Distr.: General
30 August 2023

English only

Economic Commission for Europe

Inland Transport Committee

Working Party on Transport Trends and Economics

Thirty-sixth session
Geneva, 4–6 September 2023
Item 6 of the provisional agenda
Inland transport security

Workshop on cyber threats to electric vehicles and their charging infrastructure

Note by the secretariat

I. Introduction

1. Further to the request by the Working Party on Transport Trends and Economics (WP.5) at its previous session and as endorsed by the ECE Inland Transport Committee at its eighty-fifth session in February 2023, this workshop on cyber threats to electric vehicles (EVs) and their charging infrastructure taking place on 5 September 2023 (from 15:00-17:00 CET) is organized jointly by the ECE Sustainable Transport and Sustainable Energy sub-programmes. The workshop aims to define and investigate the various cyber threats faced by EVs and EV charging infrastructure as well as in their interaction with the broader electricity grid and to identify possible preventative actions that can be taken by governments and other relevant actors.

II. Background

2. Over 2.3 million electric vehicles (EVs) were sold in the first quarter of 2023, about 25 per cent more than in the same period last year. An overall EV sale of 14 million is expected by the end of 2023, representing a 35 per cent year-on-year increase, with new purchases expected to further accelerate in the second half of this year.[1] This rapid proliferation of EVs and the development of an extensive EV charging infrastructure are expected to significantly contribute to the global shift towards more sustainable transport systems. However, EVs heavily rely on advanced technology systems and connectivity that make them susceptible to cyber threats. Malicious actors might attempt to compromise EVs' critical components, such as the battery management system, vehicle control unit (braking system/ vehicle speed), or charging system, posing significant risks to driver safety, vehicle functionality, and passenger data security. Unlawful access to personal information, geographical location, driving patterns and financial data could result in identify theft, physical harm, or financial loss. At the same time, EV charging infrastructure including

[1] Source : https://www.iea.org/reports/global-ev-outlook-2023/executive-summary

charging stations, networks, and back-end systems that manage charging operations and user data are equally vulnerable to potential cyber threats as hackers could exploit weaknesses in authentication mechanisms and communication channels being able to interfere with charging processes or gain unauthorized access to user data. In addition, EV charging infrastructure integrated with the electrical grid can inadvertently provide avenues for cyber-attacks on the grid`s infrastructure with far reaching consequences including power grid instability, disruptions, and potential blackouts.

III. Purpose of the workshop

3. In view of the rapidly expanding EV fleet and charging infrastructure in the ECE region and beyond it is crucial that governments and other relevant stakeholders develop a better understanding of what these potential cyber threats are, EVs and their charging infrastructure and which mitigation actions can be taken to prevent exposure and abuses.

4. The workshop is expected to gather transport and cyber security experts as well as EV charging infrastructure managers from relevant authorities in charge of road transport development, energy system and grid management, in addition to private sector, academia, research institutions and independent experts engaged in this field from across the UNECE region and beyond.

5. It will provide a platform to:

- Raise awareness about the broad variety and complexity of cyber threats posed to EVs and their charging infrastructure as well as the systemic implications this may have for the broader electricity grid.
- Exchange views, ideas, and national experiences on how to better identify, prevent and manage such threats and vulnerabilities, e.g. through the introduction of enhanced security measures, authentication protocols and regular security audits as well as through improved multi-stakeholder cooperation (including at the level of governments, regulators, automotive manufacturers, charging infrastructure providers and cyber security experts), increased levels of user awareness and education, the development of real time monitoring systems and enhanced incident response capabilities.
- Identify possible next steps and mitigation actions to be taken in this field by member States and other relevant stakeholders, with the support of the ECE sustainable transport and energy sub-programmes.

IV. Draft programme

Moderator: Ms. Els de Wit, Chair, Working Party on Transport Trends and Economics (WP.5), Netherlands

15:00-15:15 – Setting the scene – UNECE role and contributions

Mr. Francois Guichard, Secretary of the Working Party on Automated/Autonomous and Connected Vehicles, UNECE Sustainable Transport Division

Mr. Igor Litvinyuk, Programme Officer, Energy Efficiency, UNECE Sustainable Energy Division

15:15-16:15 – Defining cyber threats to electrical mobility and the grid and identifying possible mitigation actions

Mr. Dmytro Cherkashyn, Head of Research and Development, Institute for Security and Safety GmbH, Mannheim University for Applied Sciences

Mr. Kai Frederik Zastrow, Senior Fellow, Regulation Certification Standards/ Pilot of Cluster 4 Cybersecurity & Software Updates, International Organization of Motor Vehicle Manufacturers (OICA)

Mr. Sylvain Clermont, Vice-Chair, Group of Experts on Cleaner Electricity Systems, Canada

16:15-16:55 – National good practice examples and approaches in addressing cyber threats to EVs and the electricity grid

Mr. Harm van den Brink, Chair, National Task Force on Security and Cybersecurity, Netherlands

Mr. Mahmut Esat Yıldırım, Engineer, Information Technologies and Communication Authority, Ministry of Transport and Infrastructure, Türkiye

Questions and answers/ discussion

16:55-17:00 - Wrap-up and next steps by WP.5 Chair/ and secretariat (ECE sustainable transport and sustainable energy sub-programmes)