbers, geolocation, and driving history. Malicious actors could steal this data for financial gain and even abuse it for cyberattacks that could endanger vehicles and their drivers.
- **Increasing number of attack vectors.** Internet-of-things (IoT) technology can deliver a more personalized driving experience to meet the specific preferences of individual drivers. However, it also significantly expands the attack surface of a vehicle with vectors such as telematics systems, Wi-Fi, Bluetooth, ultra-wideband (UWB), on-board diagnostics (OBD-II), GPS, mobile phones, and even charging stations, making it harder to defend.
- **Lower barrier for successful attacks.** Using open-source information like blog posts, amateurs could easily hack connected vehicles, which are essentially data centers on wheels. In January 2022, for example, news reports emerged about a teen hacker who exploited a bug to control 25 Tesla cars remotely.

Challenges for OEMs and Suppliers

New concerns specific to the automotive and transportation industry are arising alongside its constant evolution, bringing new challenges to OEMs and Tier 1 suppliers:

- **Pressures from new standards and regulations.** New standards and regulations such as ISO/SAE 21434 and UN R155 require OEMs and suppliers to ensure that their vehicles and management systems are equipped with new cybersecurity features. But for OEMs and suppliers, creating and implementing a cybersecurity compliance strategy from scratch can be costly and burdensome.

- **Pressures from ever-evolving cyberthreats.** The interconnected nature of the expanding connected vehicle ecosystem presents a significant challenge in terms of cybersecurity. With numerous endpoints and a constantly evolving threat landscape, the attack surface becomes extensive and unpredictable. Moreover, threat actors have become more sophisticated, adopting advanced tactics and techniques to maximize the impact of their attacks. This complexity creates a scenario where early detection of malicious activities becomes increasingly challenging.

- **Scalability concern.** Since OEMs are responsible for safeguarding potentially millions of vehicles on the road, it is essential for them to have cybersecurity solutions that can effectively handle the expanded attack surface. This requires additional resources and expertise to ensure the protection of connected vehicles and their associated services.

- **Mitigation complexity.** An intricate automotive supply chain poses a rugged terrain to navigate when it comes to cybersecurity. The average vehicle includes dozens of electronic control units (ECUs) from multiple suppliers, and a single modern luxury vehicle can integrate as many as 150 ECUs and over a hundred million lines of code. With the involvement of more and more automotive stakeholders and suppliers, such complexity makes incident response more challenging.

Uniting Forces for a Comprehensive Cybersecurity Solution

In order to assist OEMs and suppliers in effectively tackling the aforementioned challenges and seamlessly transitioning to SDVs, a collaborative effort involving four parties has been established. This collaboration aims to offer a comprehensive turnkey solution that addresses all potential threats arising from ever-evolving attack surfaces.

VicOne, a leading provider of automotive cybersecurity, delivers a broad portfolio of cybersecurity software and services for the automotive industry. Equipped with proven automotive threat intelligence to support large-scale connected car deployments, VicOne provides cybersecurity solutions that support OEMs and Tier 1 suppliers in their defense against evolving threats and their compliance journey with new standards and regulations.

NXP Semiconductors N.V., the leading provider of automotive processors, provides safe and secure processing power to help accelerate the shift to SDVs. The NXP S32G vehicle network processor brings high-performance, real-time applications processing with accelerated networking capabilities, along with advanced hardware security, to offload its Arm® Cortex® processor cores. S32G processors are optimized for service-oriented central gateways and vehicle computers, and their development was certified to ISO 26262:2018 functional safety and ISO/SAE 21434 cybersecurity standards.

Amazon Web Services, Inc. (AWS), a leading provider of cloud services, provides the AWS IoT FleetWise service to make it easier for automotive companies to collect, transform, and transfer vehicle data to the cloud in near-real time. Ecosystem players in the automotive industry can use AWS IoT FleetWise to collect and organize vehicle data more easily and to store the data in a standardized way for data analysis in the cloud.

Inventec, a leading provider of ECUs, offers a highly advanced and production-ready central gateway (CGW) specifically designed for the automotive industry. Powered by NXP's S32G vehicle network processor, Inventec's CGW is pre-integrated with VicOne's cybersecurity software solutions and the AWS IoT FleetWise service.

This integration elevates Inventec's CGW beyond a simple data exchange device, transforming it into an intelligence center that can provide invaluable cybersecurity intelligence to protect SDVs against threats. With its powerful edge computing, the CGW efficiently processes real-time data within the vehicle, enabling prompt detection and response to cyberthreats. This pre-integrated security also makes for a future-ready solution that aligns strongly with compliance requirements such as the ISO/SAE 21434 cybersecurity standard, which advocates ensuring security in the entire vehicle life cycle.

