Karamba Security Introduces Carwall Software — Providing the Automotive Industry a Way to Immediately Secure New & Existing Connected Cars Against Cyberattacks

Patent-pending technology automatically secures the car's controller software to detect and prevent hackers from exploiting any software bugs to gain control over a vehicle

TU-Automotive Detroit 2016 Conference & Exhibition—June 7, 2016 — Karamba Security today announced the availability of Carwall, its in-car security software that automatically secures connected cars against cyberattacks. Carwall software keeps connected cars safe by sealing the car's controller software, so it can immediately detect and prevent cyberattacks from exploiting the car controller's software security bugs.

The U.S. Assistant Attorney General for National Security warned that connected cars, which Gartner predicts will represent 250 million vehicles on the road by 2020, "will be the next battlefield." Connected cars have hundreds to thousands of hidden security bugs (vulnerabilities) that hackers can exploit to infiltrate the vehicle, take control and compromise its safe operation.

"The risks to connected cars are real," said Richard Wallace, Director of Transportation Systems Analysis at the Center for Automotive Research. "Karamba Security's automated sealing approach offers the automotive industry a tool to immediately detect and prevent cyberattacks that exploit software bugs in the code of connected cars. Thus, drivers can be confident they will always be in complete control over their vehicles, and manufacturers learn more about the frequency and nature of such attacks."

In March, after white hat hackers repeatedly demonstrated they could successfully exploit security bugs in a connected car's code to infiltrate its safety systems, the Federal Bureau of Investigation (FBI), Department of Transportation, and the National Highway Traffic Safety Administration issued a Public Safety Alert (PSA) that highlighted the dangers to new and existing cars on the road. They warned today's vehicles are "increasingly vulnerable to remote exploits" that allow a hacker to "manipulate critical vehicle control systems."

"As vehicle control systems become increasingly automated with everything controlled by software, the probability of code flaws that can be exploited by bad actors for nefarious purposes increases dramatically," said Sam Abuelsamid, senior analyst, Navigant Research. "Compound this with the growing ubiquity of connected systems including cellular telematics, V2X communications and connected smartphones, and the need to integrate cybersecurity protection systems at multiple levels becomes clear. The full security solution set will ultimately include electronic architectures designed with security in mind, preventing intrusions to cloud-based transportation services and controlling access to in-vehicle ECUs."

Karamba's patent-pending software seals the car's electronic control units (ECUs) by automatically creating security policies, based on factory settings. In real time, Carwall detects and prevents anything not explicitly allowed to load or run on the ECU, including in-memory attacks. There's no ambiguity and no false alarms, detecting and preventing attackers, who try to exploit vulnerabilities and get into the car's network.

"Karamba's Carwall enables car manufacturers to immediately address security bugs in existing or new code and eliminate an attacker's way into a connected car," said Ami Dotan, CEO of Karamba Security. "We give car manufacturers and Tier 1 system developers the tools to detect and seal their code against exploits and detect and stop attackers before they can ever get started."

Carwall software requires zero developer resources — it's embedded during the ECU's software build process, so it simply becomes part of the regular development cycle. As a result, Carwall makes it easy to secure and retrofit automobiles on the road today and protect them from cyberattacks; it can easily be part of software updates completed during a regularly scheduled service visit.

Because Carwall is part of the ECU software build, it is always current; Carwall protects the code, as is, sealing it to detect and prevent hackers from taking advantage of any security bugs that might be in the controller's software. Carwall's unique approach gives car manufacturers and Tier 1 system providers the confidence ECUs are protected, regardless of any security bugs they may contain, allowing them to keep their product schedules and focus resources on developing new functionality and safety features.

Karamba Security will demonstrate its Carwall solution to Tier 1 suppliers and manufacturers at the world's largest connected car and auto-mobility conference and exhibition — TU-Automotive Detroit 2016, June 8-9, Novi, Michigan.

Resources

Security Bugs by the Numbers
Carwall Infographic

About Karamba Security

Karamba Security is a pioneer in electronic control unit (ECU) endpoint security to protect the connected car. The company seals and secures the connected ECUs within automobiles to detect and protect them from cyberattacks and ensure the car's safe, ongoing operations. To learn more, please visit www.karambasecurity.com.

Media contacts

Montner Tech PR
Deb Montner
dmontner@montner.com
+1-203-226-9290 x110