Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 00 (2020) 000–000

Transportation Research Procedia

www.elsevier.com/locate/procedia

23rd EURO Working Group on Transportation Meeting, EWGT 2020, 16-18 September 2020, Paphos, Cyprus

Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL

Nikolaos Argyropoulos[a]*, Pouria Sayyad Khodashenas[b], Orestis Mavropoulos[a], Eirini Karapistoli[a], Anastasios Lytos[c], Paris Alexandros Karypidis[c], Klaus-Peter Hofmann[d]

[a]CyberLens B.V., Kastanjelaan 400, Eindhoven, 5616 LZ, Netherlands
[b]i2CAT Foundation, C/Gran Capità, 2-4 Nexus I, Barcelona, 08034, Spain
[c]Sidroco Holdings Ltd., Anaximandrou, 5A, Limassol, 3113, Cyprus
[d]T-Systems International GmbH, Holzhauser Str. 4-8, Berlin, 13509, Germany

Abstract

The proliferation of next generation mobility, promotes the use of autonomous cars, connected vehicles and electromobility. It creates novel attack surfaces for high impact cyberattacks affecting the society. Addressing the cybersecurity challenges introduced by modern vehicles requires a proactive and multi-faceted approach combining techniques originating from various domains of ICT. Emerging technologies such as 5G, LiDAR, novel in-vehicle and roadside sensors and smart charging, used in modern cars, introduce new challenges and potential security gaps in the next generation mobility ecosystem. Thus, it is critical that the domain's cybersecurity must be approached in a structured manner from a multi-domain and multi-technology perspective.

The CARAMEL H2020 project aims to address the cybersecurity challenges on the pillars upon which the next generation mobility is constructed (i.e., autonomous mobility, connected mobility, electromobility). To achieve that, advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques will be utilized for the identification of anomalies and the classification of incoming signals indicating a cyber-attack or a cybersecurity risk. Apart from risk detection, methods for the mitigation of the identified risks will also be continuously incorporated to the CARAMEL solution. The final goal of CARAMEL is to create an anti-hacking platform for the European automotive cybersecurity and to demonstrate its value through extensive attack and penetration scenarios. In this paper we will expand on the unique cybersecurity-relevant characteristics of the pillars upon which the CARAMEL solution is built. Next, a number of use cases emerging from such analysis will be extracted in order to form the basis upon which the CARAMEL platform will be evaluated. Finally, we will conclude with an overview of the platform's architectural composition.

Keywords: automated mobility; connected mobility; cybersecurity; artificial intelligence

* Corresponding author. Tel.: +31 (0) 407859561
E-mail address: nikos.argyropoulos@cyberlens.eu

Acknowledgements

This work was supported by the European Union’s H2020 research and innovation programme under the CARAMEL project (Grant agreement No. 833611).