Generic CAN (FD) security requirements

This article gives an insight into the CAN (FD) security issue as asked by several companies participating within the CiA's (CAN in Automation) interest group IG safety and security.

In the past 5 years we have been reporting about various security threats and solutions for CAN and CAN FD. It is interesting to see that security requirements can differ quite a bit depending on the application, and that therefore the solutions developed also differ. An access control system has a high focus on authentication but might not care about encryption. A custom high-tech machinery in a somewhat closed housing might not worry about authentication but more about protecting the intellectual property and encryption of the data exchanged, making re-engineering more difficult. From the security viewpoint, the toughest applications are those where the system owner or user is considering the security threat. For example, when an owner is trying to bypass a machine's safety limitations such as a maximum weight, speed, or RPM (rotations per minute).

Usually, adding security to the CAN (FD) communication level is not sufficient, a more detailed view at the entire system is required to address all potential attack vectors. Nevertheless, secure CAN (FD) communication is an important "piece of the security puzzle" in more and more applications. As is, CAN (FD) systems are too easy to manipulate once an attacker has access to the CAN (FD) wiring. Adding a sniffer or even a contactless CAN interface allows recording and replaying of CAN frames, often allowing full control of a system. If such access is gained remotely because of a weak gateway, multiple systems can be at risk of misuse.

Current developments

There are currently multiple working groups at CAN in Automation (CiA) addressing security issues. The SIG (special interest group) CAN XL TF Security works on adding security to CAN XL (the third CAN generation), directly on the data link layer so that it can become part of the hardware, the CAN XL interface.

In September 2021, the IG safety and security decided to also review security options for CAN and CAN FD. The Hochschule Offenburg (Institute for reliable Embedded Systems und communication electronics) and Embedded Systems Academy (Emsa) currently work together on a proposal that defines a generic security layer for secure group communication in lightweight broadcast networks such as CAN (FD).

Being of general interest, the approach is pursued by defining the generic objects, parameters, and roles required in such a way, that they can be mapped to multiple network technologies. Although optimized for CAN and CAN FD (also covering CANopen and CANopen FD) the methods could also be mapped to I2C or EIA-485 based communication.

Key requirements

The key elements and requirements of the proposal are:

- The underlying communication system exchanges communication blocks with data and meta data (such as a CAN frame using a CAN-Identifier, DLC (data length code), and data field).
- The underlying communication system shall have a method to identify devices (e.g. using a node ID).
- To secure these communication blocks a security object is added to or associated with them.
- A manager role supervises the secure communication and initiates key refresh cycles.
- A synchronized date and timestamp with one-millisecond resolution is used for uniqueness and to prohibit replay attacks.
- If required, ALL communication blocks can be secured.

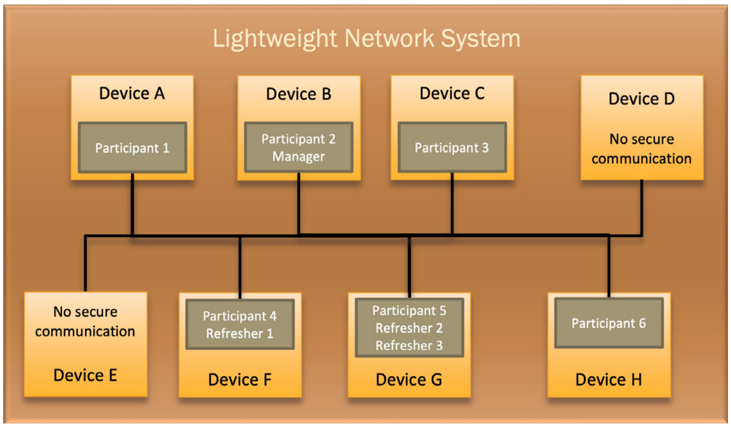

Figure 1: The various security roles that need to be assigned in the network system (Source: Emsa)

Figure 1 illustrates the various roles that need to be assigned in the network system. All devices that need to be able to produce or consume secure communication blocks need to implement the "participant role". One device must implement the "manager role" and a total of three "refresher roles" are required. These are helpers to the manager in the current communication key refresh cycles.

