

Lista lucrări publicate

T. Lenard, R. Bolboacă, B. Genge and P. Haller, "**MixCAN: Mixed and Backward-Compatible Data Authentication Scheme for Controller Area Networks**," 2020 IFIP Networking Conference (Networking), Paris, France, 2020, pp. 395-403.

Abstract: The massive proliferation of state of the art interfaces into the automotive sector has triggered a revolution in terms of the technological ecosystem that is found in today's modern car. Accordingly, on the one hand, we find dozens of Electronic Control Units (ECUs) running several hundred MB of code, and more and more sophisticated dashboards with integrated wireless communications. On the other hand, in the same vehicle we find the underlying communication infrastructure struggling to keep up with the pace of these radical changes. This paper presents MixCAN (MIXed data authentication for Control Area Networks), an approach for mixing different message signatures (i.e., authentication tags) in order to reduce the overhead of Controller Area Network (CAN) communications. MixCAN leverages the attributes of Bloom Filters in order to ensure that an ECU can sign messages with different CAN identifiers (i.e., mix different message signatures), and that other ECUs can verify the signature for a subset of monitored CAN identifiers. Extensive experimental results based on Vectors Informatik's CANoe/CANalyzer simulation environment and the data set provided by Hacking and Countermeasure Research Lab (HCRL) confirm the validity and applicability of the developed approach. Subsequent experiments including a test bed consisting of Raspberry Pi 3 Model B+ systems equipped with CAN communication modules demonstrate the practical integration of MixCAN in real automotive systems.

URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9142797&isnumber=9142691>

Roland Bolboacă, Teri Lenard, Béla Genge, and Piroška Haller. 2020. **Locality sensitive hashing for tampering detection in automotive systems**. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, Article 57, 1–7. DOI:<https://doi.org/10.1145/3407023.3409206>

Abstract: In modern auto vehicles we find dozens of Electronic Control Units (ECUs) running several hundred MBs of code, alongside sophisticated dashboards with integrated wireless communications. While this technological advancement has brought upon a wide range of advantages and integrated features, it also exposed the modern vehicle to significant cyber threats, as documented in prior works. Unfortunately, besides traditional cyber attacks, the security and normal operation of the modern vehicle are nowadays exposed to a different kind of threat. This is the tampering, which denotes a procedure that alters the vehicle's behavior in order to gain particular advantages (e.g., financial, operational). A fundamental distinction between tampering and cyber attacks, is that tampering occurs with the owner's consent. This paper presents an approach for detecting tampering within modern vehicles by leveraging the advantages of sensitive hashing, namely the Exact Euclidean Locality Sensitive Hashing (E2LSH) method. Experimental results based on a dataset collected from the On-Board Diagnostics port (OBD) of a Kia SOUL vehicle demonstrate the practical applicability of the developed methodology.

URL: <https://dl.acm.org/doi/abs/10.1145/3407023.3409206>

Teri Lenard, Roland Bolboaca and Bela Genge. **LOKI: A Lightweight Cryptographic Key Distribution Protocol for Controller Area Networks**. 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP 2020), to be held September 3 - 5, 2020 in Cluj-Napoca, Romania.

Abstract: The recent advancement in the automotive sector has led to a technological explosion. As a result, the modern car provides a wide range of features supported by state of the art hardware and software. Unfortunately, while this is the case of most major components, in the same vehicle we find dozens of sensors and sub-systems built over legacy hardware and software with limited computational capabilities. This paper presents LOKI, a lightweight cryptographic key distribution scheme applicable in the case of the classical in-vehicle communication systems. The LOKI protocol stands out compared to already proposed protocols in the literature due to its ability to use only a single broadcast message to initiate the generation of a new cryptographic key across a group of nodes. It's lightweight key derivation algorithm takes advantage of a reverse hash chain traversal algorithm to generate fresh session keys. Experimental results consisting of a laboratory-scale system based on Vector Informatik's CANoe simulation environment demonstrate the effectiveness of the developed methodology and its seamless impact manifested on the network.

Status: Paper was accepted, but is not indexed yet.

URL: <http://www.iccp.ro/iccp2020/index.php/technical-program.html>