Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

Future generation Security for smart and connected Cars - FuSeCar

Deliverable D6.2: Final report of all dissemination activities

WP6: Dissemination

Authors:
Luca Ferretti[1], Giovanni Gambigliani Zoccoli[1], Mirco Marchetti[1],
Mauro Andreolini[1], Gianluca Dini[2], and Giampaolo Bella[3]
{name.surname}@unimore.it

[1]University of Modena and Reggio Emilia
[2]University of Pisa
[3]University of Catania

Current revision: R1.1
Delivery date: February 25th, 2026

Revision history

Authors	Changes	Date	Revision
Giovanni Gambigliani Zoccoli, Mirco Marchetti	Creation of the document, tentative structure, first draft.	March 7th, 2025	R0.1
Giampaolo Bella	Added list of publications and dissemination activities	January 14th, 2026	R0.2
Gianluca Dini	Added list of publications and dissemination activities	January 23rd, 2026	R0.3
Luca Ferretti, Mirco Marchetti, Mauro Andreolini	Revision of document and minor fixes.	February 27th, 2026	R1.0

Contents

1 Introduction

The **FuSeCar** project (Future generation security for smart and connected cars) aims to advance the state of the art in the security of connected and future-generation vehicles.

Dissemination activities play a crucial role in the project by ensuring that the knowledge generated within FuSeCar is effectively communicated to the scientific community, industrial stakeholders, and the broader public. These activities contribute to increasing the visibility of the project, fostering collaboration opportunities, and promoting the adoption of the developed technologies and methodologies.

This document reports the dissemination activities carried out during the entire duration of the project. It provides a comprehensive overview of the communication and outreach actions performed by the FuSeCar consortium, including activities targeting the scientific community, industrial stakeholders, and students.

This deliverable extends and updates the intermediate dissemination report produced at Month 12 of the project. In particular, it includes all dissemination activities previously reported for the first year of the project, together with additional activities carried out during the final phase of the project. As such, it provides a consolidated view of the dissemination strategy adopted by the consortium and of the results achieved throughout the full lifetime of FuSeCar.

During the early stages of the project, the consortium focused on establishing the foundations for effective dissemination. A visual identity for the project was defined through the design and adoption of the FuSeCar logo. In parallel, the official project website was created to serve as the primary online platform for presenting the project objectives, partners, research activities, and outputs. In addition, a dedicated mailing list was set up to facilitate communication with interested stakeholders and to support the dissemination of project updates and announcements.

The project consortium also organized dissemination events aimed at presenting the project's vision, intermediate results, and expected developments to selected stakeholders. In addition, project members actively contributed to dissemination through academic seminars, invited talks, and presentations within university courses, thereby reaching students, researchers, and professionals interested in cybersecurity and connected vehicles.

Scientific dissemination has been further pursued through the publication and presentation of research papers in international peer-reviewed conferences and journals. These publications represent an essential channel for sharing the scientific contributions of the project with the broader research community.

Overall, the dissemination activities carried out during the FuSeCar project have progressively expanded the visibility of the initiative and promoted its research outcomes both nationally and internationally. This document summarizes these efforts and provides an overview of the dissemination results achieved throughout the entire duration of the project.

2 Project Visual Identity

Establishing a clear and recognizable visual identity is an important component of the dissemination strategy of the FuSeCar project. A consistent visual identity helps ensure that all dissemination materials, presentations, and online resources are immediately associated with the project and its objectives.

During the first months of the project, the consortium designed and adopted an official logo to represent the FuSeCar initiative. The logo is used across all project communication channels, including the website, presentation templates, dissemination documents, and workshop materials. The visual identity aims to convey the core themes of the project, namely secure connected vehicles, technological innovation, and cybersecurity.

2.1 Project Logo

The official FuSeCar logo is shown in Figure 1. The design combines a modern typographic representation of the project name with graphical elements that evoke the automotive domain and the concept of digital security. The visual style reflects the technological nature of the project and its focus on future-generation connected vehicles.

