nIoVe

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

Project Overview

Presenters:

Dr. Dimitrios Tzovaras, CERTH/ITI

Dr. Votis Konstantinos, CERTH/ITI

Outline

- Project Identity Card
- The Consortium
- Rationale & Motivation
- Project Vision & Objectives
- Project Pilots
- Work plan and GANTT

Project Identity Card

Title: ***A novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles***

H2020 Call: H2020-**SU-ICT-01-2018 (Dynamic Countering of cyber-attacks)**

Funding Instrument: **IA** (Innovation Action)

Duration: **36 months**

Starting Date: **1 May 2019**

EU Contribution and Total Costs: **4.997.125,00 €**

Partners: **13 partners**

Country Coverage: **7 countries**

- **Greece, Italy, Switzerland, Germany, Sweden, Spain and Israel**

The Consortium

No.	Participant organisation name	Country	Type of Organisation
1 (Coord.)	Centre for Research and Technology Hellas **[CERTH]**	GR	Research
2	University of Geneva **[UniGe]**	CH	University
3	NAVYA SAS **[NAVYA]**	FR	SME
4	Research Institutes of Sweden **[RISE]**	SE	Research
5	ARGUS Cyber Security **[ARGUS]**	ISA	Industry
6	ESCRYPT GmbH – Embedded Security **[ESCRYPT]**	DE	Industry
7	ICT Legal Consulting **[ICTLC]**	IT	SME
8	ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS **[ISI]**	GR	Research
9	SMART ENGINEERING & MANAGEMENT SOLUTIONS IKE **[SEEMS]**	GR	SME
10	Technical University of Munich **[TUM]**	DE	University
11	Transports Publics Genevois **[TPG]**	CH	Public
12	KENOTOM Private Company **[KENOTOM]**	GR	SME
13	HOP Ubiquitous **[HOPU]**	ES	SME

Challenges by the SU-ICT-01-2018 Call

- The **prevention** of and the **protection against attacks** that **target modern ICT components** and emerging technologies (e.g. IoT) **remains a difficult task.**

- The **increase of encrypted flows** over the Internet should lead to adopt **new techniques for detection** of suspicious cyber activities and **traffic patterns**, and for **classification of flows**, **while keeping privacy and confidentiality**.

- Innovative, integrated and holistic approaches in order to minimize attack surfaces through appropriate configuration of system elements, trusted and verifiable computation systems and environments, secure runtime environments, as well as assurance, advanced verification tools and secure-by-design methods

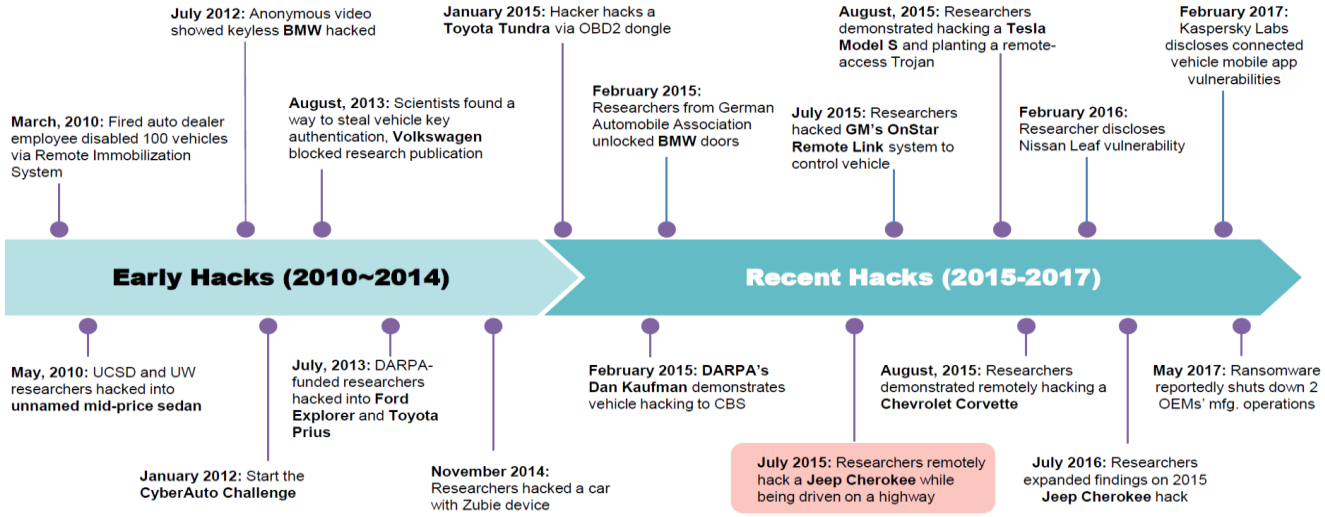
Rationale

Today's vehicles are increasingly "connected"; there is wireless data exchange with servers, infrastructure and other vehicles.

