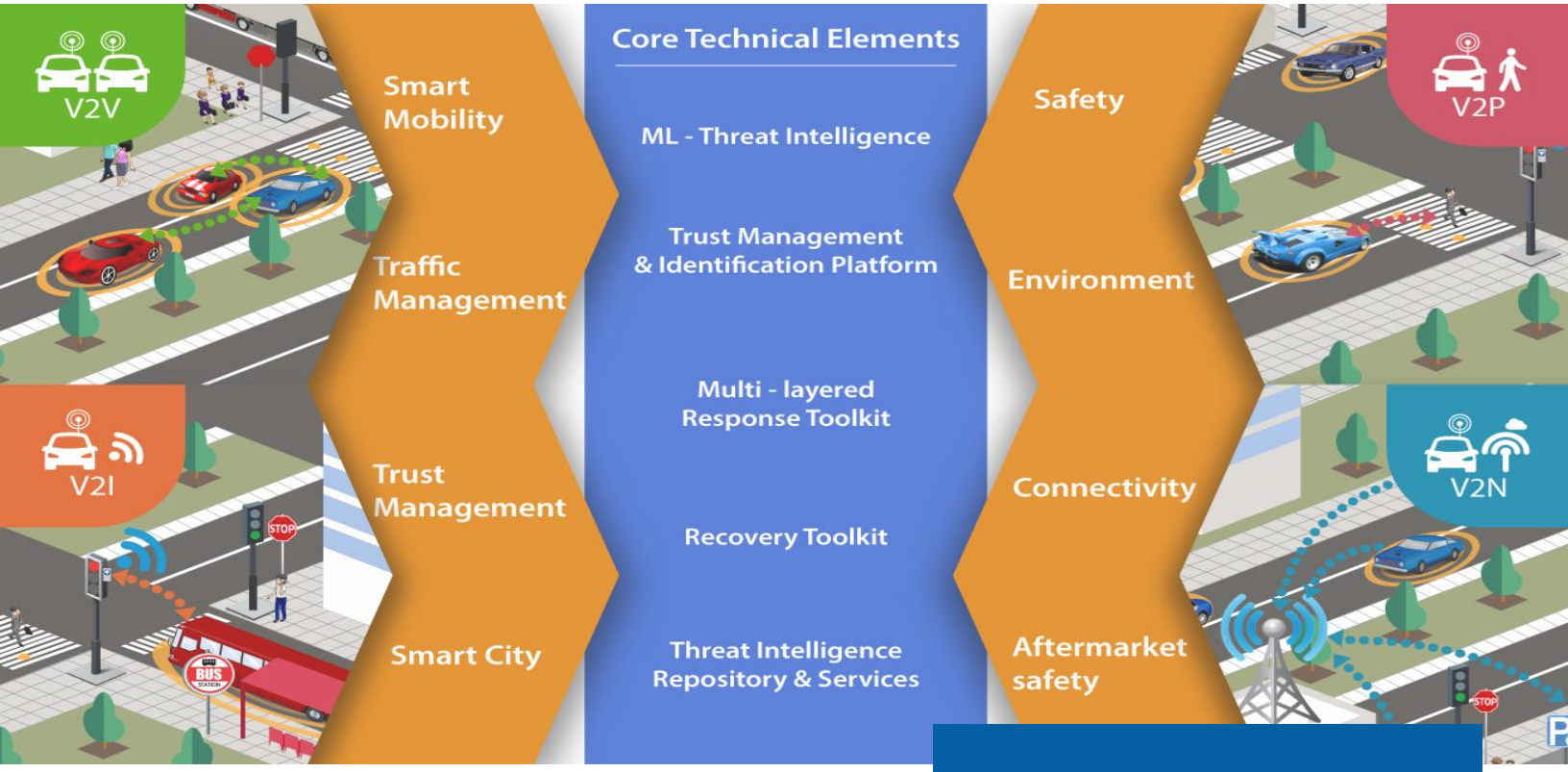
nIoVe newsletter

Volume 2 – June 2021



nIoVe Project

nIoVe project is a 36 months European project co-founded by the European Union's Horizon 2020. The project brings together European excellence to build innovative cyber-security of Connected and Autonomous Vehicles (CAVs) within the Internet-of-Vehicles (IoV) ecosystem to support automotive manufacturers and transport providers.

