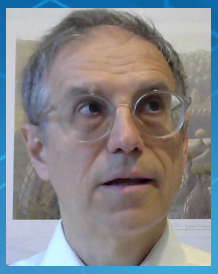
THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Can LLMs fix security bugs?
Everybody claims yes, experimentally no, not on the cloud.



Prof. Fabio MASSACCI
Professor
University of Trento, Itlay
Vrije Universiteit Amsterdam, Netherlands

Date : 24 November 2025 (Mon)
Time : 4:00 pm - 5:00 pm
Venue : CD303

Abstract

LLM-based agents are the new security "cure-all-solutions". Yet, most results published in papers are very hard to replicate as soon as you change a bit. In this talk I will discuss our experience with the use of LLMs to recognize and fix cloud misconfiguration which are typically way simpler than security vulnerabilities on code. Kubernetes Helm charts are files describing all dependencies, resources, and parameters required for deploying an application within a cloud cluster. I will discuss in this talk our years long experience on mining large repositories of Helm Charts, using state-of-the-art industrial tools, such as Checkov and KICS to find (or mislabel) security misconfigurations, and measuring to what extent LLMs could be used for fixing. Tens of thousands Helm charts times hundreds of policies times some LLms we found out the assurance that comes from automated pipelines is very shaky. I will discuss our specific findings and the general lessons for research.

About the Speaker

Prof. Fabio Massacci is a full professor at the University of Trento (IT) and Vrije Universiteit Amsterdam (NL). He has a Ph.D. in Computer Engineering from the University of Rome La Sapienza in 1998. He has been in Cambridge (UK), Toulouse (FR) and Siena (IT). He visited KULeuven, Durham Business School and ISI, University of Southern California. He has published more than 250 articles on security, software engineering and security economics. In 2015 he won the Ten Years Most Influential Paper by the IEEE Requirements Engineering Conference for his joint work on security requirements engineering. His current research interest is in empirical methods when using AI for security and software engineering. He has coordinated several European Projects on security and software engineering. He coordinates the European project Sec4AI4Sec (www.sec4ai4sec.eu) on security of AI-augmented systems and the Dutch NWO project HEWSTI on explainable AI for security and threat intelligence. He participates in the FIRST SIG world standard on CVSS (Common Vulnerability Scoring System) and he is named co-author of v4.0 of the standard.