Development and Evaluation of a Prototyping Platform for the Simulation, Transmission, and Real-Time Analysis of Realistic AUTOSAR Security Event Traffic

Thomas Bitterlich, Maximilian Engelsberger, Grit Pientka

Development and Evaluation of a Prototyping Platform for the Simulation, Transmission, and Real-Time Analysis of Realistic AUTOSAR Security Event Traffic

Thomas Bitterlich
T-Systems International GmbH
Munich, Germany
Thomas.Bitterlich@t-systems.com

Dr. rer. nat. Maximilian Engelsberger
Vector Informatik GmbH
Stuttgart, Germany
Maximilian.Engelsberger@vector.com

Dr. rer. nat. Grit Pientka
T-Systems International GmbH
Frankfurt am Main, Germany
Grit.Pientka@t-systems.com

***Abstract*— The contribution proposes a new approach of a prototyping platform simulating realistic AUTOSAR security event traffic, based on real-world attack patterns. Furthermore, their transmission between Fleethead- and SIEM-cloud systems, and their analysis within backend security services and in real-time is investigated. This advances the evaluation of technical realizations of automotive Intrusion Detection Systems, helps to gain new insights with the handling of realistic attack scenarios, and thus enables the gradual realization of the UNECE R155 regulation.**

Keywords*— *Vehicle Cyber Security, Intrusion Detection System, AUTOSAR, UNECE R155, Automotive SIEM, Security Operation Center, Cyber Security Management System, Service-oriented Platforms, Distributed Architectures

I. Motivation and Goals

Due to the rise of cyber security incidents over the past years, the UNECE R155 regulation [1] requires vehicle manufacturers to demonstrate that cyber security risks are identified, evaluated, and mitigated starting from July 2024. Road vehicles need to be continuously monitored during their operational phase to detect attacks on single vehicles as well as the entire fleet, and appropriate countermeasures must be put into place.

One approach is having an in-vehicle intrusion detection system (IDS) based on AUTOSAR IDS [2,3,4] which detects security events and reports them to a security information and event management system (SIEM) in the backend for further analysis. This allows to identify spy-outs, attack attempts, actual attacks, and eventually to derive appropriate mitigation measures.

In this contribution based on the results of a cooperation between Vector Informatik GmbH and T-Systems International GmbH, we describe the design and the prototypical realization of a platform that allows to simulate AUTOSAR security events from a vehicle fleet, which represent realistic attack patterns seen in the field. This security event traffic is transferred between a Fleethead-VPC (where the simulated fleet and the OEM's backend head is deployed) and a SIEM VPC (where the SIEM components are deployed) using an API Gateway. Finally, in the SIEM VPC, different strategies for streaming data analytics are employed to verify that realistic AUTOSAR security events can be used to identify and match known attack patterns.

The goals of this specific approach (which is work in progress) are

- to develop an understanding of real-world attack patterns,
- to simulate realistic attack patterns with the help of AUTOSAR security event mappings representing those patterns intermixed with nominal background noise,
- to demonstrate and understand the implications of data volumes, their noise/peak character, and timings,
- to evaluate and verify solutions for the transmission of this type of security event data, and
- to evaluate and verify real-time analysis and detection strategies for known attack-patterns within AUTOSAR security events.

II. State of the Art

AUTOSAR (Automotive Open System Architecture) is a standardized software framework and open E/E system architecture for mobility applications. Currently, there are three specifications released which focus on IDS-related topics. First, the general AUTOSAR requirements on Intrusion Detection Systems [2] which describes the components of a distributed onboard IDS. Second, the AUTOSAR specification of Intrusion Detection System Manager [3] which describes the functionality, API, and configuration of that basic software module. Third, the AUTOSAR Specification of Intrusion Detection System Protocol [4], which describes the format, message sequences, and semantics between the onboard AUTOSAR IDS com-ponents.