The color palette and graphical elements were selected to provide a modern and professional appearance while ensuring good visibility across both digital and printed dissemination materials. The logo is designed to be scalable and suitable for different formats, including presentations, reports, posters, and web pages.

The logo has been integrated into the project's communication infrastructure since the early stages of the project and serves as the primary visual identifier of the FuSeCar initiative.

Figure 1: Official logo of the FuSeCar project.

To ensure consistency in the use of the visual identity, the logo is systematically included in all official dissemination materials produced by the consortium, including project presentations, technical reports, and public communication resources.

3 Online Presence

A dedicated online presence is an essential component of the dissemination strategy of the FuSeCar project. The project website serves as the primary public access point for information about the project, its objectives, partners, and scientific outcomes. It is designed to ensure that researchers, stakeholders, and interested members of the public can easily access up-to-date information about the project and its activities.

3.1 Project Website

The official website of the FuSeCar project is available at the following address:

`https://secloud.ing.unimore.it/projects/fusecar/`

For simplicity and ease of access, the website adopts a modern design based on a single scrollable page. This design choice allows visitors to quickly navigate through the main project information without requiring complex menus or multiple pages. The layout is optimized for readability and accessibility across different devices, including desktop computers, tablets, and mobile devices.

The website prominently displays the FuSeCar project logo and provides a concise description of the project, outlining its main goals and research directions in the area of secure connected vehicles. In addition, the website includes the official logos of the three partner universities participating in the project, thereby clearly presenting the institutions involved in the initiative.

3.2 Website Content

The current version of the website provides the following information:

- **Project overview**: a short description of the FuSeCar project and its objectives.
- **Project partners**: presentation of the three participating universities, including their institutional logos.
- **Public deliverables**: a list of publicly available project deliverables, which can be consulted and downloaded by interested stakeholders.
- **Scientific publications**: a list of publications produced within the project, including submitted and accepted papers.

The website has been continuously updated during the project in order to reflect new dissemination activities, publications, and publicly available results. At the moment of writing the website includes all deliverables as well as all scientific papers that have already been published. Since additional publications are currently under review, the UniMoRe research unit will continue updating this list even after the end of the project. Our commitment is to keep this webpage reachable for at least 5 years after the end of the project.

3.3 Language Availability

In order to maximize accessibility and dissemination impact, the website is available in two languages. The default language is English, which allows the project to reach an international audience of researchers and industry stakeholders. In addition, an Italian version of the website is provided to facilitate communication with national stakeholders and the broader public in Italy.

This bilingual approach supports both the international visibility of the project and its dissemination within the national research and innovation ecosystem.

4 Mailing list

In order to support communication and dissemination activities, an initial mailing list has been established during the first months of the project and actively maintained throughout the project duration. The mailing list serves as a communication channel for sharing updates about project activities, dissemination events, publications, and other relevant information with both internal members of the consortium and selected external stakeholders.

The mailing list includes the contact information of all research personnel involved in the FUSECAR project across the three participating research units:

- University of Modena and Reggio Emilia
- University of Pisa
- University of Catania

In addition to the internal project participants, the mailing list also includes representatives of private companies that have expressed interest in the project and operate in the automotive and cybersecurity sectors. The involvement of these industrial stakeholders is important to foster dialogue between academia and industry and to facilitate the potential transfer of research results toward practical applications.

At the end of the project, the mailing list includes contacts from the following companies (listed in alphabetical order):

- Ad Conculting S.r.l. (cybersecurity)
- Alpitronic S.r.l. (automotive)
- AVL Italia S.r.l.
- Certego S.r.l. (cybersecurity)
- Cyberoo S.p.A. (cybersecurity)
- DriveSec S.r.l. (automotive and cybersecurity)
- Ducati S.p.A. (automotive)
- Ferrari S.p.A. (automotive)
- FEV Group GmbH (automotive)
- Flash Battery S.r.l. (automotive)
- Infosystem Security S.r.l. (cybersecurity)
- Lamborghini S.p.A. (automotive)
- Marelli S.p.A. (automotive)
- Meta System S.p.A. (automotive)
- Reinova S.r.l. (automotive)
- Silk-Faw Automotive Group Italy S.r.l. (automotive)
- TekApp S.r.l. (cybersecurity)

- Stellantis S.p.A. (automotive)

From a strategic perspective, the mailing list is intended to play a key role in the dissemination of the project's results toward industrial stakeholders. While scientific publications, conference presentations, and university seminars represent effective dissemination channels within the academic community, they are often less effective in reaching industrial actors.