> ***There is not*** *a dedicated scientific field studying the protection of Connected and Autonomous Vehicles (CAVs) against cyber-attacks and thus, the respective research endeavours are limited.*

Over ***85% of all new cars are already classed as connected****, and by 2025 there will be over 470 million connected vehicles on the roads in Europe, the USA and China alone.*

Attacks on automobile systems are **expected to increase rapidly** in the following years due to the rapid increase in connected automobile hardware & software without foundational cybersecurity principles.



nIoVe Motivation

Heterogeneous network architecture of IoV ecosystem includes many types of vehicular communications:

- Vehicle-to-Vehicle (V2V)
- Vehicle-to-Infrastructure (V2I)
- Vehicle-to-Network (V2N)
- Vehicle-to-Pedestrian (V2P), etc.

Main Goal

Overview of nIoVe Scope and Identity			
Application field:	Cybersecurity in connected and autonomous vehicles	**Mode of transport:**	Connected and autonomous vehicles of different types (e.g. mini-buses, cars)
Targeted areas:	Smart Cities; Urban Environments	**Vehicles setup:**	Fleets of CAVs
Target users:	All; Of specific interest: people with disabilities; OEMs; Tier suppliers; Cybersecurity companies		
Technologies employed:	Anomaly detection, blockchain, data & visual analytics; V2V, V2I, V2N communication, IoT	**Services to be provided & improvements:**	Risk assessment, Response and Recovery toolkits, hypothesis testing, virtualized honeypots; threat info repository
Ultimate goal:	**To develop, deploy and validate a holistic and multi-layered Cybersecurity Framework** suitable to offer security assessment in IoV ecosystem (connected and autonomous vehicles, smart cities infrastructure, etc.) and OEMs.		

nIoVe Vision

nIoVe aims to:

- **identify the risks associated** with connected of vehicles and IoV networks
- recognise and evaluate suspicious threat patterns with the use of advanced **Machine Learning (ML) algorithms**
- enable appropriate **coordinated mitigation actions** in order to address CAVs safety/security and ensure proper CAVs performance and data management
- offer (near) **real time detection of anomalies**, as well as **response against evolving complex cyber-attack** and **successful recovery**
- open up the **cybersecurity 'blackbox'** to connected and autonomous vehicles

nIoVe Objectives (1/4)

	Objective	WPs	KPIs
Obj.1	To deliver a multi-layered cybersecurity solution for the IoV ecosystem in order to provide protection against wider area of attacks	WP3-WP7	• **Meet at least 85% of users requirements** concerning cybersecurity and privacy objectives (identified during the user requirement analysis) • **Improvement by up to 100% of the usability of current services and solutions** for a given security level • **Toolkit functionalities** for cyber-risk reduction concerning privacy, data and infrastructures of the IoV ecosystem
Obj.2	To research and develop a Machine Learning (ML)-Driven Threat Analysis and Situational Awareness Platform for the IoV	WP3	• **Detection time for complex cyber-attacks** : 24 hours • **Detection effectiveness**: 99% accuracy of known threats; 90% for zero-day exploits; Improved cybersecurity in IoV ecosystem (overall): 99.5% of cyber-threats/ potential attacks are identified • **Automation metrics of the nIoVe**: (a) Increased averaged automation level: 4.5 to 5 out of 5 (or +20%) compared to existing cutting-edge solutions (measured at task/ function level); (b) Increased automation effectiveness: 3,5-4,5 / 5 or detection rate: 10% improvement; +30% reduction of false alarms and unidentified threats (FPR, FNR, TPR, TNR) • **Number of Major or Small Security Incidents**: Continuous comparison and evaluation of the current situation based on historical data for potential incidents

nIoVe Objectives (2/4)

