CANopen FD multi-level security demonstrator

Many CAN-based networks open multiple attack vectors for hackers, especially after they have gained access to the system either remotely through a gateway or even physically.

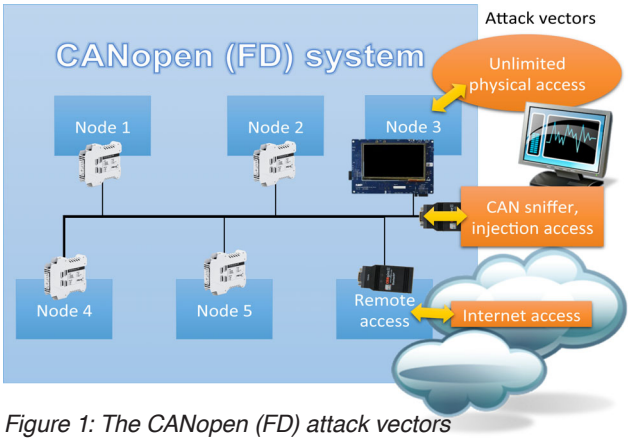

Figure 1: The CANopen (FD) attack vectors (Source: EmSA)

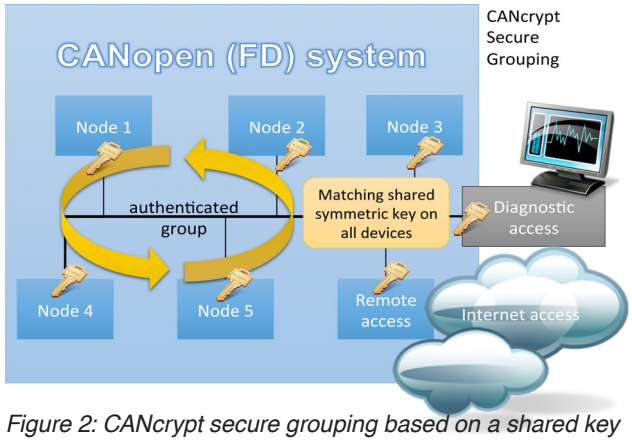

Figure 2: CANcrypt secure grouping based on a shared key (Source: EmSA)

The CANopen FD multi-level security demonstrator consists of a simple CANopen FD system with two generic I/O devices from Peak-System (buttons, signal lights) and a controller device with touch screen and text display (LED matrix). All of these are based on LPC54618 or LPC54S018 micro-controllers from NXP. An optional CANopen FD Bluetooth gateway can be used to provide a tablet remote access to the controller.

The different security levels implemented in the demonstrator protect from multiple attack levels:

- *Hardware level attack:* extract keys and/or codes from micro-controllers when unlimited physical access is available (through debug access or code extraction services).
- *Security solution:* Use micro-controllers with special protected non-volatile storage like the NXP LPC54Sxxx micro-controllers with PUF (physical unclonable functions) protection to protect code and keys.
- *CAN (FD) frame injection attack:* use a CAN sniffer connected to the system or a hijacked connected CAN (FD) device, listen to all CAN (FD) frames and inject fames to trigger control functions.
- *Security solution:* Use NXP TJA115x Secure CAN Transceiver (HW) or CANcrypt message monitoring (SW) to react to detected injections.
- *Advanced CAN (FD) frame injection attack:* perform CAN (FD) frame injections after the device monitoring these CAN IDs has been taken offline or from a hijacked, authorized device.
- *Security solution:* Use CANcrypt (FD) secure grouping with secure heartbeats and message authentication to prohibit injected, unauthorized messages from being accepted.
- *Remote access attack:* hijack a CAN (FD) device with Internet access. If that device is authorized and has the CANcrypt key available, authorized CAN messages might be generated.
- *Security solution:* Use end-to-end security with DTLS where the device providing Internet and CAN FD access does not have the keys required for the end-to-end protection.

Secure grouping with CANcrypt

CANcrypt is based on a shared key that is installed or generated at the end of the system integration process, after all components have been installed on the network. During operation a dynamic key based on that shared secret is used and continuously updated through a secure heartbeat mechanism.

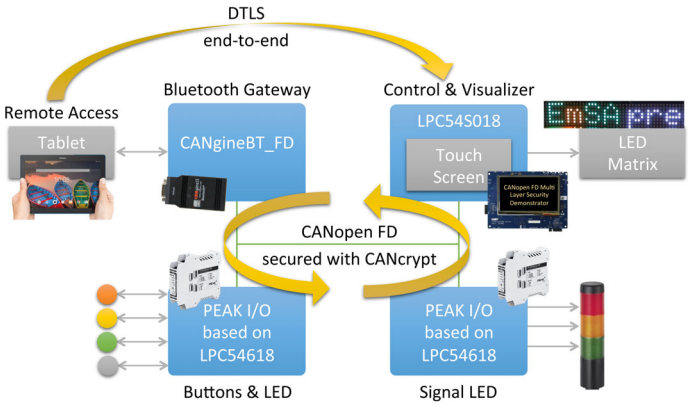

Figure 3: The CANopen (FD) multi-level security demonstrator (Source: EmSA)

End-to-end security for CANopen (FD) with DTLS

The wide-spread transport layer security (TLS) and datagram TLS (DTLS) protocols are the basis for secure Internet traffic, i.e. for secure online banking, e-commerce, or social media. Both protocols offer end-to-end (E2E) security with regard to:

- authentication using pre-shared keys or certificates,
- confidentiality using symmetric cryptography, where the keys are either pre-shared or negotiated with asymmetric cryptography,
- integrity using hash algorithms

Till today, industrial field busses are still lacking such security features. Now, developers from Embedded Systems Academy and researchers from Offenburg University of Applied Sciences demonstrate, how DTLS can be used to achieve Internet-grade protocol security in CANopen (FD) systems.

Using dedicated entries in the Object Dictionary of CANopen (FD) nodes, two nodes within the network (intradomain) or even one node within and one external node (interdomain) can establish a secure DTLS tunnel. Network intermediaries, not even CANopen (FD) gateway, need to be trusted.

Secure interdomain communication is particularly useful for remote service and configuration use cases, firmware updates, or highly security-critical transfers in general.

CANcrypt-secured messages have a security record embedded and can be encrypted if needed. Authentication is provided based on an encrypted CRC16 value. The security algorithms used are configurable. Default methods are XTEA64 or AES128.

CANopen FD multi-level security demonstrator

Figure 3 shows the functional elements of the demonstrator. All CANopen FD devices are protected with CANcrypt message monitoring and secure grouping.

A CANgineBT-FD module by ESSolutions provides an Android tablet wireless access to the CANopen FD network. DTLS end-to-end security is established between the tablet and the controller and visualizer module which accepts remote control commands and displays text strings received by the tablet.

The demonstrator is shown at the Embedded World 2019 in Nuremberg, hall 4A, booth 220. A video about the demonstrator will be released after the Embedded World. ◀

Author

Olaf Pfeiffer
EmSA (Embedded Systems Academy)
info@esacademy.com
www.esacademy.de