CitySCAPE project

City-level Cyber-Secure Multimodal Transport Ecosystem

Daniela Tapi

The Romanian National Cyber Security Directorate – DNSC

EU Village – FIC, Lille

6th of April 2023

AGENDA

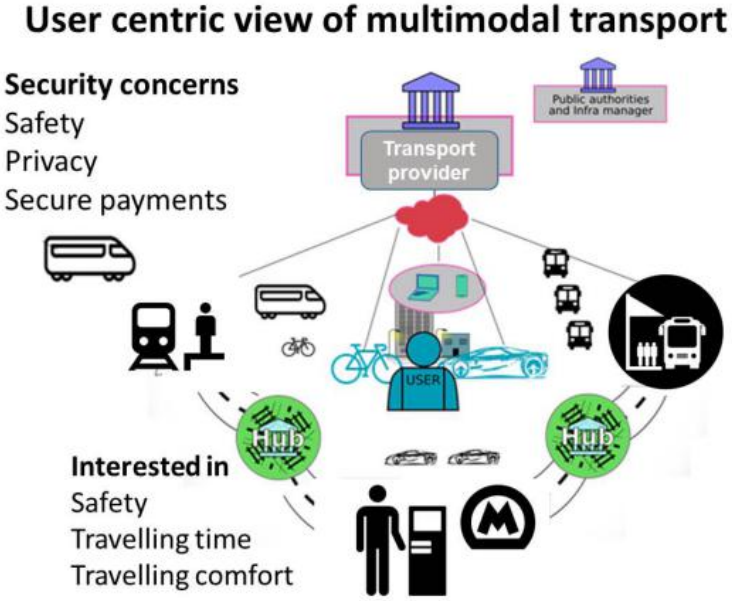
CitySCAPE project

I. Project at a Glance
II. Challenges - Cybersecurity and multimodal transport
III. Objectives
IV. Concept
V. Applications and impact

Project at a Glance

- **Call identifier**: Horizon 2020-SU-DS-2019
- **Topic**: SU-DS05-2018-2019 - Digital security, privacy, data protection and accountability in critical sectors
- **EC Funding:** 6 293 011,25 €
- **Duration**: 36 months, till 31st of August 2023
- **Consortium**: 15 partners
- **Coordinator:** Institute of Communication and Computer Systems (ICSS), Greece – Dr. Angelos Amditis (a.amditis@iccs.gr)
- **Learn more**: www. cityscape-project.eu
- **Join us**: @EUCityscape CitySCAPE Project

Challenges - Cybersecurity and multimodal transport



May 23, 2016. Dallas News reported a Texas man hacking and changing a highway sign

June 6, 2016. The Washington Post reported that Dallas road signs were hacked and messages about Donald Trump, and Harambe the gorilla were posted

November 26, 2016. The San Francisco Examiner reported that the San Francisco Municipal Transportation agency was hit with a crypto-ransomware attack, which displayed the hacker's message on their systems

May 13, 2017 The Telegraph reports that WannaCry infected German train stations, and passenger information monitors were seen displaying the ransom window

August 4, 2017. Autoblog reported that a group of university researchers have figured out how to hack self-driving cars by putting stickers on street signs

Challenges - Cybersecurity and multimodal transport

- Realization of truly interconnected transport systems
- Need for globally cyber-secure systems
- The mosaic of ICT services integrated over interconnected infrastructures makes it increasingly vulnerable to cyber-attacks
- Personal hand-held devices of users increase the system's attack surface
- Transport services relate to other NIS Directive areas that scale-up relevant cybersecurity and security-assurance challenges
- Authorities' collaboration is needed

