Status summary of CAN security specifications

There is still no dedicated CAN security specification or standard released. Nevertheless, there are committed activities ongoing.

This article originally appeared in the September issue of the CAN Newsletter magazine 2019. This is just an excerpt.

CAN-IDs used for transmissions (Source: Emsa)

In the last CAN Newsletter issue, the Micro CANcrypt concept was introduced, to show you how to add security to Classical CAN systems with limited resources both in terms of memory and performance. There, we used the additional 18 bits of a 29-bit extended CAN ID to add a digital signature. We promised you some hard, real-world numbers for both memory and CPU resources for this solution, however, got side-tracked by pursuing other CANopen FD customer projects.

Customer comes first, but once we have adapted Micro CANcrypt to run on a lower-performance micro-controller according to plan and have actually run it, you can expect to see an update in one of the upcoming CAN newsletters. End of June 2019, the CiA association hold a phone conference for safety and security issues. Holger Zeltwanger gave the participants an update regarding “base documents”. When defining security solutions for Classical CAN, CAN FD, or CAN XL systems, it would be preferable to not start from scratch defining security basics for embedded systems or embedded communication systems. Unfortunately, the current draft of ISO 21434 “Road Vehicles – Cybersecurity engineering” does not seem to be suitable, as it is very generic and not yet completed. It is more of a guideline what designers and developers need to keep in mind when designing a “secured” vehicle.

CAN-IDs of received data frames (Source: Emsa)

Another document suggested is the “Baseline Security Recommendations for IoT” by the European Union Agency for Cybersecurity. Until the next meeting, CiA will review and report, if that document is suitable to be referred to also by CiA documents. CAN XL is still in an early specification phase and the related special interest group, recognizing the possibility for security features in hardware to be part of future CAN XL controllers, therefore suggested adding security features to CAN XL first. One of the discussed options is a blacklist/whitelist scheme like the one implemented by the NXP secure CAN transceiver family. Such a scheme can eliminate several potential attack vectors at once if all participants in a CAN (XL) network actively support it. Once we see which security features made it into the CAN XL specification (and hardware), we can review if any of these can still be applied to CAN FD, too, for example on the transceiver level.

However, potential CAN controller specific hardware security features will most likely not be suitable to migrate back into CAN FD, so protocol based security solutions are still required.

The essence of blacklist and whitelist handling

In a CAN system the use of the CAN IDs is unique, aside from some very special cases. For each 11-bit CAN ID (or 29-bit when using CAN extended frames) there is only one node in the system, which may transmit a CAN data frame using this CAN ID. Figure 1 shows an example of a simplified CANopen system and the CAN IDs used by each device.

If you want to continue reading this article, you can download the PDF of Mr. Olaf Pfeiffer and Mr. Christian Keydel from Embedded Systems Academy. Or you download the full magazine. This is free-of-charge.

cw