

Lista lucrări publicate

Roland Bolboaca

[1] Teri Lenard, Roland Bolboaca, **A Stateful Firewall and Intrusion Detection System Enforced with Secure Logging for Controller Area Network**, European Interdisciplinary Cybersecurity Conference, Targu Mures, Romania, 2021.

Abstract: The Controller Area Network standard represents one of the most commonly used communication protocol present in today's vehicles. While its main properties facilitate the communication between different control units, several protocol design considerations represent security problems. While it's trivial for an attacker to gain access and control the system, solutions capable of mitigating such incidents lack from a vehicle's network. The current work proposes a Stateful Firewall, together with a signature-based Intrusion Detection System as a response. Beside this, a Secure Logging unit is brought up in addition to support our methods, enforcing them with integrity verifiable logs.

[2] Roland Bolboaca, Teri Lenard, Bela Genge and Piroska Haller, **Locality Sensitive Hashing for Tampering Detection in Automotive Systems**, ARES: The 15th International Conference on Availability, Reliability and Security, 2020, Dublin, Ireland.

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.

[3] Teri Lenard, Roland Bolboaca, Bela Genge and Piroska Haller, **MixCAN: Mixed and Backward-Compatible Data Authentication Scheme for Controller Area Networks**, IFIP Networking 2020 Conference (IFIP Networking 2020), Paris, France.

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.

[4] Teri Lenard, Roland Bolboaca, Bela Genge and Piroska Haller, **LOKI: A Lightweight Cryptographic Key Distribution Protocol for Controller Area Networks**, International Conference on Intelligent Computer Communication and Processing ICCP 2020, Cluj, 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. Its 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.

[5] Roland Bolboaca, Bela Genge and Piroska Haller, **Tampering detection for in-vehicle systems**, Fourth International Conference on Applied Informatics, Imagination, Creativity, Design, Development - ICDD, 2020, Sibiu, Romania.

Abstract: Tampering denotes the procedure that changes the behavior of a process (e.g., automotive system, process control system) for particular advantages (e.g., financial, operational). Compared to cyber attacks, the purpose of tampering is not to cause specific damages, but to alter the system's behavior in order for the owner to gain particular advantages. This paper documents, to the best of our knowledge, the first approach to detect tampering in automotive systems. The approach embraces a two-step methodology. At first, Principle component analysis (PCA) is applied to reduce the complexity of the data exploration and analysis procedure. Then, the Gaussian mixture model is applied to classify the data and to detect tampering attempts. Experimental results based on measurements extracted from the OBD II system of a KIA automobile driven by 10 drivers over a total period of 23 hours in Seoul, South Korea demonstrate the applicability of the developed approach in real-world scenarios.

[6] Bolboaca Roland, Genge Bela, Haller Piroska. **Using Side-Channels to Detect Abnormal Behavior in Industrial Control Systems**, International Conference on Intelligent Computer Communication and Processing ICCP 2019, Cluj, Romania

Abstract: As demonstrated by the large number of related studies, the field of anomaly detection in the context of Industrial Control Systems (ICS) has reached a certain level of maturity. However, we believe that additional research is needed in order to explore the side-channel specific parameters exposed by regular operations within ICS. The term “side channel” is a term usually found in cryptanalysis, where information about the behavior of the cipher, that is, the non-functional information, is used to break the ciphers. In the context of anomaly detection, side-channels denote non-functional information that can be derived from the normal operation of the system in order to infer the actual system state. This paper presents an anomaly detection system that explores the periodicity in ICS communications, where particular application-level operations are triggered periodically. To this end, we leverage the periodicity of a security protocol that has been implemented as part of our prior work to secure communications in ICS. We measure the deviations in the execution of the protocol's different phases in order to detect abnormal events that are caused at different levels in the architecture of the ICS. The main advantage of the developed approach is that it is protocol, software and application agnostic, making it suitable for legacy ICS as well. Experimental results are conducted in the context of a real industrial control system operating in a Romanian gas transportation network.

[7] Bolboaca Roland, Genge Bela, Haller Piroska. **Detecting anomalies in Industrial Control Systems by leveraging side-channel information**, EMT - XXIX. SzamOkt International Conference on Computer Science 2019, Timisoara, Romania.

Abstract: Considering the fact that the number of attacks on Industrial Control Systems are increasing, it is an emergency need for new and innovative security solutions. In the context of anomaly detection, side-channels define non-functional information that can be obtained from the normal operation of the system in order to ascertain the actual system state. In this paper we present an application level approach for detecting anomalies by leveraging side-channel information. Our approach consists of measuring the transition times of a periodic protocol states. Three detection algorithms, based on cumulative sum models, were developed and tested on a natural gas transport automation node.