COMPUTER AND CONTROL ENGINEERING

PNRR/SERICS - Security of Software Networks

Funded By	MINISTERO DELL'UNIVERSITA' E DELLA RICERCA [P.iva/CF:97429780584] Politecnico di TORINO [P.iva/CF:00518460019]
Supervisor	BASILE CATALDO - cataldo.basile@polito.it
Contact	
Context of the research activity	The massive progress in software network complexity, flexibility, and manageability was only marginally used to increase the security of these networks: attacks may remain undiscovered for months, and human errors mainly cause them. The PhD proposal has a high-level research objective: investigating and exploiting software networks' full potential to mitigate cybersecurity risks automatically and provide defensive tools that rely on artificial intelligence to achieve a higher level of automation and security guarantee. 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
	Nowadays, attackers are always one or more steps behind the security defenders. When vulnerabilities are found, patches follow only days later, and anti-virus signature updates come after discovering new malware. Intrusion Prevention Systems provide simple reactions triggered by simplistic conditions often considered ineffective by large companies. Moreover, companies face risks of misconfiguration whenever security policies or network layouts need an update. Statistics are clear: attacks are discovered with unacceptable delays, and in most cases, attacks are caused by human errors. The solution is also clear: providing defensive tools with more intelligence and a higher level of automation. This PhD proposal aims to use these features for security purposes, i.e., to develop AI-based systems able to perform policy refinement, configure the network and security controls starting from high-level security requirements, and policy reaction to respond to incidents and mitigate risks. Coupling then understanding the features of security controls and software networks will build more resilient information systems that discover and react to attacks faster and more effectively.

Objectives	The initial phases of the PhD will be devoted to formalizing the framework models needed to reach the most ambitious research objectives. During the first year, the candidate will improve the model of security controls' capabilities and define the formal model of the software networks' reconfiguration abilities. The most relevant families of security controls will be analyzed, starting from filtering (up to layer seven) and channel protection. The candidate will contribute to a journal publication that extends an existing conference publication. The work on software network modelling will start with analysing the features of Kubernetes technology. It will also identify strategies to use pods and clusters to define policy enforcement units that merge security controls with complementary features for protecting network parts, which will be used for refinement purposes. The results of this task will be first submitted to a conference and then extended to a journal publication. More attention will be devoted to the refinement and reaction models from the second year. The candidate will study the possibility of building refinement models that use advanced logic (forward and abductive reasoning) to represent decision-making processes. AI (Artificial Intelligence) and machine learning techniques will be investigated to learn from decisions overridden and manual corrections made by humans for fine-tuning security decisions. The candidate will also perform research towards an abstract framework for abstractly representing reaction strategies to security events. Every strategy requires adaptations to be enforced in each context; the research will investigate how to characterize and implement this adaptation and what the proper level of abstraction for strategies is. The effectiveness of these models will be evaluated on relevant scenarios like corporate networks, ISP, automotive, and Industrial Control Systems, also coming from two EC-funded European Projects. The candidate will be guided in evaluating and deciding on the best venues to publish the results of his research. Moreover, to increase the impact of the research and cover existing gaps, the candidate will investigate how to standardize the information used to model the scenarios requiring reactions and the reaction and threat intelligence data with the proper level of detail. One or two 3-6 months internship periods are expected in an external institution. The objective is to acquire competencies that may emerge as needed. Research collaborations are ongoing with EU academia and with leading companies in the EU. We expect at least two publications on top-level cybersecurity conferences and symposia (e.g., ACM CCS, IEEE S&P) or top conferences about software networks (e.g., IEEE NetSoft). The models of the security controls and software networks' capabilities models will be submitted to top-tier journals in the cybersecurity, networking, and modelling scope (e.g., IEEE /ACM Transactions on Networking, IEEE Transactions on Network and Service Management, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Dependable and Secure Computing). We also expect results for at least one journal article about the automatic enforcement and empirical assessments of software protections. Together with the journals reported above, if the innovation of the results will deserve it, also IEEE Transactions on Emerging Topics in Computing.

Skills and competencies for the development of the activity	The candidate needs to have a solid background in cybersecurity (risk management), defensive controls (e.g., firewall technologies and VPNs), monitoring controls (e.g., IDS/IPS and threat intelligence) and incident response. Moreover, he should also possess a background in software network technologies (SDN, NFV, Kubernetes) and cloud computing. Having skills in formal modelling and logical systems is a plus.