Doctoral Dissertation
Doctoral Program in Computer and Systems Engineering ($35^{th}$cycle)

# Methodologies and tools to support Vulnerability Assessment and Cyber Risk Analysis activities within the Italian Cybersecurity Perimeter

By

**Nicolò Maunero**
******

**Supervisor(s):**
Prof. Paolo Prinetto, Supervisor

**Doctoral Examination Committee:**
Prof. Alessandro Armando, Referee, Università degli Studi di Genova
Prof. Francesco Buccafurri, Referee, Università Mediterranea di Reggio Calabria
Prof. Roberto Baldoni, Agenzia per la Cybersicurezza Nazionale
Dr. Fabio De Rosa, CINI Cybersecurity National Lab.
Prof. Tiziana Margaria, University of Limerick
Prof. Matteo Sonza Reorda, Politecnico di Torino

Politecnico di Torino
2023

# Declaration

I hereby declare that the contents and organization of this dissertation constitute my own original work and does not compromise in any way the rights of third parties, including those relating to the security of personal data.

Nicolò Maunero
2023

* This dissertation is presented in partial fulfillment of the requirements for **Ph.D. degree** in the Graduate School of Politecnico di Torino (ScuDo).

# Methodologies and tools to support Vulnerability Assessment and Cyber Risk Analysis activities within the Italian Cybersecurity Perimeter

Nicolò Maunero

In the last decade, we have witnessed a steady increase in cyber attacks to the detriment not only of large organizations but also of small and medium-sized businesses as well as individuals. These attacks range from denial of service of provided services to data theft or destructive actions of malware. The constant presence of this menace makes it necessary and essential to set up actions to analyze the security posture of information systems, so that cyber attacks can be prevented or mitigated.

The process of *risk assessment* can be conceptually divided into 3 main phases: (i) assessment of the threats to which a computer system may be subjected, also known as *threat modeling*; (ii) assessment of the vulnerabilities present in the system, also known as *Vulnerability Assessment and Penetration Testing* (VAPT); (iii) finally the *risk evaluation* that combines the information obtained from the previous two phases with information related to the specific case under analysis (such as the impact that the implementation of a threat may have on the system). The output of this entire process aims to have a quantitative assessment of the security posture of the analyzed ICT infrastructure.

The main problem with these types of activities is that, to date, they are still performed predominantly manually and, therefore, require analysts a great deal of experience and precision to achieve significant results. In addition, the constant increase, on the one hand of new threats that are discovered every day, and, on the other hand, of the complexity of ICT infrastructures adopted even by small organizations, leads to a non-trivial complexity in the management of the large amount of security-related information items. Therefore, it becomes important to introduce some degree of automation in risk assessment activities, to support and simplify the implementation process and the management of security data. Automating, however, brings in challenges and specific requirements, including, among the others: (i) the definition of a formal modeling language to represent the infrastructure under analysis and the related security information; (ii) the identification of a set of formal rules for the automatic and effective inference of the necessary information.

The goal of this thesis work is, therefore, to provide tools to support risk assessment activities by introducing automation in different phases of the security assessment procedure.

To achieve this, an ontology has been firstly introduced supporting the definition of a formal and semantic representation of the data needed for the analysis and a representative metamodel of a generic ICT infrastructure. The defined ontology is properly enriched with information useful for effectively representing system threats and vulnerabilities.

Considering the various stages of risk assessment, approaches have been designed to automate the collection of information related to known infrastructure vulnerabilities. Starting from the list of assets present, the ontology can be automatically populated with information related to known vulnerabilities for those assets, gathered from external sources.

Concerning the threat modeling process, formal rules have been defined: interpreted by ontology automatic reasoners, these allow the automatic derivation of the threat modeling of the target infrastructure, identifying the potential threats of each involved asset.

Finally, this information is combined with the available information on possible business impact of the occurrence of a threat and its occurrence probability, to propose a qualitative cyber risk assessment for the identified threats.

The proposed solution follows an asset-oriented approach in defining the ontology metamodel; this allows to tightly link together infrastructure components and security data to facilitate the integration of automation and obtain better and more precise results.

The benefit of such a solution is that it can simplify and speed up the execution of risk assessment activities, allowing for great adaptability in an ever-changing landscape.