Department of Systems Engineering
香港城市大學
City University of Hong Kong

Automated Security through Online Learning with a Foundation Model

As the ubiquity and evolving nature of cyberattacks pose a growing concern to society, the automation of security processes and functions has been recognized as an important part of the response to this threat. In fact, since the early 2000s, researchers have studied automated security through modeling attacks and defenses on an IT infrastructure as a game between an attacker and a defender. While encouraging results have been reported following this approach, most of the methods so far have only been validated analytically or in simulation, leaving their practical utility unproven. In this talk, we present a general framework for security automation that relaxes traditional assumptions and enables the controlled evolution of optimal security strategies on an operational system. Our framework is couched on algorithmic mathematics and consists of three main components: (1) a digital twin for data collection and strategy evaluation; (2) an active causal learning method for system identification; and (3) a reinforcement learning method for deriving effective security strategies using a foundation model. We show that our framework obtains state-of-the-art performance on several benchmark problems in autonomous cyber defense. Moreover, we analyze its theoretical properties using decision theory and Bayesian statistics.

Kim Hammar is a postdoctoral researcher with joint affiliations at Arizona State University, the University of Melbourne, and Imperial College London. He received the M.Sc. and Ph.D. degrees in electrical engineering from KTH in 2018 and 2024, respectively. His research interests are in the intersection between game and decision theories and large-scale systems, focusing on networking and security applications. He received the best paper award at IEEE NOMS in 2022 and was the recipient of the VR Postdoctoral Fellowship 2025.

Dr. Kim Hammar
University of Melbourne, Australia

YEUNG - P7303
Yeung Kin Man Academic Building
City University of Hong Kong

20 Oct, 2025 (Mon)

10:00 am - 11:00 am

All are welcome