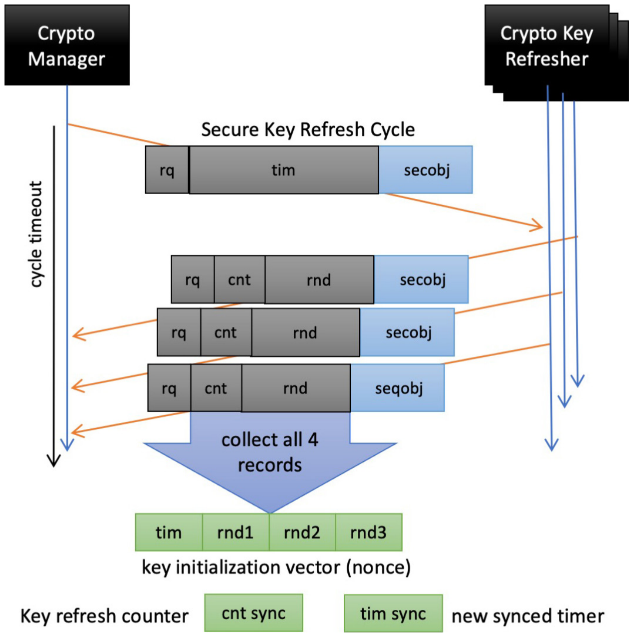

Figure 2: Basic elements of the current communication key refresh cycle (Source: Emsa)

The basic elements of the current communication key refresh cycle are shown in Figure 2. The manager role initiates the key refresh cycle and shares the current date and time value. The three refresher roles reply with an updated key refresh counter and a random value. All these messages are secured with the security object using a cryptographic checksum based on the previous key.

Once the cycle is completed, all participants build a nonce (number used once) using the timer and the random values. The nonce and the current session key is then used to generate a new communication key used to secure all communication blocks until the next refresh cycle. In addition, all participants synchronize their timers and key refresh counters.

Security object

Let us have a closer look at the security object used to protect each communication block. As a minimum, the security object contains the following data:

- The truncated timestamp (such that participants can restore the full value)
- A truncated key refresh counter (to determine which key is currently in use) and
- The cryptographic checksum for authentication

If and how many bits are used for the individual values is specified by the mapping document profiling the security layer for a specific network technology. For CAN FD, the security object could be made part of the data field, requiring only limited truncation. For CAN it could be part of the CAN-Identifier (using 29 bits instead of 11 bits) or located in an additional CAN frame if no other options are available.

Limitations

The effectiveness of the generic security layer depends on the specific cryptographic methods chosen and how its objects are mapped to the underlying communication system. The security offered provides a “secure grouping” or “point-to-multipoint” security. For each participant the security ends in the software layer implementing the participant role.

Receiving a properly authenticated communication block means that the participant determines that the transmitter sent the exact data received and that it was not manipulated during transmission or that it did not originate from an alternate source (such as an additional device injecting communication blocks to the physical media).

However, it cannot guarantee that the data was not manipulated on higher layers within the transmitting device. This could be the case if the application in the transmitter device is compromised, or sensors connected have been manipulated.

When and how the initial primary keys are installed is application-specific. Often these would be installed on the system integration level when powering up a network for the first time. The authors recommend that a change of the primary keys is only allowed through a public key certificates method.

Outlook

The detailed proposal will be submitted to the CiA and IG safety and security, which will then review it. A first prototype implementation for CANopen FD is expected to be available in quarter 1, 2022. ◀

Authors

Olaf Pfeiffer
Emsa (Embedded Systems Academy)
info@esacademy.com
www.esacademy.de
Andreas Walz
Hochschule Offenburg
info@hs-offenburg.de
www.hs-offenburg.de