The benefits of a dedicated cyber security label for multimodal transport systems

Thierry Hénault[1]

[1] CS Group, Aix en Provence, France
thierry.henault@csgroup.eu

Abstract. This paper deals with the evaluation of the feasibility of a CyberSecurity Label for multimodal transport systems. The objective of the Cybersecurity Label is to verify and share if the multimodal transport information system has a certain level of security. The challenge is that assurance is expensive and existing high assurance level evaluations (such as Common Criteria) are not affordable for large and complex systems with an active update lifecycle. The aim of this innovative label process is to be less expensive and less time consuming than existing labels and to be adapted to the continuity of assurance.

Keywords: Label, Public Transport System, Cybersecurity,

1 Foreword

The aim of this publication is to demonstrate the feasibility and propose a procedure for applying a cybersecurity label to multimodal transport systems. This is the result of work carried out within the European H2020 CitySCAPE project.

CitySCAPE is a project funded by the EU's Horizon 2020 research and innovation programme, consisting of 15 partners from 6 European countries, united in their vision to address the cybersecurity needs of multimodal transport by defining a specific cyber management toolkit for multimodal public transport systems. The CitySCAPE software toolkit allows to:

- 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.

Traditional security controls and security assurance arguments are increasingly ineffective in supporting the emerging needs and applications of interconnected transport systems, allowing threats and security incidents to disrupt all dimensions of transport.

2 Relevant use cases

The creation of a label dedicated to multimodal transport systems is based on the work carried out in the CitySCAPE project, in particular the extraction of representative use cases and their associated assets, threats and vulnerabilities.

In addition, an analysis of the social, functional and technical characteristics of these public transport systems should help to define the need for a specific label. This work has been done using the multimodal transport ecosystem use cases defined by the cities of Genoa, Italy and Tallinn, Estonia, as CitySCAPE pilot site sponsors and include the following themes.

- Mobility as a Service
- Adaptive traffic control
- Infomobility
- Electronic and mobile ticketing

These use cases, while diverse, demonstrate a variety of multimodal transport scenarios that focus on the interaction of the passenger with the transport platforms and supporting system assets. They represent realistic scenarios, selected by the cities for their importance in protecting against cyber threats. The transport modes included in the use cases are: Bus, Tram, Trolley, Trains, Autonomous vehicle shuttles.
These different use cases and the proposed methodology for the implementation of a cyber Label dedicated to multimodal transport systems form the basis of the analysis and proposals contained in this document.

3 Methodology

The methodology used to carry out this study is divided into four successive stages, which make it possible to:

1. Identify the state of the art of cybersecurity standards, public transport standards and information systems labelling by integrating the results of the previous phases of the CitySCAPE project.
2. Propose a labelling process
3. Set recommendations for the establishment of a specific standard applicable to the cybersecurity of multimodal transport systems in the city.

Fig. 1. Multimodal transport system labelling process study methodology

3.1 Step 1: Market Survey

The first stage of the analysis will allow for an inventory of existing labels:

- The labels available for public transport systems and cybersecurity and their implementation methods focusing on ITxPT label [12] management retex and ENISA certifications schemes [10][11].
- Formal [5][6][7] and non-formal [15] standards applicable in the field of cybersecurity and public transport.

As result, it should allow steps 3 and 4 to examine the existing situation in order to adapt it to the context of the study.

3.2 Step 2: MPTS specificities

This step of the process will firstly allow the characterisation of urban multimodal transport systems to identify their specificities. Secondly, based on the identified specificities, an analysis will attempt to identify the cybersecurity requirements arising from the specificities of MPTS.

The result of this analysis will be used by the next step to propose specific additions to existing cybersecurity standards.

3.3 Step 3: Recommendations a Cybersecurity Standard

As part of this task, the possibility of creating a dedicated standard or an extension to an existing cybersecurity standard will be explored. Based on the Stage 2 inventory, a proposal for cybersecurity standardisation adapted to the needs of urban multimodal transport systems will be analysed.

3.4 Step 4: Recommendations for MPTS cybersecurity labelling Process

The final step will be to investigate the possibility of establishing a cybersecurity labelling process for urban multimodal transport systems. This analysis will be based on the state of the art carried out in phase 2 and the constraints inherent in the context of the transport world.

At the end of this phase, a proposal for a labelling scheme will be defined.