For this reason, the mailing list provides a direct and efficient mechanism to communicate relevant project outcomes, announcements of events, and newly available deliverables to companies operating in the automotive and cybersecurity domains. Through this channel, the consortium aims to strengthen the interaction between academic research and industrial innovation, promoting awareness of the project's results and fostering potential collaborations with industry partners.

The mailing list has been used to disseminate information about project progress, announcements of workshops and events, and newly released publications and deliverables.

Privacy and Data Protection For privacy and data protection reasons, the detailed mailing list is not included in this public deliverable. The list contains personal contact information of researchers and representatives of private companies who have agreed to receive communications related to the FuSeCar project.

In order to comply with applicable data protection regulations, including the General Data Protection Regulation (GDPR), the consortium does not publicly disclose email addresses or other personal contact details. The mailing list is therefore maintained internally by the project partners and is used exclusively for project-related communication and dissemination activities.

5 FuSeCar Workshops

5.1 First FuSeCar Workshop

The first FuSeCar workshop was held via videoconference using the Google Meet platform on **Monday, September 9, 2024, from 16:00 to 17:30**. Its main purpose was to disseminate information about the state of the project.

In particular, Work Package 1, entitled *"Privacy analysis of current vehicular communication protocols and architectures"*, was already completed. The deliverable associated with this work package focuses on the analysis of existing vehicular communication systems and includes the results of analytical studies and simulation-based evaluations.

The following work packages were in progress at the time of the first workshop:

- **WP2:** *Privacy enhancement of current vehicular communication protocols and architectures*
- **WP3:** *Post-quantum safety for current vehicular communication protocols and architectures*

Considering the limited number of intermediate results, the consortium decided to organize a first dissemination event in the form of a closed workshop on invitation (this is also in compliance with the dissemination activities planned in the project proposal). The objective of this event was to present the overall vision of the FuSeCar project, illustrate the results obtained so far, and discuss the expected research developments with a selected group of interested stakeholders.

In order to facilitate the participation of industrial stakeholders and reduce logistical constraints, the workshop was organized in an online format.

The event began with a short introductory presentation of the FuSeCar project (approximately 15 minutes) delivered by the Principal Investigator, **Prof. Mirco Marchetti** from the University of Modena and Reggio Emilia. This presentation introduced the project objectives, research motivations, and the main challenges addressed by the project.

The introductory presentation was followed by a series of short talks (approximately 15 minutes each) delivered by the leaders of the three research units involved in the project. These presentations focused primarily on the research problems addressed by each unit and on the expected results of the project activities.

The speakers were:

- **Prof. Mirco Marchetti** – University of Modena and Reggio Emilia
- **Prof. Gianluca Dini** – University of Pisa
- **Prof. Giampaolo Bella** – University of Catania

Besides the speakers and other personnel belonging to the research units of the FuSeCar project, the workshop was participated by representatives of Drivesec S.r.l., Marelli S.p.A., Reinova S.r.l. and Stellantis S.p.A.

The workshop provided an opportunity to present the initial progress of the FuSeCar project and to initiate a dialogue with selected stakeholders interested in the security and privacy aspects of connected vehicular systems.

The discussion that followed the presentations provided useful insights from the invited stakeholders. Overall, the feedback received during the workshop was encouraging with respect to the scientific relevance of the topics addressed by the FuSeCar project, particularly in relation to the long-term security and privacy challenges posed by connected and autonomous vehicles.

