Karamba Security to Demonstrate Live and Autonomously-Prevented Cyber Attacks on Vehicles at CES 2019, Showcasing Top Industry Players Supporting This Safety-Critical Technology

Karamba Security will demonstrate state-of-the-art automotive cybersecurity at CES 2019 Booth #929

BLOOMFIELD HILLS, Mich., and HOD HASHARON, Israel – December 10, 2018 – Karamba Security, a world-leading provider of end-to-end automotive cybersecurity prevention solutions, today announced its presence at CES 2019, January 8-11, 2019, in Las Vegas. At this year's event, Karamba Security will demonstrate live car hacking, run education sessions focusing on automotive cybersecurity and showcase industry leaders partnering for cybersecurity.

"The industry has been investing heavily in transforming to smart mobility and a self-driving future. However, this future relies on assuring consumer safety," said Ami Dotan, Karamba Security's CEO. "We will use CES 2019 as an opportunity to share our customers' experiences in securing their next-generation vehicles, while maintaining safety and minimizing legal exposure. We are excited to demonstrate live attacks on connected vehicles and showcase how they are deterministically prevented, without running into risks of false alerts, and without the associate cost and legal exposure of heuristic detection solutions. We are proud to showcase six different partners from across the vehicle industry."

Teaming up with Karamba Security at CES 2019 are leading automotive platform providers Micron, STMicroelectronics, Arm, Wind River, and innovative top-tier global providers Ficosa and Alpine – all companies that are investing to increase cybersecurity protection in today's vehicles.

Micron Authenta

End-to-end security of the ECU requires a zero-trust approach to cybersecurity enforcement. Karamba Security and Micron Technology collaborate to leverage the Micron® Authenta™ security architecture for ECU hardening, using standard flash memory form factors. Micron Authenta-enabled flash memory delivers the hardware roots of trust, and security features to lock encryption keys for simplified platform-level security implementations.

STMicroelectronics

Karamba's Carwall end-to-end protection is integrated on ST's Modular Telematics Platform, leveraging the security architecture of the Telemaco3P STA1385 Automotive Telematics and Connectivity Processor. Automotive-application developers can use this modular time-to-market accelerator, customize it to test near-final product, and take advantage of the root of trust offered by the embedded Hardware Security Module for image integrity and secure connectivity, and of the Karamba runtime integrity protection, optimized in performance on ST Telemaco3P.

Arm

In-Vehicle Security depends on a root of trust that protects the key assets of the security technology. Karamba SafeCAN, running on Arm processors, is offering innovative Authentication Encryption technology for the CAN network that is providing source authentication for each message, with zero bandwidth overhead. SafeCAN key management is simple and intuitive, as it doesn't require any key exchange over the CAN Bus. In the future, basing Karamba SafeCAN's root of trust on Arm TrustZone technology will allow the encryption key to be deployed once in a highly trusted secure element, thus increasing the overall security level of the solution

Wind River

Karamba and Wind River have collaborated to help original equipment manufacturers (OEMs) and Tier 1 suppliers improve in-vehicle security by hardening ECUs to preserve original factory settings. Combining with Wind River Chassis, Karamba's runtime integrity technology can help secure in-vehicle systems, from infotainment and TCU to autonomous driving and V2X ECUs. The Wind River Chassis portfolio of automotive software includes the high-performance and market-leading VxWorks RTOS, Wind River Drive which provides Adaptive AUTOSAR-oriented software to support customers in developing ISO 26262 ASIL D–certifiable automotive safety-critical applications, Wind River Linux and other commercial-grade open source technologies, Wind River Diab Compiler, and Wind River Edge Sync that provides a software framework for remote over-the-air (OTA) updates and software lifecycle management

Ficosa
Together with Ficosa, Karamba is showcasing a hardened Telematics Control Unit (TCU) that is leveraging the latest Control Flow Integrity (CFI) technology by Karamba to prevent in-memory cyberattacks. Ficosa's innovative design was easily integrated with the Karamba Carwall, offering car manufacturers an out-of-the-box solution, securing the future of smart mobility.

Alpine
Innovative Infotainment systems provide rich interfaces and fast access to the internet. Alpine and Karamba are demonstrating the hardening of this key connected Electronic Control Unit (ECU) with the Karamba Carwall solution, preventing in-memory cyberattacks and assuring secured experience with the industry-leading CFI.

Beyond the interactive demo, show attendees can partake in education sessions focused on securing the future of smart mobility and the benefits of self-protecting vehicles. CES session titles include:

- Think Like an Automotive Hacker
- How Cybersecurity Impacts Automotive Innovation
- Recent Attacks on Cars, Lessons Learned
- In-Memory Attacks in Today's Connected Cars
- The Automotive Security Evolution, ISO and the Regulation Progress
- What is Autonomous Security and How Prevention Matters

Meet Karamba Security's executives, learn about the latest technologies and trends for in-vehicle security, and see the partners ecosystem that is enhancing automotive cybersecurity by visiting Karamba Security at CES 2019 Booth #929. Attendees can also schedule a live car hacking demo here.

About Karamba Security
Karamba Security provides industry-leading automotive cybersecurity solutions for autonomous and connected cars. Its Autonomous Security software products, including ThreatHive, Carwall, and SafeCAN, provide end-to-end in-vehicle cybersecurity for the endpoints and the internal messaging bus. Karamba Security's award-winning solutions prevent cyberattacks with zero false positives and secure communications, including OTA updates, with negligible performance impact. Karamba is engaged with 17 OEM and tier-1 customers and received numerous industry awards. More information is available at www.karambasecurity.com and follow us on Twitter @KarambaSecurity.

Karamba Security Contact:
Amir Einav, VP of Marketing
amir.einav@karambasecurity.com
214-620-7320

Karamba Security Media Contact:
PAN Communications
Kyle Tildsley
Karamba@pancomm.com
617.502.4300