The Consortium of the project is highly interdisciplinary and trans-national. It was formed of twelve experienced and committed partners, including five industrial partners, five R&D and academia partners, and one public transportation authority. The Consortium embodies six European states (Greece, Italy, Switzerland, Germany, Sweden, and Spain) and Israel, representing the end-user and market needs in Europe and globally.

TABLE OF CONTENTS

Innovations

Self-sovereign Identity Management and Anonymous Credentials

During nIoVe research activities, the project Hyperledger Indy has been identified as a promising solution to the requirement of scalable certificate management independent of problems introduced by location dynamicity. Hyperledger Indy implements a concept called "Selfsovereign Identity Management" (SSIM). With SSIM, credential holders (vehicles) manage and maintain their credentials individually without relying on central servers or third-party services for federated identity management. At the same time, credential holders have the ability to selectively disclose certain attributes of their credentials. Disclosing values associated with credential attributes can be even proven using Zero-Knowledge Proofs (ZKPs), where nothing except the validity of a statement is revealed to a verifier. This gives maximum privacy to the credential holder when participating in a verification scheme. Aside from privacy benefits, credential holders generate proofs locally at any location. The implementation of Hyperledger Indy uses two main schemes to cover the full cycle (issuing, authentication, revocation) around anonymous credential management: (1) the group signature scheme introduced by Camenisch and Lysyanskaya and (2) revocation management based on cryptographic accumulators.

Certification in the IoV powered by Permissioned Distributed Ledger Technology

To communicate the topic of credential management for trusted and secure communication, we consider the use case of a vehicle which authorizes itself at a gas/charging station before the establishment of the communication channel. To achieve trusted communication, a government authority starts by registering a Credential Schema (CS) at the ledger. The CS defines attributes of the certificate that will be issued to a holder. In the context of the IoV, possible attributes that certify vehicles could be license numbers, ownership details, insurance numbers, and proofs of value-added tax, conformity, roadworthiness, etc.. The ledger which processes the CS transaction is permissioned. This means that authorized nodes participate in the blockchain network and maintain a copy of the ledger. This assumption does not require the computing-intensive Proof of Work (PoW) consensus protocol. Instead, the plenum consensus protocol in Hyperledger Indy is a deviation of the Practical Byzantine Fault Tolerant (PBFT) consensus protocol which relies on a more efficient three-phase commit protocol to verify transactions. Changing the blockchain type to public would require a redesign of stakeholder contracting and is out of scope of this article.

With the CS registered at the ledger, a vehicle registration authority can register a Credential Definition (CD) at the ledger. The CD contains public cryptographic metadata and references the CS of the government. Crypto data of the CD supports group signature creation, verification as well as the credential revocation protocol. To allow other registration authorities to issue credentials that are linked to the government CS, CD information is decoupled from CS data and can be registered individually.

With the CS and CD stored at the ledger, the vehicle registration authority can issue a credential to a vehicle. To do so, the vehicle commits values to the attributes defined in the CS of the government. Using the CL group signature scheme, the registration authority signs the credential request and issues the credential to the vehicle. With that, the vehicle as the credential holder can prove attributes of the credential to a verifier. This is possible because the vehicle can sign data as a member of the group signature scheme. Disclosing the initial value commitments that are associated with credential attributes is left to the vehicle.

Equipped with the credential, a vehicle can approach any road side unit or IoV device. To, e.g., set up a trusted and secure communication channel to a gas/charging station, the charging station first requests a credential proof of the vehicle as it only accepts registered vehicles. By generating a proof based on a credential, the vehicle can answer the request of the charging station with a proof presentation. Afterwards, the charging station can verify all signatures and cryptographic proofs of the proof presentation with the help of publicly accessible ledger data found in the CS and CD. Upon successful verification, a secure communication channel between the vehicle and the charging station is established.

Innovations

Honeypots as an additional layer of security against cyber threats in autonomous vehicles' infrastructure

In everyday life, either as an individual or as a company, there are almost equal chances to be targeted by a cyberattack, which attempts to gain illegal access to a computer system causing damage or harm. The defensive responses against cyberattacks are cybersecurity and security principles that everyone should follow to be protected to the extent possible.
Honeypots can act as an additional layer of defense against malicious actions in any given infrastructure, including autonomous vehicles. Honeypots mimic the behavior of a selected component from an autonomous vehicle to attract the attackers to exploit it.

