Abstract Book of the CNR IMATI Workshop
https://www.sciencepg.com/ISBN/979-8-88599-188-9/002

Who Is in Control: An Introduction to Automatic Cyber Defense

Daniele Canavese*

Istituto di Matematica Applicata e Tecnologie Informatiche, Consiglio Nazionale Delle Ricerche (CNR-IMATI), Genoa, Italy

Email address:

daniele.canavese@cnr.it (Daniele Canavese)

*Corresponding author

Abstract

This talk provides an overview of the design of automated cyber-defense solutions powered by artificial intelligence. Modern cyber threats are increasingly complex, often exploiting human weaknesses, heterogeneous infrastructures, and unexpected attack vectors. This complexity underscores the need for intelligent, adaptive defense mechanisms that support—rather than replace—human decision-makers in increasingly adversarial, complex environments. The first section of the talk centers on threat intelligence, discussing both reactive and proactive approaches to detecting and anticipating malicious behaviors. Traditional defenses, such as manually configured firewalls and intrusion detection systems, struggle with encrypted traffic, large-scale networks, and evolving attack strategies. To address these limitations, machine-learning-based detection techniques and graph-based models designed for reasoning about multi-stage attacks can pave the way for significantly safer IT infrastructures. The second part of the talk revolves around autonomous networks, motivated by the fact that modern infrastructures are too dynamic and complex to be managed manually. In this context, intent-based networking can help create self-configuring, self-healing, and secure architectures. By harnessing logic-based reasoning and explainable AI, intent-based networks can become game changers in the design of highly secure, mathematically guaranteed distributed environments that also comply with a set of best practices. Finally, the talk will conclude with a discussion of a variety of software protection-related projects, such as decision-support systems for optimizing the placement of software protections, as well as AI-based techniques leveraging LSTMs and transformers to analyze binaries and identify vulnerabilities.

Keywords

Cybersecurity, Artificial Intelligence, Threat Intelligence, Intent-based Networking, Software Security