4 Multimodal urban transport systems landscape

Over the last decade, urban transport systems have been part of a social and environmental revolution that has led to regulatory changes that have had a major impact on

the architecture of these systems. This revolution has led to a migration of transport systems:

- from a siloed vision (by transport mode or business line) to an integrated vision
- from non-communicating systems to interoperable systems
- from proprietary systems to standardised and open systems

This transformation has had a major impact on the security of the systems, moving from safety issues to cyber security issues. At the same time, this revolution has made these systems much more attractive to potential cyber attackers. From systems with a small attack surface, limited impact and high investment, they have become, with much lower investment, systems with a large attack surface, high potential impact and high visibility.

4.1 A period of change

The study focuses on urban Intelligent Transport Systems (ITS). These assets are considered critical as they contribute to the normal operation of local public transport networks, including metro, bus, light rail and other modes of mass public transport found in smart cities. The Net and Information Security (NIS) Directive [13] has identified essential sectors of activity to be considered: transport systems (air, rail, water and road), energy, banking, financial market infrastructures, health, drinking water supply and digital infrastructure.

By identifying the operators of essential services and the providers of digital services, ITS could be placed at the centre of cybersecurity and multimodality by the ordinary citizen. ITS technologies include state-of-the-art wireless, electronic, ICT and automation technologies. Taken together, these technologies have the potential to integrate vehicles (public transport vehicles, pooling services, sharing services, on-demand services, private vehicles), system users and infrastructure. Many ITS technologies can help to optimise journeys (route planners), reduce unnecessary kilometres travelled, increase the use of other modes of transport, reduce time spent in congestion, reduce dependence on foreign oil and improve air quality. ITS has potential impacts on:

- optimal route planning and timing;
- reducing congestion;
- enabling pricing and demand management strategies;
- increasing the attractiveness of public transportation mode use;

As we have seen, over the last decade multimodal urban transport systems have become systems of systems interacting with other equipment and/or systems. In general, a distinction is made between the central system part (cloud or otherwise) and decentralised system part (onboard vehicle for example) and edge equipments. The main components of the central system are generally:

- The service planning system, which is used to plan the transport service and manage vehicles and drivers.

The Automatic Vehicle Monitoring System (AVMS), which locates, regulates and operates all vehicles to provide transport services.

- The Passenger Information System (PIS), which manages the information provided to users in different formats (text, audio, video), in different languages and through different channels (ground displays, on-board displays, social networks, website), in both normal and disrupted situations. Route management systems are one of the building blocks of PIS.
- The ticketing system, which manages ticket distribution, validation and transactions.

The European standards developed for public transport [5], [6], [7] allow information to be exchanged between these different systems. It should be noted that the field of standards is constantly evolving to adapt to new needs:

- Information on infrastructure and vehicle accessibility
- Information on the capacity of vehicles and infrastructure after the health crisis of 2020
- Information on the implementation of the service in order to establish KPIs and improve passenger service (*Operational Raw Data* known as OPRA).

The central system must also be able to communicate with external sub-systems such as:

- On-board vehicles
- Field displays
- Websites and social networks
- Ground equipment and service management systems (escalators, lifts, toilets, ticketing equipment, etc.)
- System partners which provide additional mobility services to be integrated in the overall transport offer (Bike/car/scooter sharing / pooling, parking management, taxi, ….)

In addition, communication with other multimodal transport systems is now a necessity in order to combine different transport offers and provide an european door-to-door vision of the journey. European regulations now require NAPs (National Access Points) to be set up so that as many people as possible can access and purchase the planned, real-time transport services available in a given area.

