Demo: Implementing CAN bus security by TOUCAN

Pietro Biondi, Giampaolo Bella
Dipartimento di Matematica e Informatica
Università degli Studi di Catania
giamp@dmi.unict.it,pietro.biondi94@gmail.com

Gianpiero Costantino, Ilaria Matteucci
Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche
name.surname@iit.cnr.it

ABSTRACT

Modern vehicles embed a lot of software that turns them into Cyper-Physical Systems (CPS). Electronic Control Units (ECUs) communicate through the CAN bus protocol, which was not designed to be secure. This paper presents a proof-of-concept of TOUCAN, a new security protocol designed to secure CAN bus communications following the AUTOSAR standard. The presentation introduces design, implementation and performance of TOUCAN on a test-bed composed by two inexpensive boards that can be demonstrated to exchange secure TOUCAN frames.

CCS CONCEPTS

• **Security and privacy → Embedded systems security**; **Security protocols**; *Hash functions and message authentication codes*;

KEYWORDS

Automotive, Cybersecurity, CAN Bus, Frame

ACM Reference Format:
Pietro Biondi, Giampaolo Bella and Gianpiero Costantino, Ilaria Matteucci. 2019. Demo: Implementing CAN bus security by TOUCAN. In *Mobihoc '19: The Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing, July 2–5, 2019, Catania, Italy*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3323679.3326614

1 THE TOUCAN PROTOCOL

Intra-vehicle communications among Electronic Control Units (ECUs) are driven by the "Controller Area Network" protocol, also known as *CAN bus* [3]. Components such as air-bags, parking sensors and others are interconnected and communicate to ensure smooth and fast reactions to ensure the smooth functioning of the vehicle. More specifically, ECUs interact through the CAN bus protocol. However, CAN is not meant to be secure [3, 4].

This paper presents TOUCAN, a new security protocol designed to secure CAN bus communications following existing standards. TOUCAN achieves security in terms of authenticity, integrity and confidentiality without the need to upgrade (the hardware of) existing ECUs or add components to the network. An essential by-design requirement of TOUCAN is to comply with existing standards in this area. Precisely, TOUCAN is CAN 2.0 compliant, which means that it can be executed on existing ECUs and infrastructures running CAN. It is also compliant with the AUTOSAR "On-board Secure Communication", *profile 1*, standard [2].

TOUCAN leverages the Chaskey [5] Message Authentication Code (MAC) to provide authentication and integrity to CAN frames. A requirement of the mentioned AUTOSAR profile is to allow a MAC field of 24 bits, which implies that we can rely on a payload of 40 bits and fit both in the 64-bit data field of a frame. Hence, TOUCAN is CAN compliant. Because the MAC must be truncated to 24 bits, the truncation resistance of Chaskey is a clear advantage for our application.

To achieve confidentiality, TOUCAN prescribed that the data field outlined above is encrypted using Speck 64/128. This is a lightweight yet robust block cipher with block size of 64 bits and keys of 128 bits.

1.1 TOUCAN on practice

Our test-bed consists of two STM32F407 Discovery boards with an ARM Cortex M4 processor each. The boards provide physical input buttons, plus light emitting diodes for visual outputs. These boards are equipped with an additional shield represented by a STM32F4 DISCOVERY COMM to provide CAN bus connectivity. To interface a PC with the boards, we use a USB-to-CAN device that allows the transmission of CAN messages between two or more devices. To conclude the test-bed, we employ the Keil IDE [1] as editor and tool to deploy the TOUCAN source code to the boards.

The goal of TOUCAN is to establish secure communications between the two boards when exchanging CAN frames. In this particular demonstration, we assume that the exchange of keys to be used by Chaskey and SPECK64/128 already occurred and focus on the actual protocol execution.

Mobihoc '19, July 2–5, 2019, Catania, Italy

ACM ISBN 978-1-4503-6764-6/19/07.
https://doi.org/10.1145/3323679.3326614

Thus, the demonstration is composed by two distinct cases: i) sending and ii) receiving TOUCAN frames.

