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

A novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles: The nIoVe approach

CyberSec
Advanced Cybersecurity Approaches for Connected, Automated and Electric Vehicles
23rd IEEE International Conference on Intelligent Transportation Systems
September 20 – 23, 2020, Rhodes, Greece

Dr. Konstantinos Votis (Project Coordinator)

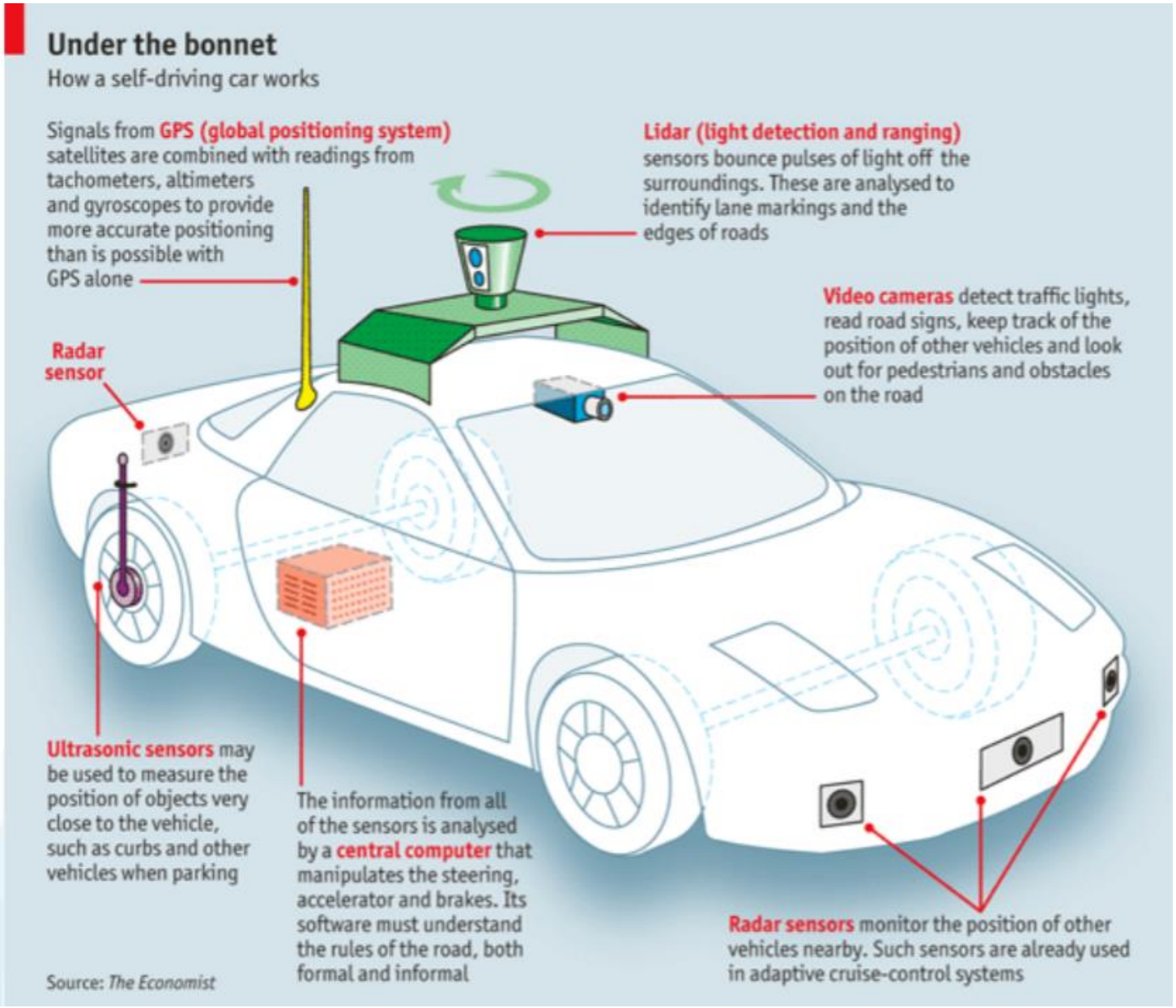
Horizon 2020
European Union funding
for Research & Innovation

Information Technologies Institute

Autonomous Vehicles….

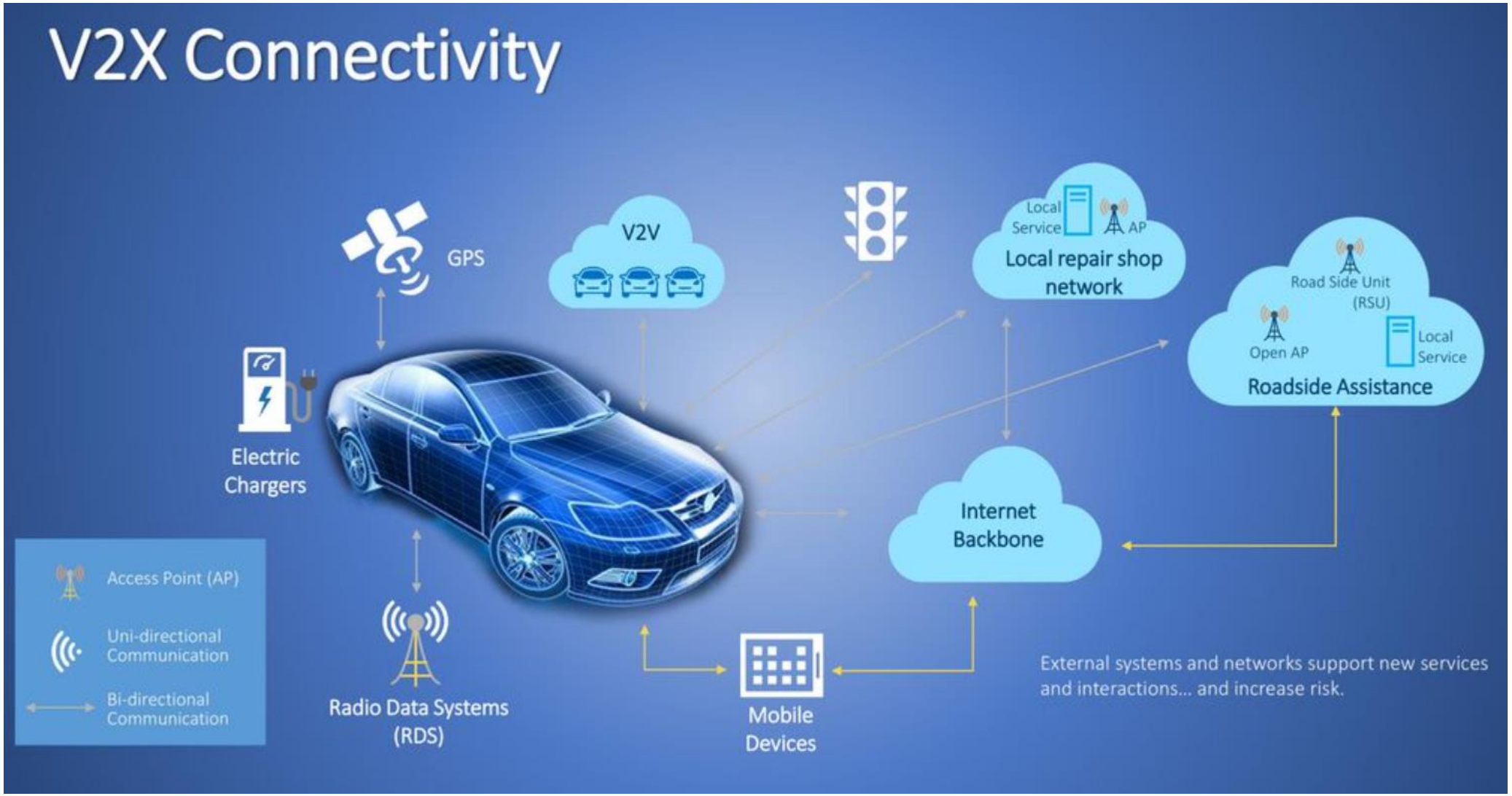
- 10 million autonomous vehicles will hit the roads by 2020
- In 10 years fully autonomous vehicles will be the norm
- AVs will generate a $7 trillion annual revenue stream by 2050
- Widespread adoption of AVs could lead to a 90% reduction in vehicle crashes

Ecosystem of Autonomous Vehicles



- ❑ Global Positioning System (GPS)
- ❑ Light Detection and Ranging
- ❑ (LIDAR)
- ❑ Cameras (Video)
- ❑ Ultrasonic Sensors
- ❑ Central Computer
- ❑ Radar Sensors
- ❑ Dedicated Short-Range
- ❑ Communications-Based Receiver

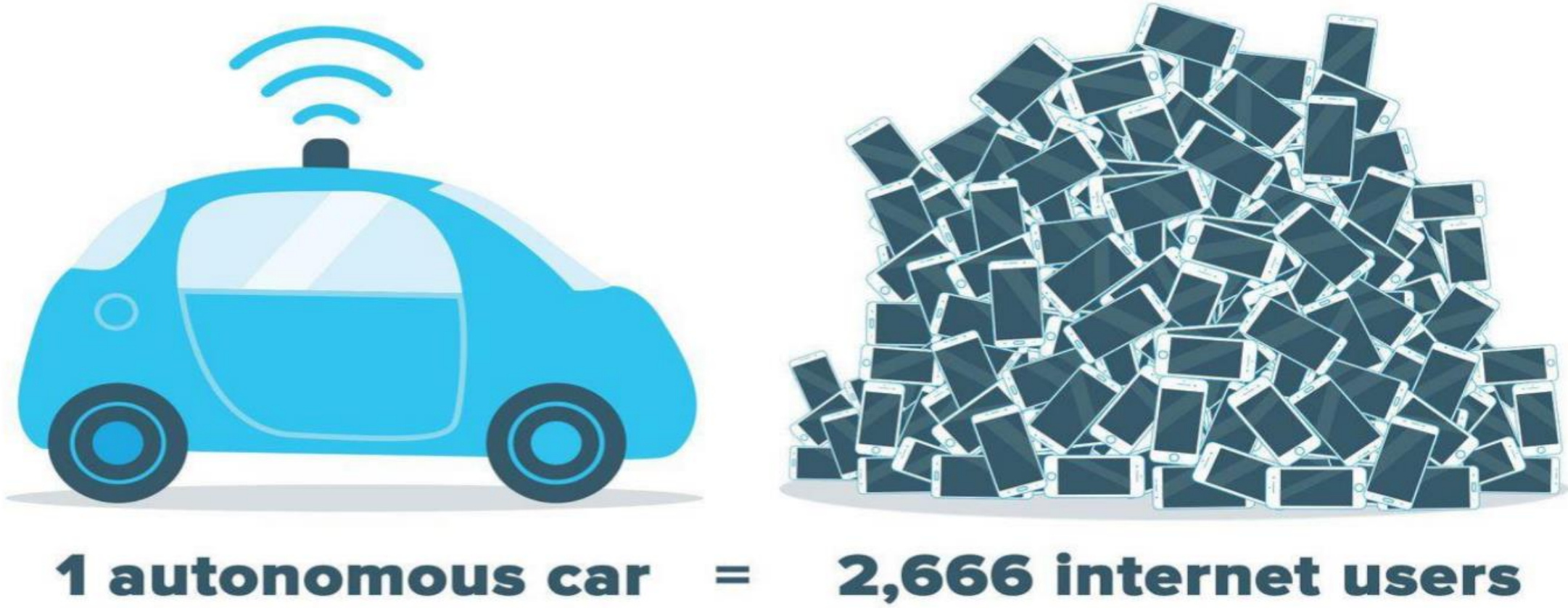
V2X connectivity…



https://slideplayer.com/slide/13611033/

Autonomous Car Data vs Human Data

In 2020, the average autonomous car may process 4,000 gigabytes of data per day, while the average internet user will process 1.5 gigabytes. That means...



1 autonomous car = 2,666 internet users

https://www.mcca.com/wp-content/uploads/2018/04/Autonomous-Vehicles.pdf

Safety-Security-Privacy

https://slideplayer.com/slide/13611033/

IoV ecosystem

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

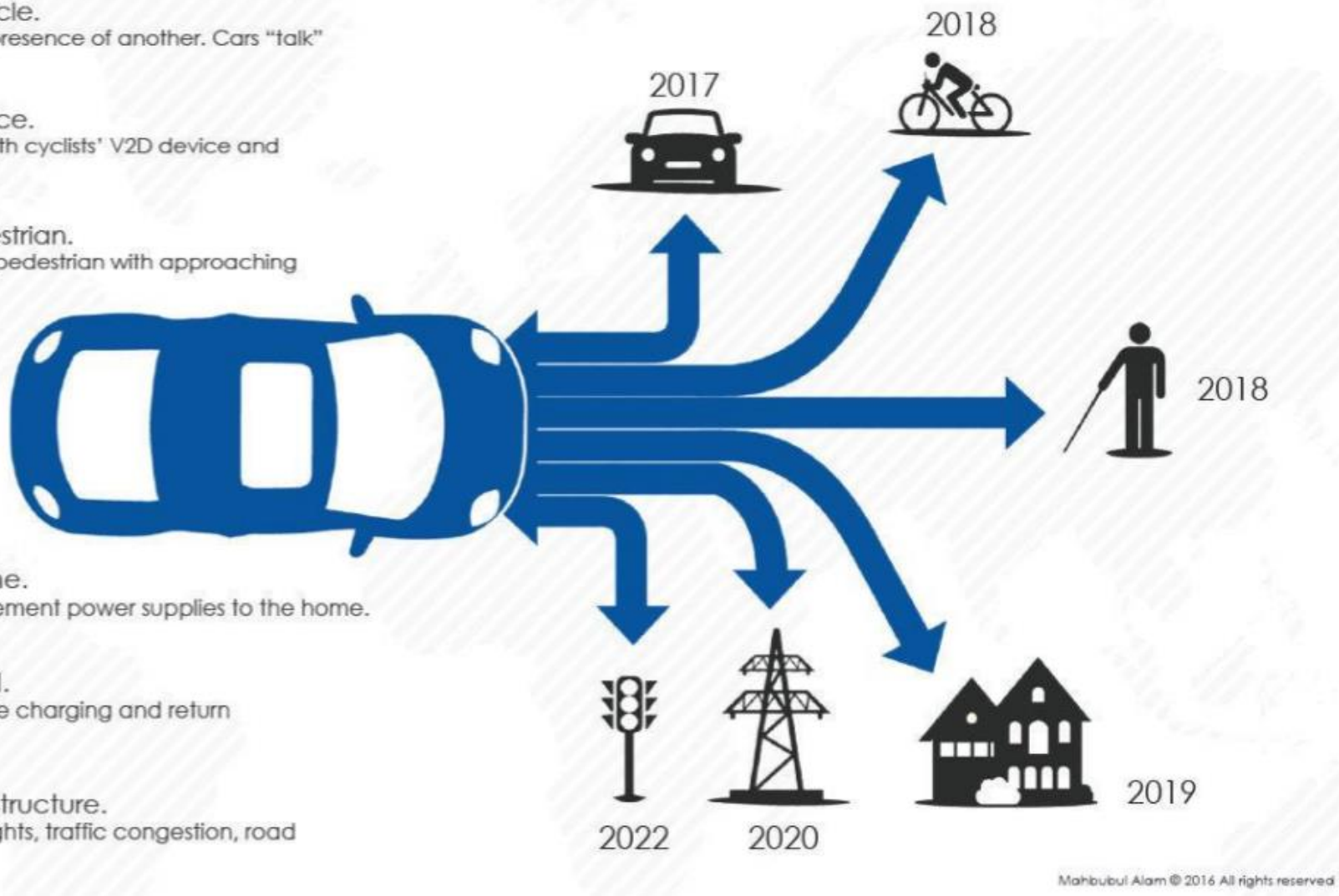
- Vehicle-to-Vehicle (V2V)
- Vehicle-to-Infrastructure (V2I)
- Vehicle-to-Network (V2N)
- Vehicle-to-Pedestrian (V2P), etc.

