Automotive World

Interview: David Barzilai, Chairman and Co-Founder, Karamba Security

By: Michael Nash

Posted: https://www.automotiveworld.com/analysis/interview-david-barzilai-chairman-co-founder-karamba-security/

--

The potential for vehicles to be hacked is growing as more in-car connectivity features emerge. Michael Nash talks to Karamba about the available solutions

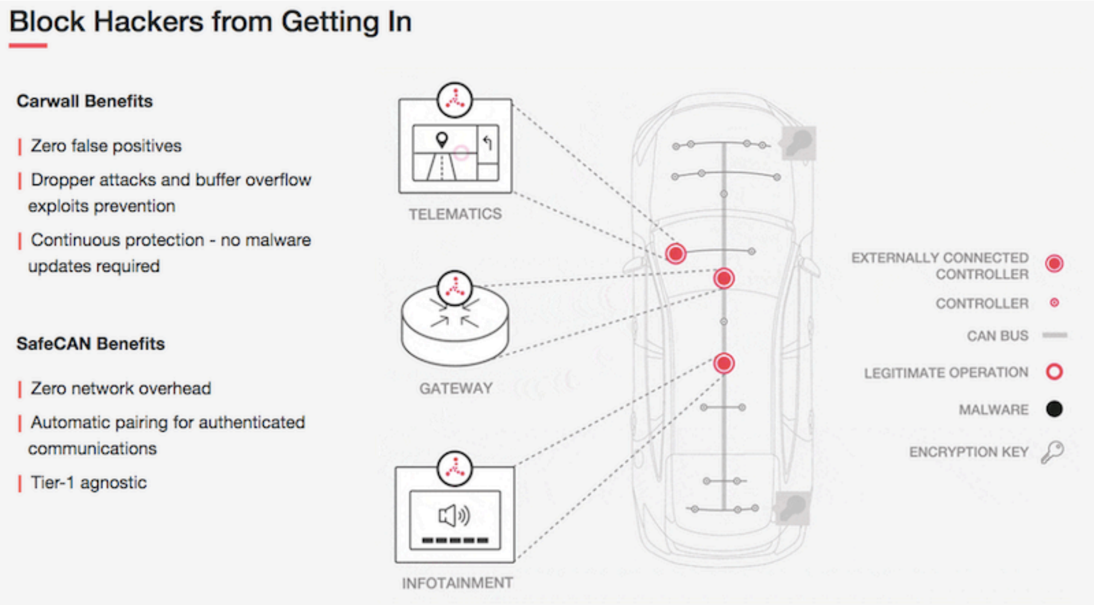
Cyber attacks can come in many different forms and are carried out at various different scales, from compromising national public health services to controlling individual electronic control units (ECUs). All industries are vulnerable, and automotive is no exception.

White-hat researchers have shown that they can control the critical functions of vehicles remotely, such as braking and steering, by hacking into the car via the on-board diagnostics port – an access point designed to give technicians information on electronically controlled systems. Experts think that it is just a matter of time before these kind of design vulnerabilities are exploited by malicious hackers with intention to cause harm or obtain valuable information.

Speaking to *Automotive World*, David Barzilai, Chairman and Co-Founder, Karamba Security, warned of the rising threat posed by hackers.

What solutions does Karamba have to ensure vehicles are safe in the event of an attempted hack?

We offer solutions that allow the vehicle to autonomously prevent attacks. Our Carwall software prevents hackers at the gate, with zero false positives. It works by hardening the connected ECUs according to factory settings, so when hackers exploit security vulnerabilities, Carwall detects their attempts as deviations from factory settings and blocks them before they infiltrate the car. It is a deterministic mechanism, which means that if there is a deviation being made to the software from the factory, it clearly must be malware.



Block Hackers from Getting In

Carwall Benefits

- Zero false positives
- Dropper attacks and buffer overflow exploits prevention
- Continuous protection - no malware updates required

SafeCAN Benefits

- Zero network overhead
- Automatic pairing for authenticated communications
- Tier-1 agnostic

How does this differ from Karamba SafeCAN?

CAN is a 30-year old networking technology that is used between safety ECUs in the car, and as such, it can't handle the authentication data between ECUs. As a result, OEMs are exposed to third party dongles that may introduce safety risks, by sending unauthorised commands to the car's safety systems, such as brakes and airbags. Our SafeCAN software seamlessly authenticates CAN traffic between selected ECUs with zero network overhead. This means that commands sent from hacked ECUs to safety systems will be ignored.

Can you combine both of these solutions in vehicles?

Yes, SafeCAN and Carwall software provide end-to-end in-vehicle security by authenticating communications, including over-the-air (OTA) updates, safeguarding them from attempts to manipulate or compromise their commands and hack into the car. Together, the products prevent cyber attacks with zero false positives, no connectivity requirements and negligible performance impact.

Do you think that the increasing number of connected car features, from telematics to vehicle-to-everything (V2X) communication, is a big problem in terms of security?

Opening the car to external connectivity enables hackers to infiltrate the car remotely and take control by sending malicious commands to the car's safety systems such as the brakes, steering wheel and airbags. Connected cars have hundreds to thousands of hidden security bugs, or vulnerabilities, that hackers can exploit.

How does the advent of autonomous driving have an impact on cyber security?

Autonomous driving elevates the risk of cyber security. Cars without a driver by the wheel are more easily taken over. Additionally, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, which are essential in autonomous driving, create new attack vectors. For example, a red traffic light signal may be construed as green, and cars would drive into an intersection on red.

What are your thoughts on the lack of government regulations when it comes to ensuring vehicles are safeguarding from hacking?

Governments follow industry standards and institute them as regulations or guidelines. US legislators didn't wait though – in September 2017 the House of Representatives passed the AV Bill, and the Senate is set to debate on its version of the bill. A key part of this bill is the best practices for cyber security, which covers multiple aspects, from identifying security vulnerabilities to protecting the car against cyber attacks.

News regarding the progress of safeguarding vehicles from hacking is kept quiet. Is this due to slow progress or is it because improvements are being made behind the scenes?

Most product evaluations are done behind the scenes, and the majority of them require many months of testing before setting the security policies. Solutions that generate a security policy automatically have a time-to-market advantage, but these are quite uncommon at the moment.

How can OEMs stay ahead of hackers? Will it be a consistently evolving challenge?

Not necessarily. The nature of cars is that they should run exactly as they do in factory, so unauthorised changes in runtime must imply hacking attempts and must be blocked. Hardening the ECUs eliminates the need to continuously update the security software with new malware signatures, and stops OEMs from having to continuously chase new hacking patterns.

How important is it for companies to work with white-hat hackers or researchers?

It's very important and could be crucial. Companies should always want to test their systems in-house and remediate security vulnerabilities before real hackers find those bugs and exploit them to compromise the car, and put the people in that car in any serious danger.

Could the hacking of vehicles have wide-ranging impacts, and potentially go beyond the automotive industry?

Yes I think so. As the former Assistant Attorney General for National Security John Carlin warned, "connected cars are the next battleground" against terrorist organisations and organised crime.