At the same time, some participants highlighted that, in the current industrial landscape, vehicle-to-vehicle (V2V) communication infrastructures are not yet among the primary operational concerns of major automotive manufacturers. As a consequence, certain results related to the protection and privacy of vehicular communication protocols may not immediately translate into deployable solutions in current production systems.

Conversely, the discussion revealed a strong interest from industrial stakeholders in the aspects of the project related to post-quantum cryptography. In particular, the adoption of post-quantum cryptographic mechanisms was considered highly relevant for security-critical automotive components such as Hardware Security Modules (HSMs) and firmware update mechanisms, including Firmware Over-The-Air (FOTA) infrastructures. In these contexts, the transition toward post-quantum secure solutions is perceived as both necessary and potentially applicable in the short to medium term.

5.2 Final FuSeCar Workshop

As a concluding dissemination activity of the project, the FuSeCar consortium organized a final workshop aimed at presenting the main results achieved during the project and fostering discussion with both academic and industrial stakeholders.

Differently from the first FuSeCar workshop, which was organized as an invitation-only event, the final workshop was conceived as an **open public event**. The objective was to maximize the visibility of the project results and encourage participation from a broader audience including researchers, students, and professionals working in the automotive and cybersecurity sectors.

The **FuSeCar Closing Event** took place on **February 26, 2026, at 15:00** at the *Department of Engineering "Enzo Ferrari"* of the University of Modena and Reggio Emilia in Modena, Italy. The event program included both industry and research presentations, as well as live demonstrations of automotive cybersecurity attacks and defenses.

The workshop opened with an introductory talk titled *"A (not too) gentle introduction to Automotive Cybersecurity"*, delivered by Prof. Mirco Marchetti (University of Modena and Reggio Emilia), which provided an overview of the main cybersecurity challenges affecting modern connected vehicles and introduced the research topics addressed by the FuSeCar project.

A dedicated **industry session** followed, featuring presentations from distinguished speakers representing leading organizations in the automotive cybersecurity ecosystem. In particular, Sara Imbeni (R&D Cybersecurity Specialist at Ferrari S.p.A.) presented the perspective of a major car manufacturer on current automotive cybersecurity challenges, while Cosimo Senni (Chief Delivery Officer, VP Product Innovation and CISO at DriveSec S.r.l., formerly Globla Product Cybersecurity Manager at Stellantis S.p.A.) discussed industrial approaches and solutions in the field of automotive security.

The **research session** was dedicated to the main scientific contributions of the FuSeCar project and included presentations by the leaders of the three research units involved in the project. The talks addressed key research topics such as securing vehicular communications, improving privacy in vehicular networks, and the adoption of post-quantum cryptographic mechanisms for future vehicular communication infrastructures. The list of talks of the research session is below:

- **Securing vehicular communications**
  Prof. Mirco Marchetti and Prof. Luca Ferretti – University of Modena and Reggio Emilia
- **Improving privacy in vehicular communications**
  Prof. Giampaolo Bella – University of Catania
- **Post-quantum encryption in vehicular communications**
  Prof. Gianluca Dini – University of Pisa

In parallel with the presentations, a **demonstration session** showcased practical cybersecurity experiments conducted within the project. In particular, demonstrations illustrated a GPS spoofing attack targeting a vehicle navigation system and an attack against V2V-aware Advanced Driving Assistance Systems (ADAS), highlighting the practical security implications of vulnerabilities in connected vehicle environments.

The event, which lasted approximately 4 hours, attracted an audience of approximately **60 participants**, including researchers, graduate students, and representatives from industry, confirming the strong interest in the security challenges of connected and software-defined vehicles.

The workshop concluded with an open discussion among speakers and participants. The discussion addressed several emerging topics in automotive cybersecurity, including the role of **post-quantum cryptography** in future vehicular infrastructures, the importance of **privacy-preserving communication protocols**, and the potential impact of **artificial intelligence and large language models (LLMs)** in the future of cybersecurity. In particular, participants highlighted both the opportunities offered by AI-driven security analysis and the new challenges posed by increasingly sophisticated attack techniques enabled by AI technologies.

