Recently, some German researchers detected vulnerability in the CAN-based communication, when intentionally deploying the car’s airbag at the end-of-life on the scrapyard.

Security of automotive electronics is in the headlines. In the last years, the well-networked computer emergency response teams (Cert) reported several times about security vulnerabilities in CAN networks. Often the CAN protocol is accused and is therefore regarded as unsecure. Of course, CAN was originally not designed for security applications. This has to be done on the higher-layer protocols. Some CAN-based networks provide already in the application some security mechanism. Examples include the ISO 16844 tachograph systems and the ISO 26021 end-of-life activation of on-board pyrotechnic device standards.

Researchers from the university in Karlsruhe (Germany) detected that the secure CAN communication specified in ISO 26021-2 has some weaknesses. They found out that under some circumstances the airbag control units (also known as pyrotechnical control units) are affected. This issue was reported in the Common Vulnerabilities and Exposures (CVE) list under CVE-2017-14937. “The airbag detonation algorithm allows injury to passenger-car occupants via predictable Security Access (SA) data to the internal CAN network (or the OBD connector). This affects the airbag control units (aka pyrotechnical control units or PCUs) of unspecified passenger vehicles manufactured in 2014 or later, when the ignition is on and the speed is less than 6 km/h. Specifically, there are only 256 possible key pairs, and authentication attempts have no rate limit. In addition, at least one manufacturer’s interpretation of the ISO 26021 standard is that it must be possible to calculate the key directly (i.e., the other 255 key pairs must not be used). Exploitation would typically involve an attacker who has already gained access to the CAN network, and sends a crafted Unified Diagnostic Service (UDS) message to detonate the pyrotechnical charges, resulting in the same passenger-injury risks as in any airbag deployment.”
HY-TTC 32 - Compact Control Unit for Cost-Sensitive Applications, Smaller Machines and Implements

Flexibility and User Friendliness
- Extensive I/O set (30 Inputs / Outputs with various options for configurability by software)
- CAN with automatic baud-rate detection
- Programmable in C/C++ or CODESYS® including support for CANopen® master
- 1 x CAN bus termination configurable via connector pin

Connectivity
- 2 x CAN 125 kbit/s up to 1 MB/s
- CANopen conformity

Performance
- Infineon XC22xx CPU running at 80 MHz
- 768 kByte int. Flash, 82 kByte int. RAM, 8 kByte EEPROM

Safety
- Certified according to EN ISO 13849 PL c
- CANopen safety protocol (CiA 304) according to EN 50325-5

Robustness and Availability
- Aluminum die-cast housing for extremely rough work conditions
- Maximum current up to 24 A

www.ttcontrol.com/HY-TTC-32-ECU
It is not that bad as described: The ISO 26021 series mentioned the password protection as an example and specifies additional optional security mechanisms—a dedicated hardwired line, for example. If OEMs just implement the mentioned 16-bit password with an 8-bit version number, it is easy to “hack” the airbags. Of course, the car has to be nearly in standstill.

Nevertheless, the seed and key pair required for the security access (SA) is calculated by means of a weak algorithm (key by complementation) complying with the example given in ISO 26021-4. “This ISO standard gives the impression that the description of the SA is not only an example for an algorithm but a binding requirement,” criticized the researchers. “Thus, we suppose that several manufacturers copied the respective SA algorithm from the standard and implemented it without any alteration. This enables an attacker to calculate the proper key for the SA if he or she has the ISO 26021 available.”

The researchers also attacked successfully the CAN interface by means of brute-force without knowing the key algorithm: “The ISO 26021 proposes to use a 2-byte key, which results in 65536 different key pairs to be checked by an attacker in case he or she does not know the algorithm. Furthermore, the ISO standard states the following: ‘There is no time period, which needs to be inserted between access attempts’. Already these two weaknesses facilitate a brute-force attack on the SA seed and key pair. Additionally, the ISO 26021 requires that byte 1 of the only two-byte long seed includes the definite version number (00h) of the implemented load detonation method. This means that the first byte of the seed is known and the resultant seed and key pairs are reduced from 65536 to only 256 possible pairs.”

The ISO 26021 application protocol, a crafted Unified Diagnostic Service (UDS) message, is running physically on the diagnostic interface. This means, for an attack you need access to the OBDII connector. Except, a wireless remote access OBDII dongle is installed and powered. In this case, you may have remote access to the diagnostic CAN network and can perhaps trigger the airbags. The airbag detonation attack is in reality very unlikely. Of course, OEMs have been already informed and the corresponding ISO working group calls for experts, in order to improve the ISO 26021 standard.

Denial-of-service attacks

Earlier this year, the ICS-Cert (Industrial control systems cyber emergency response team) listed a denial-of-service (DoS) attack related to CAN networks. Under ICS-Alert-17-209-01, Italian researchers described that they have successfully attacked CAN networks by means of insertion of a permanent CAN error frame producing electronics. Of course, this causes a malfunction of the network. Since many years, there are tools on the market for testing purposes doing the very same. To achieve the mentioned DoS attack you need access to the bus-lines. If you have physical access to the network, you can also just cut the network cable to corrupt the communication. Another DoS attack could be remove the wheels – possible when you have access to the vehicle.

The ICS-Cert recommends to limit access to input ports (specifically OBDII) on automobiles. But this does not help on the described DoS attack, which requires physical access to the bus-lines, in order to install the error frame producing component.
CAN Newsletter Online: Security

The CAN Newsletter Online reports briefly about products and services.

Security system
**Securing CAN communication**
The CANcrypt system by Esacademy (Germany) adds multiple levels of security to CAN. It supports the grouping of multiple devices and the encrypted and authenticated communication between them. [Read on]

Processors with security
**Protecting cars against cyber threats**
STMicroelectronics protects connected cars against cyber threats with its latest automotive processors that feature built-in security and CAN modules. [Read on]

End-to-end solutions
**Securing connected cars**
Continental has introduced its security strategy, which includes to check continuously the communication on the CAN-based in-vehicle networks. [Read on]

Capture-the-flag
**Hack the car using an Arduino board with two CAN ports**
Riscure and Argus Cyber Security have scheduled the RHme3 event, the third episode of a Hack Me CTF (capture-the-flag). [Read on]

Security framework
**Example software now available**
After publishing the CANcrypt book, Embedded Systems Academy (Germany) now provides software examples on its security solution. [Read on]

Secure transceiver
**Engineering samples are available**
NXP has developed a CAN FD transceiver with cyber security features. This includes an ID whitelist and a bus-load measuring capability. [Read on]

Remote attack
**Security vulnerabilities**
Recently, Keen Security Lab discovered another security vulnerabilities on Tesla cars and realized an attack to CAN-connected ECUs with latest firmware. [Read on]

CAN fault confinement
**It is a feature not a flaw!**
The CiA Managing Director, Holger Zeltwanger, responses to the accusations that the CAN error detection and fault confinement has some cyber security weaknesses. [Read on]

Flexibility with real power!

ESX-4CS-GW Freely programmable central control unit

- Freely programmable
- Flexibility through multi-function I/Os
- Multiple communication interfaces
- Excels in rough environments
- Starter kit for an efficient start

**Exhibition Dates**

- **Hannover Messe**, Hanover
  23.04. – 27.04.2018
- **Sensor+Test**, Nuremberg
  26.06. – 28.06.2018

Sensor-Technik Wiedemann GmbH · Am Bärenwald 6 · 87600 Kaufbeuren · Germany · Telephone: +49 8341 9505-0
Internet: www.sensor-technik.com