In the first case, a board is in charge of sending TOUCAN frames of 40 bits, representing the message content. Then, the board calculates the MAC and the result is truncated to 24 bits, to complete the allowed 64-bit payload. In the end, the payload is encrypted with SPECK 64/128 and finally sent to the other board over the bus.

When the other board receives the TOUCAN frame, it first decrypts the entire payload, i.e., 64 bits, then it calculates the MAC on the message content received, i.e., 40 bits. The live MAC is truncated to 24 bits and is compared with the 24 bits of the MAC received from the sending board. If all checks succeed, then the board turns on the blue led, otherwise it turns on the red led.

Figure 1 shows our test-bed to exchange TOUCAN messages through the traditional CAN bus between the STM boards. By using these two boards, we want to reproduce a real setting composed by two ECUs inside a car that is interconnected through the CAN bus. In particular, the image shows the two Discovery COMM shields that implement CAN connectivity. In addition, both boards are plugged into the USB-to-CAN interface for message debugging. The figure also shows the board on the right with the blue LED on, which implies a correct reception of a TOUCAN frame, i.e., both decryption and MAC verification were successful.

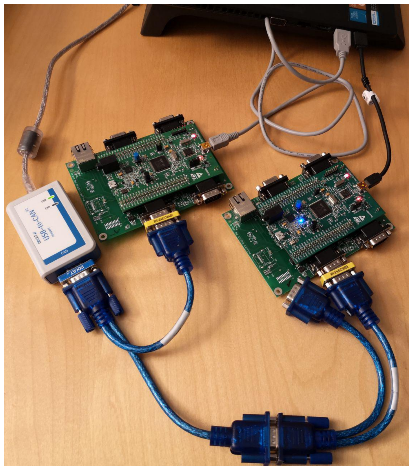

Figure 1: TOUCAN communication with two boards

1.2 Performances

One of the main requirements in the automotive industry is to minimise the reaction time when receiving and processing a frame. Traditional CAN communication requires time for building, transferring and receiving a frame. With TOUCAN, we obviously add additional computation due to the generation/verification of the MAC and the encryption/decryption of the data field. However, we were pleased to observe that the additional computation only negligibly reflects on the overall performance, despite the fact that our proof-of-concept only adopts inexpensive hardware.

Table 1 shows the algorithms used, the board speed and the execution time of each operation in microseconds. It seems fair to conclude that the runtimes are acceptable. In particular, the board speed at 168 MHz allows us to reduce MAC generation/verification to less than 1μs, and the encryption/decryption time to around 5μs. In summary, TOUCAN adds less than 6μs to generate or interpret a secure CAN frame, a finding that we deem very promising.

Algorithm	**Board Speed** [MHz]	**Time** [μs]
Chaskey	168	0,43
SPECK 64/128	168	5,36
SPECK 64/128 + Chaskey	168	5,79

Table 1: TOUCAN Performance

2 DEMO REQUIREMENTS

2.1 Equipment to be used

All equipment will be provided by the authors, consisting of:

- Two boards STM32F407 Discovery equipped with STM32F4 DISCOVERY COMM.
- USB-to-CAN interface with CAN Cables included to interface the boards with our PC.
- Monitor.

2.2 Space needed and required setup time

- Setup time: 30 minutes.
- Table length (at least): 100 cm.

2.3 Additional facilities needed

- Electric sockets and Wi-Fi access.

ACKNOWLEDGEMENT

We would like to thank Tecnologix S.r.l. that provide us all the needed material we exploit to test our implementation of TOUCAN.

REFERENCES

[1] [n. d.]. Embedded Development Tools. http://www.keil.com

[2] AUTOSAR. [n. d.]. "Specification of Secure Onboard Communication - AUTOSAR CP Release 4.3.1". https://www.autosar.org/standards/classic-platform/classic-platform-431/

[3] Charlie Miller Chris Valasek. 2014. Adventures in Automotive Networks and Control Units. http://illmatics.com/car_hacking.pdf.

[4] Charlie Miller and Chris Valasek. 2014. A survey of remote automotive attack surfaces. *Black Hat USA* (2014).

[5] Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. 2014. Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In *Selected Areas in Cryptography – SAC 2014*, Antoine Joux and Amr Youssef (Eds.). Springer International Publishing, Cham, 306–323.