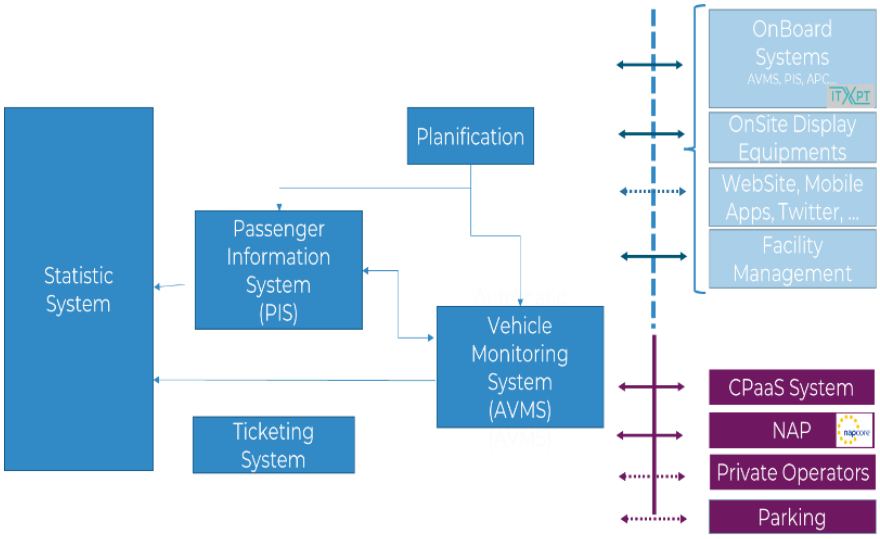

Fig. 2. : Multimodal Transport System Overview

The cybersecurity issues of multimodal transport systems only make sense to the extent that they are used by passengers. The transfer of mobility to public transport is based on user expectations, while information systems are becoming increasingly complex. Their cyber protection is one of the foundations on which they are built. Customer behaviour and expectations are at the heart of the concerns of the Public Transport Authority (PTA) and the Public Transport Operator (PTO) in defining the strategies for the development of the multimodal public transport system. This paragraph summarises a study carried out in France on the expectations and habits of travellers, both occasional and habitual, and in all types of situations nominal and disrupted.

These expectations can certainly be extrapolated to the European level and make it possible to partially qualify the specificities of the multimodal transport systems defined in the rest of this document. According to a survey carried out by MobiObserver in December 2022 [16], there is an emerging need, from the user's point of view, for real-time information linked to network data:

- Journey information (waiting time and next stop served),
- Multimodal and intermodal information,
- Bus geolocation,
- Availability of active modes (bike / scooter) at the stop.

The implementation of the services required to meet these legitimate needs makes it possible to characterise some of the emerging specificities of public transport systems, as described in the rest of this publication. The analysis of multimodal transport systems with a view to establishing recommendations for a cybersecurity labelling process poses several challenges:

- Considering the norms and standards of public transport, which for historical reasons do not cover the field of cybersecurity.
- Taking into account the standards and efforts in the field of cybersecurity, which generally address the problems of cybersecurity of information systems in a generic way.
- the acceptability of the process to be defined by the stakeholders in this field, in particular the cost-benefit ratio.
- The specificity of transport systems from a business point of view (functional and technical) and of the actors involved.
- The dynamics of the transport sector, which, for social reasons, will have to play a major role in urban mobility in the coming years, to the detriment of the private car.
- The reality and diversity of cybersecurity attacks on transport systems

Addressing these issues simultaneously through a single labelling process is a challenge. The aim is to ensure, as far as possible, that the labelled system is state of the art, considering Information Technologies security processes and measures adapted to the specificities of urban multimodal transport systems.

4.2 Multi modal transport systems specificities

The mobility sector is undergoing a period of intense change as European society becomes increasingly aware of the need to decarbonise our lifestyles.

In this context, transport is one of the main areas of development to achieve these goals. Facilitating the modal shift from private cars (thermal or otherwise) to public transport and/or active modes (cycling, scooter, walking) is the cornerstone of these new policies. The implementation of this modal shift is based on a number of societal functions that need to be taken into account in the definition of future transport systems, which are directly linked to the economic functions presented in the rest of this section.

Regulations

To implement these policies, the EU has adopted several specific regulations that have a direct impact on the functioning and design of multimodal transport systems. It should be noted that some of these regulations (NIS2, MMTIS) are currently under revision.

NIS

As part of the "EU Cybersecurity Strategy", the European Commission has proposed the EU Network and Information Security (NIS) Directive. The NIS Directive [13] is the first piece of EU-wide cybersecurity legislation. It aims to improve cybersecurity across the EU. The NIS Directive was adopted in 2016 and is currently under revision (NIS2).

Directive 2010/40

The ITS Directive 2010/40 is referenced by the NIS Directive for Public Transport ITS; the Directive aims at interoperability through European specifications and standards, and service continuity through priority actions. In the context of the ITS Action Plan, the Directive identifies four priority areas:

1. optimal use of road, traffic and travel data
2. Continuity of ITS traffic and freight management services
3. ITS applications to road safety and security
4. the connection between the vehicle and the transport infrastructure.

Within these four areas, six priority actions are identified on which functional and organizational specifications and standards will be developed: The present Study is impacted by Priority Action A for the provision, throughout the European Union, of information services (IS) on multimodal travel (data exchange and collection procedures).

