Proposta di tesi su analisi del rischio nei confronti di minacce cyber in ambito Trasporti

Title	**Development of a computation engine for Risk Analysis of cyber threats in Transportation IT systems**
Supervisors	Prof Giorgio Giacinto (UniCa) Prof Giorgio Fumera (UniCa) Umberto Battista (STAM S.r.l.) Davide Ottonello (STAM S.r.l.) Pietro De Vito (STAM S.r.l.) Giovanni Nieddu (STAM S.r.l)
Team/Company	The research group at the **University of Cagliari** has more than 20 years of experience in Machine Learning approaches to Cybersecurity. Areas of expertise include network traffic analysis and malware analysis. Recently, risk-based cybersecurity assessments have been investigated within national and international projects, as well as in teaching activities. **STAM** is a fast-growing engineering company that support its clients in addressing new businesses and technology challenges leveraging on a multidisciplinary expertise and hands-on experience across four main industrial domains: security and transports, space and defence, robotics and industry 4.0, sustainability and circular economy. The firm serves a broad range of industries, public and private companies, research organizations, no-profit agencies. A large part of Stam's activities is related to security aspects of critical infrastructures. The company has a strong expertise in crowd behaviour and terrorist attack simulations, decision-support tools based on risk assessment for the security of infrastructures, public spaces and citizens, simulation of blast effects and consequences.
Research field	Cybersecurity, Risk Assessment, Protection of Critical Infrastructures
Motivations and general objectives:	**Thesis description** The framework for the proposed thesis is composed by two ongoing H2020 projects: ▪ *SAFETY4RAILS* (https://safety4rails.eu/), whose main objective is to provide railway and metro operators with methods and systems to increase the safety and recovery capability of track-based inter-city railway and intra-city metro transportation; ▪ *CITYSCAPE* (https://www.cityscape-project.eu/), which aims to achieve a detailed characterization of cyber-threats in the ICT multimodal transport, also through the development of innovative software tools able to assess cyber-threats propagation in the system.

To achieve the aforementioned objectives, both projects will develop software platforms to support transportation operators in increasing the protection of their infrastructures, assets, services and people, by improving prevention, detection, response and mitigation capabilities. Specifically, the technologies included in both platforms will be:

- Monitoring and detection tools, to identify occurrence of threats (e.g. cyber-attacks) and early warn transportation operators to safeguard their resources and quickly put in place proper countermeasures;
- Simulation tools, to virtually run what-if attack scenarios and then analyze potential damages as well as test possible response and mitigation strategies;
- Risk Assessment and Cost-benefit analysis tools, to allow transportation operators and infrastructure managers to identify the most risky scenarios and assess the cost-effectiveness of countermeasures;
- Crisis Management tools, to facilitate coordination of resources during an emergency as well as communication among relevant stakeholders.

All the tools developed and implemented within both projects will be tested and validated in real-life use cases. For what concerns SAFETY4RAILS, railway and metro operators are involved (e.g. Metro de Madrid), while in CitySCAPE the end-users are providers of public multimodal transport services (i.e. AMT, the local public transport company of City of Genoa, and the city of Tallinn).

Within these projects, STAM is in charge of the development and deployment of an integrated web-application made of a Risk Assessment module and a Cost-benefit Analysis module, dedicated to Transportation Critical Infrastructures. The tool should generate, simulate and analyse risk scenarios starting from the topology of the infrastructure under examination and the features of the services provided by operators, as well as considering threats of different nature (physical, cyber and combined cyber-physical attacks, but also natural hazards). The Risk Assessment module will provide indicators on the likelihood, potential impact and risk of each scenario computed, while the Cost-benefit Analysis module will compare the results obtained by the risk analysis with new configurations in which the user can test the benefits and the cost-effectiveness of new security measures.

Indeed, the application will allow the user to model different configurations of his/her own infrastructure, and then visualize the results of the risk analysis and the cost-benefit analysis in intuitive dashboards.

The goal of this thesis is the development of a comprehensive risk analysis methodology to estimate the risk level of assets exposed to cyber-attacks within transportation infrastructures. The expected methodology should properly model IT assets, services relying on them, countermeasures, as well as relevant cyber threats affecting those assets. The risk analysis algorithms will then generate an exhaustive set of risk scenarios, simulating their impact according to the effect of modelled countermeasures, and finally determining the likelihood and the potential impact in terms of damages to infrastructures, people and business interruption (or, in the worst case, disruption) for each scenario. The pre-defined model will be translated into a data model (e.g., a graph DB), while the methodology will be then implemented in a computation engine to be developed in Python. This software module should be able to receive as an input the model of the infrastructure and generate as an output the results of the risk analysis.

The student will be involved in on-going EU research projects, being developed by international consortia of top-level organizations in the field of cyber/physical security of transportation infrastructures.

Required skills:

1. Remarkable knowledge of IT systems and current issues related to cybersecurity;
2. Python programming;
3. Interest in risk analysis and IT system protection topics;
4. Minimum knowledge about graph databases, Neo4j and Cypher language is a plus.

Proposed work plan and expected results:

The student will carry out the following activities:

1. Analyse IT systems and cyber-attacks occurred in the transportation environment;
2. Analysis and evaluation of the effectiveness of security measures against cyber-attacks;
3. Define a suitable model to characterize IT systems and cyber-attacks in the transportation environment;
4. Define a methodology to perform a comprehensive risk analysis of transportation IT systems towards cyber-attacks. The methodology should also consider potential cascading effect of cyber-attacks;
5. Implementation of the defined model and methodology into a computation engine developed in Python;
6. Technical and functional testing of the computation engine;
7. Application in a real use-case.

Place of activity:

Dipartimento di Ingegnera Elettrica ed Elettronica, Università di Cagliari – Edificio M – Via Is Maglias, Cagliari

Open Campus, Località Sa Illetta Strada Statale 195 Sulcitana 09123 Cagliari (CA)

(In case of restrictions due to Covid-19, the student will work remotely)

Contacts:

Prof Giorgio Giacinto (giacinto@unica.it)

Prof Giorgio Fumera (fumera@unica.it)

Umberto Battista (u.battista@stamtech.com)

Davide Ottonello (d.ottonello@stamtech.com)

Pietro De Vito (p.devito@stamtech.com)

Giovanni Nieddu (g.nieddu@stamtech.com)