On the other hand, there are several datasets available, including known attack patterns simulated, or carried out on vehicles and captured for scientific usage such as of HCRL [6]. Further approaches for the simulation and analyzation of cyber attacks on vehicle fleets are as follows: Malik and Sun [7] use a threat model to analyze and identify the most significant cyber attacks on connected and autonomous vehicles. The focus of their CARLA-based simulations is to analyze the impact of common attack scenarios on the physical world (e.g. car accidents).

Iqbal and Ball [8] use the Eclipse MOSAIC framework to model two typical road scenarios and the messaging between the vehicles and infrastructure. The model demonstrates the impact of two cyber security attacks (replay and bogus information) and generates datasets for machine learning. The approach focuses on vehicle ad-hoc networks.

Katsikeas et. al. [9] use the Meta Attack Language to develop vehicleLang, a domain-specific language which is used to codify common attack logics for the domain of automotive systems and with respect to their IT infrastructure. They use common attack patterns to generate test cases if they can be modelled with the proposed language. The approach is limited on modeling and does not focus on the simulation aspect.

To the best of our knowledge, there is currently a lack of prototyping platforms which are able to a) generate realistic AUTOSAR security event traffic based on forensic analysis of known attack patterns, b) evaluate and verify technical solutions for data transfer from the simulated vehicle fleet to the SIEM, and c) evaluate and verify analysis and detection strategies for known attack patterns within AUTOSAR security event traffic in real-time.

III. New Approach of a Prototyping Platform for the Simulation, Transmission, and Analysis of Realistic AUTOSAR Security Event Traffic

A. *Real-World Attack Vector and Simulation of Realistic Security Event Traffic*

An important aspect of the described approach is the simulation of realistic AUTOSAR security event traffic. To this end, an actual attack vector, which is seen in the field, is analyzed. The chosen example is a CAN injection attack enabling a keyless car theft with a small injection device. Our insights are based on the forensic analysis documented by CANIS Automotive Labs [3]. This attack vector is chosen because it is a well-documented example of a real-world cyberattack on the internal systems of a single vehicle.

Prior to the actual attack, the car is physically manipulated in such a way, that it becomes possible to electrically attach an injection device to the vehicle's chassis bus. The whole attack can be divided into four major phases, during each of which a set of digital traces are generated. Each of the digital traces occurring in these phases are exemplarily mapped to AUTOSAR security events and used to define a corresponding sequence of security events representing the attack pattern. Based on that, a Python script is written, which allows to generate this pattern including some variations and combine it with background noise of nominal security events as part of the fleet simulation (see Fig. 1).

B. *Transmission of High-Volume Security Event Traffic Between Fleethead- and SIEM VPC*

A basic assumption of the implemented platform is that the backend of an automotive IDS, as part of a Vehicle Security Operation Center (VSOC), can be divided into two functional domains: First, the domain which is related to the technical communication with the fleet, with optional security event transformation or refinement tasks. Second, the domain which is dedicated to classical tasks of a SIEM such as analysis, detection, and reporting. As one possible realization, the two VSOC domains are mapped on two VPCs: The Fleethead- and the SIEM-VPC. This allows a technical and organizational subdivision of the related tasks. To this end, a fully managed, reliable, and highly scalable reception infrastructure (e.g. AWS API Gateway) is set up which enables the transport of high volumes of security events from/to different and mutually decoupled producers/consumers. The reception system is also able to accept different types of messages. This is used to realize the security event transmission as well as the transport of master data, such as event- and ECU-details, from the Fleethead VPC to downstream systems in the SIEM VPC. Currently, the data flow to the vehicle is not investigated. Figure 1 illustrates the overall prototyping platform.

C. *Real-Time Analytical Approaches to Identify Attack Patterns in Security Event Traffic*

To analyze the IDS events in real-time in the SIEM VPC, stream analytics services (e.g. AWS Kinesis) are evaluated. Having established that enough relevant security events can be transferred to the backend, rule based and machine learning (ML) approaches for attack detection are tested with the aim of identifying the most universal signature or best algorithm for a given attack. Such signatures currently appear to be the most straightforward way to transfer insights gained from backend analyses back to the in-vehicle IDS systems for local attack detection. Additionally, assuming that appropriate mechanisms for software updates in the vehicles exist, realizations of vehicle-based attack detection algorithms could be evaluated as well.

