VicOne

Driving Automotive
Cybersecurity Forward

Unleashing Unparalleled Security: VicOne and NXP Join Forces for Trustworthy V2X Connections

The automotive industry has undergone a series of transformations, evolving from telematics processing to interconnected mobility, and now to autonomous driving. Through the integration of cutting-edge hardware into systems like V2X (vehicle-to-everything) technology, traditional vehicles are becoming more intelligent. V2X empowers vehicles with a comprehensive 360-degree situational awareness of their surroundings, greatly enhancing road safety, vehicle efficiency, and driving convenience. Research conducted by the US National Highway Traffic Safety Administration (NHTSA) estimates that V2X could prevent up to 80% of non-impaired crashes, potentially saving thousands of lives and mitigating millions of accidents annually.

To bring the envisioned future to life, connectivity capabilities are essential. This is why over time, automakers have progressively integrated a variety of wireless connectivity options into vehicles. This endeavor aims to amplify the benefits of V2X communication, ultimately enhancing safety and intelligence. Through these technologies, vehicles can interact with their surroundings, providing drivers with advanced features such as infotainment, navigation, and advanced driver assistance system (ADAS) capabilities.

However, this approach has led to a scattered distribution of wireless interfaces across multiple electronic control units (ECUs) in modern vehicles. This situation gives rise to coexistence challenges and heightens security concerns. With numerous wireless connections transmitting data streams from the external environment into the car, each link becomes a potential entry point for cyberattacks and a cybersecurity vulnerability. And the consequences of such threats could be significant for both the affected automaker and its customers.

Unmasking V2X Cyber Risks

There are five common types of V2X security attacks: manipulation of the environment, tampering, data leakage, denial of service (DoS), and privilege escalation. Their impact primarily revolves around authenticity, integrity, and authorization. For example, attackers could remotely disable vehicle functions, crash the system, or take unauthorized control to install backdoors and steal the car owner's personal information.

The following are examples of incidents or experiments that deal with V2X cyber risks:

- In 2022, researchers reported a flaw in the connected vehicle services of Sirius XM, which provides telematics and infotainment services to multiple brands like Acura, Honda, Infiniti, and Nissan. The vulnerability could allow malicious actors to **remotely start, unlock, and locate vehicles, among other commands**.
- In 2022, researchers reported a flaw in the Honda Connect app. This vulnerability could enable malicious actors to remotely execute actions such as **initiating a car's engine** or **locking or unlocking the vehicle** by interacting with its telematic control unit (TCU).

- In 2020, researchers successfully injected malicious code that made the compromised in-vehicle infotainment (IVI) system automatically connect to a rogue Wi-Fi hotspot, allowing the researchers to **send malicious CAN messages remotely** and make a car perform diagnosis without authentication.

Unlocking Multilayered Security

With wireless connections being established between various sources and the car, implementing a consistent security firewall across all incoming data to block malware and prevent cyberattacks becomes a formidable challenge. Through the collaborative efforts of VicOne's automotive cybersecurity solutions and NXP's OrangeBox solution, a multilayered protection solution arises to support OEMs and Tier 1 suppliers. This robust solution delivers a precise yet lightweight detection and response mechanism, effectively countering ever-evolving cyberthreats.

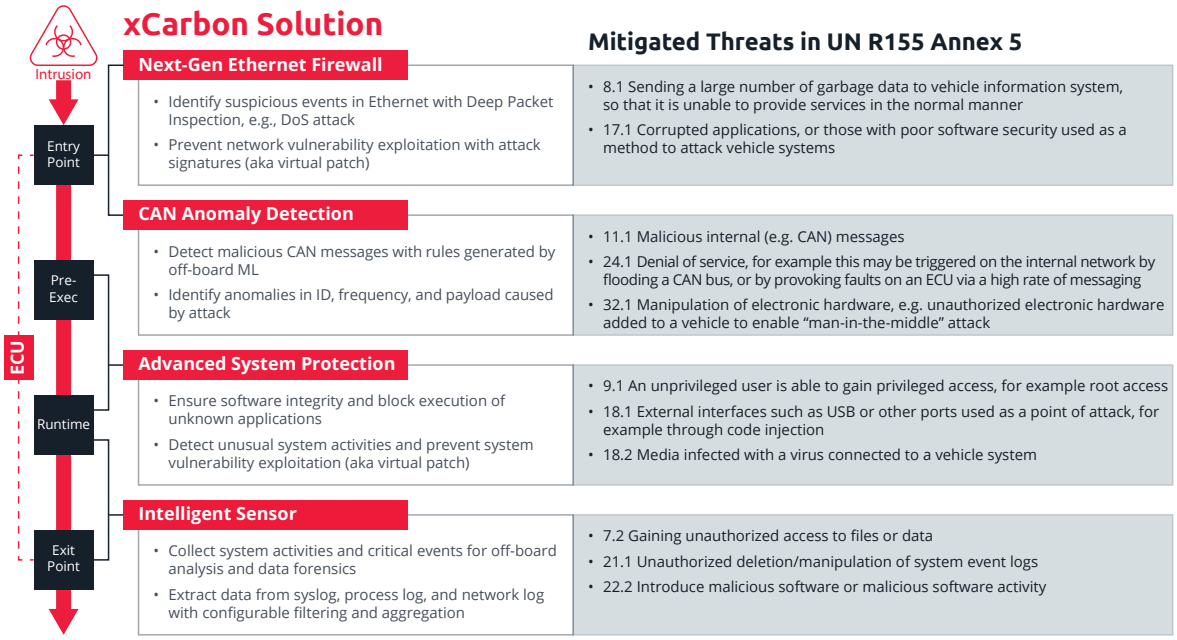
Here is how it works:

1. **Detect in Real Time**

   To effectively thwart threats within in-vehicle networks, the use of deep packet inspection (DPI) is crucial in identifying suspicious events in Ethernet, such as DoS attacks, combined with the pre-integrated VicOne xCarbon intrusion detection system (IDS) and NXP's OrangeBox. VicOne's xCarbon IDS solution integrates with NXP's OrangeBox, which allows for real-time DPI analysis of Ethernet packets. In addition, 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 data volume or traffic caused by attacks.

   xCarbon can also detect abnormal system activities or behavior to prevent exploits, as with, for example, media infected with a virus connected to a vehicle system or an unprivileged user who is able to gain privileged access. It can block unauthorized applications from running on an ECU or service-oriented architecture (SOA) by validating them through an approved application list.

