UNIVERSITÉ DE GENÈVE

UNIVERSITÉ DE GENÈVE
CENTRE UNIVERSITAIRE D'INFORMATIQUE

UNIVERSITÉ DE GENÈVE
GENEVA SCHOOL OF ECONOMICS AND MANAGEMENT

Dynamic Risk Assessment as a means to attain security and privacy in IoT ecosystems

CHIST-ERA conference 2022

Niels A. Nijdam

May, 2022

|—Information Security Group
|–Information Science Institute
|-Geneva School of Economics and Management
University of Geneva

Table of contents

1. Who are we
2. Activities
3. The idea

Who are we

We are the Information Security group

- Created in 2016
- 7 members (4 seniors, 3 PhD students)
- 3 active H2020 projects
- 2 upcoming Horizon Europe projects
- Strong focus on Cyber Security and Data Privacy
- Multidisciplinary:
  - Internet of Things
  - Connected Automated Vehicles
  - Smart Cities and Infrastructure

We are located at the University of Geneva, Switzerland

University of Geneva Founded in 1559 by Jean Calvin. With 19 000 students & 150+ different nationalities. Composed of nine faculties and supporting multiple centres and institutes.

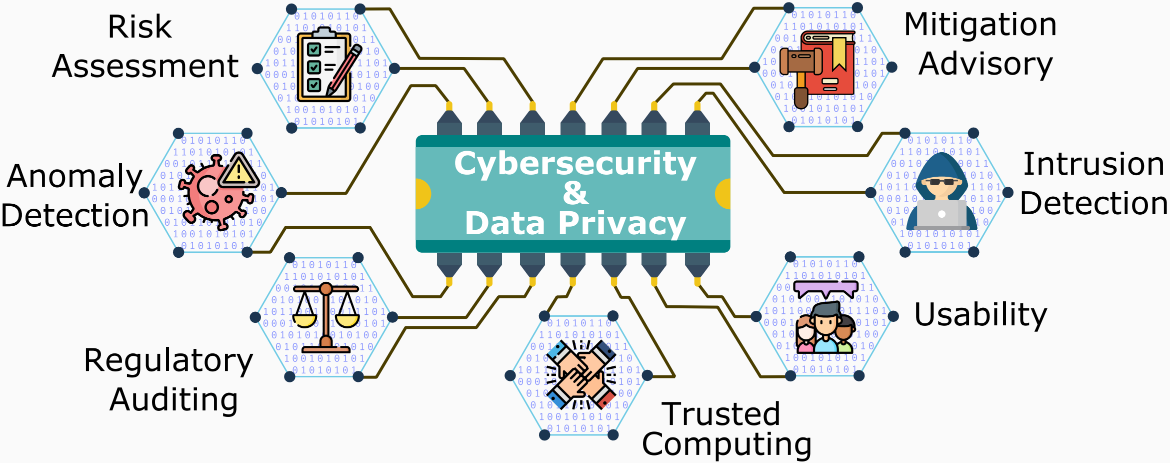
Geneva School of Economics and Management. The faculty is committed to a broad-based, multidisciplinary approach to the sciences of economics and management and is host to several institutes.

Information Science Institute. Hosting seven Laboratories.

- 30 staff members, 25+ active research projects
- Computer Graphics & Animation, Services for seniors, Geolocalisation, Cloud computing, Ecosystem of Services, Autonomic Systems, Privacy, Security, Services and Applications' Integration, Mobile systems and services
- Interdisciplinary approach to the systematic innovation in service systems.
- Large, international scientific and commercial partners' network
- Located at the Intrafaculty Computer Science Centre CUI (Batelle campus).

Activities

Research domains

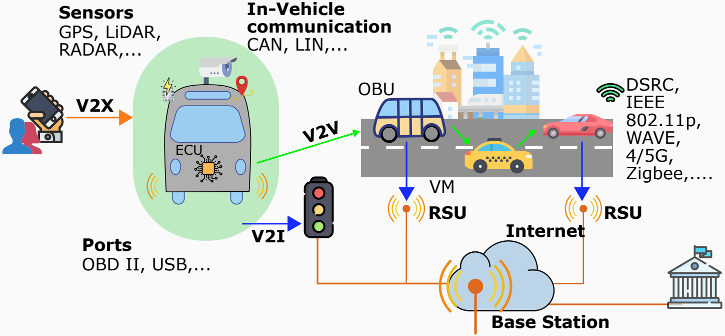


Projects

AVENUE

nIoVe

SHOW
AUTOMATED
URBAN MOBILITY



Sensors
GPS, LiDAR,
RADAR,…

In-Vehicle communication
CAN, LIN,…

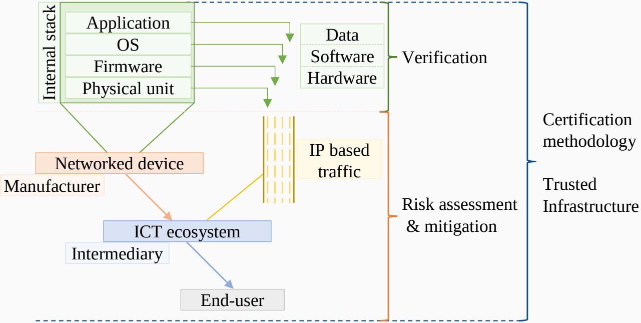
Ports
OBD II, USB,…

DSRC,
IEEE 802.11p,
WAVE,
4/5G,
Zigbee,….

