Classical CAN/CAN FD security threats

The authors already have introduced various technical solutions for distinct security threats. In this issue of their quarterly articles, they want to take a step back to look at the bigger picture of CAN security.

We've already introduced you to various technical solutions for distinct security threats: black- and whitelisting technologies for Classical CAN/CAN FD transceivers, CANcrypt for authenticated and/or encrypted Classical CAN/CAN FD communications and (D)TLS for secure end-to-end security in remote access applications. However, choosing the right one largely depends on the application's needs and the manufacturer's design goals. Some might be more worried about their intellectual property being copied while others fear unauthorized access to their systems the most.

Classical CAN or CAN FD is used in so many different applications that it will be close to impossible to find a common security solution for all use cases. In our past CiA (CAN in Automation) security meetings it has become clear that we need to collect a list of security threats for Classical CAN/CAN FD systems and address them individually. We don't claim this list to be comprehensive but rather a starting point for further explorations:

Vandalism (denial-of-service)

Vandalism often has a random component – sometimes, the affected system is just at the wrong place at the wrong time. With physical access, an attacker may destroy connectors or cut wires of the CAN network, among other damage. With remote access they might just try to flood the CAN network with high-priority messages, causing a denial-of-service attack (DOS). Either way, the system will likely malfunction or fail.

Bypassing limitations, using unauthorized spare parts (variation of jailbreaking)

This category includes all system manipulations done by a user or owner for the purpose of functional or financial gain, such as tweaking run time or total distance counters or the odometer of a moving system or using a vehicle outside its specified parameters for "tuning" it. Practical examples discovered in the field include taximeter manipulations or manipulations of the weighing system in a truck to be able to overload it. The spare parts and service business is another use case: many manufacturers want to allow only authorized workshops to install authorized spare parts. For the system designer and the required security techniques all these examples are challenging because usually the owner or user of a machine has full physical access to the machine. They can easily add or replace components on the CAN network.

Unauthorized data collection

The data communicated via the CAN network may be sensitive and include personal data, for example diagnostic measurements in medical applications or location data from any moving vehicle application. The value of the collected data is steadily increasing the more it is collected, especially when combined with large-scale networking and cloud technologies like envisioned in Industry 4.0. There are already artificial-intelligence algorithms that rate a vehicle driver as "good" or "bad" based on collected CAN vehicle data. Other systems try to collect so much data from different sources that operators can be alerted in advance that machinery components are about to fail. All the above is information that is owned by a person or a company. A leaking of this information is not in the interest of that party or even prohibited by law and must therefore be prevented.

Stealing intellectual property

Sometimes CAN communications include the exchange of intellectual property. This can be complex configuration schemes or tables, for example when multiple large electrical drives are controlled using specific acceleration ramps.

▷

Table 1: The table shows a summary of the attack vectors for the listed categories

Attack via	physical access	remote access
Vandalism, denial-of-service	cut wires	DOS (inject high prior frames)
Bypass limitations, jailbreaking	add/swap electronics	inject targeted frames
Unauthorized data collection	add sniffer	log all CAN frames
Stealing intellectual property	add sniffer	log all CAN frames
Unauthorized remote control	add electronics	inject targeted frames
Extortion, sabotage, ransomware	add/swap electronics	inject targeted frames

Table 2: The table shows possible protection options for attack cases

Attack via	physical access	primary remote access	secondary remote access
Vandalism, denial-of-service	lock access	Stinger (ltd)	Stinger
Bypass limitations, Jailbreaking	DTLS, Auth & Encr	DTLS, Auth & Encr	Stinger/DTLS, Auth & Encr
Unauthorized data collection	lock access	CANcrypt Encr (ltd)	Stinger/CANcrypt Encr
Stealing intellectual property	lock access	DTLS, Auth & Encr	DTLS, Auth & Encr
Unauthorized remote control	lock access	DTLS, Auth & Encr (ltd)	Stinger/CANcrypt Auth
Extortion, sabotage, ransomware	lock access	DTLS, Auth & Encr (ltd)	Stinger/CANcrypt Auth & Encr

Many CAN-connected devices also allow code updates through CAN. If the protection of the updating process is minimal or non-existing, a simple sniffer device might be sufficient to generate a copy of the entire firmware image and use it to clone the device.

Unauthorized remote control

An attacker with write access to a Classical CAN/CAN FD system can inject CAN frames to actively trigger controls. Past hacks have shown that more and more vehicles have active control components like power steering and power brakes that hackers can potentially trigger remotely. In industrial environments, this would translate to manipulating actuators, robots, valves etc.

