Cyber security enhancing CAN transceivers

Bernd Elend, Tony Adamson, NXP Semiconductors

CAN nodes that have an attack surface like user accessible connections (e.g. WiFi, USB, Bluetooth, CD/DVD) could be compromised and pretend to be another node by sending messages with CAN IDs that are assigned to that other node. With that, they start to control functions in a network which they normally would not interfere with. Such compromised node could also generate a high bus load by sending high priority CAN messages very frequently, causing a denial of service for messages with low priority.
To avoid such cyber-attacks, the CAN transceiver can monitor the CAN IDs sent and stop transmission when they do not comply with a whitelist of allowed CAN IDs.
Transmission can also be stopped in case the node generates too much bus load.
Current transceivers are easily replaced by security enhancing transceivers, which is way easier than upgrading the host and its software. The transceiver offers a security level that is independent from a potentially compromised host and thus enhances the cybersecurity of CAN systems. These firewall-like functions are neutral to message latency and avoid the complexity of handling cryptographic keys. Configurability allows for flexibility and reduces the chance of success for hackers. This is the next evolution in smart transceivers after partial networking and FD shield.

Overview

The fast evolution of connected vehicles enabled by information and communication technologies has radically transformed the vehicle‘s user experience. The modern connected car with various internal and external communication interfaces, up to 150 electronic control units (ECUs) and 100 million lines of code [1], is like a cyber physical system rather than a mechanical system. The challenge of the seamless connectivity to the internet and end user electronics is the full exposure of the vehicle to the malicious vulnerabilities, such as buffer overflow exploits, malware and Trojans [2]. The connected car’s resilience to attacks is decreasing as the amount of electronics and software increases continuously. A common methodology to mitigate these risks is “defense in depth”. “Defense in depth” is a concept in which multiple layers of security countermeasures are placed through a system to provide redundancy in the event a security countermeasure fails or a vulnerability is successfully exploited. This is important because the attacker will need to circumvent multiple measures to launch a successful attack. NXP proposes that security is built up in the following four layers [5]:

- Interfaces to external world (V2X)
- Gateways between networks in the car
- In-vehicle network connections
- Processing in each node

1. Introduction

This paper focuses on the in-vehicle network (IVN) layer. IVN cybersecurity and the countermeasures are a well-studied topic. Previously, intrusion detection and prevention systems based on either the CAN ID information [3] or on the verification of CMAC value [4] have been proposed. Centralized and distributed systems have been discussed. In this paper, a distributed intrusion detection methodology is proposed, implemented by just the CAN transceiver, which in our proposal, and when compared to previous approaches [3], addresses more than just spoofing attacks. The chosen methodology is based on CAN network specific parameters, like identifiers of the CAN messages and the contribution to the bus load of a node. This methodology helps

defeating network attacks like spoofing, tampering and denial of service (flooding). The reasons for implementing these smart features in a transceiver are to allow a cost-effective and stepwise introduction of cyber security features into ECUs without the need to change microcontrollers or software. Security enhancing transceivers can be drop-in compatible with today's standard CAN transceivers and do not require other ECUs to be adapted.
The paper describes the attack model (Section 2) and the methodology to counter those attacks (Section 3), as well as an exemplary implementation of the methodology (Section 4).

2. Attack model

In this section, several attacks at the in-vehicle network (IVN) layer are examined and shown how they can be mitigated using the countermeasures in the proposed security enhancing transceiver.

2.1 Spoofing

Spoofing a CAN identifier means that a compromised node attempts to use an identifier that it is not allowed to send, see Figure 1. This can be useful to pretend to be another node. (This technique has been used in practical attacks on modern cars [2].)

Figure 1: Spoofing attack.

2.2 Tampering

For the tampering attack, the attacker aims to adjust a message, which another node is currently sending on the bus. The attacker must also adjust the cyclic redundancy check (CRC) to match the tampered data, see Figure 2.

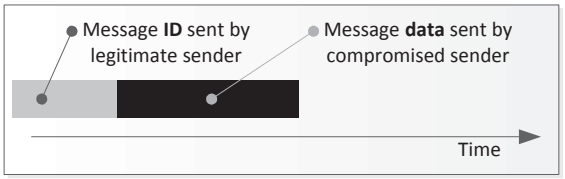

Figure 2: Tamper attack.

Before a successful tamper attack can be accomplished, the legitimate sender must be forced into the "Error Passive" state, or else it will publish an active error on the bus when the attacker causes a bit flip. The attacker can put the legitimate sender in Error Passive state by intentionally publishing errors on the bus for several times. The tampering attack is useful since it gives the attacker the power to tamper with the messages that are being sent on the bus, which may be of critical operation for the car. This kind of attack has been presented at conferences [7].

2.3 Flooding the bus (denial of service)

Flooding the bus is a way to deny service by continuously pumping the bus full of messages, see Figure 3. This makes the bus unusable for all other nodes, which can be used to disable safety relevant functionality.

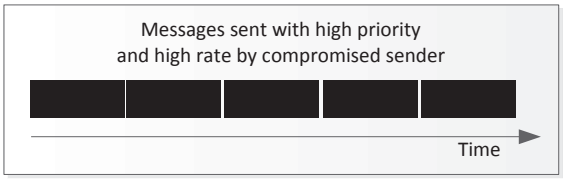

Figure 3: Flooding attack.

3. Methodology

The methodology proposed in this paper is a kind of a distributed intrusion detection and prevention system (IDS/IPS), working like a firewall that can be implemented in the transceiver. All the countermeasures are based on parameters that the trans-ceiver can perceive and are executed independently from the host, which might be compromised.