Automotive Technology V2X

V2V - Vehicle-to-Vehicle.
Alerts one vehicle to the presence of another. Cars "talk" using DSRC technology.

V2D - Vehicle-to-Device.
Vehicles communicate with cyclists' V2D device and vice versa.

V2P - Vehicle-to-Pedestrian.
Car communication with pedestrian with approaching alerts and vice versa.



V2H - Vehicle-to-Home.
Vehicles will act as supplement power supplies to the home.

V2G - Vehicle-to-Grid.
Smart grid controls vehicle charging and return electricity to the grid.

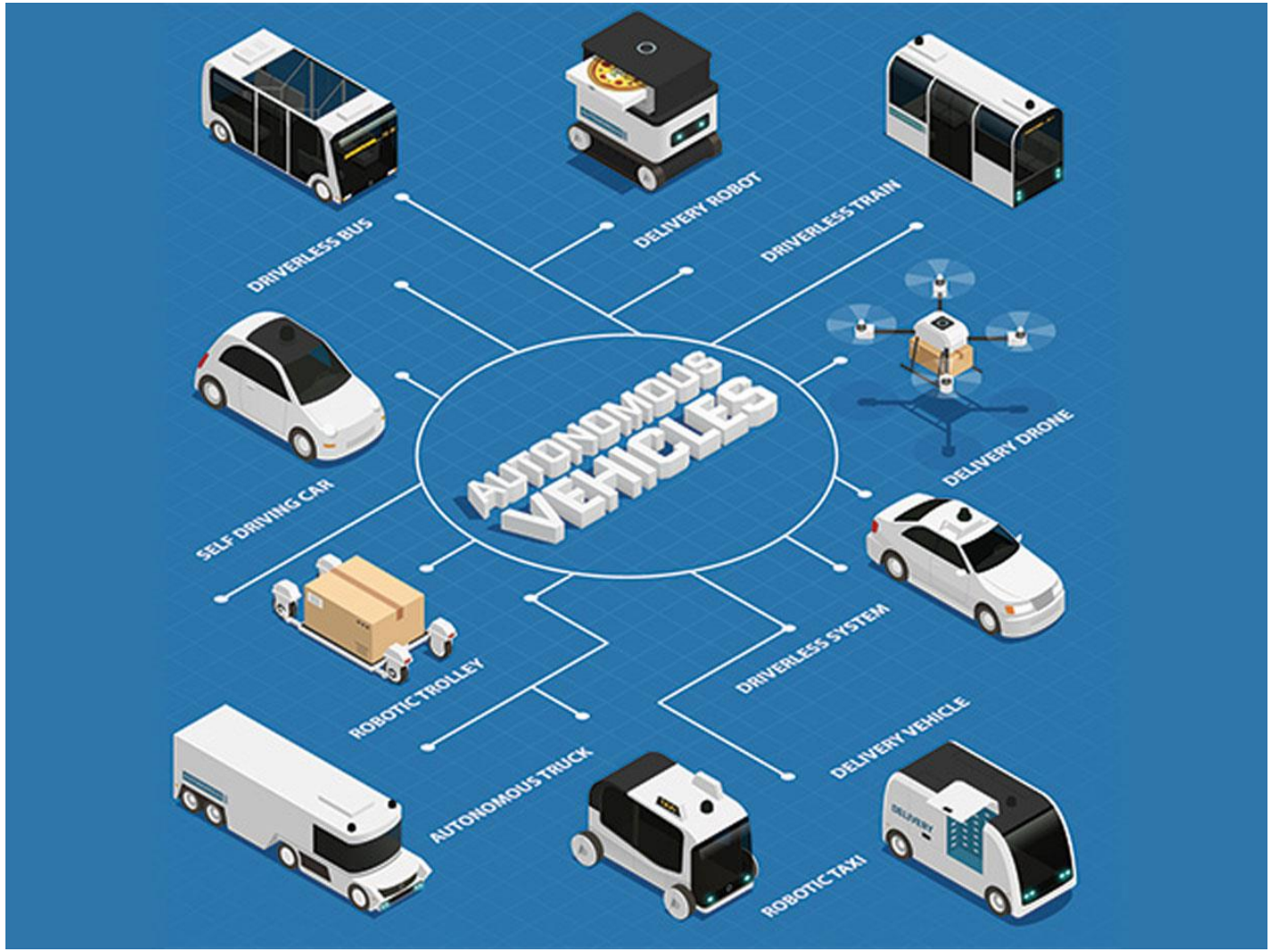
V2I - Vehicle-to-Infrastructure.
Alerts vehicles to traffic lights, traffic congestion, road conditions, etc.

Next Generation Dedicated Short Range Communications (DSRC) for Intelligent Transportation Systems (ITS) Vehicle Safety & Operations

Cybersecurity in the age of Autonomous Vehicles

Must Be a Top Concern for Automakers….

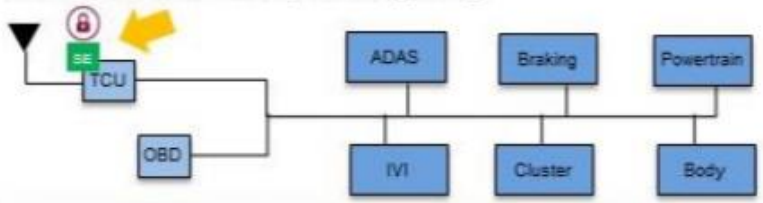
IEEE Spectrum Jan 2019



4 Layers to securing a Vehicle

Layer 1: Secure Interface

Secure M2M authentication, secure key storage

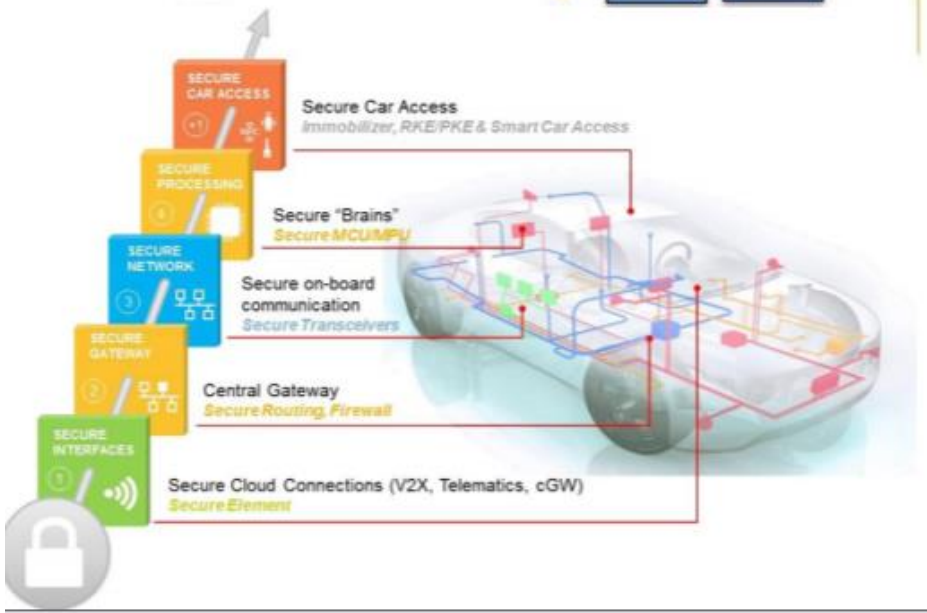


Layer 2: Secure Gateway

Domain isolation, firewall/filter, centralized intrusion detection (IDS)

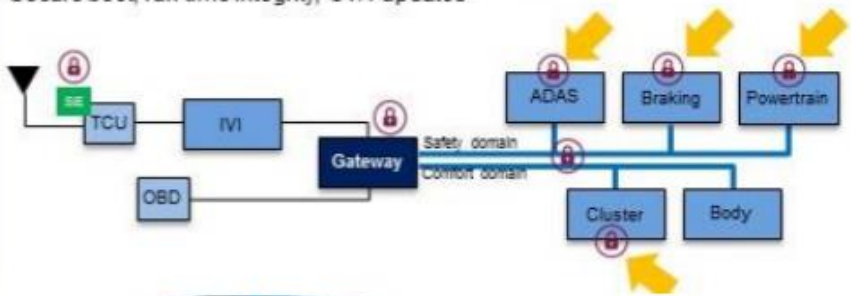
Layer 3: Secure Network

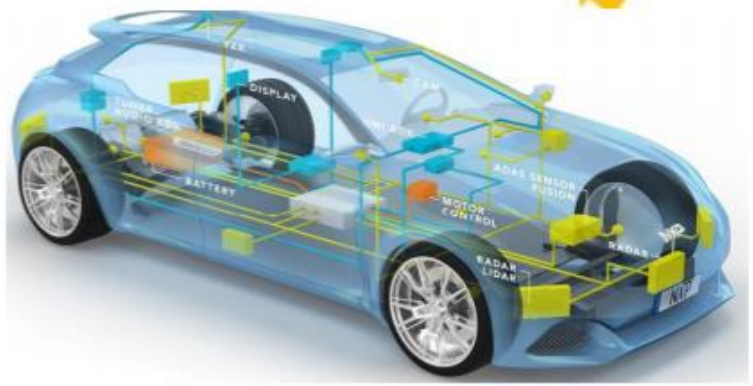
Message authentication, CAN ID killer, distributed intrusion detection (IDS)



Layer 4: Secure Processing

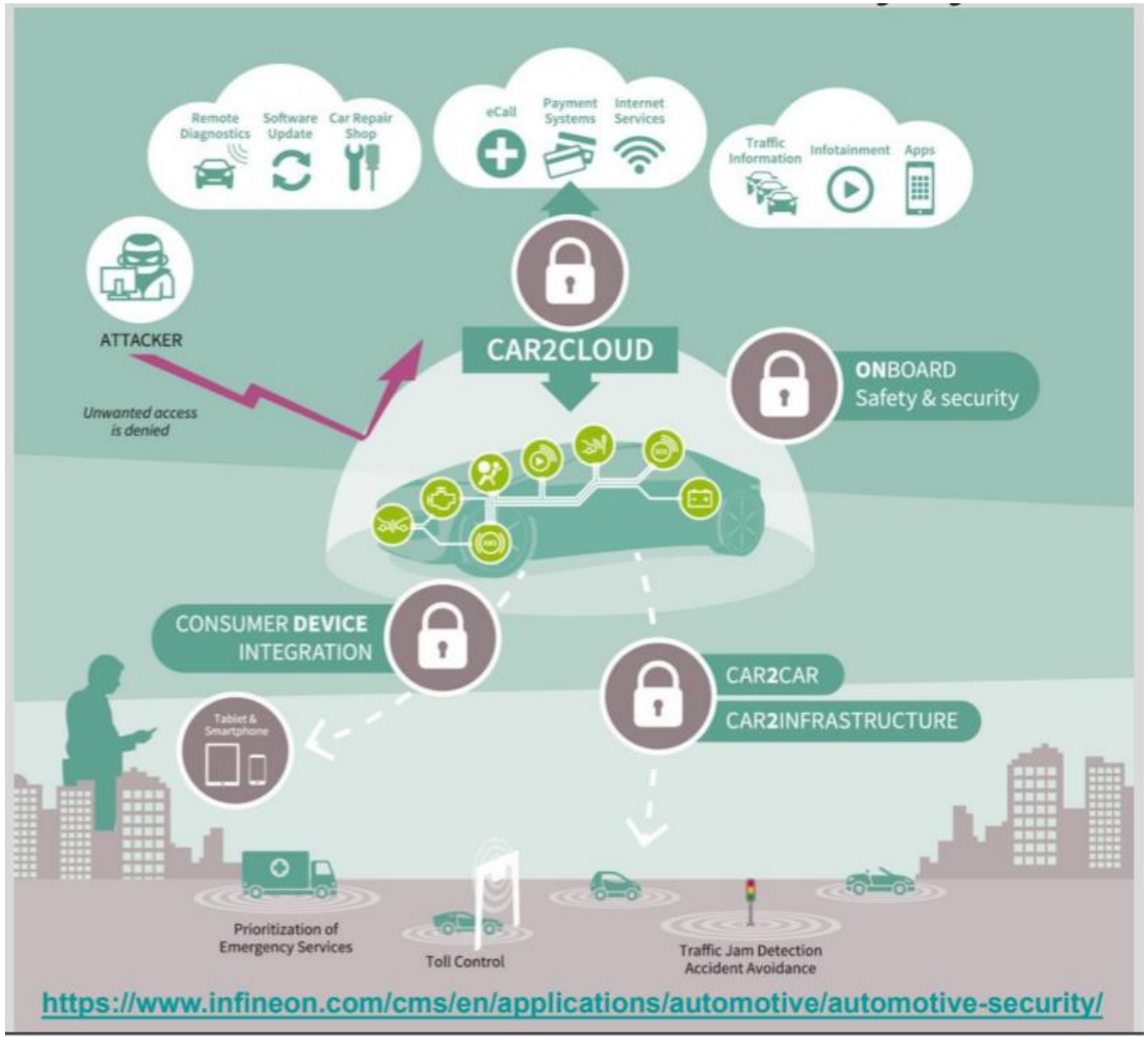
Secure boot, run time integrity, OTA updates