	Objective	WPs	KPIs
Obj.3	To introduce advanced Visualization and Big Data techniques required for the detection of complex cyber-attacks	WP4	• **Wide understanding of security services and analytics**: >75% of CAVs manufacturers comprehend the 100% of the nIoVe functionality they are interested in (in respect of security status, potential threats, risk notifications, etc.).
Obj.4	To introduce a coordinated cyber Incident Smart Response System for CAVs at national & European level	WP5	• **Amount of Time to Resolve an Incident:** 20% reduction the time it took to resolve a cyberattack incident, from the moment it was first noticed until the final wrap-up meeting or report • **Uptime (or Downtime) During an Incident**: 20% reduction the cost of downtime during a security incident keeping backup files through recovery toolkit • **Appropriate Management of End-user Impact**: Maximum collection and storage of data during the attack time and 100% recovery of saved data • **Demonstrate effective response to cyber and hybrid security and privacy threats/ attacks of > 98.5%**

nIoVe Objectives (3/4)

	Objective	WPs	KPIs
Obj.5	To maximise trust between CAVs and infrastructure components through trust management and identification platform	WP5	• **Clear accountability** (in the sense that it can be automated) for >85% of the interactions/ communications performed in integrated IoV settings (defining who is accountable for what)
Obj.6	To establish and operate a continuously updated and shared Threat Intelligence Repository for CAVs cyber threats to support OEMs and Tier suppliers	WP6	• **Threat intelligence**: aggregation of threat intelligence from all CAVs pilots, sensitive data & user accountability • **Reported Incidents of End-user Impact**: Continuous information sharing between CAVs manufacturers, ECUs providers, automotive industries, CSIRTs etc. for threats, attacks and recovery/response services

nIoVe Objectives (4/4)

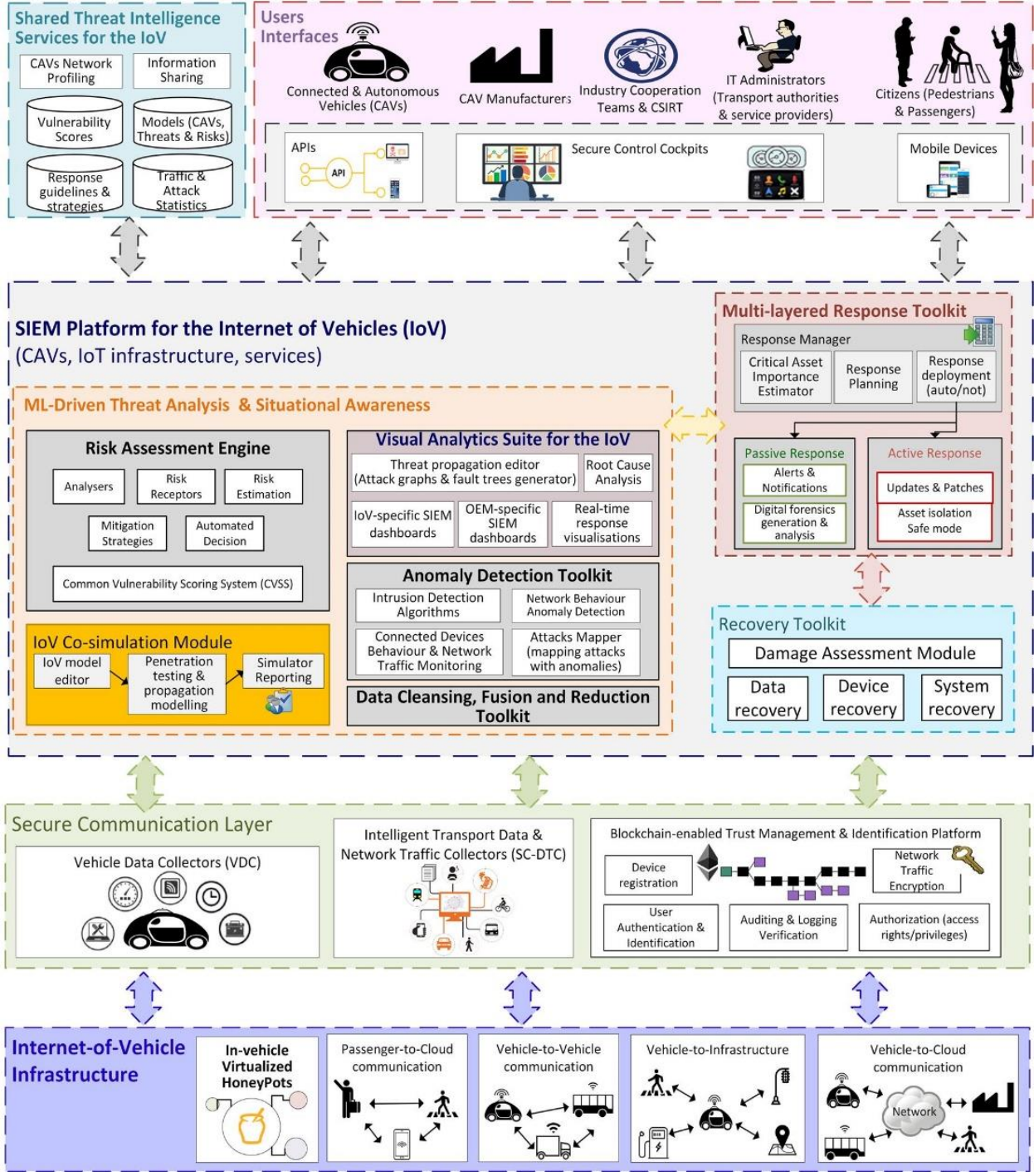
	Objective	WPs	KPIs
Obj.7	To support of secure-by-design production lifecycle for all vehicle communications	WP7	• **Operating capacity of the simulation infrastructure**: Support secure-by-design new product development of CAVs; execution of the certification process for the CAVs • **Meeting Regulatory Requirements**: Training and compliance the CAVs manufacturers and providers regarding regulations and rules for the secure and safe development of new hardware and software components.
Obj.8	To provide cybersecurity solutions to cover execution environments (Smart Cities' infrastructure elements) including all mechanisms (authentication/access control mechanisms, etc.)	WP7	• **Demonstration of the system prototype in an execution environment (TRL6)**
Obj.9	To validate the nIoVe architecture capabilities in proof-of-concept Use Cases	WP7	• **Number of Demonstrations**: Hybrid execution environment for use case 1, simulated environment for use case 2 and real-world conditions (Geneva City) for use case 3

