Massimiliano Albanese, PhD

Associate Professor, Information Sciences and Technology
Associate Director, Center for Secure Information Systems

Education

PhD, Computer Science and Engineering, University of Naples Federico II, Italy

Key Interests

Cybersecurity | Adaptive Cyber Defense | Cyber Situational Awareness | Internet of Things | Cloud Computing

CONTACT

Phone: 703-993-1629 | Email: malbanes@gmu.edu
Website: https://csis.gmu.edu/albanese/

SELECT PUBLICATIONS

- M. Albanese *et al.*, "SCIBORG: Secure Configurations for the IOT Based on Optimization and Reasoning on Graphs," in Proceedings of the *8th IEEE Conference on Communications and Network Security (IEEE CNS 2020)*, virtual conference, [Best Paper Award]. (2020).
- M. Albanese *et al.*, "A Quantitative Framework to Model Reconnaissance by Stealthy Attackers and Support Deception-Based Defenses," in Proceedings of the *8th IEEE Conference on Communications and Network Security (IEEE CNS 2020)*, virtual conference. (2020).

Research Focus

In today's connected world, both government and commercial organizations face increasingly sophisticated and potentially devastating threats from state actors, organized crime, and other malicious actors. While defenders have to protect from all possible attacks, malicious actors have a tremendous advantage as they only need to find a weak entry point to penetrate a system and cause irreparable damage. A 2018 report of the White House's Council of Economic Advisers estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 alone. My research focuses on mitigating such threats by tackling the problem on multiple fronts. First, my work on cyber situational awareness aims at improving the defender's understanding of the cyber landscape in which the organization operates, including potential threats and attacker's objectives and strategies. Second, my work on moving target defense and adaptive cyber defense aims at developing advanced techniques to continuously adapt to an evolving security landscape, create uncertainty for the attacker, and increase the cost for a malicious actor to conduct an attack campaign.

Current Projects

- Secure Configuration for the IoT Based on Optimization & Reasoning on Graphs. In collaboration with PARC, this project aims at developing a framework to automatically optimize the configuration of complex IoT systems, balancing security and functionality constraints.
- Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Building the Scientific Foundation. This MURI project aims at defining the scientific foundation of Adaptive Cyber Defense, focusing on modeling the behavior of adversaries and reasoning in the presence of uncertainty.
- Center for Cybersecurity Analytics and Automation (CCAA). Established under the NSF IUCRC program, CCAA aims at advancing cyber defense on multiple fronts.