CAN Newsletter Online

CES 2020

Integrating security into existing automotive networks

Microchip has introduced Cryptoautomotive. It is a solution that enables OEMs and Tier 1 suppliers to add security to existing systems without costly redesigns. The company is part of the CES 2020 in Las Vegas in South Hall, MP26066.

The CES 2020 (Consumer Electronics Show) takes place in Las Vegas from 7 January to 10 January (Source: AdobeStock)

More and more consumer conveniences like Bluetooth, 3G, 4G, LTE, etc. are being added to vehicles each year much to the delight of consumers as well as the hackers. There is no shortage of real-world vehicle hacking stories and videos available on the web and virtually all OEMs (original equipment manufacturers) in all regions have been negatively impacted by these attacks. The attack surface will certainly continue to grow so the pressure is mounting for OEMs and Tier 1 suppliers to quickly secure in-vehicle networks with long-term solutions.

OEM cybersecurity specs have begun to roll out requiring improved security including hardware-based secure boot and CAN message authentication. Implementing these new specs can be burdensome for Tier 1 suppliers to implement with the first investigation typically involving switching out their existing host micro-controller (MCU) to a higher horsepower dual-core 32-bit MCU with crypto. This can introduce significant additional silicon cost, software development expense and introduces risk associated with getting the security software in the MCU implemented correctly. Microchip has introduced a solution that enables OEMs and Tier 1 suppliers to add security to existing systems without costly redesigns.

This Cryptoautomotive Security ICs In-Vehicle Network (IVN) Trustanchor/Border Security Device (TA/BSD) development kit provides a way for developers to begin architecting their security into existing systems. The emulated secure companion solution initially targets secure boot and CAN message authentication use cases, and upcoming kit software releases for key agreement, TLS, content protection schemes, and more will be available in the future. The kit can be conveniently paired with Microchip automotive host micro-controller development kits which include example projects for secure boot.

hz