nIoVe Concept

nIoVe Architecture

nIoVe Technical Architecture is divided **into 4 layers**:

- **Bottom layer**: Internet-of-Vehicles Infrastructure
- **Second Layer**: Secure Communication Layer
- **Main Layer**: SIEM (Security Information and Event Management) Platform for IoV
- **Topmost layer**: Users and Beneficiaries

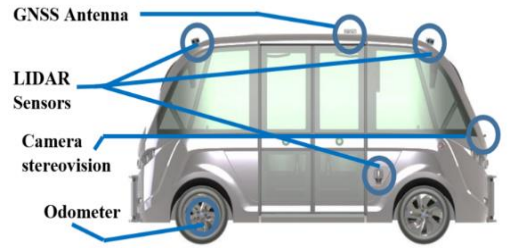


nIoVe Pilot Site #1

Category: Hybrid execution environment

Scenarios to be tested:

- **Minor issues**: blinking leds, false speedometer and fuel readings, infotainment and telematics
- **Critical issues**: attack on GPS position and navigation, cyber-ransom
- **Privacy**: collect information from the vehicle and/or from its passengers
- **Safety**: damage engine, accelerate vehicle, disable brakes, take control of steering wheels, emergency breaking (especially when operating in high Levels of Automation)
- Apply nIoVe active and passive responses to CAV
- Run diagnostics and software updates during operation



End Users: Automated Vehicles Manufactures; IoT devices providers; Cybersecurity experts

