Karamba Security Releases XGuard 2.0 to Protect Hypervisors and Containers, in Automotive and Enterprise Edge Deployments

Karamba also announces a seamlessly embedded self-protection solution to protect the PikeOS hypervisor

RSAC, San Francisco, CA – February 25, 2020 – Karamba Security, a world-leading provider of embedded cybersecurity for connected devices, today announce the general availability of XGuard 2.0, its flagship product for automotive ECUs, IoT, and enterprise edge devices.

Automotive, enterprise edge, and 5G Telecom device providers are moving to an architecture that consolidates hardware platforms and promotes hardware-software separation in the domain controller architecture. Multi-domain controllers are prime targets for hackers, due to the heavy workload implemented on them and the connection between mission-critical applications and other virtualized guests on the shared hardware.

With XGuard 2.0, Karamba provides its customers with seamlessly applied runtime integrity, for multiple guest applications on a single hardware platform. The product adds automatically-generated control flow integrity (CFI) and binary whitelisting to hypervisor and container native isolation, enabling strong security to the host, the container infrastructure, and guest applications. From the delevoper perspective, Karamba's protection is added seamlessly, i.e., without developer intervention, and it is done with negligible CPU and RAM overhead.

"We are excited to serve our customers' roadmaps to multi-domain edge and IoT devices and enable them to seamlessly secure their next-gen architecture", said Ami Dotan, Karamba Security CEO and Co-founder, "with over 1 million devices signed for production, and over 50 completed projects in automotive, IoT and edge devices, the need to secure virtualized architectures on the edge device was raised in various industries and we are proud to enable runtime integrity for this architecture."

Embedded runtime integrity in a hypervisor provides a strong defense against breakouts between the guest applications and the host, preventing traversal between guests and allowing safety applications to trust the host. The evolution into a multi-application domain controller in IoT and edge depends on the ability to trust application segregation and assure that each application is not affected by its neighbors.

In addition to supporting containers and virtual machines, Karamba also announces an out-of-the-box integration with SYSGO's PikeOS. PikeOS customers can now protect their applications against in-memory attacks, without requiring any developer intervention.

"We are excited to partner with Karamba Security on their XGuard 2.0" said Jose Almeida, VP Automotive SYSGO. "When it comes to cybersecurity in automotive, PikeOS is a leading hypervisor choice with its EAL3+ CC certification, and our ability to offer Karamba's award-winning XGuard as a built-in optional feature for PikeOS gives developers access to additional state of the art embedded cybersecurity that integrates seamlessly into the development process of advanced domain controllers."

Further to supporting and out-of-the-box hypervisor architecture, XGuard 2.0 now supports deployments of applications in containers (Dockers and others) that are considered simple to develop and deploy across various Linux-based systems. Providing software integrity – including CFI and

whitelisting – to applications in containers, further promotes Karamba's leadership in seamless deployment of single-purpose devices such as automotive ECUs and enterprise edge devices.

XGuard in Secured Domain Controller architectures assures that the software is shielded on all levels. For example, a safety-critical-application running on RTOS, and protected by XGuard, shares hardware with XGuard-protected Linux applications in a Docker container. They all leverage the hypervisor infrastructure, which in its own right is protected by Karamba's runtime integrity.

About Karamba Security
Karamba Security is the embedded security powerhouse, providing industry-leading embedded cybersecurity solutions for connected devices. Manufacturers in automotive, Industry 4.0, enterprise edge, and Industrial IoT rely on Karamba's products and services to seamlessly protect their connected devices against Remote Code Execution (RCE) and Command Injection. After over 50 successful engagements with Fortune 100 companies, automotive OEMs, tier-1 providers and other manufacturers, connected device manufacturers trust Karamba's award-winning solutions for protecting their customers against cyberthreats.

More information is available at www.karambasecurity.com and follow us on Twitter @KarambaSecurity.

Karamba Security Business Contact:
Amir Einav, VP of Marketing
+1-214-620-7320

Media Contact:
Kyle Tildsley, PAN Communications
Karamba@pancomm.com
+1-617-502-4352