A supplementing the European Directive 2010/40/EU (MMTIS)

Regarding the provision of EU-wide multimodal travel information service, this regulation concretely implements Directive 2010/40 of 7 July 2010. Its main characteristics are:

- Only static data is mandatory:
- The choice to make dynamic data available is left to the Member States.
- The requirements of neutrality, non-discrimination, or bias in the reuse of data are recognized.
- It applies to all modes of transport, public or private, collective, or individual.
- It requires standardized formatting to promote interoperability (choice of standards or specifications Transmodel/NeTEx/SIRI for public transport, TPA-TSI for rail, Datex for road).

Both regular and on demand services and personal modes are part of this regulation. Only a subset of these services is considered as part of CitySCAPE : Regular services, On-demand services, Personal modes.

Functions & services

The main differentiating characteristics of multimodal transport systems that have emerged from my study are summarised below.

Multimodality

The user is encouraged to use several modes of public or private collective transport in succession when moving in an urban environment. The multimodal operation may involve different players (Company A operating one or more metro lines, Company B operating one or more bus lines, the user using the metro and the bus in the same journey) who must cooperate to provide the user with consolidated data on his route and/or contribute to the use of a coherent network (for example to allow dynamic monitoring of connections).

The methods for exchanging information are defined on a case-by-case basis: directly between operators or via the NAPs. On the other hand, the quality of the data and the maintenance of the physical links between the players must be guaranteed by the security of the systems involved. The public transport networks of agglomerations have traditionally been based on buses, trams and metros. The implementation of these systems is generally based on dedicated systems operated by the same organisation.

While the operation of these systems remains closely linked to the associated mode of transport, the need to integrate information to improve the information required by the operator and the users leads operators to set up data centres to provide management and real-time information on the state of the network. The presence of multi-modal systems within the incumbent operators of agglomerations is now complemented by the arrival of real-time information systems implemented by private operators using new means of transport such as shared modes and pooling mode.

This observation of multimodality in agglomerations cannot be completed without mentioning the private car, the use of which will be increasingly restricted within the city. The question of the modal transfer of these vehicles to transport networks has an impact on the organisation and architecture of urban transport systems: park and ride facilities, electric charging stations are all constraints to be integrated into the future urban transport system. All these openings, from a cybersecurity point of view, are so many vulnerabilities that need to be monitored and verified.

Multiservices

After eliminating modal silos, urban public transport systems are now committed to eliminating business silos (ticketing, passenger information, operational support systems, infrastructure) and technical silos (information systems, displays, loudspeakers, electronic banking equipment, telephony, mechanical equipment, etc.). The integration of operators and traditional transport modes (rail, bus, tram, ferry) is no longer sufficient to meet the mobility needs of city dwellers.

MaaS is a system that brings together different mobility services and makes them dynamically available to users before and during their journey.

A MaaS covers different realities depending on the territory it covers, in particular the level of integration of partner systems. The emergence of MaaS at the local level will reshape the urbanisation of the urban mobility system. As mentioned above, the transport system will want to cooperate with other transport systems, local or distant, to form a system of systems. If the potential cybersecurity vulnerabilities created by these new platforms are not considered in advance, this social and technological revolution could be accompanied by its share of cyber-attack campaigns.

Accessibility

To make public transport networks accessible to as many people as possible, it is necessary to take account of accessibility requirements when preparing and carrying out a multimodal journey. To this end, the European standards for the exchange of information (NeTEx / SIRI) offer various services to define and update the relevant data.

The concept of accessibility is defined by CEN in its white paper (Support for Accessibility in NeTEx [14]). As NeTEx describes the public transport representation for

each mode of transport (rail, bus, metro, ferry, new modes), it also allows the description of accessibility and facilities for locations on the network (stations, airports, bus stops, etc.) and transport services (on trains, buses, etc.) accessibility data, including physical limitations, facilities and assistance services.

The status of changes to lifts, elevators and human assistance services should be updated in real time to allow passengers with mobility impairments to change their travel strategy or to allow travel planners to suggest new routes or navigation paths. This information must be available to users thanks to the SIRI Facility Monitoring Service.

Technical

Interoperability

Interoperability of multimodal transport systems is about ensuring that they can exchange and use data as far as possible with a common understanding of the concept carried by the data. For example, the term "stop" can have different interpretations: bus stop, platform, station, group of stops.

Without a common interpretation of the concepts, the interfacing systems cannot interoperate. The concept of interoperability is stronger than the concept of physical interface, as it presupposes a common understanding of the data by the different actors using it on the different systems. In this respect, efforts to standardise the exchange of transport data are a strong vector for improving the level of interoperability of urban transport systems by defining conceptual data, Exchange formats and Exchange protocols.

