AW
Automotive World

‘Indefensible’ hack puts CAN standard in the spotlight

August 22, 2017

Researchers have warned of serious cyber vulnerabilities that may require sweeping changes in standards and the ways in-vehicle networks and devices are made. By Megan Lampinen

The latest headline grabbing connected car hack could prove a game changer for the automotive industry. The protocol could allow hackers to shut down pivotal systems such as airbags and anti-lock brakes. According to those involved, there’s no way to protect against it and there’s no easy fix.

As usual, this is a white hat hack geared at helping the industry address weaknesses before anyone with dishonest intentions can take advantage. Unlike many other hacks brought to light, the weakness uncovered here is not reliant on any specific make or brand of cars but is linked to the controller area network (CAN) standard.

The problem

Security software company Trend Micro, working with Politecnico di Milano and Linklayer Labs, has discovered what it claims is a stealthy and vendor neutral hack that can “drastically” affect the performance and function of the vehicle. It disables a device – such as an airbag, parking sensors, active safety systems – that is connected to the car’s device network in a way that is invisible to even the latest security mechanisms. The researchers warn that “it is currently indefensible by modern car security technology, and to completely resolve it would require broad, sweeping changes in standards and the ways in-vehicle networks and devices are made. Realistically, it would take an entire generation of vehicles for such a vulnerability to be resolved, not just a recall or an OTA (on-the-air) upgrade.”

Trend Micro is calling on the industry to revise the design of the cyber-physical systems that govern future vehicles to make them more secure. “It’s not the car manufacturers’ fault, and it’s not a problem introduced by them. The security issue that we leveraged in our research lies in the standard that specifies how the car device network (i.e., CAN) works,” Trend Micro explains. “Car manufacturers can only mitigate the attack we demonstrated by adopting specific network countermeasures, but cannot eliminate it entirely. To eliminate the risk entirely, an updated CAN standard should be proposed, adopted, and implemented. This whole process would likely require another generation of vehicles.”

Alarming, but not surprising

While the vulnerabilities uncovered are clearly serious, they don’t come as much of a surprise to some. “The discovery may be alarming for the industry, but it’s not surprising as bugs will always exist that can be exploited, including in well-used technologies such as CAN,” observed Stacy Janes, Chief Security Architect at Irdeto. However, he’s not panicking just yet and suggests there are defensive steps to take.

“In order for an attacker to really exploit this attack remotely, he would need to come in through a telematics device and cause it to act improperly, injecting the malicious CAN messages,” said Janes. David Barzilai, Co-founder and Chairman of automotive cyber security firm Karamba Security, shared a similar point: “In order to remotely launch Denial of Service (DoS) CAN attacks, a hacker must compromise an externally-connected electronic control unit (ECU) and interfere with its factory settings. Such interference enables the hackers to start sending CAN messages that generate errors leading to a device DoS.”

Strategies

Industry players like Irdeto and Karamba have suggested various approaches to the problem. Janes is pushing for a “proper security-in-depth strategy” that includes on-ECU protection for telematics devices that detect and prevent on-disc and in memory tampering. This would effectively future-proof vehicles from being exploited when vulnerabilities like this are found.

“Security of communication between peer devices is always an important part of the overall security strategy and we have seen some innovative and interesting ideas over the past year around CAN message authentication and anomaly detection,” he told *Automotive World*. “It is important to remember, though, that even with technologies such as message authentication, if the end-point – ECU in this case – has been compromised, it may be possible for an attacker to send a malicious message that will be authenticated properly, thus still requiring a security in-depth strategy that includes full run-time integrity validation of the ECU.”

It is currently indefensible by modern car security technology, and to completely resolve it would require broad, sweeping changes in standards and the ways in-vehicle networks and devices are made – Trend Micro

While Trend Micro wants to change the legacy CAN protocol in all cars, Barzilai has warned that it would be a big job, as this covers practically all vehicles. “CAN is a legacy protocol, which most current ECUs support. The industry has been trying to update the protocol (e.g. CAN FD) and introduce new networks such as Ethernet and HDbaseT for faster communication, but the overhead of replacing the entire CAN protocol is so high, that the current thesis is that the new protocols will co-exist with CAN, rather than replace it,” he explained. On the whole, Karamba “does not believe that the industry will carry the weight of replacing CAN due to the security flaw that Trend Micro has reported on, but rather find ways to ensure that such a vulnerability will not be exploited.”

Barzilai advocates that the industry harden the externally-connected ECUs according to their factory settings, to prevent any unauthorised change to the ECU. “Blocking such changes enables the industry to prevent cyber attacks, including the DoS attack that Trend Micro reported on,” he added.

Taking it seriously

Despite continued vulnerabilities, the industry is making progress on cyber security. “In our opinion, since early 2016, the automotive industry has shown great interest in properly understanding not only the attack vectors against individual components but also understanding the full attack surface of the vehicle,” said Janes. “Their knowledge of security is continuously improving and I have confidence that the industry will do what is necessary to stay ahead of cyber security threats.”

Barzilai echoed this sentiment, observing how automotive companies are taking the cyber security challenge “very seriously.” Specifically, he points to the adoption of some IT security measures for car architectures. Some vehicle manufacturers and Tier 1 suppliers have been applying internal firewalls to try to segregate mission-critical ECUs from non-mission-critical ECUs. At the same time, they are conducting code scanning exercises in an attempt to flash out security bugs during the quality assurance phase. He also notes how OEMs are brainstorming with Tier 1s on the best ways to both detect and prevent attacks. But that said, he adds: “Vehicle security is not the same as IT security, if just for the dire consequences of an attack. The vendors are now starting to move to the next phase, and to search for solutions that provide reliable prevention of attacks, at the exploit attempt, not after the hackers succeed in hacking the car.”