The idea

Dynamic Risk Assessment to attain security and privacy in IoT ecosystems

- Automate S&P certification and verification of IoT devices and its software components
- Audit the processes and procedures upon key relevant standards and regulations leading to required certifications
- Incorporate chain of trust
- Establish S&P governance and compliance framework

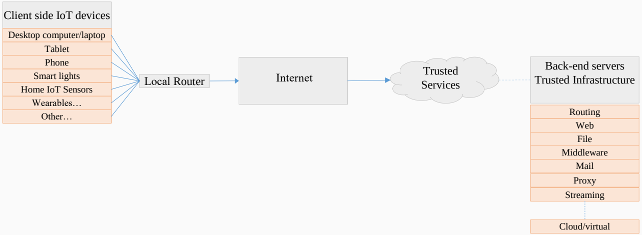


Keywords: Cybersecurity audit, trust, IoT, ICT systems, risk assessment, blockchain, verification, consensus networking, anomaly detection, behaviour profiling

Trust concept

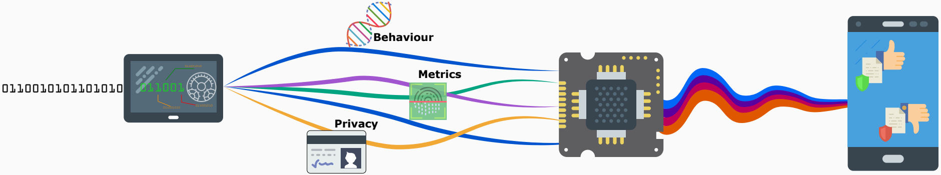
Verify the data generation and access capabilities of network devices.

- Automation of decision
- Control the balance between S&P compromise in terms of:
  - Embedded services usability
  - End-users' expectations
  - Cyber risks perception

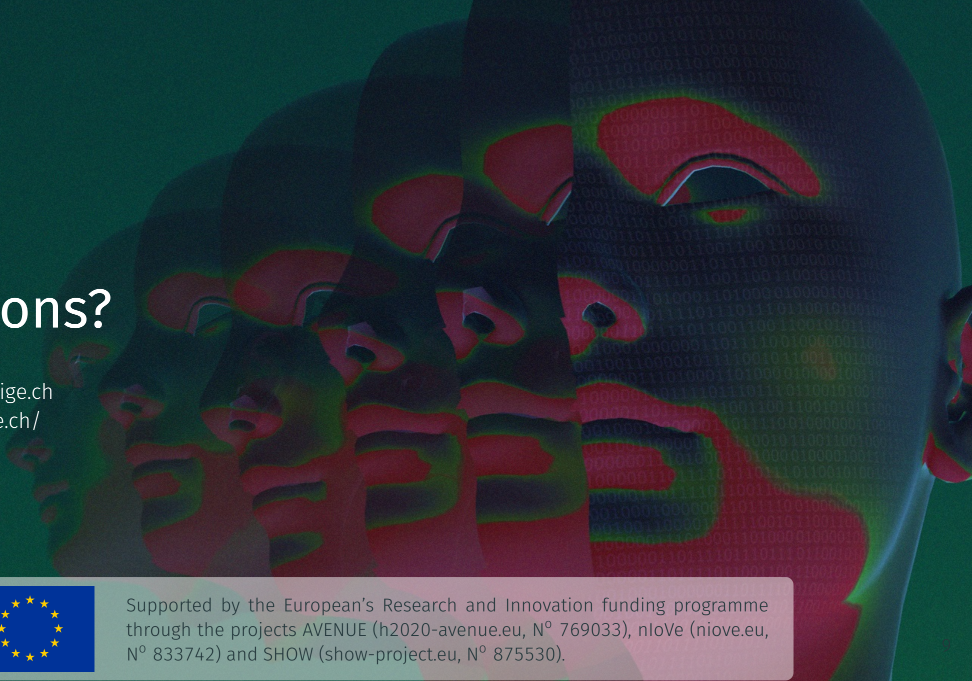


Challenges of Dynamic Risk Assessment

Leveraging two domains: cybersecurity and risk assessment.



- Continuous and automated identification of (ongoing) attacks
- Evaluation of the likelihood of associated risks
- Dynamic appointment of mitigation strategies for threat prevention
- Integrity of firmware and software with the help of certification schemes and consensus agreements.



Questions?

Niels A. Nijdam
niels.nijdam@unige.ch
https://isec.unige.ch/

Supported by the European's Research and Innovation funding programme through the projects AVENUE (h2020-avenue.eu, N^{o} 769033), nIoVe (niove.eu, N^{o} 833742) and SHOW (show-project.eu, N^{o} 875530).