Honeypots and honeyfarm inside the autonomous vehicle
A proper approach to deploying honeypots inside an autonomous vehicle is, first, to accurately identify the current architecture. Then, decide which components are more valuable based on the operational value they provide. The next step is to create a honeypot for each component by simulating a real operation without exposing any security information that can be used to compromise the vehicle. Honeypots need to be configured to the network topology of the overall architecture but do not require the same hardware resources as the physical implementation. Virtual honeypots can be hosted and deployed on one or more physical machines if their hardware requirements are insufficient.

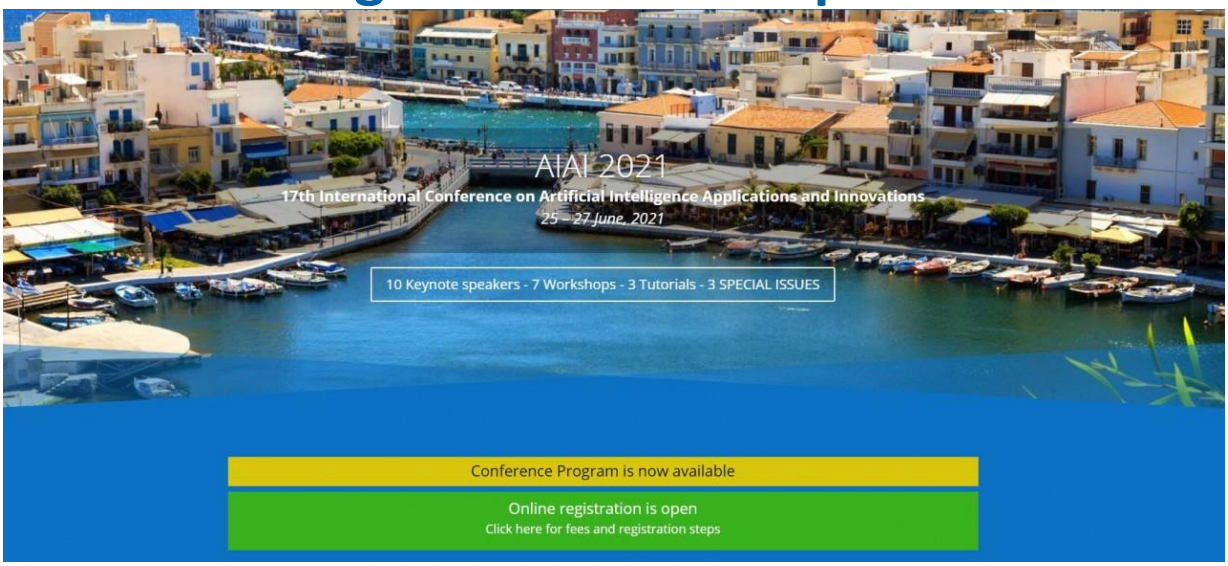
A honeyfarm is a combination of honeypots. To employ the honeyfarm, additional vulnerabilities should be added within each honeypot. This will provoke the attackers to expose their tools and mechanisms towards exploitation of these vulnerabilities.

Solutions up to date
Any traffic in the network initiated by honeypots means that the system most likely has been compromised, and the attackers make changes or even outbound connections. For that reason, the honeyfarm's network should be thoroughly monitored and analyzed by SIEM software that combines security information management (SIM) and security event management (SEM), providing real-time analysis of security alerts. When properly configured and adapted to the system's needs, SIEM can give an additional layer of security. Considering that human rights and might be even lives are at stake, more security measures should be applied to increase the system's resistance to the attack.

Extensive utilization of the stated in-vehicle monitoring approaches is expected to be part of future cyber-defense mechanisms of AV ecosystems as security measures towards out-of-the-vehicle networks to create a holistic cyber-defense solution.

*"**Dissemination activities** aim to raise public awareness of the project's achievements among the key end-user groups and stakeholders, the scientific community, and the general public and to facilitate sharing of knowledge inside the Consortium, as well as establishing project's communication and dissemination methodology."*

Organized Workshops



nIoVe has organized on the 25th of June 2021, the "Designing a Novel Adaptive Cybersecurity Solution for Internet-of-Vehicle (nIoVe)" workshop in the context of the "17th International Conference on Artificial Intelligence Applications and Innovations". The workshop aimed to demonstrate and discuss the requirements to be considered in a complex cybersecurity system, respecting the need of original equipment manufacturers, designers of post-market CAVs components, cybersecurity experts and response teams, public transportation authorities, smart city administrators, as well as passengers and pedestrians.

