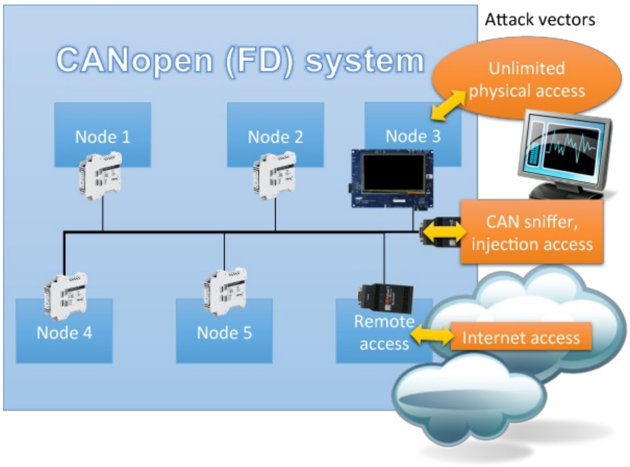
CAN Newsletter Online

CAN NEWSLETTER MAGAZINE

CANopen FD multi-level security demonstrator

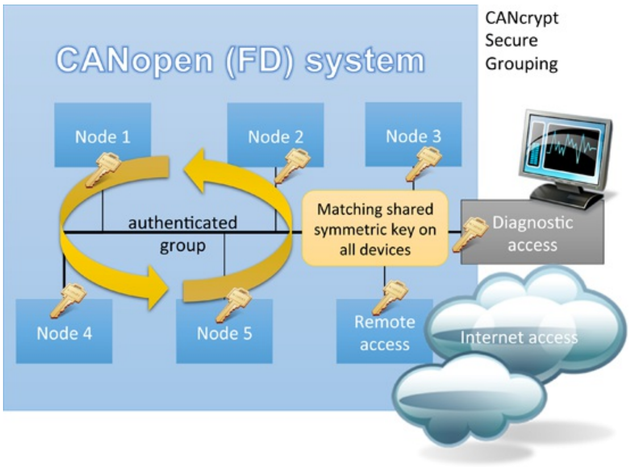
Many CAN-based networks open multiple attack vectors for hackers, especially after they have gained access to the system either remotely through a gateway or even physically.



The CANopen (FD) attack vectors (Photo: Emsa)

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

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:



CANcrypt secure grouping based on a shared key (Photo: Emsa)

- 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.

If you want to continue reading this article, you can download the PDF of Olaf Pfeiffer. Or you download the full magazine. This is free-of-charge.

cw