Over the Air component

Multimodal transport systems include an air link that allows data to be exchanged with different components. These are (non-exhaustive list) the links between the central system and vehicles, field agents and some ground displays.

The protection of this air component must be taken into account when assessing the cyber security of an urban multimodal transport system.

Legacy Systems

As system, multimodal transport systems will inevitably consist of legacy systems that may have been designed without cybersecurity constraints in mind. Special attention must therefore be paid to these historical components of the overall system from a cybersecurity perspective.

Data protection and integrity

The security of transport data (planned, actual and statistical) is vital for transport network operators. Compromise of this data could lead to a loss of user confidence in the reliability of transport networks and undermine the whole European policy of shifting travel towards more environmentally friendly options.

The security of transport data (storage) and its exchange is therefore essential for the credibility and paradigm shift of people's mobility in Europe.

5 Dedicated labelling process

The aim of this part is to describe a labelling process for multimodal transport operators to help them maintain a certain level of security for their information systems. To define this labelling process for operators of multimodal transport systems, three documents were required:

- An innovative assurance methodology defined within the CitySCAPE project, from risk analysis to assurance activities for critical and non-critical components.

The main characteristics to be considered for multimodal public transport systems are:

a. low cost,
b. repeatable,
c. not very restrictive
d. and adapts the assurance activities according to these needs.

- The Evaluation Methodology document of the Common Criteria [1][2] is used to provide a more technical understanding of how a functionality test and vulnerability analysis are performed. This document is therefore used to precisely define the assurance activities of the label.
- ANSSI's document "Assessment methodology for first-level security certification - Content and structure of the RTE"[16] was a source of inspiration to define the guide for documenting the follow-up labelling. Its sister document “Criteria for the evaluation for a first level security certification” [17] helped it to shape the labelling process and assurance activities.

In recent years, cybersecurity has become increasingly important in various sectors due to threats from cyber attackers. Cybersecurity improvements (standards, recommendations) have been made in several sectors, such as health and energy, but not yet in the multimodal transport sector.

The aim of this cybersecurity label is to verify that the multimodal transport information system has a certain level of security. The challenge is that assurance is expensive and existing high assurance level assessments (such as CC) are not affordable for large and complex systems. The objective of this label is to be less expensive and less time consuming than existing cybersecurity labels and to be adapted to the assurance continuity to be adopted by manufacturers and operators of multimodal transport systems. The CitySCAPE project, based on the use cases of Tallinn and Genoa, has made it possible to identify the required assurance levels using the following three parameters:

- Risk Levels: This is the critical level when a component is attacked. This level can be assessed higher when it is a component linked to sensitive confidential data, a component essential to the operation of the system, etc.

- System component exposure: the level of assurance of a component also depends on its exposure to attacks. The more a component is exposed, the higher its level of assurance must be.
- System Component Lifecycle and Update Frequency: This setting helps to assess how often the label should be reviewed.

Two different needs for the level of assurance are identified:

- A high level of assurance for a small part of the system, which may involve personal security problems, financial transaction problems, or when the exposure is very high.
- An average level of assurance for most of the system including end-user traveling experience and potential targets for cascading effects.

Thus, it is necessary to distinguish critical components from non-critical components. Components deemed critical must have an individual assurance assessment that guarantees a high level of assurance. Components deemed non-critical need overall system protection provided by the proper configuration of network equipment, such as firewalls, IDS/IPS and SIEM.

5.1 The labelling process

The labelling process for multimodal transport systems relies on three components:

- The process itself which is composed of nine interdependent stages.
- The stakeholders involved and in charge of monitoring the process.
- The labelling process follow up document which support the process.

The award of the label is based on the implementation of the different stages listed below. Each stage contributes to the implementation and verification of good practices in the field of security for multimodal transport systems.

Preparation

This stage consists of 2 sub-phases. The risk identification/ analysis phase can begin before the official application, thereby speeding up the process of awarding the label.

Stage 1 Candidacy

Contact and application with an identified organization to validate this label, and consideration of the procedures to be completed.

Stage 2 Risk Identification & Analysis

Risk analysis at a system level to have a global vision of the most critical risk and asset exposition.

Stage 3 Critical / Non critical components identification

From the risk analysis, define critical and non-critical components to have adapted assurance activities.

Stage 4 Security Target for Critical Components

Identify a security target for each critical components so the components will be clearly defined.

Stage 5 Assurance activities for critical components

Assurance activities the evaluations for critical components: Security target evaluation, specification evaluation, functional tests, and vulnerability analysis.

