A Digital Twin for Enhanced Cybersecurity in Connected Vehicles

A Digital Twin for Enhanced Cybersecurity in Connected Vehicles

Invited paper

Chiara Grasselli, Andrea Melis, Roberto Girau, Franco Callegati
Department of Computer Science and Engineering, University of Bologna, Italy
E-mail: {name.surname}@unibo.it
Corresponding author e-mail: chiara.grasselli@unibo.it

ABSTRACT

In this paper, we propose an architecture and implementation methodology based on the NFV-MANO approach used in the telco industry to achieve automated deployment and configuration of digital twin instances for modern connected vehicles. The digital twin instance serves as a cyber range to safely experiment with potential attacks and countermeasures tailored for in-vehicle scenarios within a controlled virtualized environment.

Keywords: Automotive, Cybersecurity, Cyber Range, Digital Twin, In-vehicle Security.

1 INTRODUCTION

Connected vehicles are a hot topic, although not a new one. According to forecasts in [1], by 2030, the share of new vehicles shipped worldwide with built-in connectivity will be 96%, up from nearly 50% today. As usual, connectivity is both a joy and a pain because it paves the way for many new services that benefit passengers and drivers but can expose vehicles to cyber threats.

The safety standards of vehicles are set in the ISO 26262 document family [2], defining Automotive Safety Integrity Level (ASIL) for the components and the overall system. In connected vehicles, cybersecurity threats represent potential hazards to people and therefore impair the ASIL of the vehicles [3, 4]. The ISO 21434 [5] recommendation published in 2021 tackles the issue.

However, ISO 21434 calls for continuous cybersecurity analysis and risk assessment that are not easy to perform or even impossible if we consider running vehicles. Therefore, we argue that digital twin technologies could be of help in the field.

The work presented in this paper focuses on in-vehicle scenarios proposing the implementation of a Digital Twin (DT) of a typical Electrical and Electronic (E/E) vehicle architecture to safely perform cybersecurity testing, vulnerability assessment, and countermeasures validation in a virtualized environment. Our main research contribution is the definition of an implementation methodology that allows users to build up and configure digital twin instances of automotive vehicles in an automated and flexible manner. For this purpose, we envision an architecture that aligns with the current trends in telecommunication infrastructures exploiting the capabilities offered by virtualization technologies and the NFV-MANO framework for digital twin provisioning and life-cycle management.

2 DIGITAL TWIN FOR ENHANCED CYBERSECURITY

Modern connected vehicles are complex cyber-physical systems with an E/E architecture that enables a seamless interplay between various subsystems, including Electronic Control Units (ECUs), sensors, actuators, and communication networks, to support vital vehicle functions.

One potential solution to enhance their cybersecurity lies in leveraging the concept of DT, a virtual replica that accurately mimics the behavior of the physical counterpart, to conduct security tests in a virtualized environment as we would in a cyber range. This has already been addressed in other domains, such as for industrial cyber-physical systems in [6].

However, implementing virtual replicas of vehicular systems poses significant challenges. First, it is not easy to replicate hardware-bound components such as cameras, sensors, and actuators in the DT virtualized environment. Still, we can inject real-world inputs and traffic traces in the DT to simulate their behavior. Second, effective management and orchestration are essential to ensure an automated and dynamic deployment of the DT components. In fact, the DT should be a flexible infrastructure that:

- can be switched on and off at will;
- can easily integrate new software components;
- is easy to modify in terms of the connectivity architecture.

In other words, the DT should be an infrastructure manageable during its whole lifecycle in a flexible way. To achieve this goal, we propose to apply the approach based on the telecom-oriented NFV paradigm

that enables the design and implementation of complex and composite network services by concatenating one or more virtualized components [7]. In particular, the reference NFV-MANO (Network Functions Virtualization - Management and Orchestration) architectural framework, outlined by ETSI in [8], fosters the automation of the lifecycle management of a complex communication infrastructure, starting from high-level templates called *descriptors* and including all the operations to enforce configurations during the instantiation phase and at run-time (usually called *Day 0/1/2 operations*).

By applying the above principles to the provisioning and configuration of the DT, we can draw a parallel between its lifecycle management and the one defined by 3GPP and ETSI standards for network slices [9]. The lifecycle management covers several steps, including the preparation phase, where the digital twin architecture is modeled using the descriptors, followed by the commissioning phase, where the digital twin is instantiated. Then, the operation phase involves the run-time monitoring and reconfiguration of the digital twin components. Last, the decommissioning phase consists of eliminating the digital twin instance and releasing allocated resources.