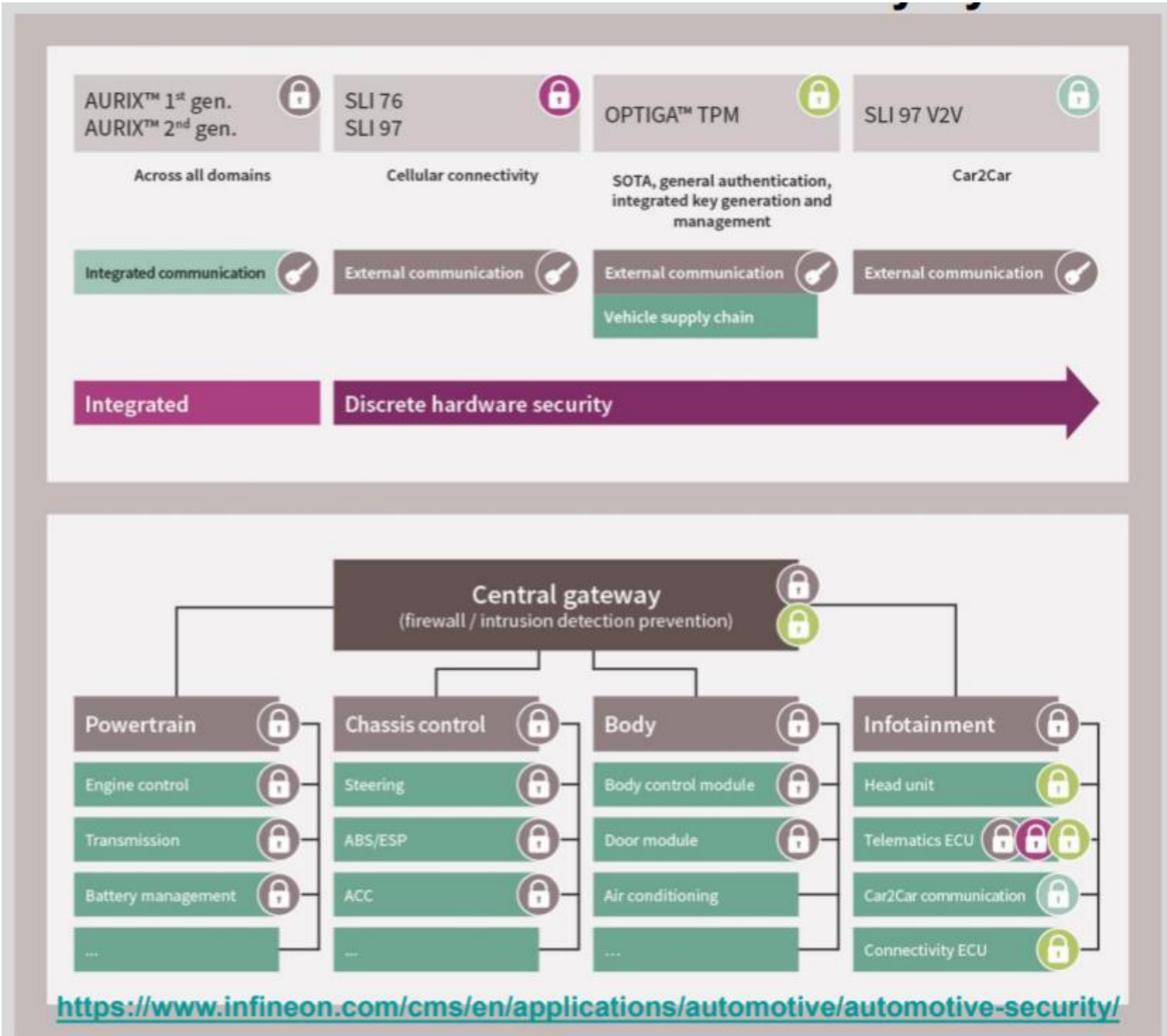


https://www.nxp.com/applications/solutions/automotive/secure-gateway-in-vehicle-networking

Infineon Solution Example



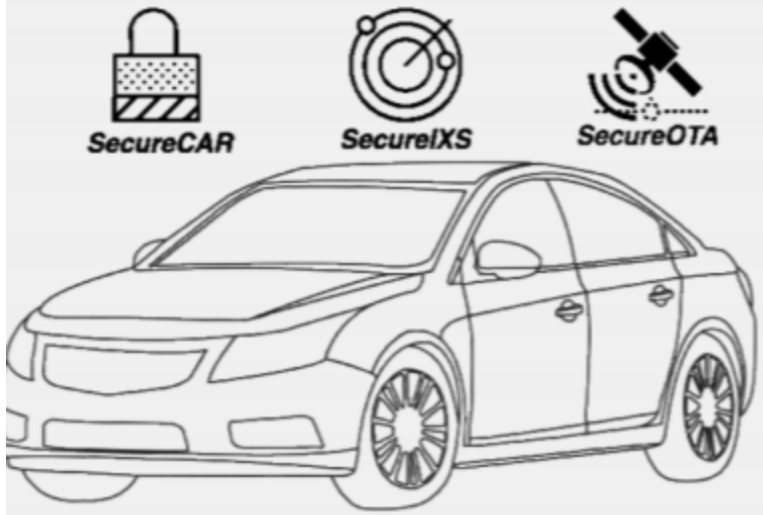
Infineon Solution Example



Trilium Solution Example

A Comprehensive Automotive Cyber Security Suite, Covering The Entire Automotive Cyber-System From IVN, IPS to OTA.

Our technology is software-based, designed to run on resource constrained ECU devices and IVN configurations - it is fully HW, RTOS and cypher agnostic thus requires minimal optimisation to run on unique chipset / RTOS combinations.



SECURE CAR

Authentication, Encryption And Key Management For All Relevant IVN (In Vehicle Networks).

SECURE IXS

Artificial Intelligence / Machine Learning Driven Smart Firewall Technology That Provides A Feedback Loop Into Crypto Library (SecureCAR) Optimisation.

SECURE OTA

Offers A Total And Unified Solution For Long-Term Protection Against Dynamic Cyber Threats.

http://www.trillium.co.jp/

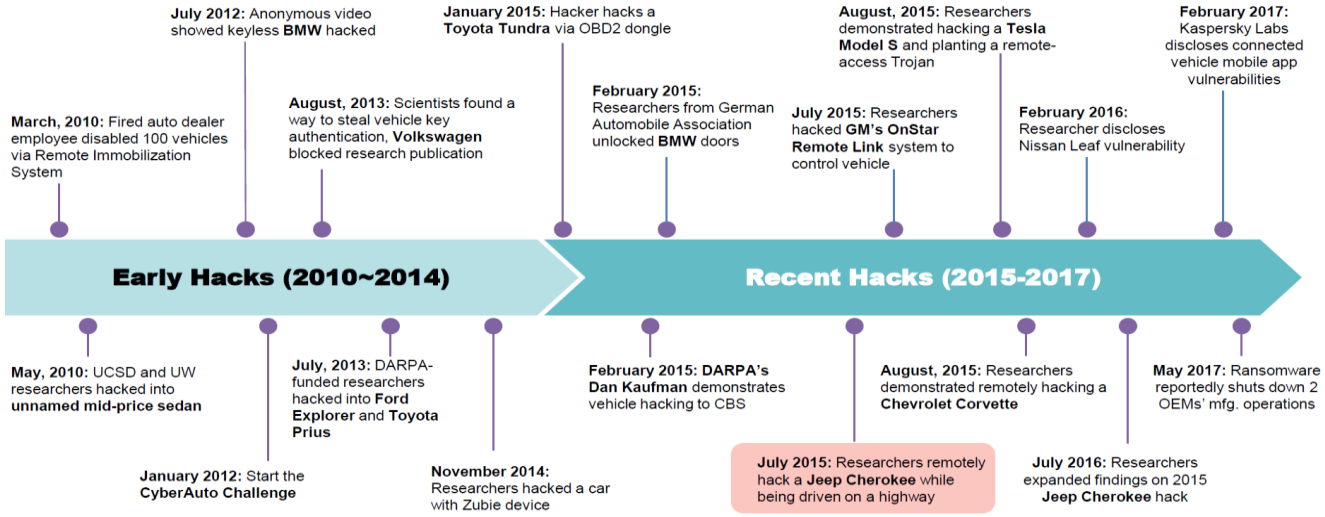
Rationale of nIoVe…

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.



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

- **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 can **response against evolving complex cyber-attack** and **successfully recovery**
- open up the **cybersecurity 'blackbox'** to connected and autonomous vehicles

nIoVe Objectives (1/4)

	Objective	KPIs
Obj.1	To deliver **a multi-layered cybersecurity solution** for the IoV ecosystem in order to provide protection against wider area of attacks	• **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	• **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	KPIs
Obj.3	To introduce advanced Visualization and Big Data techniques required for the detection of complex cyber-attacks	• **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	• **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	KPIs
Obj.5	To maximise trust between CAVs and infrastructure components through trust management and identification platform	• **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	• **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	KPIs
Obj.7	To support **of secure-by-design production lifecycle** for all vehicle communications	• **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.)	• **Demonstration of the system prototype in an execution environment**
Obj.9	To **validate the nIoVe architecture capabilities** in proof-of-concept Use Cases	• **Number of Demonstrations**: Hybrid execution environment for use case 1, simulated environment for use case 2 & real-world conditions (Geneva City)

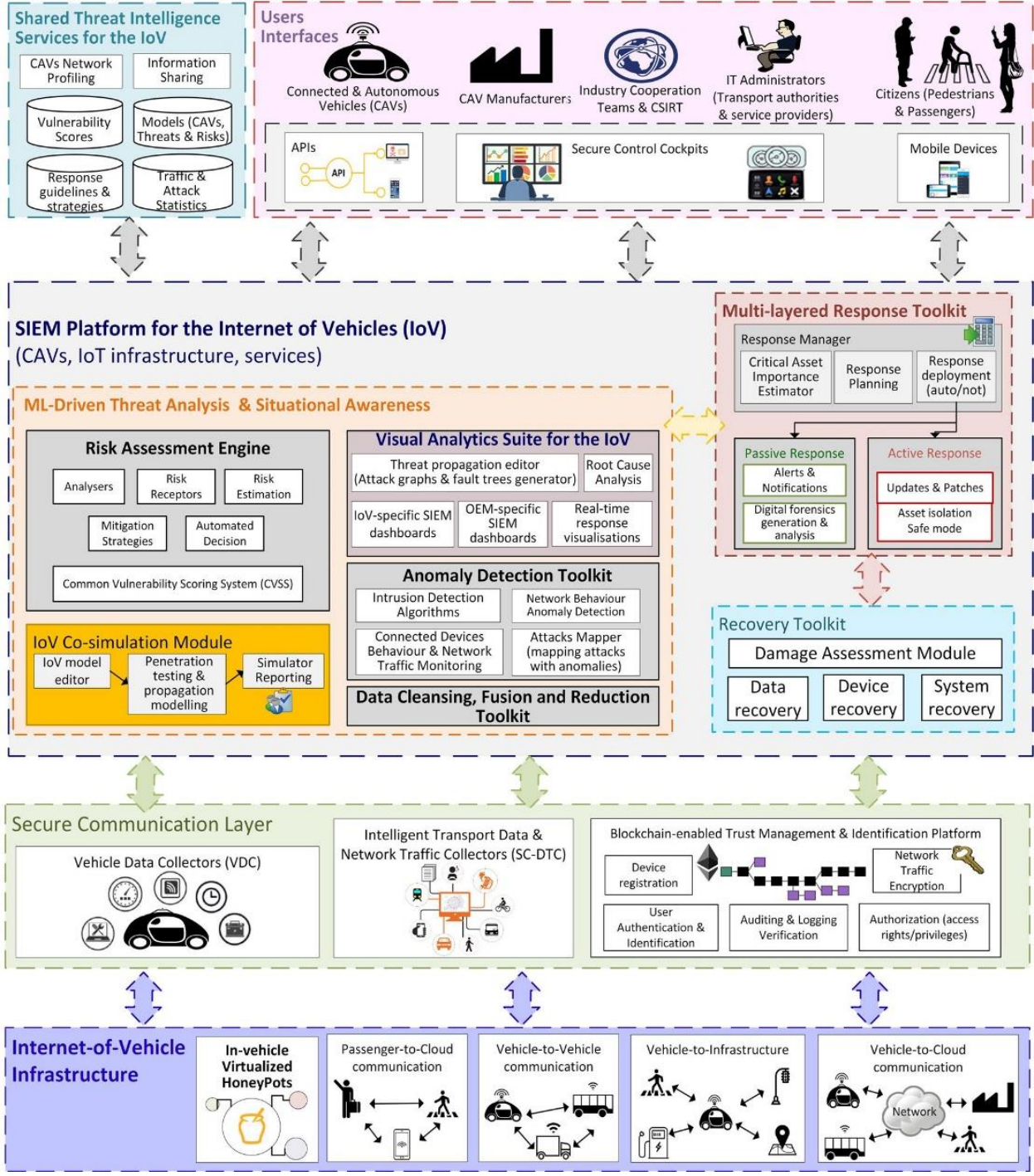
nIoVe Concept

Autonomous Shuttles..navya

nIoVe Architecture (1/5)

…is divided **into 4 layers**:

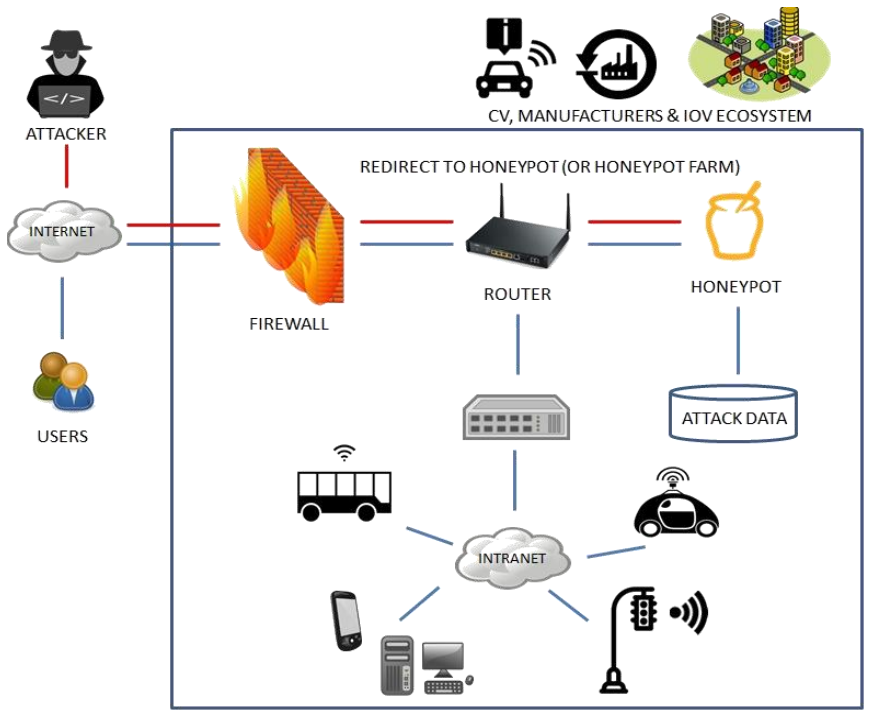
- **Bottom layer**: Internet-of-Vehicles Infrastructure
- **Second Layer**: Secure Communication Layer
- **Main Layer**: SIEM Platform for IoV
- **Topmost layer**: Users and Beneficiaries



nIoVe Architecture (2/5)

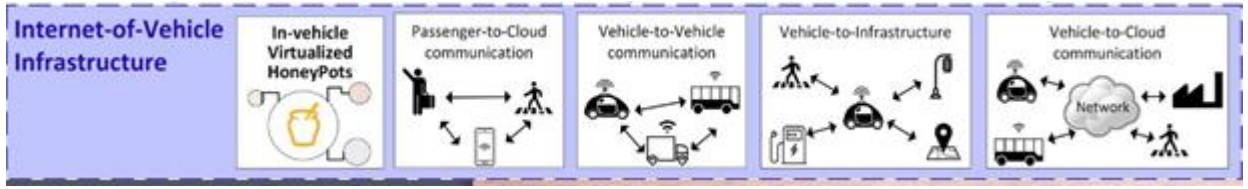
consists of Internet of Vehicle Infrastructure:

- *Vehicle-to-Vehicle Communication (V2V)*
- *Vehicle-to-Infrastructure Communication (V2I)*
- *Vehicle-to-Cloud (V2C)*
- *Passenger-to-Cloud (P2C), etc.*
- *In-Vehicle Virtualized Honeypots*



Virtualized Honeypot is a **software component installed on a device** (e.g. on a mobile phone, computer, virtual machine, or a device's pairing gateway) **or on a central network node** (e.g. a server), in order **to emulate a real device or node, exposed to attackers**

