Karamba Security's Carwall™ system locks down ECU, prevents cyber attacks

Ami Dotan has spent his 30-year career finding solutions that make a difference in communication systems, software and state-of-the-art technologies.

He continues that commitment with his 15-month-old company, Karamba Security, where he is applying his expertise to cyber security solutions for the auto industry as the company's CEO and co-founder.

The need for solutions is great, and the pain from cyber threats is real.

Dotan says, statistically, there is an inherent bug in every 1600 to 1800 lines of code and it has been found that 8 percent of these bugs are cyber security vulnerabilities. A modern high-end car has more than 100 million lines of code so there is more than ample opportunity for exposure.

Before Karamba's Carwall™ cyber security solutions were ported from the enterprise environment, which are based on heuristics, or running tests by trial and error, he says. That created a big drawback – false positives, which result in commands being either missed, executed or aborted.

In the automotive environment this is unacceptable. Unlike the enterprise and data centers' IT environment, cyber security risks in cars are tightly coupled with the safety of consumers. For example, 5 percent false positives, the average rate in enterprise IT, means one out of every 20 commands is mistrusted or will not be executed. A very dangerous condition.

The danger will grow as autonomous vehicles hit the road. In 2025 partially autonomous cars and completely autonomous cars are expected to account for more than 15 percent of all cars shipped that year. This number will jump to 70 percent of all cars shipped in 2025, nearly 72 million cars annually.

Creation of Karamba Security

Dotan is using the expertise he learned in the Israeli military and as a venture capitalist to make a difference that will allow vehicles to protect themselves from cyber threats.

He first spent 17 years with Rafael Advanced Defense Systems Ltd. The organization was founded as Israel's National R&D Defense Laboratory, which is the largest and most important Israel Defense Forces R&D center with responsibility for the development of weapons and military technology. He held senior positions there including vice president of the Electronics Systems Division. He also served as corporate vice president for strategy, responsible for restructuring Rafael and its new strategy, corporate governance, business units. In addition, he led the incorporation of Rafael into a private company.

After retiring from the Ministry of Defense he turned to venture capitalism and co-founded Neurone Ventures I, a pioneer seed-investing firm in Israel. Following that, he co-founded Neurone Ventures II, which later became PNV (Platinum Neurone Ventures), a $105 million Israeli VC Fund specializing in growth stage hi-tech companies.

Dotan then was managing general partner of CIVC (China Israel Value Capital), a joint venture capital fund with China's No. 1 ranked VC fund, SCGC - Shenzhen Capital Group. CIVC has invested in growth stage Chinese companies and has migrated Israeli technologies into those companies. So far, CIVC has invested in 10 companies in the electronics industry, drug discovery, petro-chemical and consumer products.

“I’ve spent years fighting to make a difference,” he says.

Two years ago when flying back from a board meeting of one of Neurone Ventures portfolio companies based in New York City, he had a chance to chat with a Tier 1 automotive executive, who told him his biggest concern was cyber security. Seeing the possibilities to again make a difference, Dotan decided to dig deeper.

No “Me Too” Solution

“I didn’t want a ‘me too’ solution,” he says. “We needed to find a solution that takes into account the automotive industry’s constraints – a different cyber approach, unlike those that existed, which are basically imported from the enterprise IT solutions that have their drawbacks.”

Working hand-in-hand with the Tier 1, Dotan and his team analyzed the network centric approach and data transfers to find out what was wrong with those offerings in a vehicle.

“We found a false positive phenomena, which the automotive industry can’t sustain, introducing greater risks, instead of reducing them,” he says. “The risk is often caused by decisions made by network centric solutions that are based on heuristics, therefore bogged with false positives that risk consumers’ lives.”

After eight months of self-funded stealth mode work with developers and designers at Tier 1s and OEMs, the team created a software solution that produced zero false positives, doesn’t require security patches and updates and can be automatically and seamlessly integrated into a vehicles’ existing architecture.

