Cybersecurity and Multimodal Transport Systems

For more than a century and until about 30 years ago, different transportation means served "individually" society's needs. The associated business paradigm was developed based on the principle of service provision to customers using the resources of a single mean (i.e., rail-way transport), typically orchestrated by one organization.

With the emergence of information digitization, ICT infrastructure and data communications gave an unprecedented push towards the realization of truly interconnected transport systems, mainly observed at a city level.

The emerging concept of "multimodality," as it is called the digital and organizational interconnection of the various modes and means of transport, presupposes the existence of technologically and digitally interconnected transport and fleet infrastructures, which are supported by intelligent mobility applications and compose a complete, integrated, transport ecosystem.

This ecosystem offers a lot of advantages to users and transport and infrastructure managers. On the other hand, it poses several challenges, mainly in terms of safety and cybersecurity.

One of the main advantages of a multimodal transport system is the optimization of itineraries. With the interconnection of the different means of transport, a significant volume of anonymous real-time data is collected, such as data regarding each mean's routes, the passengers' number and habits, the traffic on the roads, etc. By processing and analyzing all the data mentioned above, public transport managers have all the necessary tools to optimize the provided services, drastically reduce travel time and the related transportation costs.

Simultaneously, both the purchase of the ticket and the charging of the provided services are being facilitated. The passenger now can have a single ticket or personalized card, which they validate in any transport means they use. The data coming out of the ticket or the card usage captures the utilization rate of each means of transport and helps draw useful conclusions about the cost-benefit ratio.

However, one of the main challenges that arise from the ongoing digitization and interconnection of the various information systems lies in protecting the circulated data and the performed procedures' safety. The more interconnected the different information systems are getting, the more vulnerable to possible cyber-attacks the system is becoming. Especially in the case of multimodal transport, traditional security controls prove inadequate and there are various reasons for that. The mosaic of involved data and non-standardized data types, the plethora of diverse transport services and the strong interdependencies between software components residing at interconnected infrastructures allow threats and security incidents to propagate between assets of these interconnected networks. At the user level, the hand-held devices and mobile transport applications (e.g., ticketing) increase the system's attack surface. Moreover, transport services relate to other NIS Directive areas that scale-up relevant cybersecurity and security-assurance challenges. Authorities' collaboration is needed to handle cyber-incidents proactively.

If we wanted to present all the challenges, in simple words, we would conclude in five basic needs:

- Uninterrupted transportation of passengers
- Protection of sensitive personal data
- Coordination of the competent cybersecurity service providers
- Upgrade of the database that records possible cyber threats in a multimodal transport system

- Standardization of all data in multimodal transportation with emphasis given to the security labelling

CitySCAPE is a new innovative project, coordinated by the I-SENSE Group of the Institute of Communication and Computer Systems (ICCS). It is funded by the EU’s Horizon 2020 research and innovation programme and consists of 15 partners from 6 European countries, united in their vision to cover the cybersecurity needs of multimodal transportation. The CitySCAPE project will realize an interoperable toolkit that seamlessly integrates to any multimodal transport system. 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 and finally, instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay.

The CitySCAPE solution will be tested in two pilots that will be facilitated in the regional transport system of Tallinn, Estonia and Genoa, Italy, to showcase its effectiveness. The findings that will derive from the pilots will steer training sessions of both expert and non-expert audiences and shape the standardization contribution to security (labelling) protocols.