Overall, the final FuSeCar workshop represented an important opportunity to disseminate the results of the project, strengthen the dialogue between academia and industry, and stimulate discussion on future research directions in automotive cybersecurity.

The leaflet of the final FuSeCar workshop is included in the below image.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

FUSECAR

Future Generation **Se**curity
for Smart and Connected **Ca**rs

26 Febbraio 2026, ore 15:00
Aula **P0.5**, Dipartimento di Ingegneria "Enzo Ferrari",
Via P. Vivarelli 10, 41125 Modena

15:00 – A short introduction to Automotive Cybersecurity
Mirco Marchetti – University of Modena and Reggio Emilia

Industry Session

15:30 – Automotive Cybersecurity: the insights of Ferrari
Sara Imbeni – R&D Cybersecurity Specialist, Ferrari S.p.A.

16:10 – Automotive Cybersecurity: the insights of Drivesec
Cosimo Senni – Chief Delivery Officer, VP Product Innovation and CISO, Drivesec S.r.l.

16:30 – Open Q&A

Research Session

17:00 – Securing vehicular communications
Mirco Marchetti and Luca Ferretti – University of Modena and Reggio Emilia

17:30 – Improving privacy in vehicular communications
Giampaolo Bella – University of Catania

18:00 – Post-quantum encryption in vehicular communications
Gianluca Dini – University of Pisa

Demo Session (15:00 - 19:00, outside of the main room)

GPS spoofing on a car navigation system
Dario Stabili and Dr. Mattia Trabucco
Attacking V2V-aware Advanced Driving Assistance Systems
Dario Stabili and Dr. Edoardo Torrini
V2V communications: simulation vs reality
Dario Stabili and Dr. Giovanni Gambigliani Zoccoli

6 Academic and Public Dissemination Activities

In addition to the dissemination channels described in the previous sections, the FuSeCar project has been presented through a number of academic seminars, invited talks, and public events. These activities contribute to increasing the visibility of the project within the scientific community and among students, researchers, and practitioners working in cybersecurity, distributed systems, and automotive technologies.

Such dissemination initiatives represent an important opportunity to present the motivations and research directions of the project, discuss intermediate results, and gather feedback from the broader research community.

6.1 List of Talks delivered in scientific conferences

The following list includes presentations of scientific papers acknowledging the FuSeCar project at international conferences and workshops. These venues are primarily attended by members of the international research community.

1. UniMoRe research unit. Presentation of the scientific paper "Are VANETs pseudonyms effective? An experimental evaluation of pseudonym tracking in adversarial scenario", which acknowledges FuSeCar, at the 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall), Hong Kong, Hong Kong, Oct. 10-13, 2023

2. UniCt research unit. Presentation of the scientific paper "A meta-ontological approach to securing the semantic web data", which acknowledge FuSeCar, at the Joint Ontology Workshops (JOWO), Twente, Netherlands, July 15-19, 2024

3. UniCt research unit. Presentation of the scientific paper "Modelling the privacy landscape of the Internet of Vehicles", which acknowledges FuSeCar, at the 19th International Conference on Availability, Reliability and Security (ARES '24), Jul 30 - Aug. 2, 2024

4. UniCt research unit. Presentation of the scientific paper "Not sure your car withstands cyberwarfare", which acknowledges FuSeCar, at the2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense), Nov. 2024

5. UniCt research unit. Presentation of the scientific paper "Privacy-enrooted car systems (pecs): Preliminary design", which acknowledges FuSeCar, at the International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (pp. 344-358). Cham: Springer Nature Switzerland. Nov. 2024

6. UniCt research unit. Presentation of the scientific paper "Private and Verifiable Storage of User Vehicles' Privacy Settings through Decentralisation", which acknowledges FuSeCar, at the DLT2025: 7th Distributed Ledger Technology Workshop, June, 12-14 2025

7. UniCt research unit. Presentation of the scientific paper "Capillary Static Policy Setup and Multisensory Dynamic Feedback in Modern Cars", which acknowledges FuSeCar, at the International Conference on Human-Computer Interaction (pp. 180-192). Cham: Springer Nature Switzerland, Jun. 2025.