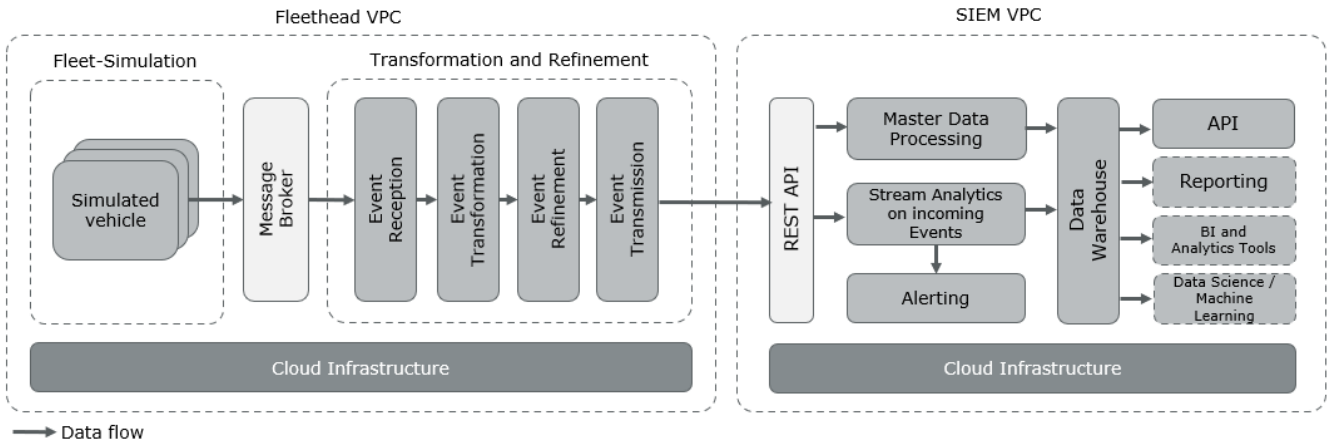

Figure 1: System architecture of the prototyping platform consisting of two domains: First, the Fleethead VPC, and second, the SIEM VPC.

Furthermore, we plan to investigate which additional data sources can aid attack detection in the vehicles as well as in the backend. Additional backend data could turn out to be particularly relevant for analyzing fleet attacks and classifying the types of affected vehicles using e.g. tree-based classification algorithms.

All results of the backend analyses are recorded, and alerts are generated if an attack has been detected. The findings are made accessible in a user-friendly application which also offers further analysis and reporting capabilities as required by UN R155.

IV. Current Results and Further Plans

The contribution describes the development and ongoing evaluation of a prototyping platform for the simulation, transmission, and analysis of AUTOSAR security events. Starting from an architectural design, a working prototype of the evaluation platform has been realized. This includes the implementation and integration of all important parts: (1) Fleet simulation, (2) event transmission and (3) stream analysis.

A first real-world attack simulation has been implemented on top of the platform. This comprises the execution of attack campaigns including approximately 5300 security events per vehicle consisting of actual attack events as well as background noise. Further, first rule based real-time analytical algorithms have been realized and have been proven to reliably detect the attacks within the stream of random noise events. To study the runtimes of the algorithm with the minimal signature, 50 runs of the analytical algorithm were executed. The average runtime on the attack campaign is τ = 1.941 s (median: $\tilde{\tau}$ = 1.934 s, standard deviation: σ = 0.035 s). This translates to an average processing time of 368 µs per event and thus indicates the suitability of the algorithm for real-time analyses.