   The following figure breaks down the cyberattack life cycle into its component stages to show how xCarbon can help on each stage:



2. **Analyze With Cloud-to-Car 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.

   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 other solutions that inundate users with overwhelming and unexplainable anomaly events, xNexus can offer high-confidence security alerts with actionable intelligence, eliminating false positives and facilitating rapid investigation. xNexus is able to do this as it leverages over 30 years of threat intelligence from Trend Micro 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.

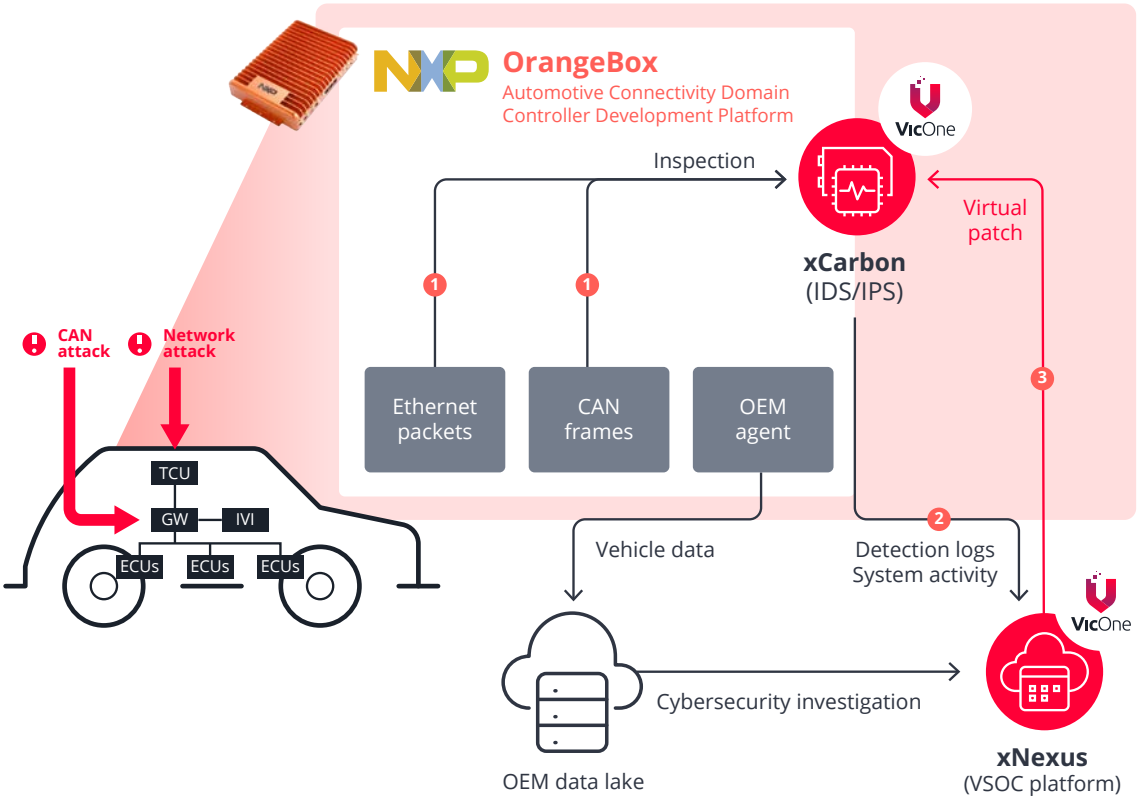
   In addition, through artificial intelligence–driven detection (machine learning), after detecting abnormal events, xNexus can correlate scattered events into "attack stories." These allow VSOC teams to conduct rapid investigation and proactive threat mitigation through rich actionable context, identifying potential threats before the attack chain is even completed.

3. **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, enabling OrangeBox to prevent network vulnerability exploitation with attack signatures and detection of unusual system activities.

   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 NXP's OrangeBox, 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.

The following figure illustrates the pre-integrated, multilayered protection platform for automotive connectivity domain controllers against network/CAN attacks:



Conclusion

Through the collaborative efforts of VicOne's automotive cybersecurity solutions and NXP's OrangeBox solution, VicOne and NXP's partnership delivers a multilayered protection solution to OEMs and Tier 1 suppliers: a consistent and state-of-the-art preemptive next-generation Ethernet firewall solution based on a unified connectivity platform that seeks to prevent malware from entering the vehicle in the first place.

This collaboration highlights the following major advantages:

- Built-in security aligns strongly with compliance requirements such as the ISO/SAE 21434 cybersecurity standard and the UN R155 regulation, which advocates ensuring security in the entire vehicle life cycle.
- An integrated solution delivers comprehensive visibility from cloud to car, eliminating the blind spots of the entire vehicle ecosystem and accelerating investigation.
- The integration of VicOne's solutions with NXP's OrangeBox improves overall compatibility and performance, and eliminates integration efforts.
- A modular design allows for streamlined customization, with a focus on minimizing any potential impact on ECU performance.
- Support for various operating systems, including Embedded Linux, Android Automotive OS, and QNX, ensures seamless integration.

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