COMPUTER AND CONTROL ENGINEERING

PNRR/SERICS - Adaptive, Agile and Automated Cybersecurity Management

Funded By	MINISTERO DELL'UNIVERSITA' E DELLA RICERCA [P.iva/CF:97429780584] Politecnico di TORINO [P.iva/CF:00518460019]
Supervisor	VALENZA FULVIO - fulvio.valenza@polito.it
Contact	VALENZA FULVIO - fulvio.valenza@polito.it BRINGHENTI DANIELE - daniele.bringhenti@polito.it
Context of the research activity	Modern digital systems, like cloud-edge computing, software, and virtualized networks, use complex services, devices, data, and infrastructure with many entwined, recursive, and often hidden relationships. Unfortunately, managing cybersecurity and configuring enough protection in these novel systems is challenging due to the fragmentation of cybersecurity operations in such multi-ownership systems. The proposed research aims to study adaptive, agile, and automated cybersecurity management. Progetto finanziato nell'ambito del PNRR M4C2, Investimento 1.3 - Avviso n. 341 del 15/03/2022 - PE0000014 Security and Rights in the CyberSpace (SERICS) - CUP E13C22001850001
	The main objective of the proposed research is to improve the state of the art of cybersecurity management and automation in digital systems (i.e., cloud-edge computing, software, and virtualized networks), mainly focusing on adaptive, agile, and automated cybersecurity configuration and reaction. Although some methodologies and tools are available today with this target, they support these activities only partially and still have severe limitations. Most notably, they leave a lot of the work and responsibility in charge of the human user, who is expected to configure adequate protection mechanisms and instantly react to cyberattacks. The candidate will pursue highly automated approaches that go beyond the state of the art, limiting human intervention as much as possible, so reducing the risk of introducing human errors and speeding up security analysis and reconfigurations. This last aspect is essential because novel systems are highly dynamic. Moreover, if security attacks or policy violations are detected at runtime, the system should recover rapidly by reconfiguring its security

Objectives	promptly. Another feature that the candidate will pursue in the proposed solution is a formal approach, capable of providing formal correctness by construction. This way, high correctness confidence is achieved without needing a posteriori formal verification of the solution. Finally, the proposed approach will pursue optimization by selecting the best solution among the many possible ones. In this work, the candidate will exploit the results and the expertise recently achieved by the proposer's research group in the related field of traditional network security automation. Although there are significant differences between the two application fields, there are also some similarities, and the underlying expertise on formal methods held by the group will be fundamental in the candidate's research work. If successful, this research work can have a high impact because improving automation can simplify and improve the quality of the verification and reconfigurations in these modern systems, which are crucial for our society. Even if the results are less than expected, this research would still contribute significantly to defining the methodology and tools that support security administrators. The research activity will be organized in three phases: Phase 1 (1st year): The candidate will analyze and identify the main issues and limitations of recent methodologies in adaptive and agile configuration and reconfiguration. Also, the candidate will study the state-of-the-art literature on security automation and optimization of cloud-edge computing environments and software/virtualized networks, with particular attention to formal approaches for modeling and configuring security properties and devices. Subsequently, with the tutor's guidance, the candidate will start identifying and defining new approaches for defining novel models and processes for automating and enforcing network and access control and isolation mechanisms. Some preliminary results are expected to be published at this phase's end. During the first year, the candidate will also acquire the background necessary for the research. This will be done by attending courses and by personal study. Phase 2 (2nd year): The candidate will consolidate the proposed approaches, fully implement them, and conduct experiments with them, e.g., to study their correctness, generality, and performance. In this year, particular emphasis will be given to the identified use cases, properly tuning the developed solutions to real scenarios. The results of this consolidated work will also be submitted for publication, aiming at least at a journal publication. Phase 3 (3rd year): based on the results achieved in the previous phase, the proposed approach will be further refined to improve its scalability, performance, and applicability (e.g., different security properties and strategies will be considered), and the related dissemination activity will be completed. The contributions produced by the proposed research can be published in conferences and journals belonging to the areas of cybersecurity (e.g. IEEE S&P, ACM CCS, NDSS, ESORICS, IFIP SEC, DSN, ACM Transactions on Information and System Security, or IEEE Transactions on Secure and Dependable Computing), and applications (e.g. IEEE Transactions on Industrial Informatics or IEEE Transactions on Vehicular Technology).

	Moreover, the proposed research will be conducted in the context of the EU project Miranda, which will be started in September 2024.

Skills and competencies for the development of the activity	In order to successfully develop the proposed activity, the candidate should have a good background in cybersecurity (especially in network security) and good programming skills. Some knowledge of formal methods can be useful, but it is not required: the candidate can acquire this knowledge and related skills as part of the PhD Program by exploiting specialized courses.