講演番号	168	文献番号	20225168

Cloud-Based Vehicle Cyber Security in the New Software-Enabled Ecosystem

Simiao Wang [1)] **Monique Lance** [2)]

1) Argus Cyber Security (Japan)
Osaki New City No.1 Building 16F, 1-6-1 Osaki, Shinagawa-ku, Tokyo 141-0032, Japan (E-mail: simiao.wang@argus-sec.com)
2) Argus Cyber Security (HQ)
Floor 36,. 94 Yigal Alon Street, Tel-Aviv, Israel(E-mail: monique.lance@argus-sec.com)

KEY WORDS: **0-day vulnerability, vulnerability management, security operation center, attack detection, asset management, life-cycle security, cloud-based security, supply-chain security** information system, cloud system, information, communication, and control (E2)

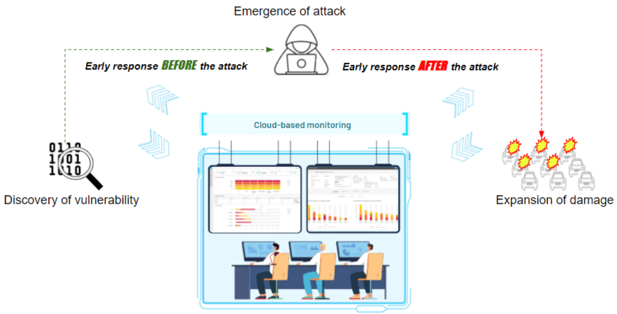
As vehicles become increasingly software driven and connected, their exposure to cyber attacks increases. In fact vehicles are part of a large and increasingly connected V2X ecosystem that is making the attack surface far more complicated and diverse. The risk of cyber attacks on vehicles was recently acknowledged by UNECE and regulations mandating vehicle cyber security are already going into effect in June, 2022. The presentation will cover the key insights and trends that are driving automotive cyber security and the unique challenges that the automotive industry faces. We will show how to best manage the security of vehicle assets throughout the vehicle lifecycle using cloud-based cyber security techniques, and how vehicle manufacturers across the supply chain can work together to help ensure the cyber security of modern vehicles.

Once the feasibility of cyber attacks on vehicles was acknowledged, vehicle manufacturers have substantially improved their in-vehicle security measures. However, there is no silver bullet in cyber security. There is always a risk that a new vulnerability or attack method emerges during the vehicle's lifecycle. In addition to detection and protection, it is also important to provide a quick diagnosis to support an early response to a new vulnerability or attack.

Vehicle manufactures face multiple challenges that are unique to the automotive industry. Firstly, unlike smartphones and computers, which require security updates for a limited time of 3-4 years, vehicles will require security updates for the entire time that they are on the road, approximately 20 years. Tech savvy companies like Google and Apple do not have this challenge.

In addition, the fact that each vehicle is composed of over 100 components with software and hardware assets sourced from multiple suppliers, further complicates the security challenge. It is a well known fact that with more software comes more vulnerabilities, also known as security weaknesses. Now for the first time, vehicle manufacturers must take extra precautions to understand what code is running on their vehicles, what vulnerabilities are present, and how to measure their risk exposure.

In order for vehicle manufacturers to increase their ability to respond to cyber threats, they need early detection tools. Firstly, they need the tools to detect vulnerabilities before they are exploited and secondly, they require the tools to identify the attacks when those weaknesses are exploited.


Emergence of attack
Early response BEFORE the attack
Early response AFTER the attack
Cloud-based monitoring
Discovery of vulnerability
Expansion of damage

To understand what vulnerabilities are hiding in their vehicle code, OEMs need vulnerability management tools that enable them to manage their software and hardware assets, monitor them for vulnerabilities, measure the potential risk impact of the vulnerabilities, and prioritize them accordingly. High impact vulnerabilities on safety critical ECUs should be mitigated as early as possible in order to reduce potential damage and harm to public safety.

Unfortunately, not all security weaknesses will be found in time to mitigate attacks. In the event that an attack does penetrate a vehicle, vehicle security operation centers enable OEM security analysts to identify indicators of compromise (IOCs) on individual vehicles, or an entire fleet. Security events can be further analyzed with other OEM data to understand the attack and its motivation in order to enable rapid response, mitigate the damage and prevent its recurrence in the future.

In conclusion, in order to increase their cyber security posture throughout the vehicle lifecycle, OEMs require greater visibility across their vehicle hardware and software assets both in production and while on the road so that they can identify and rapidly respond to cyber threats, vulnerabilities, and attacks. Using cloud-based cyber security techniques OEMs and their supply chain can significantly increase their time to detection and reduce their exposure to cyber risk.

2022 JSAE Annual Congress (Spring) - Summarized Paper
Issued on May 20, 2022