8. UniCt research unit. Presentation of the scientific paper "Fast and Secure Service Continuity in the Edge-Cloud Continuum: A Study of TLS 1.3 Resumption and Post-Quantum Key Exchange", which acknowledges FuSeCar, at the 2025 IEEE International Conference on Smart Computing (SMARTCOMP), Cork, Ireland, Jun. 16-19 2025

9. UniCt research unit. Presentation of the scientific paper "On Post-Quantum Attribute-Based Encryption for Automotive Over-the-Air Software Updates", which acknowledges FuSeCar, at the 2025 IEEE 31st

International Symposium on On-Line Testing and Robust System Design (IOLTS), Ischia, Italy, Jul. 7-9 2025

10. UniCt research unit. Presentation of the scientific paper “Human-Artificial Intelligent Threat Modelling in the Automotive Domain”, which acknowledges FuSeCar, at the In 2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design (IOLTS), Ischia, Italy, Jul. 7-9 2025

11. UniCt research unit. Presentation of the scientific paper “TLS 1.3 for Fast and Secure Edge Service Continuity in Smart Cities”, which acknowledges FuSeCar, at the 11th Italian Conference on ICT for Smart Cities and Communities, 17-19 Settembre, 2025

12. UniCt research unit. Presentation of the scientific paper "RADAR: a Radio-based Analytics for Dynamic Association and Recognition of pseudonyms in VANETs", which acknowledges FuSeCar, at the 2025 IEEE 102nd Vehicular Technology Conference (VTC2025-Fall), Chengdu, China, Oct. 19-22 2025

13. UniCt research unit. Presentation of the scientific paper "Network-efficient authenticated pseudonym-based V2X communications with constant revocation costs", which acknowledges FuSeCar, at the 2025 23rd International Symposium on Network Computing and Applications (NCA), Lisbon, Portugal, Nov. 5-7 2025

6.2 List of Seminars

The following list includes seminars aimed at disseminating the activities and preliminary results of FuSeCar to graduate students with prior experience in cybersecurity or in automotive.

1. UniMoRe research unit. Presentation of the FuSeCar project within the course "Automotive Cyber Security". This course is attended by students of the Masters Degree in Computer Engineering of the University of Modena and Reggio Emilia, as well as by students of the Masters Degree in Electronic Engineering for intelligent Vehicles of the Motorvehicle University of Emilia Romagna. Dec. 13, 2023

2. UniMoRe research unit. Presentation of the FuSeCar project within the course "Automotive Cyber Security". This course is attended by students of the Masters Degree in Computer Engineering of the University of Modena and Reggio Emilia, as well as by students of the Masters Degree in Electronic Engineering for intelligent Vehicles of the Motorvehicle University of Emilia Romagna. Dec. 18, 2024

3. UniMoRe research unit. Presentation of the FuSeCar project within the course "Automotive Cyber Security". This course is attended by students of the Masters Degree in Computer Engineering of the University of Modena and Reggio Emilia, as well as by students of the Masters Degree in Electronic Engineering for intelligent Vehicles of the Motorvehicle University of Emilia Romagna. Nov. 20, 2025

6.3 List of talks in public events

The following list includes talks in public events organized by industries and organizations, in which members of the FuSeCar consortium delivered a speech on the themes of the FuSeCar and disseminate project information and results.

1. UniMoRe research unit. Presentation on Automotive Cyber Security within the event "Driving Tomorrow. The Sustainable Road Towards Future Mobility & Infrastructures", organized by AVL Italia S.r.l. on Oct. 18th 2024. Speaker: Mirco Marchetti

2. UniMoRe research unit. Presentation on Automotive Cyber Security within the event "Guida autonoma urbana: Modena e il progetto europeo FRODDO ", organized by the municipality of Modena and by the consortium of th eFRODDO EU project on Oct. 18th 2025. Speaker: Mirco Marchetti

3. UniMoRe research unit. Presentation on "Intelligent detection for connected vehicles: cybersecurity in automotive and IoT ecosystems" within the event "23rd Forum ICT Security", organized by ICT Security Magazine S.r.l. on Nov. 20th 2025. Speaker: Mirco Marchetti

7 Scientific publication

Scientific publications represent one of the primary channels for disseminating the research results produced within the FuSeCar project. Through publications in international peer-reviewed venues, the project contributes to advancing the state of the art in the areas of vehicular communications security, privacy-preserving protocols, and post-quantum cryptography for automotive systems.