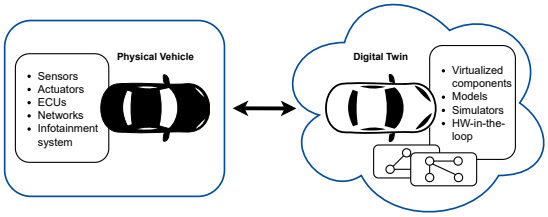

Figure 1: Digital twin of a vehicle

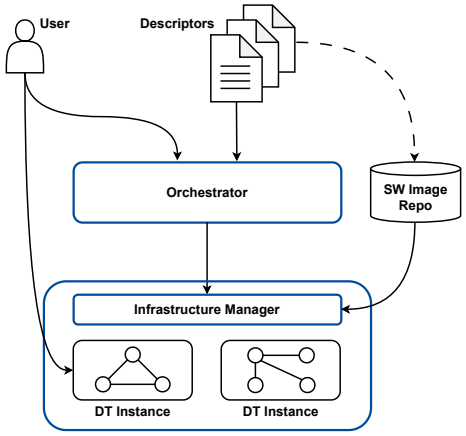

Figure 2: Architecture supporting the Digital Twin (DT) implementation

3 ARCHITECTURE AND IMPLEMENTATION TECHNOLOGIES

Figure 2 shows a representation of the proposed architecture to support the implementation of the digital twin. The architecture aligns with the NFV-MANO framework and ensures the management of the digital twin instances during their entire lifecycle. As traditional cyber ranges, it also provides all capabilities to experiment with configurations and tests in the playground. Users can interact with the orchestration platform and request on-demand the deployment of digital twin instances with an "as-a-Service" (aaS) approach.

The digital twin is modeled starting from two types of descriptors that specify the characteristics of its "building-block" components, providing any information required to instantiate and configure them in the underlying infrastructure (e.g., virtual resources and software images), and how they are interconnected. The virtual components may run on virtual machines (VMs) or containers. This modular approach allows the reuse of descriptors and eases the extension with new components. Moreover, in this way, we can flexibly define different digital twins that include only the specific vehicle subsystems and interconnection networks on which users want to focus testing. The descriptors are passed to the orchestrator, the entity in charge of all orchestration decisions at the service and resource levels. When a user triggers a new digital twin instance, the orchestrator converts the high-level specifications in the descriptors into a precise set of directives that the infrastructure manager executes to deploy all needed virtual resources in the controlled infrastructure. Thanks to the interactions between these entities, the process is fully automated. That also applies to the other lifecycle phases. The user can trigger the modification or deletion of the instance simply by interacting with the orchestrator.

Several open-source and commercial solutions available nowadays for resource virtualization and service orchestration can fit this architecture. In our testbed we adopted Open Source MANO, the software solution promoted by ETSI itself, as an orchestration platform and OpenStack as a cloud infrastructure manager. OpenStack is natively supported by OSM ensuring a seamless integration with the cloud infrastructure and a dynamic control over the compute, storage, and network resources needed for the digital twin instantiation. Along with them, Kubernetes can be integrated for container management.

4 USE CASE

In this section, we present a simple use case to validate our framework delving into the issues of network segmentation and risk assessment, as well as of potential cyber threats to vehicle sensors. The complexity and interconnection of automotive systems can make them susceptible to external malicious attacks. For example, the infotainment system can serve as a potential access point if not adequately protected. Therefore, it is crucial to conduct thorough risk assessments when introducing new applications or peripherals. The objectives of these assessments include evaluating network segmentation, identifying compromised components, and verifying the "ease" of action of an attacker as a result of an attack. In this use case, we showcase a scenario to illustrate these concepts.

We suppose that we must develop a new application for the infotainment system. This application requires the ability to access the Bluetooth interface to establish communication with the user through a mobile app. Furthermore, it should possess the functionality to directly interface with some actuators within the car. Specifically, it should enable the adjustment of suspension tension and offer control over the car lights via the mobile app.

In this case, it is crucial to assess the extent of the attacker's potential access to different components upon a breach of the app and subsequent unauthorized Bluetooth communication with the infotainment system. In particular, we need to assess whether the attacker gets confined access solely to the Bluetooth interface, suspensions, and lights or if he can also establish communication with other sensors within the car.