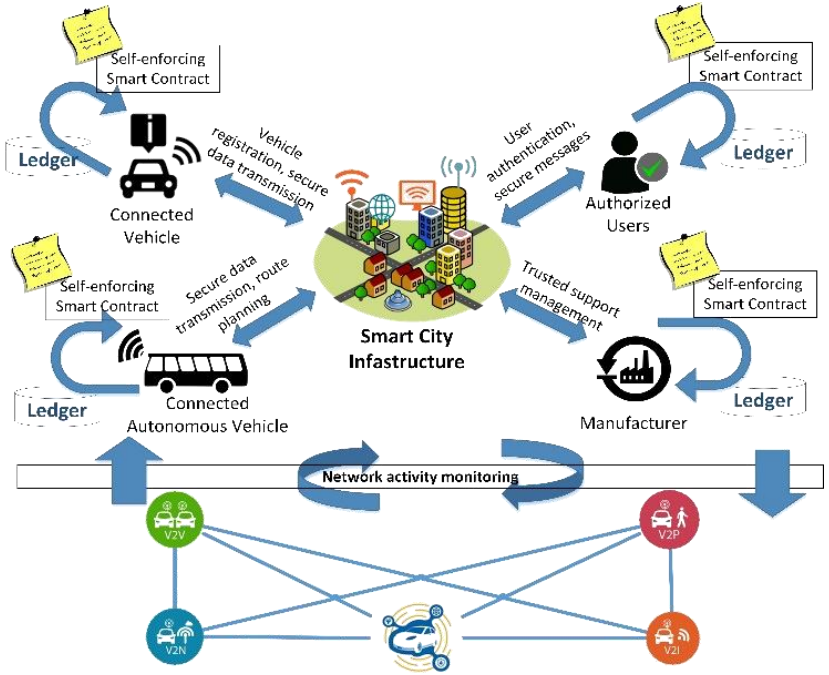
Bottom-up Layer



nIoVe Architecture (3/5)

The **Second layer** **includes:**

- ***Vehicle Data Collectors*** are dedicated to sensing components build-in the CAVs
- ***Other Data Collectors*** (Intelligent Transport Data & Network Traffic Collectors) from **smart-city infrastructure**
- ***Blockchain-enabled Trust Management & Identification Platform***



nIoVe Blockchain Infrastructure concerns distributed management, control and validation of connected-autonomous vehicles and their transactions with a view of assuring high reliability

nIoVe Architecture (4/5)

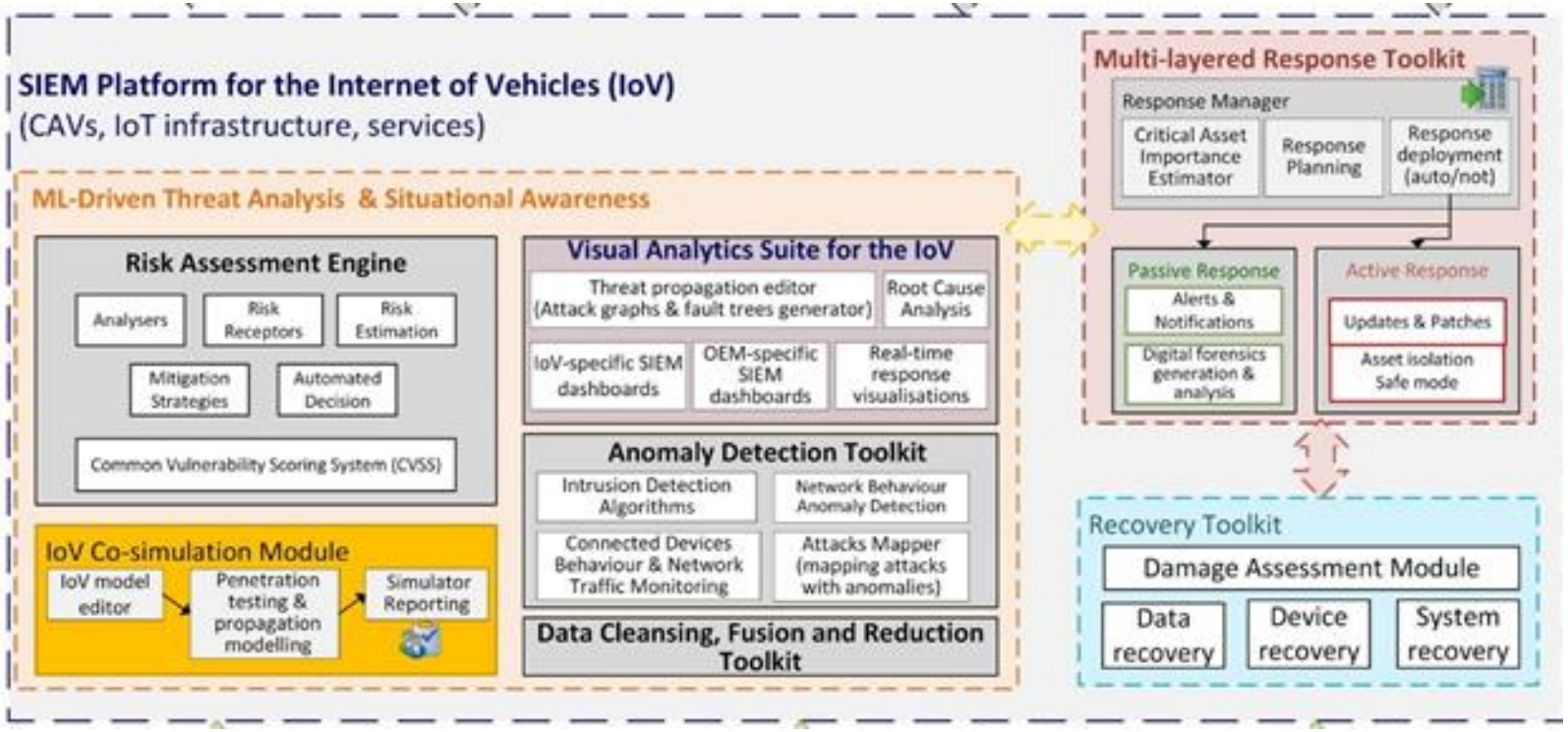
The Main layer **includes:**

ML-Driven Threat Analysis & Situational Awareness is divided into:

- Risk Assessment Engine
- Visual Analytics Suite of IoV
- Anomaly Detector Toolkit
- Data Cleansing, Fusion and Reduction Toolkit

Multi-layer Response Toolkit provides active & passive responses.

Recovery Toolkit provides three kinds of recovery
actions: a) Data recovery, b) Device recovery and c) System recovery



nIoVe Architecture (5/5)

The Topmost Layer **includes:**

- *Shared Threat Intelligence Services for the IoV,* will **store** and **share system vulnerabilities information** and **allow access to supportive cybersecurity related information** retrieved from and shared among the nIoVe installations

Group of Users:

- Connected and Autonomous Vehicles (CAVs)
- CAVs manufacturers and providers
- Industry Cooperation Teams (ICTs) and Computer Security Incident Response Teams (CSIRTs)
- IT administrators
- Citizens (Pedestrians, Passengers, etc.)

Envisioned Use Cases (1/7)

General scenarios

ID	Title	Description
G1-1	Personal data is leaked.	An attacker retrieves personal data (e.g. through the camera stream, the position of the vehicles, billing logs or passenger usage pattern) of passengers, pedestrians or other persons that may be involved in the ecosystem of the AV.
G1-2	Run diagnostics and software updates during operation	The vehicle is running diagnostics and software updates over the air while in operation on the road with onboard passengers.
G1-3	False reading	(e.g. speedometer, battery level, engine status), the operation of after-market products (mostly related to infotainment and telematics)
G1-4	Abnormal driving behavior	An attacker successful its attack and impact the vehicle driving behaviour.

Attacker near the vehicle

ID	Title	Description
A1-1	GNSS signals are jammed.	An attacker uses a jammer against GNSS signals. The autonomous vehicle is not able to retrieve GNSS localization data.
A1-2	GNSS signals are spoofed.	An attacker spoofs GNSS signals. The autonomous vehicle receives wrong GNSS localization data.
A1-3	RTK/NTRIP (GNSS corrections) signals are jammed.	An attacker uses a jammer against GNSS corrections signals. The autonomous vehicle is not able to retrieve corrections.
A1-4	RTK/NTRIP (GNSS corrections) signals are spoofed.	An attacker spoofs GNSS corrections signals. The autonomous vehicle receives wrong corrections.
A1-5	V2X signals are jammed.	An attacker uses a jammer against V2X signals. The autonomous vehicle is not able to receive V2X signals from other vehicles or from road infrastructure.

Envisioned Use Cases (2/7)

Attacker near the vehicle

ID	Title	Description
A1-6	V2X signals are spoofed.	An attacker spoofs V2X signals. The autonomous vehicle receives wrong V2X signals. It detects ghost vehicles or wrong road infrastructure signal status.
A1-7	Traffic light status are remotely altered.	An attacker analyzes the V2X signal between the onboard OBU and the traffic light RSU. From this analysis, the attacker sends a ghost vehicle signal to trigger the traffic light status (link to A1-6).
A1-8	The traffic light sends a V2X signal which does not correspond to the actual physical light status.	An attacker manipulates the V2X signals sends by the traffic light to alert it on the fly. The received V2X status will not match the current physical light status.
A1-9	Mobile broadband communications signals are jammed.	An attacker uses a jammer against mobile broadband communications signals. The autonomous vehicle is disconnected from the cloud. It cannot be supervised properly.
A1-10	Cellular communications are hijacked.	An attacker hijacks the cellular communication and spoofs the Supervision center.

Envisioned Use Cases (3/7)

Attacker acting as passenger

ID	Title	Description
A2-1	Users' inputs are altered.	An attacker altered users' inputs. The vehicle does not follow the user's wanted mission.

Attacker acting as insider (maintainer access and knowledge)

ID	Title	Description
A3-1	Sensors data is altered.	An attacker alters data collected by sensors. The autonomous vehicle receives wrong obstacle from one VLP.
A3-2	CAN messages are altered.	An attacker sends wrong CAN messages on the bus. The autonomous vehicle targeted ECU receives malicious messages or a wrong command.
A3-3	Denial-of-service on the CAN.	An attacker floods the CAN bus with messages. The autonomous vehicle targeted will no longer be able to operate as expected.
A3-4	Cameras stream is altered.	An attacker sends wrong data on the camera stream. The supervision center is not able to have a clear vision of the vehicle environment or ghost obstacles are detected.
A3-5	Data sent to the supervision center is altered.	An attacker alters data sent to the supervision center. The autonomous vehicle cannot be supervised properly.
A3-6	Embedded firmware and / or software is altered.	An attacker infects embedded firmware. A driving function is impacted.
A3-7	Backdoor in driving software	An attacker alters the software adding a backdoor during the development.
A3-8	Software / OS weakness	Developers can intentionally or not, develop code with weaknesses that could be exploited, making the vehicle's security unreliable.

Envisioned Use Cases (4/7)

Attacker acting as insider (maintainer access and knowledge)

ID	Title	Description
A3-9	Ransomware	An attacker blocks access to the vehicle's software requiring a ransom to release the vehicle's systems. Can also threaten to disclose sensitive data.
A3-10	Rogue updates	An attacker acting as a maintainer could upload a rogue or outdated update inside the vehicle making the CAV exposed to attacks.
A3-11	False maneuvers	An attacker alerts intentionally the speed, the steering wheels and/or the breaks.
A3-12	The traffic light infrastructure is altered.	An attacker takes the control of the traffic light infrastructure and remotely manipulate the status of monitored traffic lights.
A3-13	The OBU platform is altered.	An attacker infects the OBU to alters input/output signals.
A3-14	The attacker obtains a physical access to the all the shuttle's systems.	An attacker gets access to the on-board computers and systems inside the shuttle.
A3-15	The vehicle light status is altered.	An attacker alerts the vehicle light controller function.
A3-16	Car Theft	An attacker unlocks doors or opens windows, bypass immobilizer and can now drive the vehicle.
A3-17	Lock the shuttle	An attacker remotely locks the CAV making the use of the shuttle impossible.

Envisioned Use Cases (5/7)

Attacker without Supervision center/API credentials

IDA	Title	Description
A4-1	The supervision software usage is prevented.	An attacker performs a massive denial-of-service attack against the supervision software. The fleet cannot be supervised anymore.
A4-2	Supervision software credentials are leaked.	An attacker performs social engineering campaign. Credentials are stolen.

Attacker having Supervision center/API credentials

ID	Title	Description
A5-1	Information related to a site or a vehicle is leaked.	An attacker leaks information related to a private or sensitive site.
A5-2	Stored data is altered.	An attacker sends malicious data (impersonate a vehicle) or alter the data stored. The supervision cannot be performed properly.
A5-3	Remote commands are altered.	An attacker alters or spoof commands sent from the supervision center to the autonomous vehicle. The autonomous vehicle stops at a wrong stop.

Envisioned Use Cases (6/7)

Attacker without smart city infrastructure/IoT credentials

ID	Title	Description
A1-11	The infrastructure/IoT software usage is prevented.	An attacker performs a massive denial-of-service attack against the targeted IoT software. The fleet cannot communicate with the given IoT.
A1-12	An IoT software credentials is leaked.	An attacker performs social engineering campaign. Credentials are stolen. Data transferred with vehicle are altered.

Attacker having smart city infrastructure/IoT credentials

ID	Title	Description
A1-13	Information related to a site or a vehicle is leaked.	An attacker leaks information related to a private or sensitive site.
A1-14	Stored data is altered.	An attacker modifies stored data. The IoT sends altered data.
A1-15	Remote commands are altered.	An attacker alters commands sent from the IoT to the autonomous vehicle. The autonomous vehicle does not work as expected.

Envisioned Use Cases (7/7)

Attacker using rogue infrastructure/IoT to spoof the vehicle

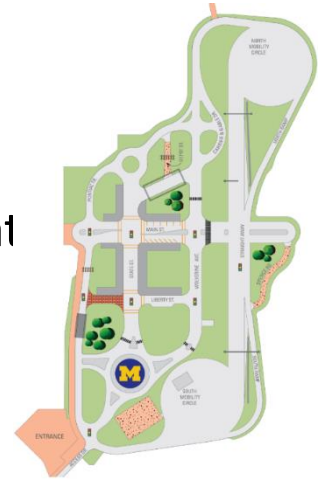
ID	Title	Description
A1-16	Remote commands are purposely wrong	An attacker alters commands sent from the IoT to the autonomous vehicle. The autonomous vehicle does not work as expected.

Attacker using a rogue connected autonomous vehicle

ID	Title	Description
A1-17	Rogue vehicle communicating to the supervision center	An attacker sends commands from the rogue autonomous vehicle to the supervision center.
A1-18	Rogue vehicle communicating with another CAV	An attacker sends commands from the rogue autonomous vPEehicle to other CAVs.
A1-19	Rogue vehicle communicating with IoT	An attacker sends messages from the rogue CAV to IoTs.