7.1 Accepted publications

The following publications acknowledge the support of the FuSeCar project and have been published in international conferences and journals that adopt a peer-review process and are indexed in major scientific databases (including Scopus). These publications contribute to the visibility of the project within the international research community and provide a formal record of the scientific results achieved during the project.

1. G. G. Zoccoli, D. Stabili and M. Marchetti, "Are VANETs pseudonyms effective? An experimental evaluation of pseudonym tracking in adversarial scenario," 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall), Hong Kong, Hong Kong, Oct. 10-13, 2023

2. Bella G, Cantone D, Castiglione G, Nicolosi Asmundo M, Santamaria DF. "A behaviouristic semantic approach to blockchain-based e-commerce". In Semantic Web: – Interoperability, Usability, Applicability. Mar. 2024

3. Bella, G., Cantone, D., Castiglione, G., Nicolosi-Asmundo, M., Santamaria, D. F. (2024). "A meta-ontological approach to securing the semantic web data". In Proceedings of the Joint Ontology Workshops (JOWO), July 15-19, 2024

4. Ruben Cacciato, Mario Raciti, Sergio Esposito, and Giampaolo Bella. Modelling the privacy landscape of the Internet of Vehicles. In Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24), Jul. 30 - Aug. 2 2024

5. Pericle Perazzo, Stefano Di Matteo, Gianluca Dini, Sergio Saponara, "On hardware acceleration of quantum-resistant FOTA systems in automotive," Computers and Electrical Engineering, Volume 118, Part A, Aug. 2024

6. Pericle Perazzo, Stefano Di Matteo, Gianluca Dini, Sergio Saponara, "On hardware acceleration of quantum-resistant FOTA systems in automotive," Computers and Electrical Engineering, Volume 118, Part A, Aug. 2024 Bella, G., Castiglione, G., Esposito, S., Raciti, M., Riccobene, S. "Not sure your car withstands cyber-warfare". In 2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense), Nov. 2024

7. Bella, G., Castiglione, G., Esposito, S., Mangano, M. G., Marchetti, M., Maugeri, M., Santamaria, D. F. "Privacy-enrooted car systems (pecs): Preliminary design". In International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (pp. 344-358). Cham: Springer Nature Switzerland. Nov. 2024

8. Castiglione, G., Bella, G., Santamaria, D. F. "SecOnto: Ontological representation of security directives". Elsevier Computers & Security, 148, Jan. 2025

9. Castiglione, G., Esposito, S., Santamaria, D. F., Bella, G. (2025). Private and Verifiable Storage of User Vehicles' Privacy Settings through Decentralisation. In DLT2025: 7th Distributed Ledger Technology Workshop, June, 12-14 2025

10. Bella, G., Esposito, S., Mangano, M. G., Raciti, M. “Capillary Static Policy Setup and Multisensory Dynamic Feedback in Modern Cars”. In International Conference on Human-Computer Interaction (pp. 180-192). Cham: Springer Nature Switzerland, Jun. 2025.

