Karamba Security and eSOL, in Cooperation with Asgent, Demonstrate How to Stop Automotive and Medical IoT Hacks at ESEC 2017

ANN ARBOR, Michigan, HOD HASHARON, Israel and TOKYO, Japan — April 26, 2017 – Karamba Security, a provider of autonomous cybersecurity solutions for connected and autonomous vehicles and eSOL, a leading developer of real-time embedded software solutions, have partnered to demonstrate how their integrated cybersecurity technology solutions can keep self-driving cars and medical IoT devices safe from hackers.

The demonstration will take place during the Embedded Systems Expo & Conference (ESEC) in Tokyo, Japan, May 10-12, 2017 at eSOL Booth # West 10-1 at Tokyo Big Sight.

Karamba's software enables electronic control units (ECUs) to autonomously protect themselves from hackers. It automatically hardens car ECUs, preventing hackers from compromising those ECUs and hacking into the car, with zero false positives.

eSOL's eT-Kernel real-time operating system (RTOS) is designed for embedded systems that require real-time capability and reliability. It has been selected worldwide for use in a wide range of applications, including automotive devices, industrial equipment, satellites and consumer appliances. The eT-Kernel Compact basic profile has been certified for ISO 26262 Automotive Safety Integrity Level D (ASIL D) and IEC 61508 Safety Integrity Level 4 (SIL 4). In addition, the development processes for eSOL's RTOS products have been certified as complying with the IEC 62304:2006 (medical device software – software life cycle processes).

At ESEC, eSOL and Karamba, in cooperation with Asgent, are demonstrating how Karamba can be applied to ECUs where eT-Kernel is running to provide protection against in-memory vulnerabilities with zero false positives.

Karamba's solution is integrated into the eT-Kernel RTOS-based platform where it automatically protects the ECU binaries against attack attempts. The demo environment shows a system based on eT-Kernel that contains a buffer overflow vulnerability.

The demo includes two parallel systems:

- The first is not protected, hence an attacker can exploit the in-memory vulnerability to run unexpected functions
- The second is the same system, but with protection applied. The demo shows that the same attack attempt that worked on the first system fails on the second. In addition, after preventing an attack, a forensic log is generated

"With Karamba's software embedded as part of eSOL's eT-Kernel RTOS-based platform infection from malware is prevented, while allowing only good code to run," explained Bob N. Ueyama, eSOL executive vice president. "This shows we can block external threats, preventing hacks to self-driving cars' braking and steering systems and other critical safety functions. It will also deter remote attacks to medical IoT devices, including MRI scanners, X-Ray machines and insulin pumps," he added.

"We are delighted to enhance Karamba's partnerships in Japan with eSOL," said Ami Dotan, CEO of Karamba Security. "Karamba has been seeing strong demand from Japanese automotive companies, and the ability to serve their needs with a hardened version of eT-Kernel will enable the industry to continue protecting cars and ECUs, without the risk of false positives."

"Asgent, as the distributor of Karamba, is excited to have the opportunity to demonstrate in-memory protection which only Karamba can practically provide today," said Takahiro Sugimoto, Asgent CEO and president.

How Hackers Attack

Attackers try to inject malicious messages designed to modify a vehicle's behavior, either by a local or remote attack. In April 2016, Karamba Security emerged from stealth to solve this problem. Within a year, the company's Autonomous Security product is being evaluated with 12 different proofs of concept, and in the pipeline are dozens of other companies, owing to the advantages Autonomous Security brings to the car industry:

- A software solution that prevents cyberattacks with zero false positives, eliminating the risk of safety impacts
- No malware updates required
- Automatic policy generation with zero development efforts

Asgent, Inc., a Tokyo Stock Exchange-traded pioneer in cyber security and operations management solutions, is distributing Karamba Security Autonomous Security technology to the automotive and Internet of Things (IoT) markets in Japan, putting Japanese manufacturers at the leading edge of global efforts to protect vehicles and Internet of Things devices from cyberthreats.

Resources

Karamba Security Autonomous Security FAQ
Karamba Security Autonomous Security Chart
Karamba Security Carwall Animation

About Karamba Security

Karamba Security provides industry-leading autonomous cybersecurity solutions for connected and autonomous vehicles. Karamba's software products automatically harden the ECUs of connected and autonomous cars, preventing hackers from manipulating and compromising those ECUs and hacking into the car. Karamba's Autonomous Security prevents cyberattacks with zero false positives, no connectivity requirements and negligible performance impact. More information is available at www.karambasecurity.com.

About eSOL Co., Ltd.

Founded in 1975, eSOL is a leading developer of real-time embedded software solutions that seeks to create a rich IoT society using its innovative computer technologies. eSOL's software platform products and professional services, centered around its real-time operating system technology, are used worldwide in every field, starting with automotive systems, which conform to the most stringent quality standards, and including industrial equipment, satellitesand digital consumer electronics. In addition to the research and development of its own leading-edge products, and joint research with major manufacturers and universities, eSOL is actively engaged in AUTOSAR and Multi-Many-Core technology standardization activities. For more information, please visit www.esol.com.