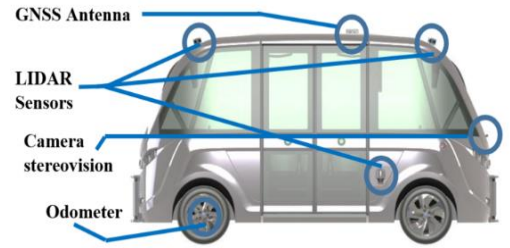
nIoVe Pilot Site #1

Category: Hybrid execution environment



Scenarios to be tested:

- **Minor issues**: blinking leds, false speedometer and fuel readings, infotainment and telemat
- **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;

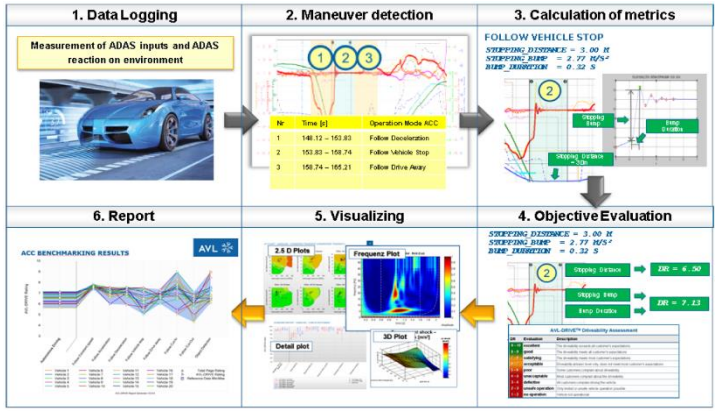
Cybersecurity experts

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

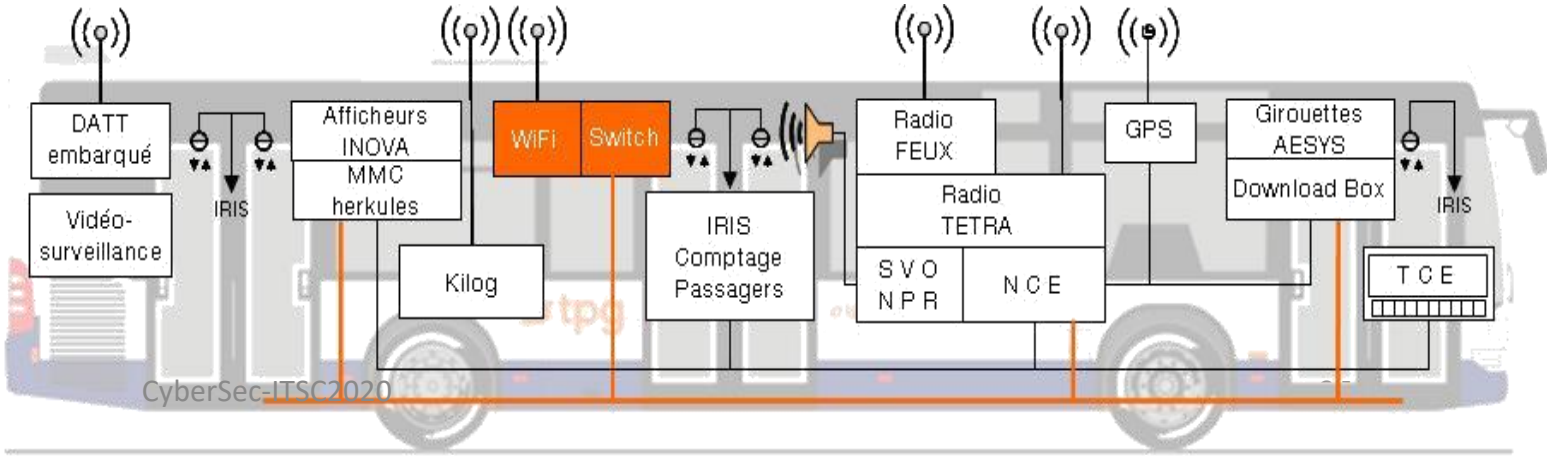
Category: Real smart city execution environment

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



Visual Analytics Suite for the IoV

Data streams from the CAVs connected devices and network are send to the cloud for analysis and visualization. VAS aims to assist the human analysts to visually spot attacks and their causes.

Main features:

- Analysis and visualization of the input data → Interactive graphs generation for analytic reporting to end-users
- AI algorithms application for anomaly detection → Visualization of their results for threat detection on the entire fleet
- Alerts for possible cybersecurity attacks → Threats detection and identification
- Enrich the pool of shared known threats
- Basis for applying mitigation strategies
- Active monitoring of the CAV fleet

Visual Analytics Suite - Algorithms

Data from the CAV network are collected and stored for analysis regarding anomaly detection and prediction of forthcoming attacks.

Algorithms:

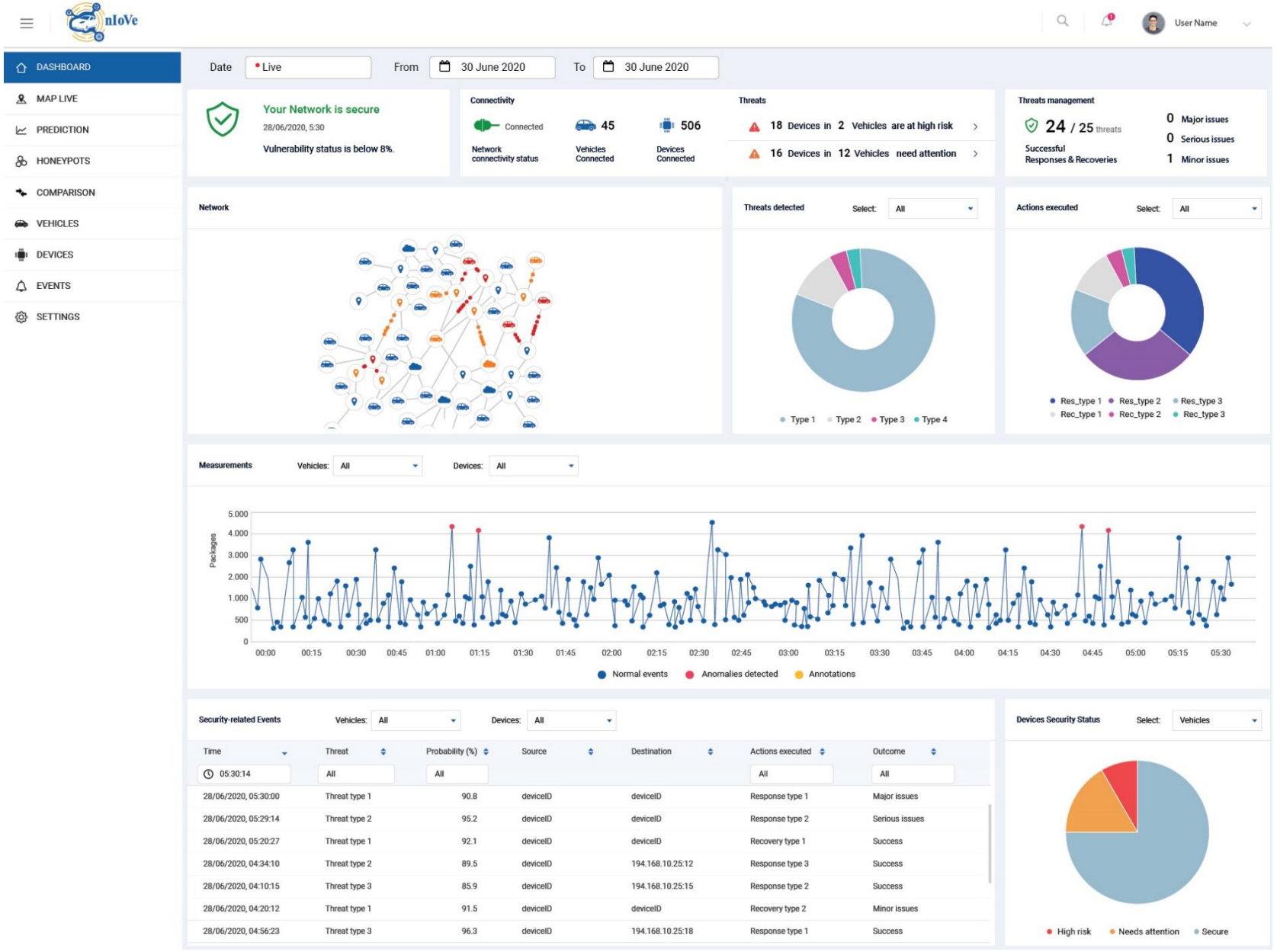
- LSTM → Forthcoming attack prediction - time series data
- Slope Statistic Profile → Anomaly detection on live data streams
- Recurrent Neural Networks, K-means, SVM → Classification of attacks from multiple variables analysis
- K-partite graph visualization →
  - Visualization of multidimensional data correlations
  - Enables the clustering of common attributes in the dataset
  - Root cause analysis and anomaly detection in an interactive way

Visual Analytics Suite – Operator functionalities

Dashboard for monitoring the CAV fleet

- The operator can monitor on real time a map with the connected vehicles
- The dashboard shows alerts about the security status of each vehicle and its components (devices, sensors etc)
- The type of threats and their descriptions are directly associated with a device of a CAV and they are presented to the operator in an understandable way
- A log status for the vehicles and the connected network is stored with analytical descriptions and timestamps
- The operator can see in real time the data values that are received from the connected components (vehicle speed, acceleration, coordinates, vehicle's internal network traffic, lidar sensor data, other sensors data etc)
  - Graphic plots with vehicle's sensor data showcase whether the CAV is operating normally or not
- Holistic monitoring of CAVs network and detected threats through various interactive charts and plots

Visual Analytics Suite – Operator's Dashboard



Types of threats detected and responses/mitigations for the selected time window

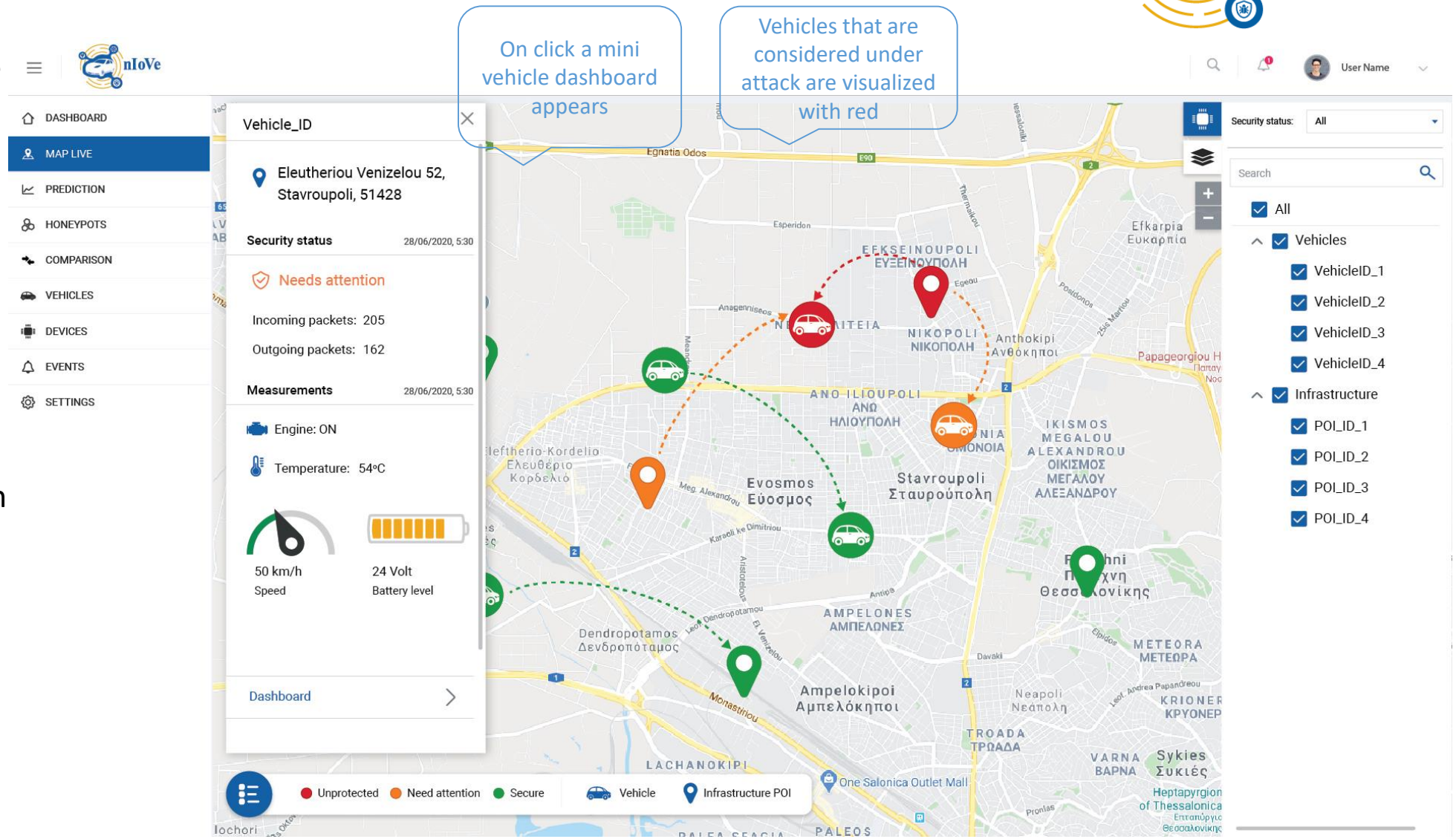
Measurements from selected sensor/vehicle/time window. Abnormalities are visualized with red dots.

Total threats detected from selected vehicles

Visual Analytics Suite – Live Map

Live map showcasing the CAV fleet with its respective information

- The user can select vehicles & points of interest (traffic lights, cloud server)
- The network connections between vehicles and point of interest are shown on the map in real time
- Vehicle status
  - **Secure**
  - **Need attention**
  - **High chance of threat**



Trust Management and Identification Platform

- **Secure communication in the IoV ecosystem** aims to ensure **confidentiality**, **integrity**, and **authenticity** of the exchanged messages
- Common solutions to provide **confidentiality** of exchanged messages
  - **Symmetric** Encryption → uses the same shared key between communicating parties
  - **Asymmetric** Encryption → uses pairs of private and public keys for each communicating party
  - Combination of symmetric and asymmetric encryption schemes
    - Usage of asymmetric encryption for the initial key exchange and symmetric encryption for the actual communication
    - Example application: Transport Layer Security (TLS) protocol

Trust Management and Identification Platform

- **Secure communication in the IoV ecosystem** aims to ensure **confidentiality**, **integrity**, and **authenticity** of the exchanged messages
- Common solutions to provide **authenticity** and **integrity** of the exchanged messages
  - Digital signatures

Trust Management and Identification Platform
Identifiers

Identifiers are used to identify specific instances, organizations, devices, people and things.