Stage 6 Protection of non-critical components

It consists of the protection of non-critical components by the network components, and verification of evidence which prove that they are in fact non-critical components (evidence from risk analysis above).

Stage 7 Third party verification

Third Party verification is required to prove that all the label process has been followed, and all parts are clear and well-filled.

Stage 8 Label delivery

Label delivery when all the requirements to obtain the label have been validated by a certified organization.

Stage 9 Label Contiuity

Management of the system to remain in compliance, management and continuity of the label as part of these activity the label could be maintain, extended, cancelled, suspended.

5.2 Risk Analysis

Methodology for carrying out this risk analysis is based on CitySCAPE work. It describes a top-down approach to properly define all assets. This means identifying composite assets, which are assets at a system level, and then breaking them down into basic assets. This asset-centric approach, which considers all types of assets (hardware, software, connectivity, data, users, etc.), optimises the effort required to perform risk analysis and remains focused on multimodal transport systems.

The methodology allows a dynamic risk analysis to be set up as needed, updated in real time and equipped to facilitate management (thanks to the CitySCAPE toolkit). This decomposition is important to identify the threats and vulnerabilities associated

with the basic assets. The risk analysis of the multimodal transport system follows the following steps:

1. Identification of Assets – which includes the process of identifying the tangible or intangible entities of the system that have value and should be protected.
2. Organisational domain mapping – which includes the architectural view of the system/organisation.
3. Threat modelling – which contains the identification of threats for the system, including cascading threat analysis.
4. Elicitation of security vulnerabilities – which contains the definition of security vulnerabilities.

Once these tasks have been completed, the risk can be identified. From the identified risk, the following steps will be to define the likelihood and probability of the risk before being able to level it. The CitySCAPE project has developed a dedicated risk analysis methodology for multimodal transport systems "Multimodal Transport Chain Risk Assessment" (MTCRA) methodology and has been implemented as part of the CitySCAPE RITA tools.

Other approaches are of course possible. ENISA's work on reconciling risk analysis and assurance level methodologies is available [3] and has been analysed as part of this study. This common approach, like that of the Common Criteria or ISO 27xxx series [8][9], does not meet the objective set for the dedicated Multimodal Transport System label, independent of certification, which is positioned as a first step towards certification by validating a set of cybersecurity best practices throughout the system lifecycle.

Part 1 Identification of Assets

The identification of activities is based on a top-down approach. The first analysis identifies the composite assets and their interactions. For each composite assets, this list must contain the following elements: Composite asset ID, Composite asset name, Composite asset description.

To facilitate this identification, it is recommended to create a high-level overview diagram of the composite assets and their interrelationships. The second step is to identify and list Basic Assets, as already done for Composite Assets. Basic assets are assets that make up composite assets. For each basic asset, this list must include the following elements: Basic Asset ID, Basic Asset Name, Basic Asset Type.

The CitySCAPE project has described the top-down approach for decomposing and representing the system and its composite assets. The breakdown of the composite assets into basic assets then allows them to be matched with the identified threats.

Part 2 Threat modelling.

Once the composite and basic assets have been found, the developer needs to identify the associated threats and their impact. For each threat, this list should include the following elements: Threat type: this can be software, hardware, network and/or data, Threat ID, Threat name or short description, Impact of the threat: whether the threat affects the confidentiality, integrity and/or availability of data.

To get a better idea of the impact of these threats on the assets, the developer should list all the threats that have an impact on each asset.

Ideally, Cyber Threat Intelligence should not be overlooked in risk assessment and threat analysis, particularly when it comes to characterising potential attackers (motivation, means and opportunities). The availability of dedicated investigation tools can thus contribute to the relevance of the analyses carried out.

Part 3 Elicitation of security vulnerabilities

Finally, the last step of this risk analysis is to list the vulnerabilities facing the information system, and to link them to the identified threats. For each vulnerability, this list must contain the following elements: Vulnerability ID; Vulnerability description, Threat ID, Threat name or short description. Then, the vulnerabilities related to the multimodal ecosystem are presented and associated with the threats, to form a triplet (asset, threat, vulnerability) that will be used for risk evaluation. A vulnerability can be linked to several threats.

5.3 Critical / noncritical component identification

After the risk analysis, the next step is to identify the sensitivity of each system component and to know which components are critical or non-critical. The necessary parameters to be able to assign an assurance level to a component are:

1. Capability for assurance assessment: to identify the sponsor's assurance capacity and available resources for labelling (e.g. human and financial resources). This should be used to determine the maximum number of critical components.
2. Level of risks : As part of this approach, only those system assets exposed to the most critical risks are considered critical.