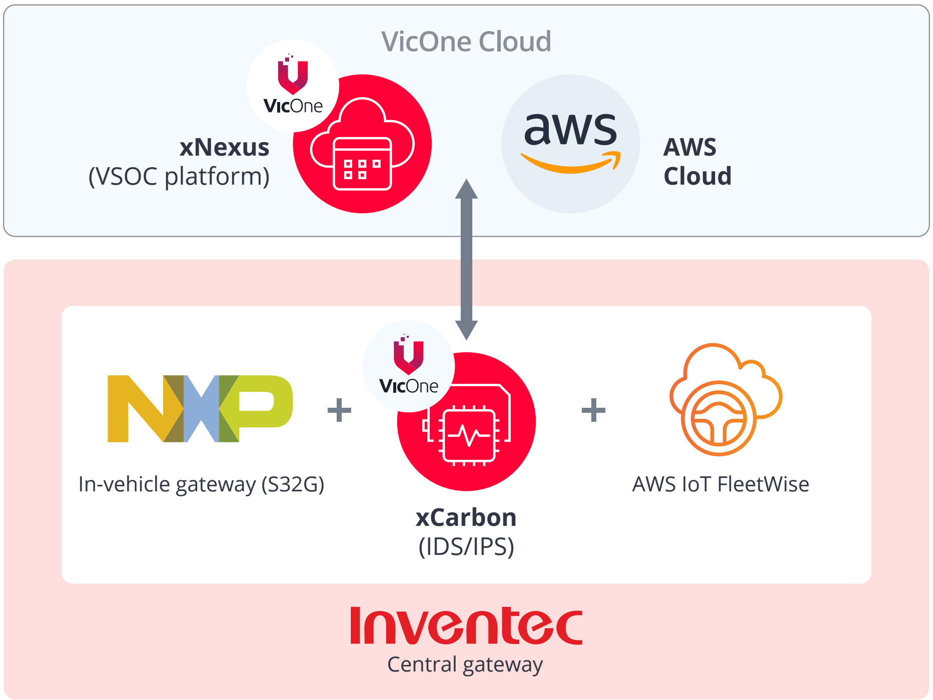

Figure 1. The roles in the four-way collaboration

Through this four-way collaboration including VicOne, NXP, AWS, and Inventec, a complete picture of proven electronics in combination with well-integrated security is created, one that can meet the protection needs of OEMs. This comprehensive solution enhances the automotive industry's cybersecurity capabilities and ensures a safer and more secure driving experience for all.

Unveiling the Inner Workings: How Does This Work?

By combining VicOne's automotive cybersecurity solutions, NXP's S32G vehicle network processor, the AWS IoT FleetWise service, and Inventec's CGW, this four-way collaboration offers a comprehensive, pre-integrated, and end-to-end protection solution. This robust solution ensures the complete detection and response process to combat constantly evolving cyberthreats:

- **Detect in Real Time**
  To effectively thwart threats within in-vehicle networks, the use of deep packet inspection (DPI) is crucial in detecting the exploitation of system vulnerabilities, combined with the pre-integrated VicOne xCarbon intrusion detection system (IDS) and NXP S32G vehicle network processor in Inventec's CGW. VicOne's xCarbon IDS solution harnesses the S32G's impressive computing power, which allows for real-time DPI analysis of Ethernet packets. In addition, powered by an off-board machine learning (ML) engine, xCarbon can distinguish between normal and abnormal operations on the CAN bus to detect malicious CAN messages, such as messages with abnormal IDs, frequencies, and loads caused by attacks.

- **Analyze With Comprehensive Visibility**
  Once malicious threats are detected, VicOne's xCarbon transmits the detection logs and system activities back to VicOne's xNexus vehicle security operations center (VSOC) platform for further threat investigation. To optimize bandwidth usage and save cost, xCarbon reports only high-confidence alerts to xNexus.

  Additionally, the pre-integrated AWS IoT FleetWise agent in Inventec's CGW can collect, transform, and transfer vehicle telemetry data to xNexus in near-real time. With the capabilities of AWS IoT FleetWise, threat experts can leverage xNexus to identify suspicious activities and collect more logs dynamically through AWS IoT Core Channel for investigation purposes. The flexibility of AWS IoT FleetWise's logs-collecting mechanism can also lower the effort and time for threat experts to understand the root cause.

