Embedded software protects cars

Tower Sec claims to have the solution to automotive cyber security threats. The company runs projects with automakers and suppliers, integrating its Ecushield embedded software technology into vehicles.

Researchers have demonstrated that the connected vehicle is vulnerable to car hacks (Photo: Tower Sec)

THE RECENT DISPLAY OF A REMOTE CAR HACK has demonstrated the need for automotive cyber security as modern technologies open the door to hackers. It wasn't the first time that Charlie Miller and Chris Valasek, two security researchers, managed to hack a car, but it was the first time they did it remotely. They accessed the vehicle's CAN network via its entertainment and navigation system, which in turn they accessed via the Internet.

According to the company, Tower Sec's Ecushield technology can protect vehicles against every hacking event discussed in the article such as taking over the steering, brakes, transmission, and entertainment system from a remote location. "Hacking is a very real threat today and will be more so in the future as autonomous vehicles evolve and new technologies become part of the Internet of Things. Ecushield is the only tested and proven software cyber security solution available for immediate deployment," said Saar Dickman, Tower Sec's CEO. "We invested years of research and engineering effort in developing this product. It detects and prevents cyber threats on vehicles in real time and can be integrated into existing and future vehicles with no redesign."

Once integrated into a CAN-accessible ECU, infotainment system, or telematics control unit, Ecushield provides continuous monitoring while identifying new threats to the vehicle. It is supposed to prevent malicious communication from reaching mission critical systems inside the vehicle that could put lives and personal data at risk. No redesign is needed. It can be integrated into new and used vehicles, including fleets. It turns any ECU into an Intrusion Detection and Prevention (IDS/IPS) system and any gateway ECU into a smart firewall. For systems with access to external communication channels (Wi-Fi, cellular, Bluetooth, SRC/DSRC), the security system provides continuous monitoring and protection of both internal and external communication channels, serving as a double-perimeter security protection.

While the need for a cyber-protection for vehicles is clear, Dickman pointed out there is much more "under the hood" in terms of providing cyber security for future vehicles than is publicly known. He said that automakers and suppliers are working to deal with cyber security threats and to make sure all the security and safety technologies work in concert to protect vehicles and their passengers. "While we cannot comment on specific attacks on vehicles and devices by hackers, we can say our goal, as well as the goal of our customers, is to ensure vehicles are safe and secure," Dickman said. "That is a complex process. We must be sure all the technologies work together to best protect the vehicle."

About Tower Sec

Tower Sec, an automotive cyber security supplier, delivers on-board cyber security technology to OEMs, suppliers, and the aftermarket. Founded in 2012, the company combines auto industry knowledge with cyber security to deliver its on-board solutions. Headquartered in Ann Arbor, Michigan, the company also has an office in Annapolis Junction, Maryland, and Berlin, Germany, and an R&D center in Tel-Aviv, Israel.