Decentralised Identifiers (DIDs)

are identifiers that do not require a centralized registration authority because they are registered with distributed ledger technology or other form of decentralized network

DID charactertisitics

- **Decentralised**
- **Persistent**
- **Cryptographically Verifiable**
- **Resolvable**

DID Syntax

Trust Management and Identification Platform
Credentials

Credentials are sets of claims (or statements), made by one entity, i.e. the **Issuer**, (normally) for another entity, i.e. the **Holder** (or **Prover**)

digital signature is the most usual type of digital proof

Verifiable Credentials (VCs) wrap the claims mentioned above with a set of metadata and digital proofs which cryptographically prove who is the Issuer of the Credentials [2]

Images taken from https://www.w3.org/TR/vc-data-model/

VC structure

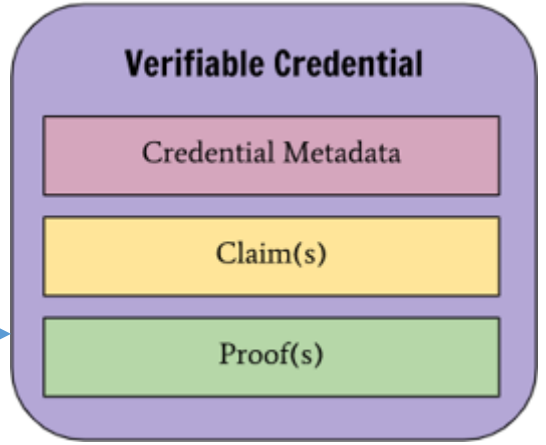


Image taken from [2]

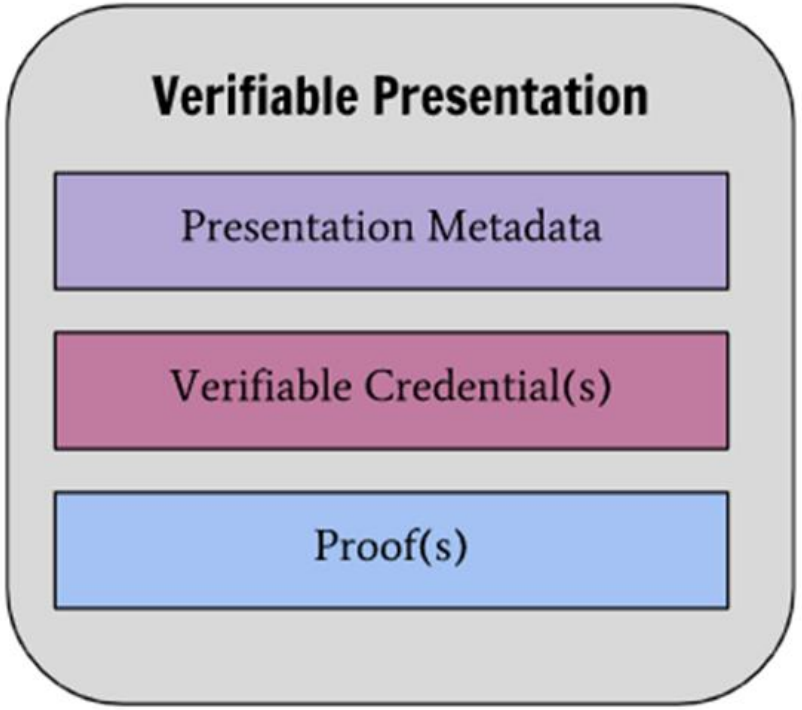
Trust Management and Identification Platform

Credential Management Systems (CMS)s are responsible for the issuing, verification, and management process of credentials.

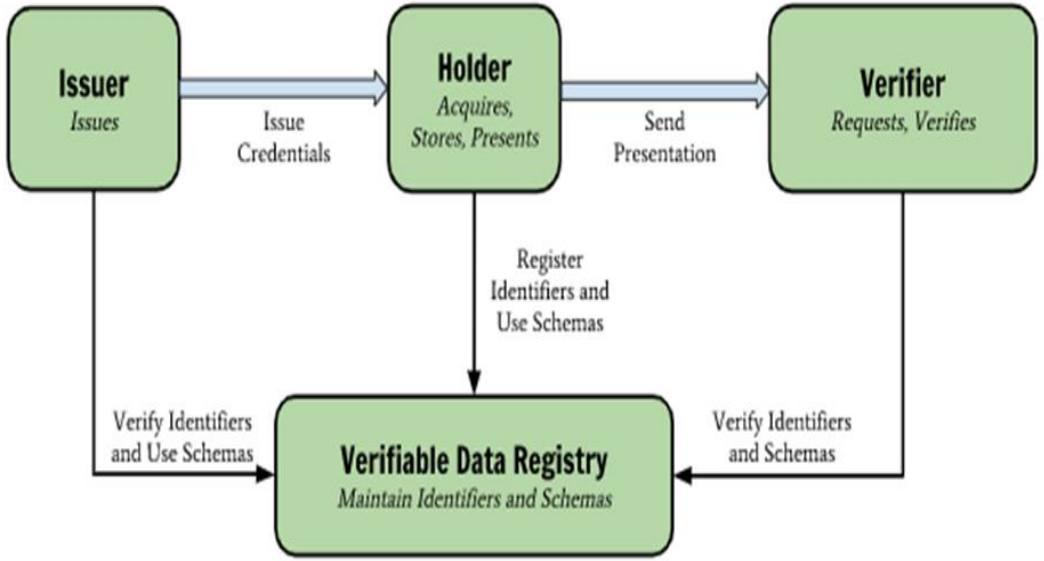
An example CMS is the Public Key Infrastructure (PKI),which manages public key encryption key pairs

Trust Management and Identification Platform
Credential Presentations and Ecosystem roles

Credential Presentations



Ecosystem roles



Images taken from https://www.w3.org/TR/vc-data-model/

Trust Management and Identification Platform Blockchain Platform Selection

- Appropriate transactions for DID management
- Good privacy and performance
- Not very complex architecture design
- Good community adoption

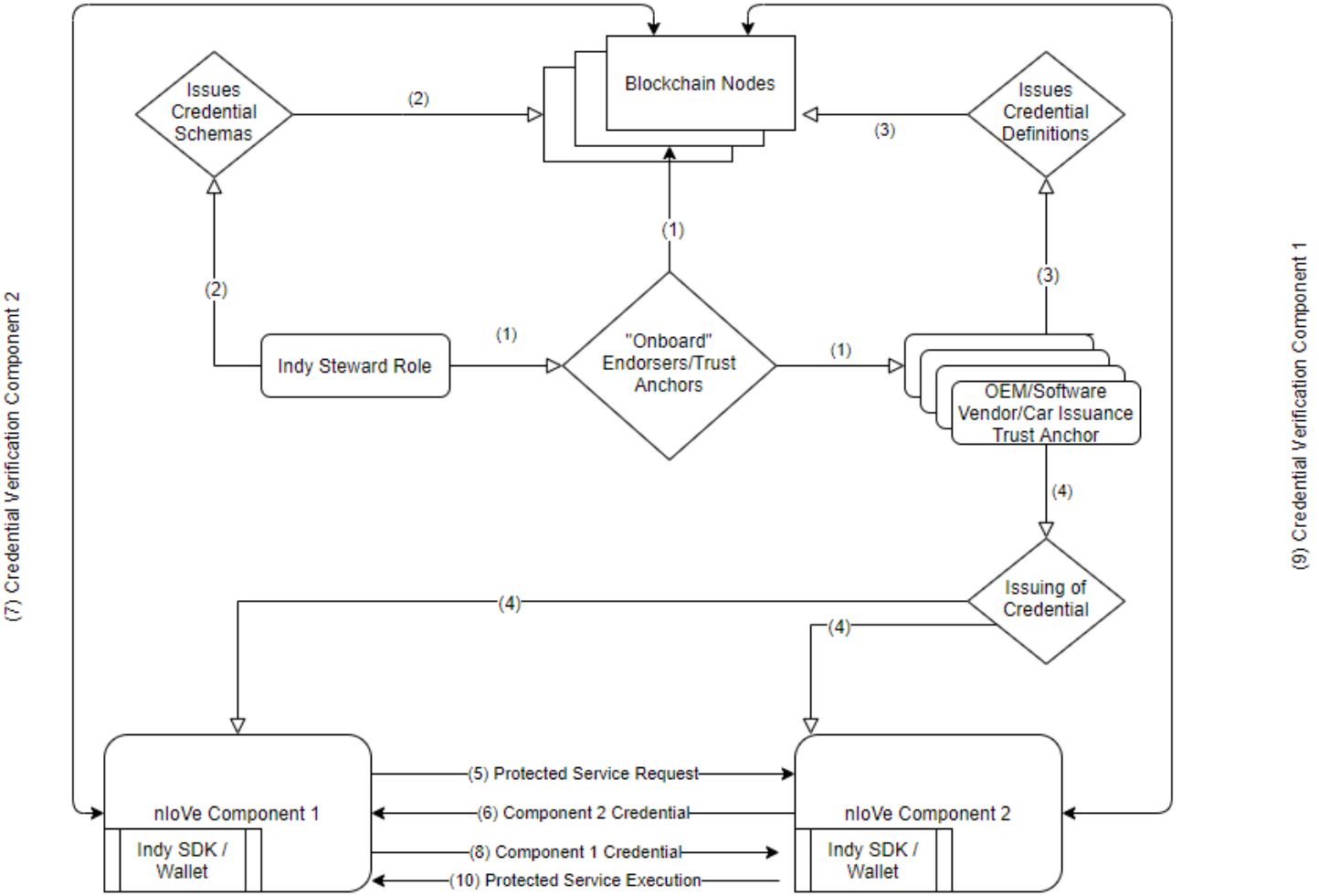
Trust Management and Identification Platform
Hyperledger Indy Roles

Hyperledger Indy Roles	Role Description
(Board of) Trustees	Trustees build trust in the network. They can create Endorsers and Stewards
Stewards	Stewards run the nodes of the network. They can create Endorsers
Endorsers	Endorsers are able to bootstrap other Users. They can publish Credential Schemas and Credential Definitions to the ledger
Users / Identity owners	They control their identities and credentials.

Trust Management and Identification Platform Processes

Process ID (PID)	Process Name	Process Description
1	User Identification and Registration	• Creation of Unique DID by the User • Secure connection establishment between the User and an Endorser • Endorser publishes the DID and verification key of the User to the Ledger • Endorser assigns role to the User
2	Authentication	• VC Presentation • VC Verification • VC Revocation

Trust Management and Identification Platform
Logical View of Communication Scenario



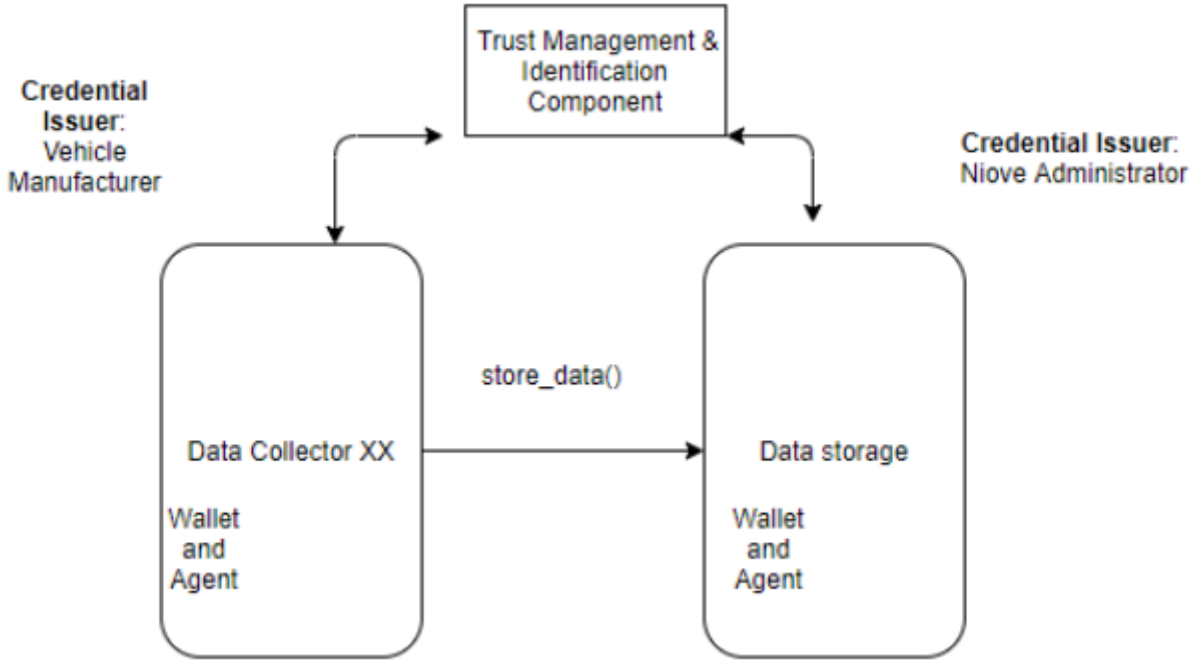
Establishing a secure communication between **nIoVe components** is of paramount importance since calling a service and receiving data from an unauthorized component could lead to the usage of tampered data in any of the fusion, analysis, response, recovery, visualization, and threat storage and sharing mechanisms of the nIoVe ecosystem, practically invalidating the credibility of the whole system.

Trust Management and Identification Platform
Identified Actors of the Communication Scenario

Table 1: Identified Actors and their Ecosystem Role

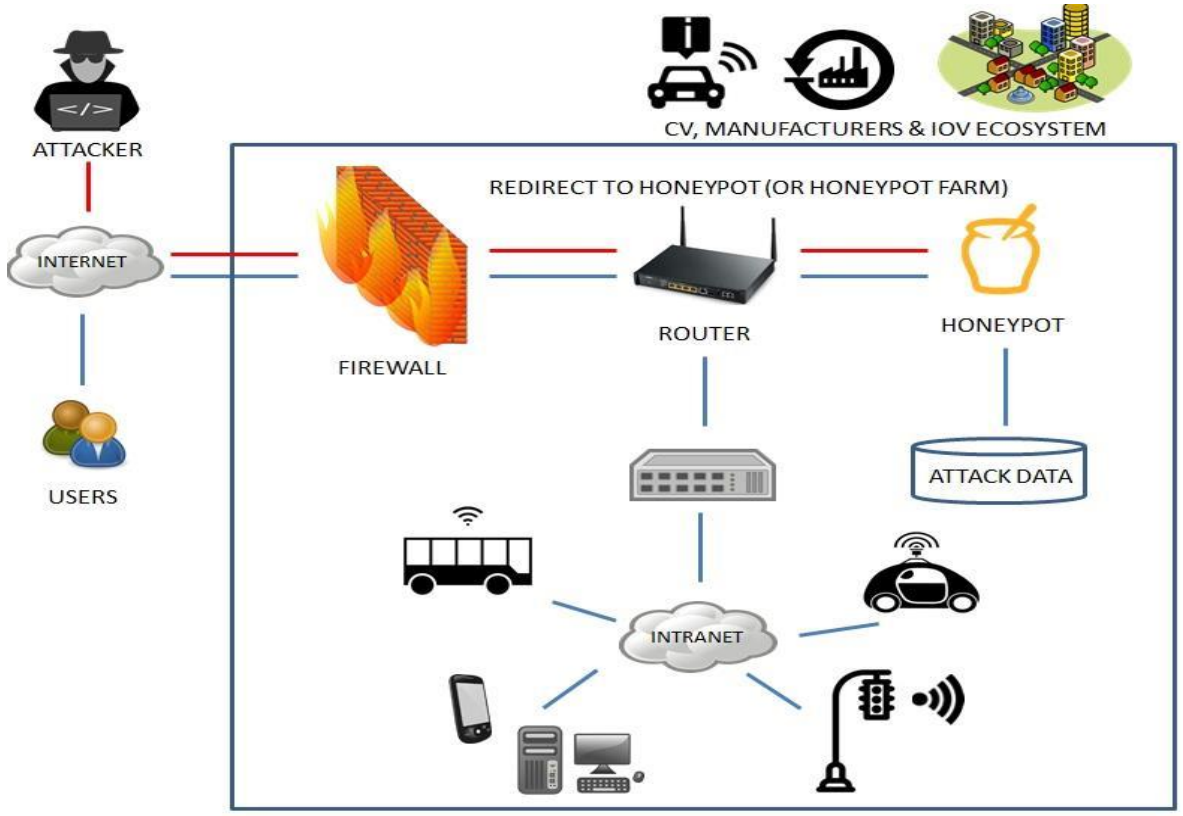
Actor	Ecosystem Role
nIoVe administrator	The issuer of Credential Schemas The issuer of Credential Definition
Vehicle Manufacturer	The issuer of Credential Definition
Data collectors	Credential Prover/Verifier
Data Storage	Credential Prover/Verifier
Virtualized Honeypots	Credential Prover/Verifier
Security Information and Event Management (SIEM)	Credential Prover/Verifier
Shared Threat Intelligence Repository	Credential Prover/Verifier
Adaptive User Interfaces	Credential Prover/Verifier