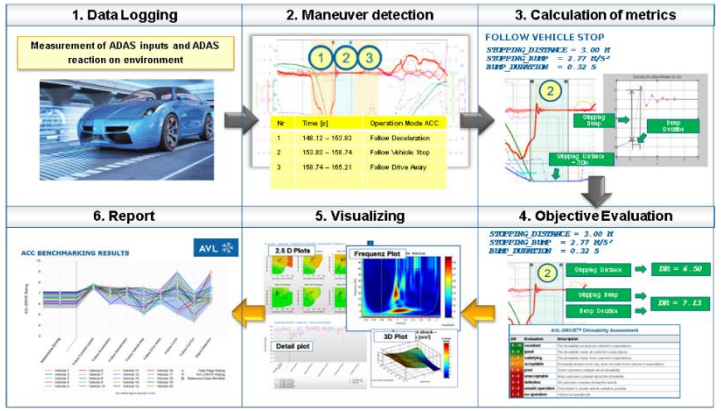
nIoVe Pilot Site #2

Category: Simulated Environment

Scenarios to be tested:

- **Minor issues**: blinking leds, false readings (e.g. speedometer, fuel readings, engine status), the operation of after-market products (mostly related to infotainment and telematics)
- **Critical issues**: GPS position and guided navigation, lock the car by distance, false manoeuvre detection, false Smart-City readings (e.g. traffic light status, traffic alerts)
- **Car Theft**: Unlock doors, open windows, bypass immobilizer
- **Privacy**: Eavesdrop, GPS location tracking, access to personal data, collect information from the vehicle
- **Safety**: damage engine, accelerate, disable brakes, take control of steering wheels, emergency breaks
- **Emergency**: attacks to the eCall and emergency services
- **Drive analysis**

End Users: CAV manufactures; ECUs providers; Automotive Industries; CSIRTs



nIoVe Pilot Site #3

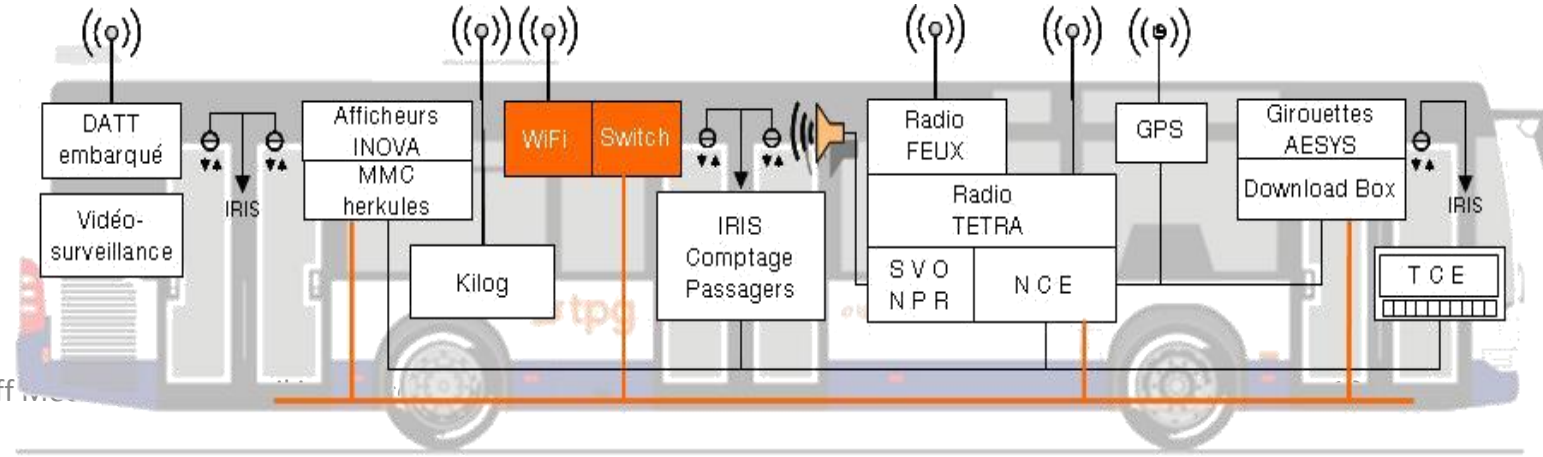
Category: Real smart city execution environment

Scenarios to be tested:

- **Smart City infrastructure**: sensors return incorrect readings;
- **Transport Information System**: incorrect transport information readings, like incorrect occupancy (for buses, trains, metro, tram & trolleys), destination (for public transportation means), expected arrival time, transportation availability;
- **CAVs**: incorrect GPS position, guided navigation, drive analysis;
- **Privacy**: Citizens eavesdrop, unauthorized access to passenger's data

End Users: All, Passengers, Citizens,

Pedestrians, Drivers



nIoVe

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