11. L. Catoni, C. Puliafito and G. Dini, "Fast and Secure Service Continuity in the Edge-Cloud Continuum: A Study of TLS 1.3 Resumption and Post-Quantum Key Exchange," 2025 IEEE International Conference on Smart Computing (SMARTCOMP), Cork, Ireland, Jun. 16-19 2025

12. G. Dini, S. Lombardi and T. Antonini, "On Post-Quantum Attribute-Based Encryption for Automotive Over-the-Air Software Updates," 2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design (IOLTS), Ischia, Italy, Jul. 7-9 2025

13. Bella, G., Castiglione, G., Esposito, S., Mangano, M. G., Pampallona, G., Raciti, M., Santamaria, D. F. “Human-Artificial Intelligent Threat Modelling in the Automotive Domain”. In 2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design (IOLTS), Ischia, Italy, Jul. 7-9 2025

14. Lorenzo Catoni, Carlo Puliafito, Gianluca Dini, “TLS 1.3 for Fast and Secure Edge Service Continuity in Smart Cities,” 11th Italian Conference on ICT for Smart Cities and Communities, 17-19 Settembre, 2025

15. G. G. Zoccoli, F. Valgimigli, D. Stabili and M. Marchetti, "RADAR: a Radio-based Analytics for Dynamic Association and Recognition of pseudonyms in VANETs," 2025 IEEE 102nd Vehicular Technology Conference (VTC2025-Fall), Chengdu, China, Oct. 19-22 2025

16. M. Trabucco, G. G. Zoccoli, M. Marchetti and L. Ferretti, "Network-efficient authenticated pseudonym-based V2X communications with constant revocation costs," 2025 23rd International Symposium on Network Computing and Applications (NCA), Lisbon, Portugal, Nov. 5-7 2025

7.2 Publications under review

We also remark that two other publications are currently under review:

1. G. G. Zoccoli, F. Valgimigli, D. Stabili e M. Marchetti, "Detecting stealthy attacks to V2X communications via vehicular or infrastructural perceptual systems: an experimental evaluation"

2. G. G. Zoccoli, F. Valgimigli, D. Stabili e M. Marchetti, "An experimental evaluation of timing differences of CAN logging interfaces"

8 Conclusions

9 Conclusions

This document has presented the dissemination activities carried out throughout the entire duration of the FuSeCar project. During the project, the consortium progressively developed a structured dissemination strategy aimed at maximizing the visibility of the project and promoting its results within both the scientific community and the industrial ecosystem.

In the early stages of the project, particular effort was devoted to establishing the core infrastructure required for effective communication and outreach. This included the creation of the FuSeCar visual identity, the deployment of the official project website, and the establishment of a dedicated mailing list used to maintain contact with researchers, companies, and other stakeholders interested in automotive cybersecurity. These tools provided a stable foundation for all subsequent dissemination activities.

The project consortium also organized two workshops at different stages of the project. The first FuSeCar workshop, organized as an invitation-only event, allowed the consortium to present the initial vision of the project and its preliminary results to selected industrial stakeholders. The final FuSeCar workshop, organized as a public event, provided a broader dissemination opportunity, bringing together researchers, students, and industry representatives. The presence of industrial speakers and the lively discussion that followed the presentations confirmed the strong interest of both academia and industry in the security challenges of connected and software-defined vehicles.

In parallel with these events, the project partners actively disseminated the results of FuSeCar through numerous academic activities. These included presentations at international scientific conferences and workshops, seminars delivered within university courses, and invited talks in public events organized by companies and institutions. Such initiatives contributed to raising awareness of the project among researchers, students, and professionals working in cybersecurity, distributed systems, and automotive technologies.

Scientific publications represented another key dissemination channel. During the project, the consortium produced a significant number of peer-reviewed publications in international conferences and journals, addressing topics such as secure vehicular communications, privacy-preserving vehicular systems, post-quantum cryptography, and cybersecurity for connected vehicles. These publications constitute a lasting scientific output of the project and contribute to advancing the state of the art in automotive cybersecurity.

Overall, the dissemination activities carried out within the FuSeCar project have successfully promoted its objectives, research directions, and results to a wide and diverse audience. By combining academic dissemination, industrial engagement, and public outreach, the consortium has contributed to strengthening the dialogue between research institutions and the automotive cybersecurity ecosystem.

Even after the formal conclusion of the project, the consortium will continue to support the long-term visibility of FuSeCar results. In particular, the project website will remain accessible and updated with new publications for at least five years after the end of the project, ensuring continued access to the knowledge and outputs produced within the initiative.