Trust Management and Identification Platform
Mutual authentication between nIoVe components

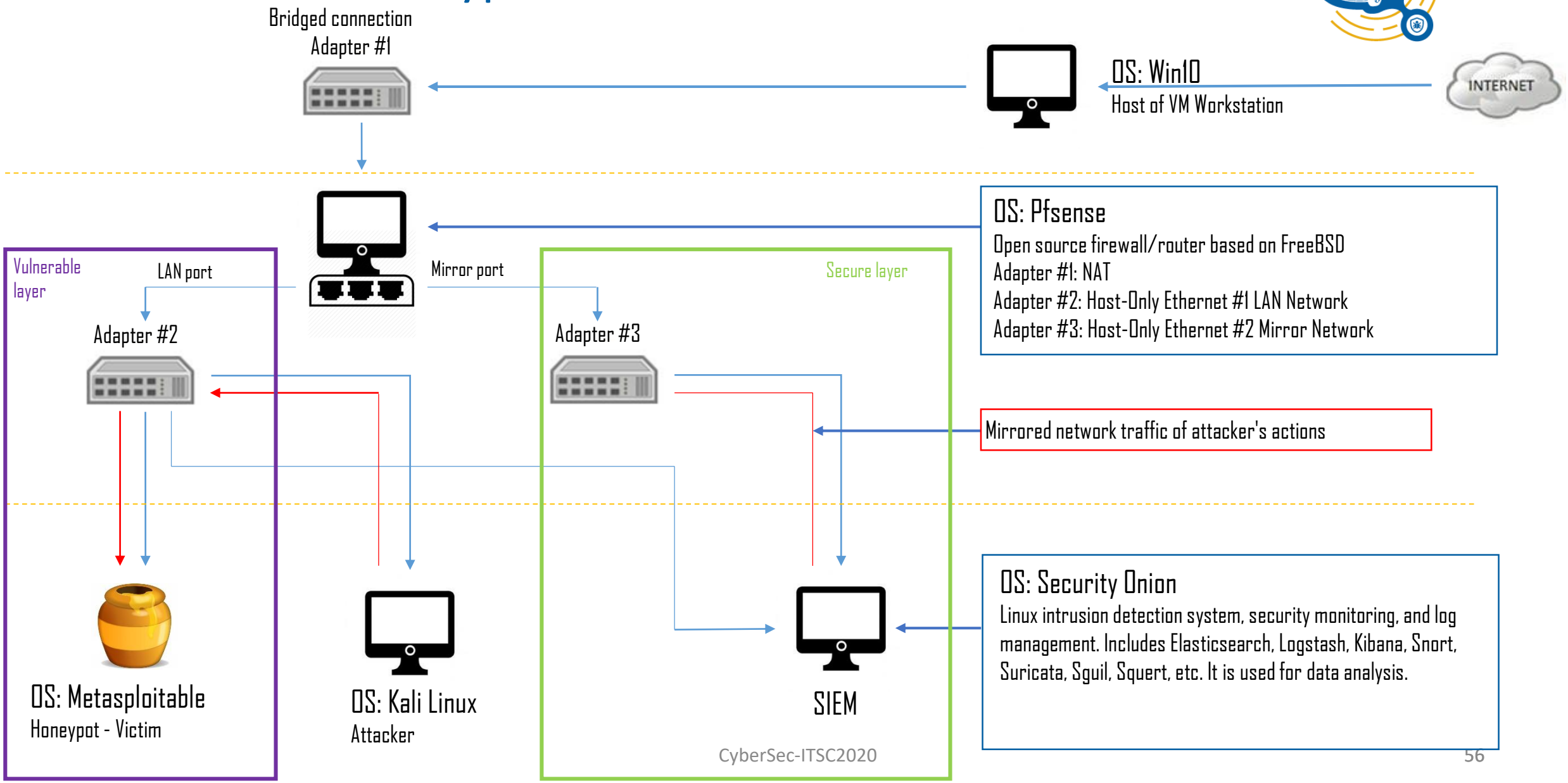


Virtualized Honeypots – Objectives

- *"A **honeypot is an information system resource** whose value lies in unauthorized or illicit use of that resource"*
- Decoy system, **poses as a legit system** offering services over the internet
- **Exposes security vulnerabilities** to attract attackers
- Owners gather information about attackers and their actions that can help **identify network vulnerabilities** and take actions to protect weak points
- **Hidden** amongst production systems
- **Looks and behaves** just as any normal system



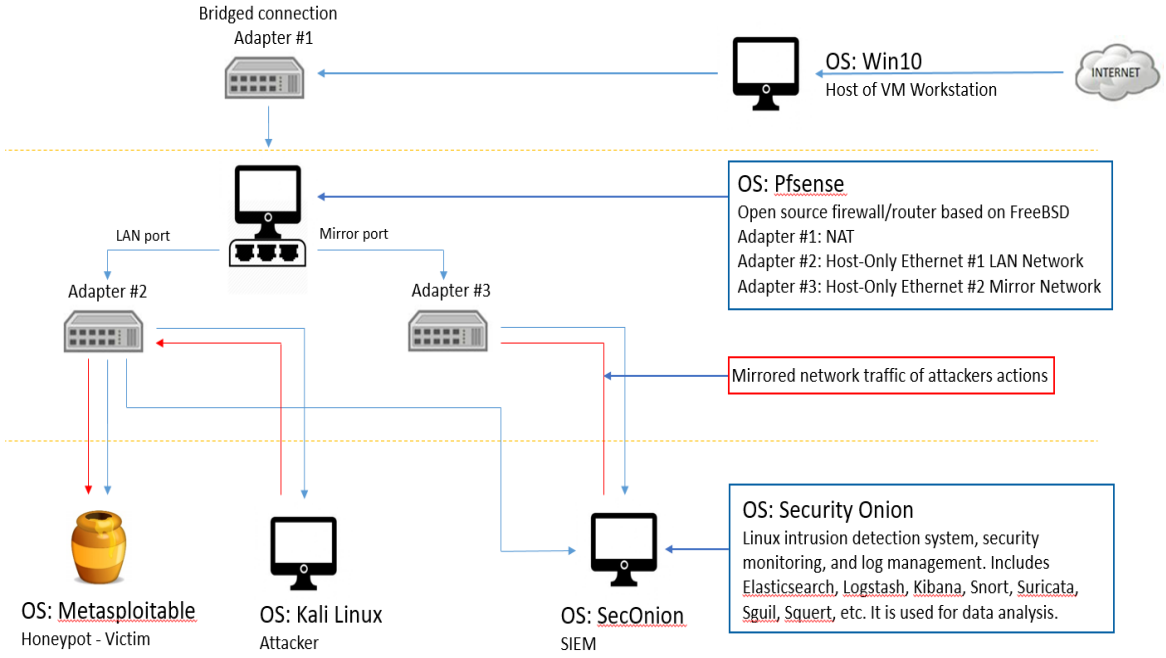
Virtualized Honeypots – Simulated Architecture



Virtualized Honeypots – Characteristics

Simulated honeypot characteristics:

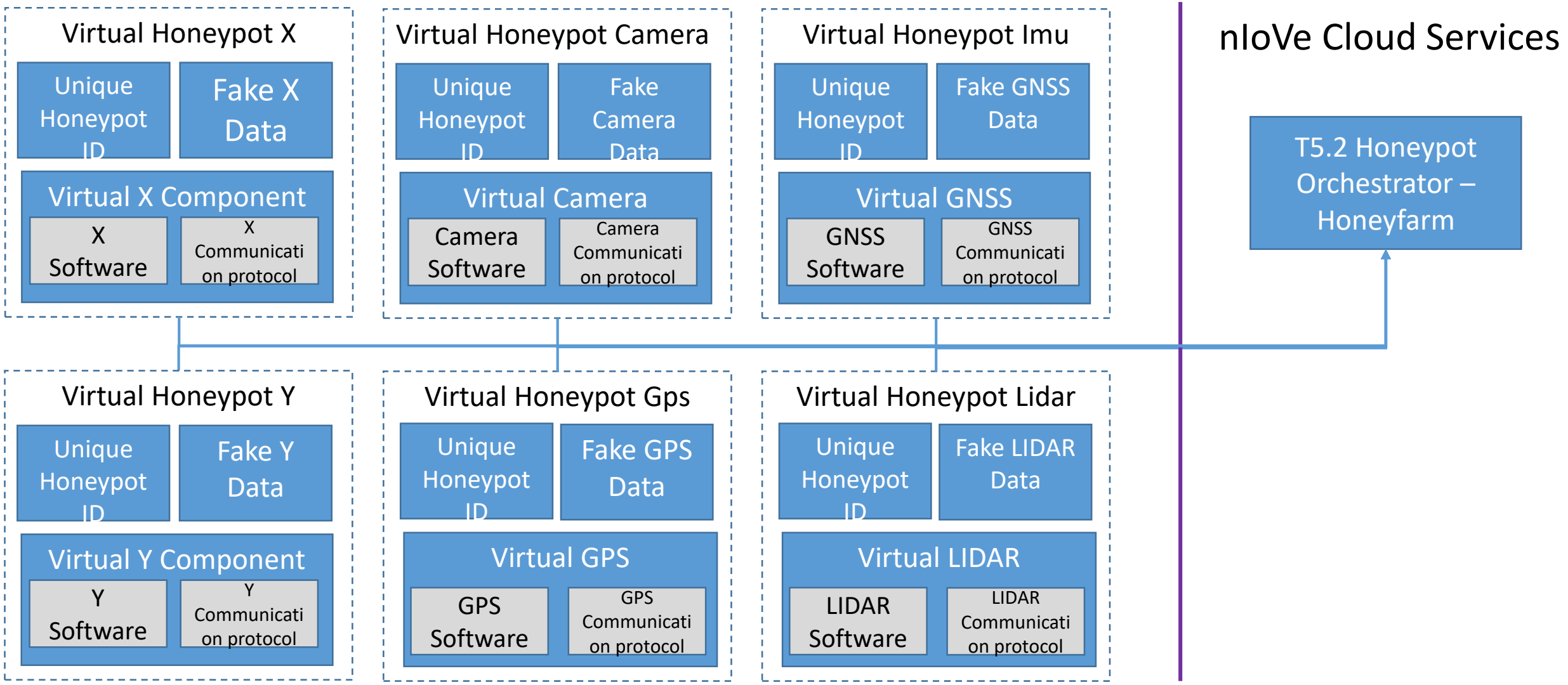
- The virtual honeypot is Metasploitable, a **vulnerable machine** used for penetration testing
- A virtual machine **hosted in the LAN** network created for that purpose (simulation of real environment)
- Acting as a regular device and appears to be in the same network as **the target application or system**
- The network traffic data (red arrowed line) is mirrored and monitored from the **SIEM** (red line)



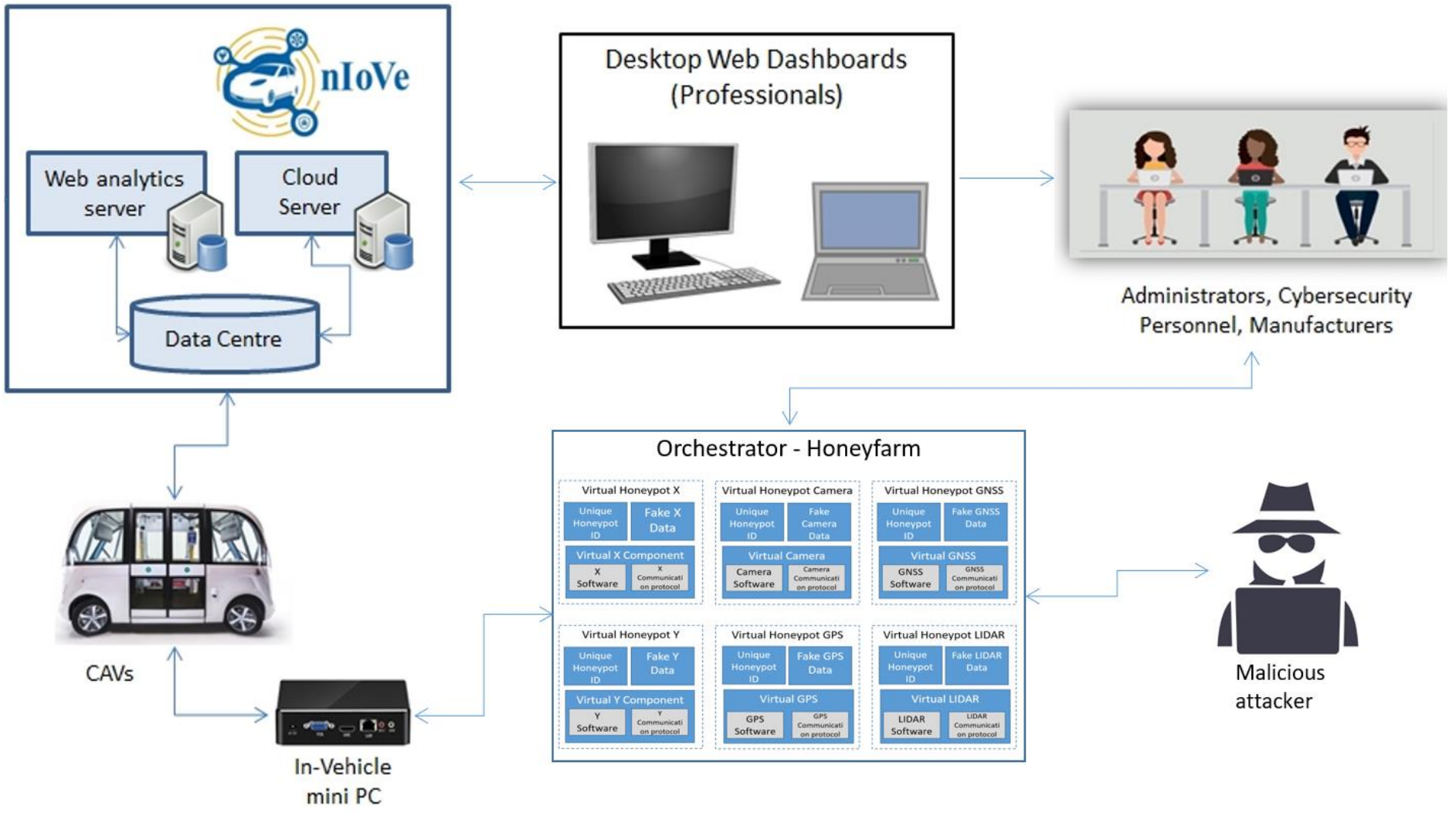
Honeyfarm for attack propagation – Objectives

1. **Root cause analysis** of the attacks on the honeypots
2. **Detect propagation trends** and discover sequential patterns based on Markov Chain Models in the honeyfarm data
3. **Rank honeypots** based on their vulnerability and the attack propagation results
4. **Prediction** of the next attacked honeypot
5. **Estimate** the relative importance of the honeypots

