TOUCAN
a proTocol tO secUre Controller Area Network

Giampaolo Bella[1], Pietro Biondi[1], Gianpiero Costantino[2], Ilaria Matteucci[2]

[1] Dipartimento di Matematica e Informatic Università di Catania
giamp@dmi.unict.it, pietro.biondi94@gmail.com
[2]Istituto di Informatica e Telematica-Consiglio Nazionale Delle Ricerche
{gianpiero.costantino, ilaria.matteucci}@iit.cnr.it

Modern vehicles abound with Electronic Control Units (ECUs) that need to speak with each other. Components such as airbags, power doors, electric mirrors need to interconnect and communicate to ensure the smooth and synergistic functioning of all. They adopt a binary language and form an in-vehicle network that must be precisely regulated. This was the aim for the inception of "Controller Area Network" protocol, also known as *CAN bus*, which dates back to 1983 with Bosch [3] and is widespread today. It is standardised in ISO 11898-1:2015 [4] as a simple protocol based on two bus lines. The CAN protocol runs through two of these pins.

The CAN bus is not meant to be secure. It signifies that it was designed in the assumption that it would execute in a friendly environment, with participants sharing the common goal of the smoothest possible functioning of the host car. Cybersecurity researchers are well aware that overly optimistic assumptions are deemed to be broken eventually. The current automotive landscape makes no exception and clearly breaks the assumption of a friendly execution environment for several reasons. One is that cars' functioning is closely related to passenger safety, hence potential threats may be ill-driven towards harming people. Another one is that cars are becoming more and more tightly interconnected to the external world, not only by GPS, but also by 4G and by dedicated connections such as for *e-call* boxes [1]. They hold a variety of driver's (and, progressively, passengers') data, such as driving style or significant episodes, environmental data acquired through various sensors and cameras, as well as data received from the passengers' smartphones. Where biometric techniques are used to authenticate the driver, cars even treat sensitive data. All such data is obviously appealing for profiling and marketing reasons, for example for insurance companies.

Therefore, awareness is growing on the need to secure in-vehicle communication, but this goal is daunting: whatever novel technology should be tested on the large scale, should not be prohibitively expensive and, above all, should not clash with efficiency of the communication, because this is tightly related to the latency of the various devices of a car, hence again to passenger safety.

We propose TOUCAN [2], a protocol to secure the CAN bus against an active eavesdropper. The protocol enjoys backward compatibility with existing standards and requires no hardware upgrade but solely a firmware update to implement TOUCAN. TOUCAN uses a fast hashing algorithm, Chaskey [5], to provide authenticity and integrity of the payload of a frame, and AES-128 encryption for confidentiality. The TOUCAN frame complies with the CAN standard hence its Data field is of 64 bits, although it carries an actual payload of 40 bits because its hash is carried by the remaining 24 bits of the field.

The prototype implementation of both hashing and encryption algorithms used in TOUCAN has been tested on inexpensive hardware. In particular, our test-bed is composed by a STM32F407 Discovery board in which we deploy programs computing Chaskey hash values as well as AES-128 cyphertexts, as we shall see. The runtimes we measured were promising, a result that also makes TOUCAN a potentially good candidate for adoption as an AUTOSAR in-vehicle security protocol.

References

[1] ecall in all new cars from april 2018.

[2] Giampaolo Bella, Pietro Biondi, Gianpiero Costantino, and Ilaria Matteucci. Toucan - a protocol to secure controller area network. In *Proceeding of ACM AutoSec@CODASPY 2019*, Accepted to be published. 2019.

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

[4] International Organization for Standardization. Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling. https://www.iso.org/standard/63648.html, 2015.

[5] Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An efficient mac algorithm for 32-bit microcontrollers. In Antoine Joux and Amr Youssef, editors, *Selected Areas in Cryptography – SAC 2014*, pages 306–323, Cham, 2014. Springer International Publishing.