TUM co-organized the "Autonomous Systems Design (ASD): A Two-Day Special Initiative", in context of DATE21 virtual Conference and Exhibition on the 4th - 5th February of 2021. This Special Initiative started with an opening session where industry leaders from Airbus, Porsche and Robert Bosch shared their visions of autonomous systems, the challenges they see in the development of autonomous systems as well as how autonomous systems will impact the business in their industries.

Project Presence in Events

Conferences

- HOPU - IoT for cities, Conference: Smart City Expo World Congress, Barcelona-Spain, 17/11/2020-20/11/2020.
- HOPU - Global Startup Cities, Conference: New business opportunities, European Union (Online), 25/11/2020.
- HOPU - Smart Region: The future of smart territories, Conference: Smart Cities, Murcia-Spain, 01/12/2020.
- HOPU – Intelligence Cities challenge Cartagena, Conference: Objectives and challenges of Cartagena, Cartagena-Spain, 18/12/2020.
- TUM - Oral presentation at the DATE21 conference, February 2021.
- HOPU - Transfiere 2021, Conference: I+D+i for Smart Cities, Malaga-Spain, 16/02/2021-17/02/2021.
- ICTLC, Round table, [Protecting Consumers in Digital Society: a matter of regulation or enforcement - Facebook decision of the Bundeskartellamt and the Google decision of the CNIL - Consumer rights for your personal data (data user vs data subjects) – How / Is it acceptable to pay with your data? Transposing Directives 2019/770 & 2019/2161], 7th Conference on Technology & communication law "Who governs the internet?", organized by Nomiki Bibliothiki, Greece/Remotely, 04/03/2021.

Workshops

The nIoVe consortium participated in the virtual workshop organized by the CARAMEL project on the 27th of May 2021. The CARAMEL project introduced its activities to representatives of OEMs to increase the reach and gather opinions about the topics addressed by CARAMEL. The objective of the workshop was to highlight the achieved results toward the development of Artificial Intelligence-based cybersecurity for connected and automated vehicles.

Lectures

- TUM- Lecture: "Software Architecture for Distributed Embedded Systems, 2021.
- ICTLC, Lecture, [Privacy principles, actors and data subject rights in practice -Data protection by design and default - Data protection impact assessments - Data transfers: options and solutions to ensure compliance- Data protection impact assessment and data protection by design in practice], Data Protection Officer Certification course, Belgium (Brussels) / Remotely, organized by European Centre on Privacy and Cybersecurity - Maastricht University, 01/03/2021-05/03/2021.
- ICTLC, Lecture, ["Data Protection Contract Management", "Data Protection Impact Assessment" and "Cloud Computing"], Privacy Executive Week, organized by the European Centre on Privacy and Cybersecurity - Maastricht University, The Netherlands / Remotely, 08/03/2021-12/03/2021.
- ICTLC, Lecture, AFGE (Associazione per l'Alta Formazione Giuridico-Economica), Masterclass Privacy 2020, Italy / Remotely, 30/03/2021.
- ICTLC, Debate-Discussion Legal Innovation Days, organized by the 4cLegal, Italy /Remotely, 30/03/2021- 31/03/2021.
- ICTLC, Lecture, [Key data protection concepts, principles, and obligations, Grounds for processing, including legitimate interest and consent, Sensitive Data, Data protection by design and default, Data protection impact assessments and privacy risk assessments], European Commission's "Data Protection Academy" project - for the Brazilian Data Protection Authority (ANPD), organized by the European Centre on Privacy and Cybersecurity - Maastricht University, Brazil / Remotely, 12/04/2021-23/04/2021.
- ICTLC, Lecture, Master of Privacy Officer, and General Counsel of Privacy (TÜV certified), organized by the Federprivacy, Italy/Remotely, 17/05/2021- 21/05/2021.
- ICTLC, Lecture, Shaping Europe's digital future: Latest State of the Draft ePrivacy Regulation - The interplay between GDPR and e-Privacy: What about cookies and consent, Emerging Issues and Challenges Course, organized by the European Centre on Privacy and Cybersecurity - Maastricht University, The Netherlands/Remotely, 09/06/2021-11/06/2021.
- ICTLC, Lecture, Legal cybersecurity landscape: how to create an effective and integrated privacy and cybersecurity compliance framework, organized by The Legal 500 and ICT Legal Consulting, Remotely, 15/06/2021.