With the Carwall technology proven and in-hand Dotan and co-founders, David Barzilai, Tal Ben-David and Assaf Harel, formed Karamba Security on March 29, 2016. Barzilai serves as executive chairman, Ben-David as vice president of R&D, and Harel as CTO. All are former Israeli military.

“Karamba’s autonomous security technology, Carwall, enables a vehicle’s Electronic Control Units (ECUs) to protect themselves and block hackers at the gate,” says Dotan.

The technology makes sure ECUs’ factory setting cannot be changed by unauthorized people, detects bugs and prevents attacks. There are no service updates. It is a one-time installation that seals feedback settings at the Tier 1.

“There is an inherent bug in every 1600 to 1800 lines of code developers naturally embed unintentionally during their development cycles, mostly because they are not security experts … rest assured,” Dotan says. “Every one is a cause for a recall. The cost of recalls per car is high and the automotive industry allocates more than $10 billion annually for recalls and warranty issues, including insurance policies to cover such cases.”

The risk for bugs continues to grow as vehicles become more and more complex. While today a high-end car has more than 100 million lines of code that will grow to 200-300 million in the near future with autonomous vehicles. In those 100 million lines there are 60,000 bugs, and about 5,000 of those pose security vulnerabilities. Compare that to a Boeing 787 Dreamliner, which has 15 million lines of code behind its avionics and online support systems. There are 9,000 bugs and 700 security vulnerabilities in those 15 million lines.

That’s today. By 2020, an estimated 188 million connected vehicles will be on the road, according to Navigant Research. As the number of autonomous vehicles grows, so does the cyber security threat. By 2025 – a short eight years from now – 70 percent of all cars shipped will be autonomous or nearly 72 million cars annually.

How Carwall Works

Karamba’s Carwall software can protect those vehicles, says Dotan.

Carwall automatically hardens the ECU according to its factory settings and verifies its operations in runtime. If an operation does not comply with factory settings it indicates a hacker is trying to get in. That’s blocked by the software.

Since Carwall is embedded within the ECU’s software it also reports detailed forensic information on the processes and functions being attacked. That means hackers are not only blocked, they are giving away their knowledge on current vulnerabilities. That lets

Karamba prevent the attack attempts as well as give a full report to automakers and suppliers on what to fix in their software.

Today, just 14 months since coming out of stealth mode, Karamba is working with 16 OEMs and Tier 1s and has raised $17 million from industry-focused funds supporting its global operations. They include YL Ventures (Bay Area & Tel Aviv – cyber security focused), Fontinalis Partners (Detroit – mobility and transportation focused), GlenRock (Tel Aviv – mobility focused), Liberty Mutual (Boston – automotive insurance focused), Paladin Capital (DC – Ex. NSA & CIA veterans), Presidio/Sumitomo (a large conglomerate from Japan), and Asgent (Karamba's valued-added resaler (VAR) in Japan.

The technology is receiving industry recognition.

In early June, Karamba Security was unanimously awarded TU-Automotive's *Best Auto Cybersecurity Product/Service of 2017*. Awards winners were judged based on innovation, industry engagement, user experience and market update.

"The judges appreciated the Karamba Autonomous Security product because it showed a new and interesting approach. They also highlighted the fact that this product solves a concrete problem at a low cost," said Gareth Ragg, managing director at TU-Automotive.

TU-Automotive also said "until Karamba, there were no preventive solutions with zero false positives, and many questioned whether it was even achievable. Now that the industry is aware that prevention is attainable, it is choosing Karamba and, in doing so, enabling safe outcomes."

Karamba Security has established its US offices in Michigan and currently is growing its US team of sales engineers and business development experts. Dotan relocated with his wife to Michigan to work closely with Karamba's partners and customers and be close to the decision-making executives and researchers.

"Based here and being involved in Michigan's leading commercial and technology global companies accelerates our growth path and expedites our learning curve," says

Dotan. “We appreciate the support and recognition we are receiving from Michigan’s governor, the different associations and government branches, the MEDC, and, of course, the Michigan Israel Business Bridge.”

For more information please visit https://www.karambasecurity.com/.