Upper bounds for the execution time of the different stages in the Fleethead VPC are given in Table 1. Fleet simulations (including simulated OTA transmission) are intentionally delayed simulating realistic system constraints. The number of events does not exactly scale with the number of vehicles due to some pseudo-random degrees of freedom in the noise- and attack-simulation. The throughput on fleet simulation side decreases with an increasing number of vehicles which are simulated on a given number of virtual machines. This is a bottleneck and most-likely caused by the limitations of the VM resources. This behavior can be improved by an optimized deployment strategy to allow higher numbers of fleet sizes simulated time-efficiently.

The SIEM VPC can handle events at rates up to 1000 events/s. This configuration parameter proved sufficient for the investigations performed so far. At this reception rate, analyzing and persisting a run with 100 vehicles takes on average τ = 7.4 s (min: τ = 3.6 s, max: τ = 29.2 s, standard deviation: σ = 3.1 s) indicating that the bottleneck currently is in the Fleethead VPC.

Further plans are a) to accomplish further evaluations of the performance of the evaluation platform itself and b) to evaluate different analytical approaches for real-time attack detection in the SIEM VPC. In this way valuable clues for the design of next-generation in-vehicle and backend-based ID(P)S – including possible strategies for real-time attack prevention – can be derived.

Acknowledgment

This work was funded by the Federal Ministry of Economic Affairs and Climate Action (BMWK), following a decision of the German Bundestag in the context of the SofDCar project (grant agreement 19S21002K).

References

[1] UNECE, UN Regulation No. 155 - Cyber security and cyber security management system, https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security , last accessed 2023/05/09.

[2] AUTOSAR RS Intrusion Detection System - Requirements on Intrusion Detection System, https://www.autosar.org/fileadmin/standards/R20-11/FO/AUTOSAR_RS_IntrusionDetectionSystem.pdf , last accessed 2023/06/01.

[3] AUTOSAR SWS Intrusion Detection System Manager – Specification of Intrusion Detection System Manager, https://www.autosar.org/fileadmin/standards/R20-11/CP/AUTOSAR_SWS_IntrusionDetectionSystemManager.pdf , last accessed 2023/06/01.

[4] AUTOSAR PRS Intrusion Detection System - Specification of Intrusion Detection System Protocol, https://www.autosar.org/fileadmin/standards/R20-11/FO/AUTOSAR_PRS_IntrusionDetectionSystem.pdf , last accessed 2023/06/01.

[5] Tindell, K., CAN Injection: keyless car theft, CANIS Automotive Labs, https://kentindell.github.io/2023/04/03/can-injection/, last accessed 2023/06/01.

[6] HCRL (Hacking and Countermesaure Research Lab): Datasets for intrusion detection for automobile, https://ocslab.hksecurity.net/Datasets, last accessed 2022/06/07.

[7] Malik, S., Sun, W., Analysis and Simulation of Cyber Attacks Against Connected and Autonomous Vehicles, 2020 International Conference on Connected and Autonomous Driving (MetroCAD) , last accessed 2024/03/20.

[8] Iqbal, S., Ball, P., Simulating Malicious Attacks on VANETs for Connected and Autonomous Vehicle Cybersecurity: A Machine Learning Dataset, arxiv.org, last accessed 2024/03/20.

[9] Katsikeas, S. Johnson, P., Hacks, S., Lagerström, R. Probabilistic Modeling and Simulation of Vehicular Cyber Attacks: An Application of the Meta Attack Language, ICISSP 2019, last accessed 2024/03/20.

Run ID	Fleet Size	#Events	Total Data Volume (MB)	Fleet Simulation (including simulated OTA-transmission)			Transformation and Refinement	
				Total Execution Time (s)	AVG Noise Throughput per vehicle (Events/s)	#Vehicles per VM	Execution Time (s)	AVG Noise Throughput (Events/s)
22	1	2742	0.68	280	9.5	1	280	9.5
23	10	30586	7.6	420	8.4	10	420	72
24	100	303340	75.1	920	5.4	10	880	343

Table 1: Measurement results of the execution times and event throughputs of the different stages