Vision

nIoVe project is making a step-change in Europe to bring down the number of fatalities, reduce harmful emissions from transport work, and reduce congestion within urban environments. nIoVe aims to detect cyber-attacks in real-time while simultaneously preventing them. Regarding the automotive market, nIoVe purpose is to uptake innovative cybersecurity solutions to protect all Connected and Autonomous Vehicles (CAVs) and infrastructure of the Internet of Vehicles (IoV) network against complex cyber-attacks.

The overall objectives of nIoVe are to:

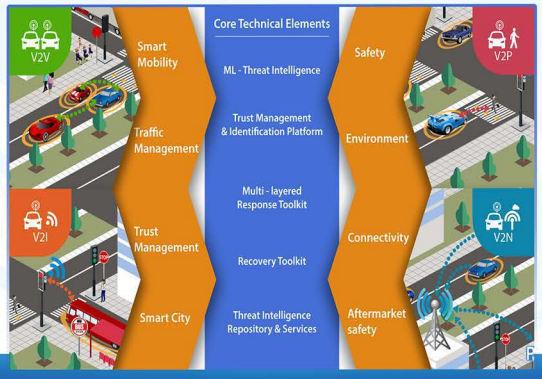
- Deliver a multi-layered cybersecurity solution for the IoV ecosystem in order to provide protection against wider area of attacks.
- Reach and develop a Machine Learning (ML)-Driven Threat Analysis and Situational Awareness Platform for IoV.
- Introduce advanced Visualization and Big Data technique required for the detection of complex cyber-attacks.
- Introduce a coordinated cyber Incident Smart Response System for CAVs at the national & European level.
- Maximize trust between CAVs and infrastructure components through trust management and identification platform.
- Establish and operate a continuously updated and shared Threat Intelligence Repository for CAVs cyber threats to support Original Equipment Manufacturers (OEMs) and tier suppliers.
- Support of secure-by-design production lifecycle for all vehicle communications.
- Provide cybersecurity solutions to cover execution environments, including all mechanisms.
- Validate the nIoVe architecture capabilities in proof-of-concept Use Cases.

Impact

The project will work towards more robust, resilient, and effective cybersecurity solutions that can be effortlessly tailored to each organization's evolving needs and speedily adapt to the changing cyber threat landscape.

The strategic impact of nIoVe involves:

1. Enhanced protection against novel advanced threats.
2. Advanced technologies and services to manage complex cyber-attacks and to reduce the impact of breaches.
3. The technological and operational enablers of co-operation in response and recovery, contributing to the development of the Computer Security Incident Response Team (CSIRT) Network across the EU, which is one of the critical targets of the NIS Directive.
4. Robust, transversal, and scalable Information and Communication (ICT) infrastructures resilient to cyber-attacks that can underpin relevant domain-specific ICT systems, providing them with sustainable cybersecurity, digital privacy, and accountability.



Innovation

nIoVe aims at advancing the state-of-the-art and current state-of-practice in cybersecurity, including the following.

Early Prediction and Detection:

- The attack prediction and detection tool will allow cyber-defence companies to automate the process of correlating specific security, system, and network events that may have been logged at different places in the network over a short or long time.
- Risk assessment Engine will detect intrusions of attacks from the internet at an early stage and detect intrusions to the in-vehicle network as a second step.
- Anomaly detection based on ML will provide abnormal system behaviour first, and all other behavioural patterns will be considered normal. This process will be dynamic, and new abnormal system behaviour entries will increase the system's ability.

Response and Recovery Mechanisms:

- The response mechanism is multi-layered, offering a robust response to the complex attacks in the IoV ecosystem at its various layers.
- The response plans may differ depending on whether the attack was directed to single vehicles or single components (nodes) of the IoV network infrastructure.
- Both active and passive responses will be used according to the critical asset profile and role on the IoV network.
- nIoVe Recovery Toolkit has three kinds of recovery actions that will be possible to take place: data recovery, device recovery, and system recovery.
- Automatic process of data, device, and system recovery after a real-world attack, or as a simulated IoV simulated incident.

Partners

- CERTH – Center For Research & Technology Hellas – https://www.certh.gr/
- ATHENA – Research & Innovation Information Technologies, Athens, Greece – https://www.athena-innovation.gr/en
- RISE – Research Institutes of Sweden – Research Institute of Sweden – https://www.ri.se/sv
- ARGUS – Cyber Security Israel – https://argus-sec.com/
- UNIVERSITÉ DE GENÈVE – University of Geneva, Switzerland – https://www.unige.ch/
- KENOTOM – Embedded Engineering Excellence, Thessaloniki, Greece – https://www.kenotom.com/
- navya – self-driving made real – NAVYA, France – https://navya.tech/en/
- seems – Smart Engineering & Management Solutions IKE, Greece – https://www.seems.gr/
- tpg – TPG, Switzerland – https://www.tpg.ch/fr
- ICT LEGAL CONSULTING – ICT Legal Consulting – https://www.ictlegalconsulting.com/
- TUM – Technische Universität München, Germany – https://www.ei.tum.de/esi/startseite/
- hop – HOPU Smart Cities, Spain – https://hopu.eu/

Contact Us

Coordinator

Dr. Dimitrios Tzovaras
Information Technologies Institute
Centre of Research & Technology – Hellas

Email: info-niove@iti.gr

Follow Us

https://www.niove.eu/index.php

https://www.facebook.com/NioveProject/

https://twitter.com/NioveProject

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

nIoVe

A Novel Adaptive Cybersecurity Framework for the Internet-Of-Vehicles