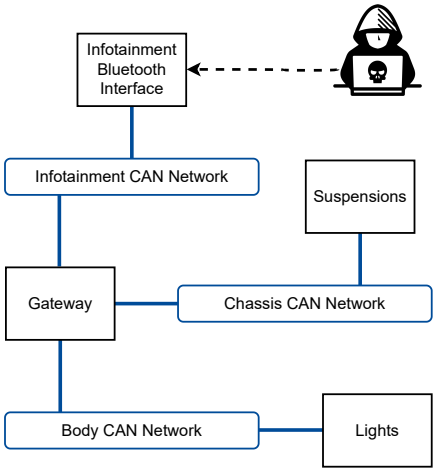

Figure 3: Schematic of the DT architecture

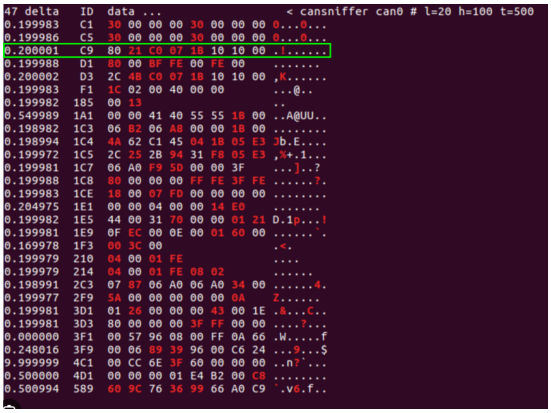

Figure 4: Output of the network scanning

Figure 3 shows the schematic of the DT architecture we implemented to test this scenario. The DT reproduces the CAN network segments of the car related to the infotainment, body, and chassis systems.

Simulating the situation where the infotainment system was compromised through Bluetooth, we performed network scan tests to understand which devices were visible through the vulnerable app access layer. Figure 4 shows an example of a network scanning performed with cansniffer[1] from the VM simulating the infotainment bluetooth interface.

It is worth outlining that the DT can be deployed with building blocks implementing the same software as the real counterparts. Moreover, the interconnection between them can be changed at will, and attacks can be simulated assuming different possible locations of the attacker. Together with the flexibility of deployment guaranteed by the platform adopted, this makes the whole system very adaptable in order to match the real environment.

5 CONCLUSION

In this manuscript, we presented an architecture to manage a flexible and on-demand implementation of digital twins of connected vehicles. The digital twin has the goal to allow testing the nature of possible cybersecurity threats and related countermeasures either before their field deployment or in the presence of any form of change of set up.

[1] https://manpages.debian.org/testing/can-utils/cansniffer.1.en.html

ACKNOWLEDGEMENTS

This study was carried out within the MOST – Sustainable Mobility National Research Center and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.4 – D.D. 1033 17/06/2022, CN00000023). This manuscript reflects only the authors' views and opinions, neither the European Union nor the European Commission can be considered responsible for them.

References

[1] M. Placek, "Share of new vehicles shipped worldwide with built-in connectivity in 2020 and 2030," 2023.

[2] "Iso 26262 road vehicles — functional safety," standard, International Organization for Standardization, Geneva, CH, Dec. 2018.

[3] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (cavs)," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 6240–6259, 2022.

[4] A. A. Elkhail, R. U. D. Refat, R. Habre, A. Hafeez, A. Bacha, and H. Malik, "Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses," *IEEE Access*, vol. 9, pp. 162401–162437, 2021.

[5] "Iso 21434 road vehicles — cybersecurity engineering," standard, International Organization for Standardization, Geneva, CH, Aug. 2021.

[6] C. Grasselli, A. Melis, L. Rinieri, D. Berardi, G. Gori, and A. A. Sadi, "An industrial network digital twin for enhanced security of cyber-physical systems," in *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–7, 2022.

[7] D. Borsatti, G. Davoli, W. Cerroni, and F. Callegati, "Service function chaining leveraging segment routing for 5g network slicing," in *2019 15th International Conference on Network and Service Management (CNSM)*, pp. 1–6, 2019.

[8] "Network Functions Virtualisation (NFV); Management and Orchestration, Report on Management and Orchestration Framework," group rep. nfv-man 001 version 1.2.1, ETSI, Dec. 2021.

[9] "Technical Specification Group Services and System Aspects; Management and orchestration; Concepts, use cases and requirements (Release 17)," ts 28.530 v17.2.0, 3GPP, Dec. 2021.