Trust and the ethics of CAVs

Trust is a fundamental precondition for a fair and sustainable Internet of Vehicles landscape and is widely regarded as a prerequisite for technological uptake.[1] It, therefore, comes as no surprise that new and emerging technologies like CAVs bring with them not only technical difficulties, but also ethical, legal, and more generally, societal questions. Can I trust an autonomous vehicle? Who will my data be shared with? Can hackers cause collisions? Whose life will the CAV save in a situation where at least one fatality is inevitable? Will taxi drivers lose their jobs? How do I know that my children are safe going to school in an autonomous shuttle?

In recent years, a great deal of attention has been paid to ethical aspects of data processing activities and more specifically, of technologies and Artificial Intelligence (AI). Such attention is not only warranted but necessary as our lives are ever-more connected. With specific reference to CAV ethics, the work of the European Commission's Horizon 2020 Commission Expert Group (EG) to advise on specific ethical issues raised by driverless mobility [2] is particularly useful. In 2020, the EG published a report that "aims to promote a safe and responsible transition to connected and automated vehicles…by supporting stakeholders in the systematic inclusion of ethical considerations in the development and regulation of CAVs." [3] The report provides 20 ethical recommendations for CAVs, which range from privacy, data protection, and data security, to safety concerns to questions of fairness and transparency, to responsibility and liability,[4] all of which can be linked to trustworthiness, and provides an important contribution to the understanding of ethics in the emerging IoV field. Along these lines, the authors of the report underline the role that ethics and the inclusion of social issues in the development of CAVs plays in fostering trust.[5]

To bridge this gap, the nIoVe project has actively considered relevant stakeholder requirements, including those of passengers and pedestrians, automotive manufacturers, smart city administrators, and public transportation authorities, in a concrete attempt to build user needs and concerns into the nIoVe technology itself and promote a trustworthy cybersecurity framework for the Internet of Vehicles.

While current European legislation such as the GDPR and the ePrivacy Directive provide safeguards for citizens and drivers when it comes to data processing and data security minimum standards in the CAV context, it is vital that also ethics and notions of fairness are built into these vehicles by design in order to promote trust. An adequate and complete understanding of the ethical complexities of the CAV ecosystem and a true "by design" approach that encompasses notions of fairness, transparency, and human rights in addition to data protection, privacy, and data security, will permit CAV developers to ensure that their vehicles are not only safe and secure, but fair, transparent, and fully benefit society.

References

[1] See, e.g., Bahmanziari, T., Pearson, J. & Crosby, L. (2003). Is trust important in technology adoption? A policy capturing approach. Journal of Computer Information Systems. 43. 46-54; Mcknight, D., Carter, Michelle & Thatcher, Jason & Clay, Paul. (2011). Trust in a specific technology: An Investigation of its Components and Measures. ACM Transactions on Management Information Systems. 2. 12-32, 10.1145/1985347.1985353.
[2] Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659). Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability, and responsibility. 2020. Publication Office of the European Union: Luxembourg.
[3] Ibid p. 4.
[4] Ibid p. 5.
[5] Ibid p. 16.

Project Partners

CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

ATHENA Research & Innovation Information Technologies

hop ubiquitous

UNIVERSITÉ DE GENÈVE

ARGUS CYBER SECURITY

ICT LEGAL CONSULTING

RI.SE Research Institutes of Sweden

KENOTOM EMBEDDED ENGINEERING EXCELLENCE

TECHNISCHE UNIVERSITÄT MÜNCHEN

tpg

seems

navya self-driving made real

Contact

Dr. Dimitrios Tzovaras

Building A - Office 1.1A
Information Technologies Institute Centre
of Research & Technology- Hellas
6th km Harilaou - Thermi, 57001, Thessaloniki, Greece
Email: info-niove@iti.gr

https://www.niove.eu

https://twitter.com/NioveProject

https://www.facebook.com/NioveProject

https://www.youtube.com/channel/UCuwSJbWhPwquBMxlr__XQGA

https://www.linkedin.com/in/nioveproject/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833742.