CitySCAPE Objectives

- **Enhance** cybersecurity technologies in the multimodal passenger transportation ecosystem at city-level addressing users and data privacy concerns
- **Introduce** risk analysis tools to identify threats and their propagation mechanism focusing on transport/ digital infrastructure but also relevant in other NIS Directive critical sectors and assess the impact of a potential attack
- **Improve** the proactive approach of handling cybersecurity challenges and actively contribute to the predictability of threats in (regional) multimodal transport systems
- **Enhance** end-user engagement towards the definition and provision of multimodal passenger transport requirements about digital security, privacy and personal data protection

CitySCAPE Objectives

- Further **strengthen** the role of CERTs/CSIRTs by providing them with direct/real-time informative notifications about observed cybersecurity incidents and facilitate the collaborative investigation of incidents in line with the NIS Directive
- Significantly **contribute** to multimodal transport standards and gain experimental evidence on the feasibility of security labelling in city-level multimodal transport
- **Showcase** and **validate** the CitySCAPE solution efficiency in large scale pilot demonstrators involving all relevant entities and digital infrastructure of transport providers, under use cases of interest : **Tallinn Pilot** (July-August 2022) and **Genoa Pilot** (November 2022 -February 2023)
- **Analyze** and **outreach** the multimodal transport security market to maximize the CitySCAPE footprint and exploitation.

Concept

CitySCAPE puts the multi-modal transport ecosystem under the microscope while also considering its interplay with related critical NIS Directive sectors (energy, banking).

It introduces innovative risk analysis techniques and orchestrates a number of software solutions to realize an interoperable toolkit that seamlessly integrates to any multimodal transport system.

It allows the collaborative analysis of security/privacy persistent threats, forecasts cyber-security incidents, counteracts at highly-possible attack entry-points, assesses the impact in both technical and financial terms and finally, provides informative notifications to CERT/CSIRT authorities.

Concept

More specifically, the CitySCAPE software toolkit will:

- Detect suspicious traffic-data values and identify persistent threats
- Evaluate an attack's impact in both technical and financial terms
- Combine external knowledge and internally-observed activities to enhance the predictability of zero-day attacks
- Instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay.

Concept


Risk analysis and impact assessment engine
Financial impact assessment engine
Collaborative threat investigation platform
CitySCAPE
Training
IPS
IDS/IPS engines
SIEM as a Correlation engine with backlog of markers
Collaborative security incident response platform

Applications and impact

CitySCAPE

- ✓ will offer the **concrete technical basis** for a unique opportunity of an efficient collaborative threat investigation among a broad set of CERTs/CSIRTs by introducing **a platform capable of sharing information coming from different sources** and therefore achieve the maximization of the CSIRTs network added value
- ✓ will allow **an accurate identification of so-far under-explored/hidden privacy risks** serving the in-depth application of privacy-by-default principle and GDPR regulation in all city-level transportation stakeholders
- ✓ will **introduce and validate an agile concept of a standalone interoperable solution** to manage current cybersecurity/privacy risks across complex interconnected infrastructures
- ✓ will **estimate the attack impact on both technology and financial terms** that will drive a cost-benefit analysis on potential further investments to cybersecurity and privacy countermeasures
- ✓ will provide a scheme for **cybersecurity labelling** for City-level multimodal travel

Applications and impact

CitySCAPE

- ✓will address related security issues of mobile devices, **increasing passengers' safety** in city-level transport
- ✓will **identify and track the potential path of a cyber-attack** across the whole multimodal transport chain showcasing how an attack may unexpectedly affect modules that are not directly connected to its entry point
- ✓will **strength the CERTs/CSIRTs link to the transportation stakeholders**
- ✓will **promote best practices in cybersecurity management solutions** to the multimodal transport community and through **training of security experts** will seek to communicate their value and thus, increase their acceptance
- ✓will **fill the gap in security labelling** showcasing the solid basis of a mature EU market and rendering the compliance to standards a clear path for commercial growth

Any questions?

Thank you!

CitySCAPE

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Daniela Tapi(DNSC)
daniela.tapi@dnsc.ro

This project has received funding from the EU's Research and Innovation programme Horizon 2020 under grant agreement No 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.