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

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

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

nIoVe aims to deploy a novel multi-layered interoperable cybersecurity solution for the IoV, emphasizing the CAVs by employing an advanced cybersecurity system enabling all relevant stakeholders and incident response teams to share cyber-threat intelligence, synchronize and coordinate their cybersecurity strategies, response, and recovery activities. For that purpose, the project develops a set of in-vehicle and Vehicle-to-Everything (V2X) data collectors that will support nIoVe's machine learning platform and tools for threat analysis and situational awareness across the IoV ecosystem. Advanced visual and data analytics are further enhanced and adapted to boost cyber-threat detection performance under complex attack scenarios. Simultaneously, IoV stakeholders are jointly engaged in incident response activities through trusted mechanisms. The approach is supported by interoperable data exchange between existing and newly proposed cybersecurity tools.

The overall objectives of nIoVe's are to

- Deliver a multi-layered cybersecurity solution against the wider area of attacks in the Internet-of-Vehicles (IoV).
- Develop a Machine Learning (ML)-Driven Threat Analysis and Situational Awareness Platform for IoV.
- Introduce advanced Visualization and Big Data technique for the detection of complex cyber-attacks.
- Introduce a coordinated cyber Incident Smart Response System for CAVs at the national & European levels.

- 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 OEMs and tier suppliers.
- Support of secure-by-design production lifecycle for all vehicle communications.
- Provide cybersecurity solutions to cover execution environments.
- Validate the nIoVe architecture capabilities in proof-of-concept Use Cases.

nIoVe solution will be demonstrated and validated in 3 pilots:

1. Cybersecurity in a hybrid environment: The first pilot will be implemented in a hybrid environment. The deployment and tests of nIoVe are executed in a real-world-like environment set up specifically for the nIoVe solution.
2. Security in Connected Vehicles Communication: The second pilot will be organized using a simulated environment. This environment will provide the flexibility needed to implement and test a variety of scenarios.
3. Performance of real execution environment: The third pilot will be conducted in a real-world environment with a setup of the nIoVe solution inside the shuttle.

The Consortium of the project is highly interdisciplinary and trans-national. It was formed of twelve experienced and committed partners, namely five industrial partners (NAVYA, ARGUS, ICTLC, SEEMS, HOPU, KENOTOM), five R&D and academia partners (CERTH, UniGe, RISE, TUM, ATHENA), and one public transportation authority (TPG). 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.

Overall, nIoVe ambitiously expects to

- Reduce the attack surface of the overall IoV ecosystem.
- Showcase effective and real-time detection of novel advanced threats and cyber-attacks in IoV ecosystems.
- Substantially reduce the response time and the impact of breaches.
- Contribute to Computer Security Incident Response Teams (CSIRTs) establishment and sustainable operation, stimulating information and knowledge sharing across the IoV ecosystem.
- Support the next generation robust, scalable and resilient IoV infrastructure.

Acknowledgment
nIoVe project is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833742.