Extortion, sabotage, ransomware

Ransomware-style attacks are designed to specifically cause real damage and either use it as a threat for extortion or to perform sabotage. They could start with slight manipulations of production parameters that lower the quality of your product but otherwise can go unnoticed for a long time and end with a complete halt of your production line if parameters are screwed up completely. To exercise that level of control, simply capturing CAN traffic or inject messages typically won't be enough but you'd have to replace hardware or firmware. Past hacks have already demonstrated that if the firmware update process over CAN is understood well enough, it can be used to remotely alter the firmware of devices in a way that makes them the gateway to launch further, more far-reaching attacks. ▷

Attack vectors and security protection options

Table 1 shows a summary of the attack vectors for the listed categories. An attacker with physical access to the CAN system can cut wires and remove, add, or replace electronic components. With any sort of remote access, e.g. by hacking into a component that has both Internet and CAN access, the attackers' intermediate goal would be to get access to be able to read all CAN frames communicated and to inject any CAN frame desired at any time.

In Table 2 we list protection options for these cases. We distinguish between secondary and primary remote access, where primary remote access is the access to a main control device that actively sends cyclic control commands. A secondary remote access goes to a device that does not perform active control algorithms. Typically, this would be a generic gateway between CAN and some other network or the Internet.

The security options referred to are:

- Stinger: Hardware protection based on the CAN ID using black- and whitelist filtering, as provided by the NXP TJA115x secure transceiver devices for example.
- CANcrypt: Software layer including secure grouping of multiple CAN devices providing encryption and/or authentication based on a symmetric key.
- DTLS: Software datagram transport layer security for end-to-end security providing encryption and/or authentication based on a public/private key pair.

"Lock access" means that no full physical access to the system shall be granted or possible. Full physical access by an attacker is the worst-case scenario as they might not even need CAN network access to obtain collected data collected intellectual property – instead, they may just lift it from embedded flash memory directly for example. In some cases, DTLS can still protect the system if the private keys can't be extracted and one of the communication end points of the DTLS connection is outside of the system. For example, code updates only happening through an encrypted and authenticated DTLS connection between the manufacturer's secure server and the target system.

If an attacker has successfully hacked into a component that does primary controls ("primary remote access" in table), then security options at the CAN communication level are limited in their effectiveness. If the device was authorized to send control messages and is equipped with appropriate keys in the beginning, then it will keep its authorization, even when hacked. All private keys stored on that device must be considered "compromised" at that point.

Conclusion

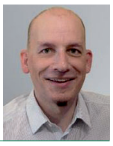
The bad news is that no matter what we do to add security to a CAN system, there will be always some cases left that cannot be protected with reasonable effort. We must work under the assumption that an attacker with unlimited physical access might be able to extract private keys stored in the devices. That would result in unlimited access to the protected CAN network, if the used security methods are based on these keys. There are several micro-controllers offering secure key storage that can't be extracted but while they are getting more common they are not yet extremely widespread. Also, if we learned anything from the past, it will only be a matter of time until new extraction methods are found.

But remotely-exercised attacks are a serious threat, too. A main control unit that is authorized to produce all CAN commands and has possession of all used keys will still be able to actively participate in any protected CAN communications. Therefore, the number one recommendation we can give you for any remote access to CAN: do not realize it via the main control unit. Any remote access should be implemented using a dedicated gateway where it is less challenging to configure it to also act as a firewall and better protect a CAN-based system.

The good news is that with a combination of Stinger, CANcrypt, and DTLS technologies you can still effectively protect your system from many attack vectors. The combination of Stinger and CANcrypt alone ensures that exploitation attempts by a determined attacker that manages to obtain CAN read and write access can do no harm.

Related articles

- Olaf Pfeiffer, Christian Keydel (Emsa): Status summary of CAN security specifications
- Olaf Pfeiffer, Christian Keydel (Emsa): Smart-bridging CANopen and CANopen FD
- Olaf Pfeiffer, Christian Keydel (Emsa): CAN security: How small can we go?
- Olaf Pfeiffer, Christian Keydel (Emsa): CANopen FD multi-level security demonstrator
- Olaf Pfeiffer, Christian Keydel (Emsa): No excuses for not securing your CAN FD communication!
- Olaf Pfeiffer, Christian Keydel (Emsa): Security expectations vs. limitations



Authors

Olaf Pfeiffer, Christian Keydel
Emsa (Embedded Systems Academy)
info@esacademy.com
www.esacademy.de

Products for mobile automation

WARRANTY 5 years on ifm products

Maximum reliability for extreme conditions

If there is one thing we know after many years of experience with sensors and control systems:
Products used in mobile machines must be extremely robust. Exposed to heat, cold, moisture, dust and vibrations, they must guarantee maximum reliability – even if the going gets tough. This is why we offer corresponding solutions for operation, communication and remote maintenance. The result: increased uptime and maximum reliability of your machines. ifm – close to you!

Go ifmonline
ifm.com / gb / mobile