

GEORGE EMIL PALADE UNIVERSITY OF MEDICINE, PHARMACY, SCIENCE,
AND TECHNOLOGY OF TÂRGU MUREŞ
DOCTORAL SCHOOL OF LETTERS, HUMANITIES AND APPLIED SCIENCES
INFORMATICS

UNIVERSITY OF GENEVA
SCHOOL OF ECONOMICS AND MANAGEMENT
INFORMATION SYSTEMS

TRUSTED SOFTWARE-DEFINED VEHICLES

Joint PhD Thesis

by

Teri LENARD

Scientific Supervisors:

Prof. Béla GENGE - G. E. Palade University of Medicine, Pharmacy, Science, and
Technology of Târgu Mureş, Romania

Dr. Niels A. NIJDAM - University of Geneva, Switzerland

Dr. Anastasija COLLEN - University of Geneva, Switzerland

Prof. Dimitri KONSTANTAS - University of Geneva, Switzerland

2024

Software-Defined Systems (SDSs) emerged in the past decades as a promising Service-Oriented Architecture (SOA) that leverages the hardware of the underlying system to provide an agnostic basis for building controllable and feature-rich software environments. A SOA encapsulates groups of software services distributed across a networking system. Through a SOA, system designers can define flexible standardized communication interfaces, service separation and abstraction from the underlying hardware through virtualization, continuous over-the-air updates, system monitoring and management. The technological and operational benefits of a SOA have started to be adopted by manufacturers that develop Electrical/Electronic Architectures (EEAs). The motivation for this phenomenon lies in several limitations imposed by an EEA, in terms of system maintenance, software updates, feature deployment, and management. An EEA requires physical access and usually human intervention to perform these operations. Consequently, EEA devices (e.g., sensor, control unit) were designed with long life expectancy.

A concrete example is the automotive EEA, which is a distributed system that offers a reliable communication infrastructure, resilient against network errors, that can safely manage driving tasks. The EEA of automotive systems was designed to be self-contained and disconnected from the Internet. The contemporary and future vehicle architecture is expected to incorporate complex software features, capable of processing sensors information (e.g. GPS, LiDAR, ultrasound, video) to achieve vehicle autonomy, communication with the infrastructure to optimize route planning, or cloud data reporting for service management. Consequently, this implies the need for interconnectivity with the infrastructure, and the maintenance of vehicle-to-cloud service connections.

Nowadays, the automotive EEA is complemented with a SOA, transforming the traditional vehicle into a Software-Defined Vehicle (SDV). The foundation of SDVs consists of the functional hardware (e.g., digital and analog sensors, control units), which is interconnected by the communication channels offered by the EEA, on top of which a functional and control software is implemented to handle vehicle functions. At the SOA layer, the basis consists of a real-time operating system and a middleware for service communication, on top of which the service layer of SOA. Thus, vehicle functions are implemented as functional or service applications. Lastly, cloud services assist and communicate with the onboard (i.e., in-vehicle) SDV service layer.

The complexity introduced by this additional layer of software features, the fast-paced and feature-oriented development process frequently associated with a SOA, together with safety requirements of automotive systems, raises concerns in terms of security and trust in SDVs. Moreover, at each layer of the SDV architecture different security mechanisms must be considered. The EEA layer received significant attention from the scientific and industry communities, proposing security protocols to ensure communication security, firewalls and intrusion detection to filter communication traffic and to detect malicious behaviour.

In this thesis, we design, analyze and validate a Trusted Software-Defined Vehicle (T-SDV) for SDV. A system of security services is proposed to provide defense mechanisms against

SDV threats and malicious interventions. The proposed services were designed to leverage security hardware as a root-of-trust. With the integration of security hardware in the design process of security services, the T-SDV ensures the protection of security primitives (e.g., cryptographic keys), allows secure distribution of long-term encryption and short-term authentication cryptographic keys with state-of-the-art standards, message authentication tags can be aggregated under a single data structure and can be verified independently, the network is monitored with a rule-based stateful firewall and an intrusion detection system, and security alerts are securely logged.

We formalize and model trust as the ability of the security services to react, resist, and protect the system from threats and malicious interventions. A Markov Decision Process (MDP) based approach is considered to model trust and to understand the consequences and propagation of an attack in the system. The outcome of the proposed trust analysis provides quantitative results through which we were able to determine the most important service parameters that contribute to the probability of a successful attack, and thus adjust the system's parameters such that the probability of a successful attack is minimized.

The proposed services were validated through extensive security analysis, experimentation, and evaluation. From a formal point of view, the design of the proposed security services was verified through a Burrows–Abadi–Needham (BAN) logic analysis and an automated formal analysis under the Dolev-Yao adversary model. A testbed platform was designed and implemented to show the functionalities of the proposed security services. On the testbed, a performance evaluation was conducted to measure the computational and network overhead of the security services. In addition, security experiments were performed on the testbed. The results obtained prove the correctness of the proposed security services, together with their feasibility and applicability in SDVs.