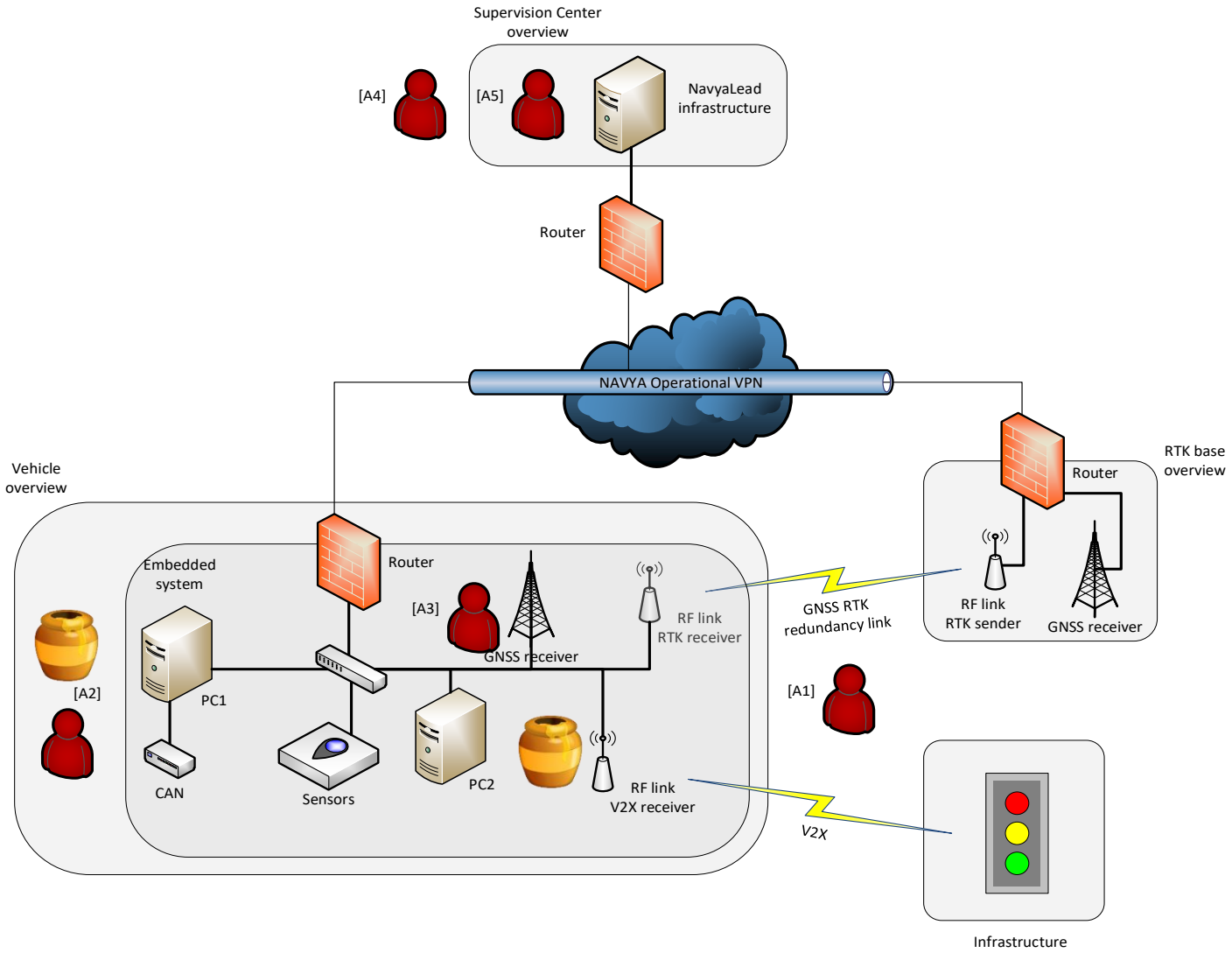
Honeyfarm for attack propagation – Architecture



Honeyfarm for attack propagation – Implementation



Honeyfarm for attack propagation – Use cases



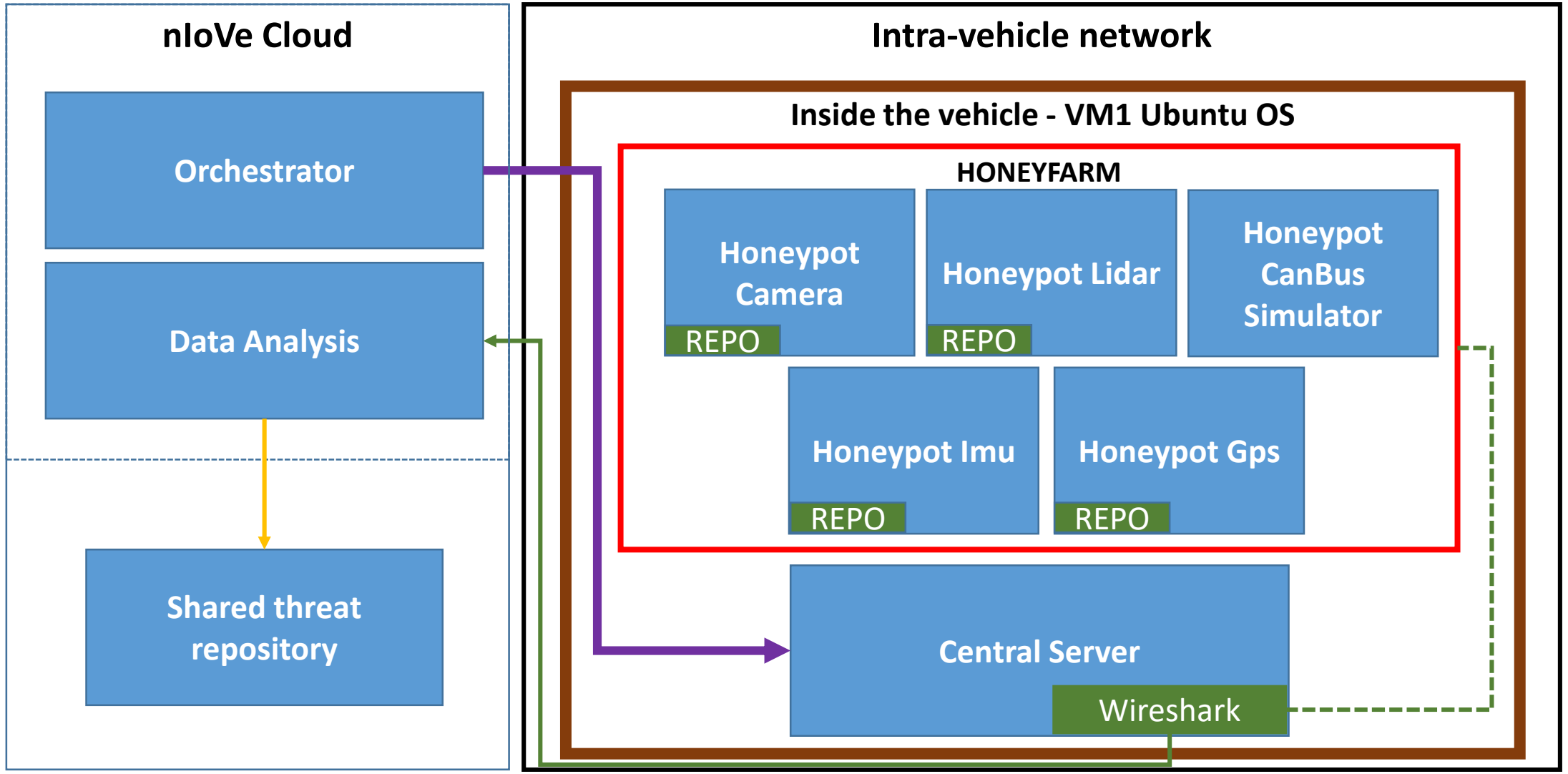
Focus on two kind of attackers:

- A2 : Attacker acting as a passenger
- A3 : Attacker acting as insider (maintainer access and knowledge)

Why?

- Honeyfarm is a combination of virtualized honeypots which will be implemented inside the vehicle

Honeyfarm for attack propagation – Development



Honeyfarm for attack propagation – Datasets

Dataset	Supported Sensors	Data Format	Route	Useful links
Ford	Lidar, Camera, IMU, GPS	Rosbag files	Detroit	https://avdata.ford.com/data/default.aspx
EU LONG-term	Lidar, Camera, IMU, GNSS	Rosbag files	Montebeliard	https://epan-utbm.github.io/utbm_robocar_dataset/

Honeyfarm for attack propagation – Markov Chains

- We consider a set of **H** which are possible to be attacked:
$$\boldsymbol{S = \{H_1, H_2, H_3, H_4, H_5\}}$$
- Define a Markov Chain on **S** in distinct time: $\{A_t\}_{t=1,\dots,n}$
- The possibility each **H** to be attacked is shown in the transition matrix
- The probability sum of each row is equal to 1, for $\forall i = 1, \dots, 5$ we have $\sum_{j=1}^{5} p_{ij} = 1$
- Each transition possibility can be estimated given a set of data transitions using the maximum likelihood estimator equation : $\widehat{p_{ij}} = \frac{N(H_i \to H_j)}{N(H_i)}$
- The transition matrix in order to have a propagation with attacks on **H**, it should be the transition matrix of an district and ergodic (concrete) homogeneous Markovian chain

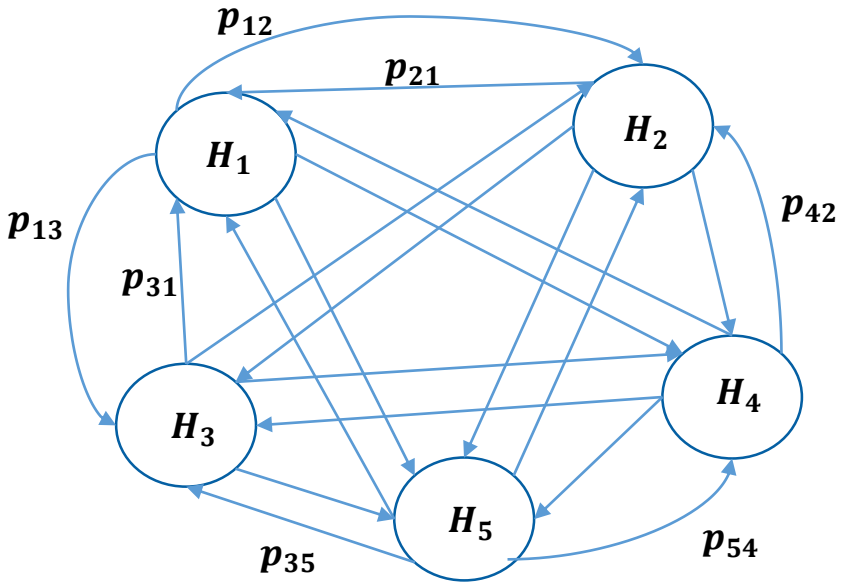
- We define as initial distribution in which the attacker chooses to attack at an initial **H** to be the distribution $\tilde{p} = (p_1, p_2, p_3, p_4, p_5)$ with $\sum_{i=1}^{5} p_i = 1$

- Define the key characteristics of each **H**, which the attacker pick out to exploit **and** examine the problem if other parameters should be considered

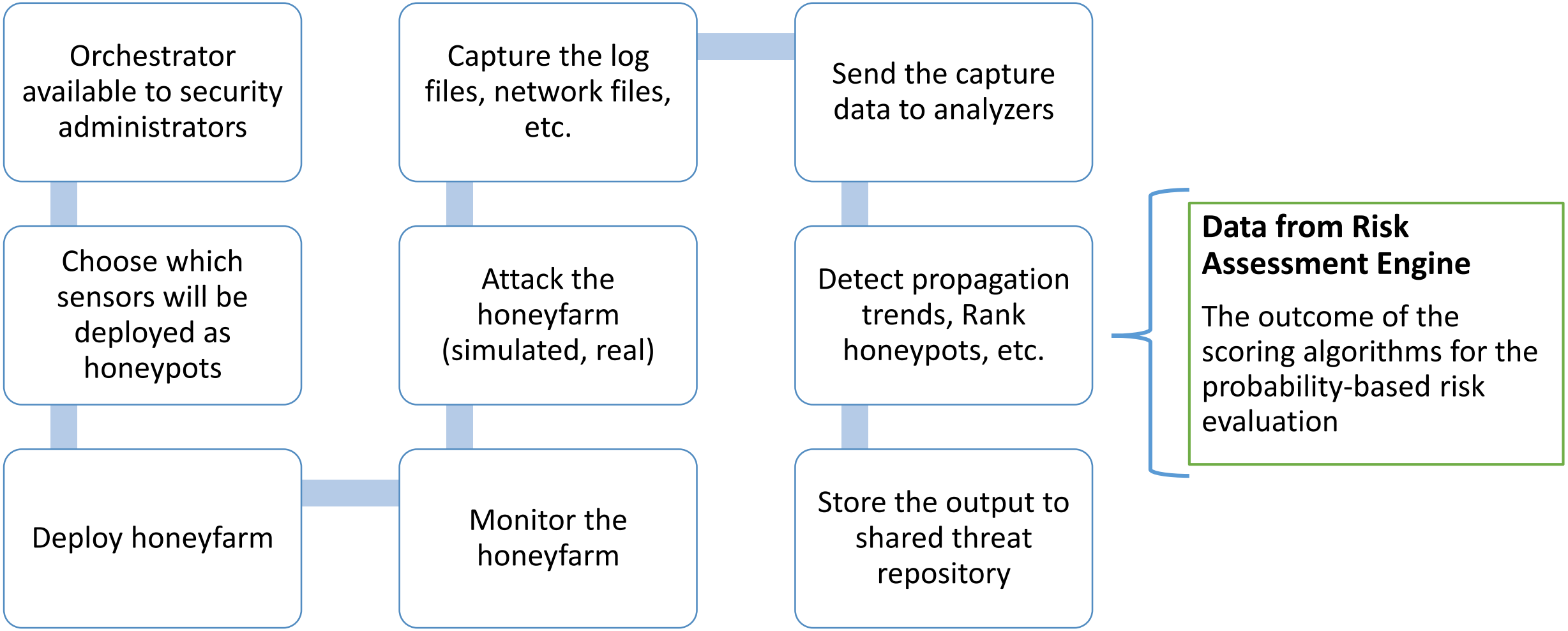
Transition matrix

P	H_1	H_2	H_3	H_4	H_5
H_1	0	p_{12}	p_{13}	p_{14}	p_{15}
H_2	p_{21}	0	p_{23}	p_{24}	p_{25}
H_3	p_{31}	p_{32}	0	p_{34}	p_{35}
H_4	p_{41}	p_{42}	p_{43}	0	p_{45}
H_5	p_{51}	p_{52}	p_{53}	p_{54}	0

Markov Graph



Honeyfarm for attack propagation – Process Steps



The nIoVe Consortium

Participant organisation name	Short Name	Country	Org. Type	Logo
Centre for Research and Technology Hellas - Information Technologies Institute	CERTH	Greece	Research	
University of Geneva	UniGe	Switzerland	Academic	
Navya SAS	NAVYA	France	SME	
Research Institutes of Sweden – RISE AB	RISE	Sweden	Research	
Argus Cyber Security Ltd.	Argus	Israel	SME	
ICT Legal Consulting	ICTLC	Italy	Law Firm	
ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS	ATHINA	Greece	Research	

The nIoVe Consortium

Participant organisation name	Short Name	Country	Org. Type	Logo
SMART ENGINEERING & MANAGEMENT SOLUTIONS IKE	SEEMS IKE	Greece	Private Company	
Technical University of Munich	TUM	Germany	University	
Transports Publics Genevois	TPG	Switzerland	Public Transport Operator	
KENOTOM Private Company	KENOTOM	Greece	SME	

nIoVe

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

Konstantinos Votis

CERTH/ITI
Kvotis@iti.gr