If too many critical components are identified relative to the assurance assessment capacity, a reassessment of critical versus non-critical components shall be considered.

3. Size of the critical sub-system: It is possible that too many critical components have been identified. This may be due to a low maturity of the risk analysis. In this case go back to step 1 (Capability for Assurance Assessment) or revise the risk analysis. It may also be because the assurance requirements are too high (sensitive systems).

Classification of components could be done using the following parameters :

- Exposure of the component: The most exposed components (e.g. those exposed to the Internet) are the most likely to be attacked.
- Feasibility of high assurance evaluation of a specific component: This parameter corresponds to the feasibility of the assurance activities according to the resources available. In fact, some components are too complex and make evaluation too expensive. The most effective evaluation should be selected in accordance with the Label Acceptance Body(LAB).

If there are still too many critical components identified, the sponsor is free to choose which components are considered critical (if possible with the recommendation of the LAB or assessor). An organizational domain mapping will support this identification.

5.4 Security target Definition

The identified critical components require an advanced evaluation process based on the concept of a security target (in the sense of CC). A security target (ST) is defined for each critical component. This concept, derived from the Common Criteria, is the cornerstone of the security assurance policy as it defines and specifies the problems faced by the system under evaluation. A security target will be defined by:

- Target Of Evaluation overview.
- Security problem definition including:
  - Assets to be protected by the TOE.
  - The threats that are to be countered by the TOE.
  - Assumptions.
- Security requirements (security functions to be evaluated).
- Security requirement rational that demonstrates that the identified security requirements are covering all identified threats. This includes showing that each threat and assumption is addressed.

The central point of the security target for multimodal transport systems is the relevant identification of security issues to identify threats to the different components of the system.

5.5 Assurance activities for critical components

The assurance activities implemented for critical components within the labelling process for multimodal transport systems are based on an asset-centric assurance methodology, as recommended by the CitySCAPE project, which focuses on assets assessed as critical, considering that the security of non-critical assets is mainly based on the system design.

Part 1 Security Target evaluation

As recommended by the CitySCAPE assurance methodology designed for multimodal transport systems, the validation of the requirements and scope of the security target is the first step in the assessment of the system with a view to label award. It should be noted that unlike the assessments carried out as part of the CCs, those carried out as part of the labelling process can be carried out directly by the end user without going through an approved laboratory.

It is the responsibility of the end user to check that all the required information is included in the Security Target and that the justifications are consistent.

Part 2 Specification validation

The objective of this evaluation task is to verify the existence and validity of the functional specification of the TOE and its interfaces against the security requirements defined in the ST. Interfaces include all connections to external entities. This step provides direct assurance by enabling the evaluator to understand whether the TOE security functions (TSF) meets the claimed Security Functional Requirements (SFRs). For this task evaluation, developers need to identify all TSF accessible through the TOE interfaces: HMI, API, Network interfaces, Physical interfaces.

Once the TSF are identified, for each of them, developers must describe:

- The purpose and SFR enforced (extract from the ST),
- Interfaces and exchanged data,
- Description of operations,
- Logs and error messages,
- How to configure the function (parameters).

The existence and the validity of the functional specification of the TOE and its interfaces will be evaluated by the end-user in this task to verify that they meet the security requirements in the security target.

All security functions accessible through an interface shall be provided. Particular attention is paid to checking that the TSF is clearly defined and identified. This part can be done by filling a table, but no standardized format is required.

Part 3 Functional tests

To perform the functional tests, the end-user must test all the security functions defined in the "Specification validation" paragraph. The end-user must give, for each security function, the description of the security function, its use cases, and the expected results.

Then, the end-user must test all the security functions by filling in the labelling follow-up document by describing the approach adopted, the time, the human and IT resources, and the skills necessary for the execution of the tests and finally the test result.

Part 4 Vulnerability tests and analysis

The following paragraph refers to the evaluation activity AVA_VAN.1. taken from the CEM document of the Common Criteria. This evaluation activity is also recommended by the CitySCAPE project to perform the vulnerability analysis.

The tests are based on a list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable.

5.6 Assurance activities for non-critical components

Non-critical components are indirectly protected by security components such as firewalls, SIEM, IDS/IPS, etc.

The purpose of this part is to verify that, following the risk analysis, there are no unidentified critical risks and that the identified threats do not exploit non-critical

components. To maintain a good level of security, the information system must be based on a system with IDS/IPS and SIEM tools, tools that can be offered by the City-SCAPE solution to monitor attacks on these components and check for any violation of security requirements. As part of this approach, it will be necessary to ensure on an ongoing basis that no critical risk applicable to these components has been overlooked.

