Protection for the entire vehicle ecosystem

Argus Cyber Security has unveiled the capabilities of its multi-layered car protection portfolio. The portfolio aims to deliver end-to-end security for connected cars. One suite examines CAN and CAN FD communication.

With hundreds of millions of connected cars expected to be on the road by 2020, Argus works with car manufacturers, their Tier 1 suppliers, fleet operators, and aftermarket connectivity providers to meet the cyber security challenges posed by car connectivity. “A full-throttled, technologically innovative approach that combines deep cyber security knowledge with automotive best practices is critical to protecting connected cars of today and tomorrow from cyber threats,” said Ofer Ben-Noon, Co-founder and CEO of Argus.

"Underpinning everything we do is the belief that by taking proactive measures we can significantly reduce cyber risks and their related costs while driving the automotive cyber security industry forward. When it comes to cyber security, there is no silver bullet that can effectively protect cars against dynamic, sophisticated cyber attacks. Our customers require multi-layered protection to prepare them for virtually any scenario."

Argus’ multi-layered, end-to-end protection includes the following suites: Connectivity, In-Vehicle Network, ECU, Lifespan, and Aftermarket Protection, as well as Automotive Cyber Security Services. The In-Vehicle Network Protection provides network-wide security by detecting attacks, suspicious activity, and changes in in-vehicle network behavior. Deployed centrally, the suit examines all network communication and stops attacks from advancing in the network. Supporting an array of network protocols - CAN and CAN FD, Flexray, Ethernet (with SOME/IP, DoIP, etc.), and more – this suite is positioned to defend current and future vehicle architectures.

The Connectivity Protection defends the infotainment or telematics units by preventing malware installation, detecting operating system (OS) anomalies, isolating suspicious applications, and stopping attacks from spreading to the in-vehicle network. In addition, this suite secures the two-way communication channel with the outside world. It operates cross-platform (Linux, QNX, Android, and more) to protect the car’s most vulnerable attack surfaces.

The ECU Protection reinforces select ECUs such as brakes, ADAS, or other units deemed critical from attacks originating inside and outside the ECU. Located on the ECU, this suite detects and prevents incoming attacks as well as neutralizes malware resulting from supply chain attacks or other attack vectors. Non-intrusive and with a small footprint, this suite supports many ECUs.

The Lifespan Protection aims to future-proof the fleet with an additional layer of protection. It collects and analyzes data from Argus’ in-vehicle solutions and other sources. Operating from the cloud or integrated into a security operations center, this suite provides OEMs and fleet managers with situational awareness of fleet cyber health on an intuitive dashboard. It also generates insights on new attacks and trends from big data analytics of OEM and fleet data, and provides the tools to take preemptive action.

The Aftermarket Protection delivers solutions for telematics technology providers, connectivity service providers, fleet managers, insurance companies, and dongle manufacturers. It provides in-vehicle network protection and dongle protection to retrofit cars and commercial vehicles on the road.

The Automotive Cyber Security Services offer an additional layer of security through an array of tailored advisory services from an automotive cyber security research team. Working with its customers on short and long term projects, Argus helps them integrate cyber security practices and processes into the entire product lifecycle. Its team works on and off-site to provide penetration testing, vulnerability assessments, code reviews, risk assessments, threat analyses, and incident response.

“Argus solution suites are built specifically for the automotive industry by a team of experts with decades of experience in both cyber security and automotive," said Yaron Galula, Co-founder and CTO of Argus. "Argus is committed to helping our customers stay ahead of threats by delivering truly innovative solutions based on 20 pending automotive patents and the insights of Argus' dedicated automotive cyber security research team. Our award winning research team is committed to keeping up-to-date with current and future cyber threats to continually ensure that our solutions remain on the cutting edge."