  Once vehicle telemetry data and detection logs are transmitted to the xNexus platform, it effectively correlates this information, providing an enhanced level of visibility and context to the VSOC. This enables the VSOC to identify threats and proactively search for potential risks. Unlike traditional VSOC solutions, xNexus leverages over 30 years of threat intelligence and round-the-clock vulnerability research by a global network of independent researchers through the Zero Day Initiative (ZDI). This extensive knowledge empowers xNexus' analytics engine to learn attack behaviors and stay ahead of constantly evolving cyberthreats, resulting in a higher rate of detection. In addition, with AI-driven detection (ML), xNexus combines multiple rules, filters, and a unique analytics engine to deliver early and accurate threat detection.

- **Respond via Unique Virtual Patch**
  As the automotive industry involves an increasing number of stakeholders and suppliers, the complexity of incident response becomes more challenging. To address this, the combination of the xNexus VSOC platform and the xCarbon intrusion prevention system (IPS) offers a solution that provides virtual patches for effective postproduction mitigations.

  By leveraging virtual patching, xCarbon enforces attack signatures and security rules, allowing OEMs to protect the systems without making any changes. This approach provides an average of 102 days of protection while waiting for a vendor patch to become available. Since xCarbon is already integrated with the NXP S32G processor in Inventec's CGW, OEMs can deploy virtual patches without requiring code changes or firmware updates. This capability helps block zero-day exploits and gives OEMs more time to develop mitigation plans and solutions.

All of the above processes have been validated on Inventec's mature CGW.

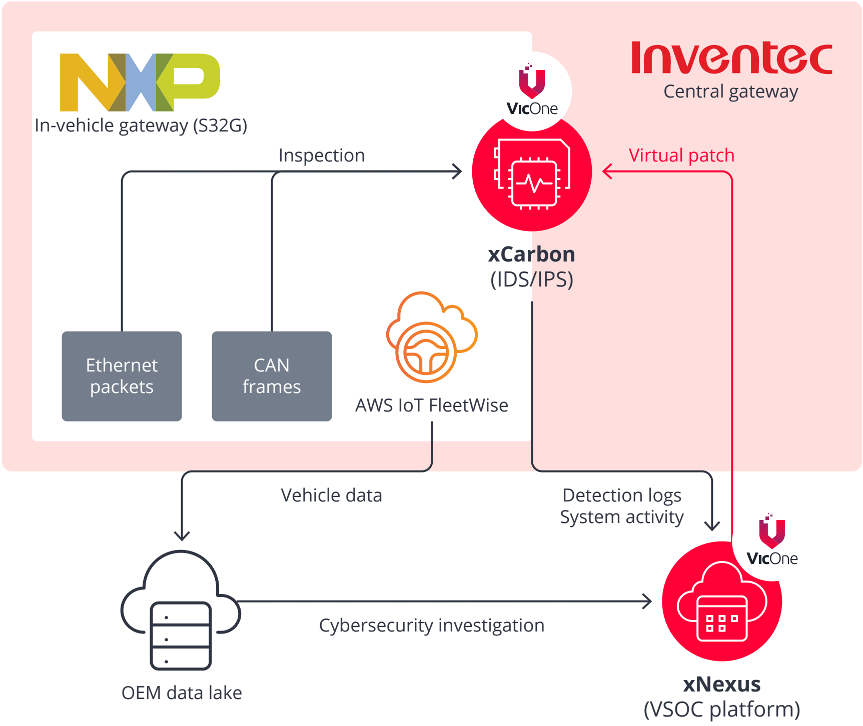

Figure 2. A comprehensive, pre-integrated, and end-to-end protection through a four-way collaboration including VicOne, NXP, AWS, and Inventec

Conclusion

This envisioned four-way collaboration stems from the pre-integrated protection already offered by VicOne to Inventec's CGW and, by relation, NXP's S32G platform for vehicle network processing. As mentioned earlier, the value of this collaboration lies in the effective integration of VicOne's security solutions with NXP's state-of-the-art technology and the AWS IoT FleetWise service. All of these are pre-integrated in Inventec's CGW.

This collaboration highlights four major advantages:

- Built-in security aligns strongly with compliance requirements such as the ISO/SAE 21434 cybersecurity standard, which advocates ensuring security in the entire vehicle life cycle.
- A turnkey and embedded solution creates a one-stop-shop solution amid the complexity of the entire vehicle ecosystem.
- The integration of VicOne solutions with the NXP S32G processor improves overall compatibility and performance.
- This four-way collaboration creates a shorter design flow leading to a shorter go-to-market strategy, and also addresses the scalability concern.

Overall, VicOne's aim is to add value with the integration of cloud service providers and explore avenues that can further enrich these collaborative efforts. In the process, this allows for the development of more secure solutions and automotive products, and creates opportunities to better fulfill OEMs and suppliers' needs.

To learn more about VicOne's solutions and partnerships, contact our experts and schedule a demo at automotive@vicone.com.