6 Stakeholders

Two types of stakeholders are identified:

- Operational stakeholders, who are directly involved in the implementation of the process.
- Non-operational stakeholders, who are the authorities responsible for the protection of critical information systems and who regulate the label and the awarding process.

The following definitions of stakeholders in the labelling process are voluntary not precise, as it should be possible to adapt the proposed labelling process to the maximum number of use cases.

For example, a system provider could take on the role of developer and sponsor if it decides to label its system on its own. It is the responsibility of the sponsor to influence the labelling roles of all implied bodies.

6.1 Sponsor

The party requesting labelling and financing the assessment service. It could also be named as “System owner”.

It could be a PTO or PTA, usually the sponsor owned the System (system owner).

6.2 End User

The party that operates the System, it could be a PTO

6.3 Developer

The organisation that specifies, develops or maintains the product or some of its components. The developer is responsible for the possible development of supplies and for providing technical assistance to the evaluators, if required. Depending on who is responsible for the system, the developer may be a supplier or the sponsor itself. He oversees the following tasks:

- Risk analysis,
- Component identification.

The developer can also act as a sponsor if he decides on his own to initiate a labelling process for the transport system or one of its components.

6.4 Label Acceptance Body

On behalf of an European National Security authority, he oversees the following tasks:

- Fill in the « document identification » part in the labelling follow-up document, and give the instructions to the developer and the sponsor for labelling,
- Third party verification,
- Deliver the label and manage thru the label life cycle (updating the label state).

6.5 Assessor

A body approved by the national authority, necessary to apply for labelling and obtain the label. He is designated by the LAB to lead the vulnerability analysis.

7 Recommendation

An analysis of existing public transport standards shows that they focus on data modelling and the mechanisms for exchanging this business information: protocol, payload. Cyber security issues are deliberately not addressed, as it is assumed that they are dealt with elsewhere. This observation reinforces the need to formalise the adoption of cyber protection processes and measures throughout the lifecycle of multimodal transport systems by means of a label, the basics of which are described in this document.

On the other hand, the introduction of a European label to ensure that the system is continuously adapted to changing threats and vulnerabilities would be a milestone in the cyber protection of multimodal urban transport systems. However, this objective requires the introduction of a new generation of collaborative and adaptive tools, such as those developed in the CitySCAPE project.

The emergence of the digital world and new technologies in the multimodal transport system landscape is opening it up to new players from the digital world who are driving innovation. The introduction of a label must not act as a brake on innovation by creating costs that are incompatible with the size of these new entrants. This is why the introduction of innovative tools (such as the CitySCAPE toolkit), shared in a laboratory that is accessible in ways yet to be defined, must be one of the pillars of this new sectoral label.

In addition, the next stage in the implementation of this label should be a 'dry run' consisting of carrying out the entire process on a voluntary basis, in order to improve and confirm the hypotheses of this study.

References

1. Common criteria, Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, 2017
2. Common criteria, Common Methodology for Information Technology Security Evaluation, 2017
3. ENISA, SCSA - Methodology for sectoral cybersecurity assessments
4. NISTIR 7693 Specification for Asset Identification
5. prCEN TS 16614 – Public transport — Network and Timetable Exchange (NeTEx)
6. prEN 12896 Public Transport Reference Data Model (TRANSMODEL)
7. SIRI: EN 15531: Service Interface for Real-time Information relating to public transport operations
8. ISO/IEC 27001 (2013) Information security management systems
9. ISO/IEC 27002 (2013) Information security, cybersecurity and privacy protection — Information security controls
10. ENISA, EUCC - Common Criteria based European candidate cybersecurity certification scheme.
11. ENISA, EUCS – Cloud Services Scheme
12. ITxPT, https://itxpt.org/labeling/
13. NIS DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
14. Kasia Bourée PUBLIC TRANSPORT NETWORK TIMETABLE EXCHANGE (NeTEx) SUPPORT FOR ACCESSIBILITY IN NeTEx CEN TC278/WG3/SG9 NeTEx PT00
15. www.mobilitydata.org/data-standards/
16. www.transdev.com/fr/publication/mobiobserver-etude-information-voyageur/
17. ANSSI, Methodology for evaluation for a first level security certification – ETR content, 2014
18. ANSSI, Criteria for evaluation in view of a first level security certification, 2020