3.1 Filtering spoofed messages in transmit path

The first countermeasure, filtering CAN messages based on IDs in the transmit path, is a way for the transceiver to protect the bus from a compromised host. If the host tries to send a message with an ID that is originally not assigned to it, the transceiver can refuse to transmit this message on the bus by invalidating the message and deny to transmit the subsequent transmissions. CAN ID-based filtering can be done using a whitelist of IDs that is user configurable. For

example, the identifiers for Unified Diagnostic Services (UDS) as specified in ISO 14229 for off board testers may be excluded from the whitelist. This would prevent a compromised node from starting a diagnostic session with another node in the vehicle to, for example, to manipulate calibration values.

3.2 Invalidating spoofed messages on bus

The second possible countermeasure against spoofing is the monitoring and invalidating messages on the bus based on the ID. This technique enables every node to protect its own IDs in case a rouge node it not prevented from sending this ID as described in 3.1. When any node sends a message on the bus, the transceiver of the legitimate sender can actively invalidate that message by writing an active error frame to the bus. It can do this based of the same whitelist as the filtering in the transmit path. In case the compromised sender is compliant to ISO11898-1, it will repeat the spoofed message 16 times before entering the “Error Passive” state and the “Suspend Transmission” behavior kicks in. Finally, another 16 repetitions will occur before the attacking node enters “Bus Off”. When all nodes are equipped with a whitelist filter, as described in section 3.1, this odd scenario will not happen. However, in case after market components, which are not under control of the OEM, are attached, this method has a high value.

3.3 Tamper protection

Invalidating messages on the bus can be used to prevent tampering, when a node is in the Error Passive state. The security en-hancing transceiver can check whether there was a valid message on the bus, for which the local node has won arbitration, but stopped transmission (due to receiving a dominant bit while sending recessive). This is a clear sign that a compromised node has stepped into the transmission.

3.4 Leaky bucket bandwidth control in transmit path

Limiting the number of transmitted messages per unit of time can prevent flooding the bus, when implemented at the sender side. In certain applications, a burst of messages on the CAN bus is desirable, but this should only last for a certain amount of time. To prevent flooding, a leaky bucket mechanism can be used. In order, not to hamper diagnostic services, e.g. for uploading data, the contribution of messages with low priority IDs is neglected when filling the bucket.

4. Implementation

The proposed methodology is deployed on CAN transceivers. So, the implementation in transceivers provides an environment that is isolated from the host micro-controller. Additional advantage of implementing this in the transceiver is that it exploits the pervasiveness of the CAN transceivers in the IVN, enabling a fast and cost effective upgrade of existing ECUs to secure communications. For this work, a proof of concept has been developed. A demo silicon in SO8 package with standard transceiver pinout, which will be shown at the iCC 2017 in a small network, is available.

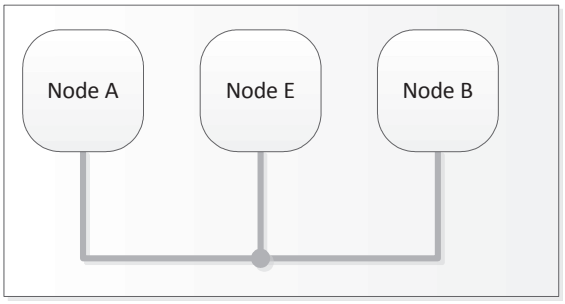

Figure 4: Network that demonstrates the functionality of the demo silicon of a security enhancing CAN transceiver. The grey lines indicate the CAN bus. The nodes from left to right are the legitimate sender Alice (A), the compromised node Eve (E) and the receiver Bob (B). For both the legitimate sender and the compromised node it can be selected whether a standard transceiver or the security enhancing transceiver is used to see the effect of the countermeasures when Eve launches an attack.

5. Discussion

Most countermeasures described above can be implemented in either the micro-controller or the transceiver. Upgrading a microcontroller‘s hardware and software in

existing control modules (ECUs) is expensive, while upgrading transceivers is an attractive alternative to that. This simple but effective IDS/IPS system is a “firewall” that sanitizes than CAN traffic.
As no cryptography is involved to allow a cost-effective solution, the configuration is protected by a passcode and the user can permanently lock the configuration once after testing the module.

6. Conclusions

This paper describes possible attacks on the data link layer of the CAN bus and proposes countermeasures that mitigate these threats. NXP is further working on demo silicon of the security enhancing transceiver with all the essential counter-measures: invalidating messages on the bus based on ID, filtering messages in transmit path based on ID, invalidating tampered messages on bus and rate control with a leaky bucket in transmit path.

References

[1] Charette, Robert N. This Car Runs on Code. http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code
[2] Miller, Charlie & Valasek, Chris Remote Exploitation of an Unaltered Passenger Vehicle. http://illmatics.com/RemoteCarHacking.pdf
[3] Matsumoto, T et.al. A Method of Preventing Unauthorized Data Transmission in Controller Area Network. Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th. 2012, pp. 15. doi: 10.1109/VETECS.2012.6240294
[4] Ueda, H et.al. Security Authentication System for In-Vehicle Network. SEI Technical Review, pp. 5- 9, Number 81, October 2015
[5] Secure Vehicle Architecture. http://www.nxp.com/applications/solutions-for-the-iot-and-adas/secure-connected-car-and-adas/secure-vehicle-architecture:AUTOMOTIVE-SECURITY
[6] Microsoft. Threats and Countermeasures Chapter. https://msdn.microsoft.com/en-us/library/ff648641.aspx

Bernd Elend
NXP Semiconductors GmbH
Stresemannallee 101
DE-22459 Hamburg
Tel.: +49-40-5613-2663
bernd.elend@nxp.com
www.nxp.com

Tony Adamson
NXP Semiconductors
Gerstweg 2
NL-6534AE Nijmegen
tony.adamson@nxp.com
www.nxp.com