Vittorio Orbinato

Next generation Cyber Range-as-a-service

Tutor: prof. Domenico Cotroneo
Cycle: XXXVI

co-Tutor: prof. Roberto Natella
Year: II

My background

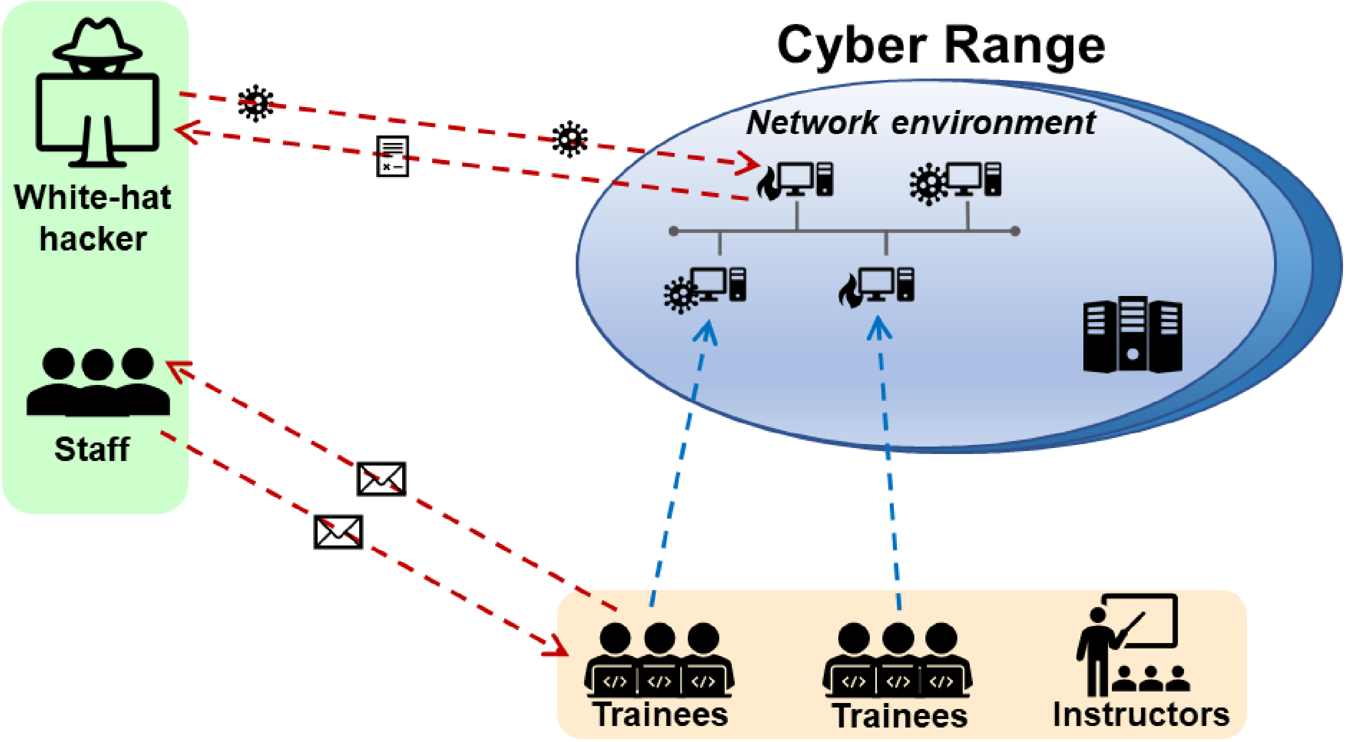
- MSc degree: Computer Engineering (October 2020)
- Research group: DESSERT
- PhD start date: 01/11/2020
- Scholarship type: MUR (PON Ricerca e Innovazione 2014-2020 - “Dottorati innovativi con caratterizzazione industriale”)
- Partner company: System Management S.p.A.

Summary of study activities

- Ad hoc PhD courses/schools:
  - **Virtualization technologies and their applications**
- Conferences/events attended:
  - **33rd International Symposium on Software Reliability Engineering** (ISSRE), Charlotte, North Carolina, October 31 - November 3, 2022, *presenting author*

Research field of interest

My research field concerns the **enhancement of training environments** for **cybersecurity professionals**, in particular **Cyber Ranges**, which represent the most popular and widespread solution.



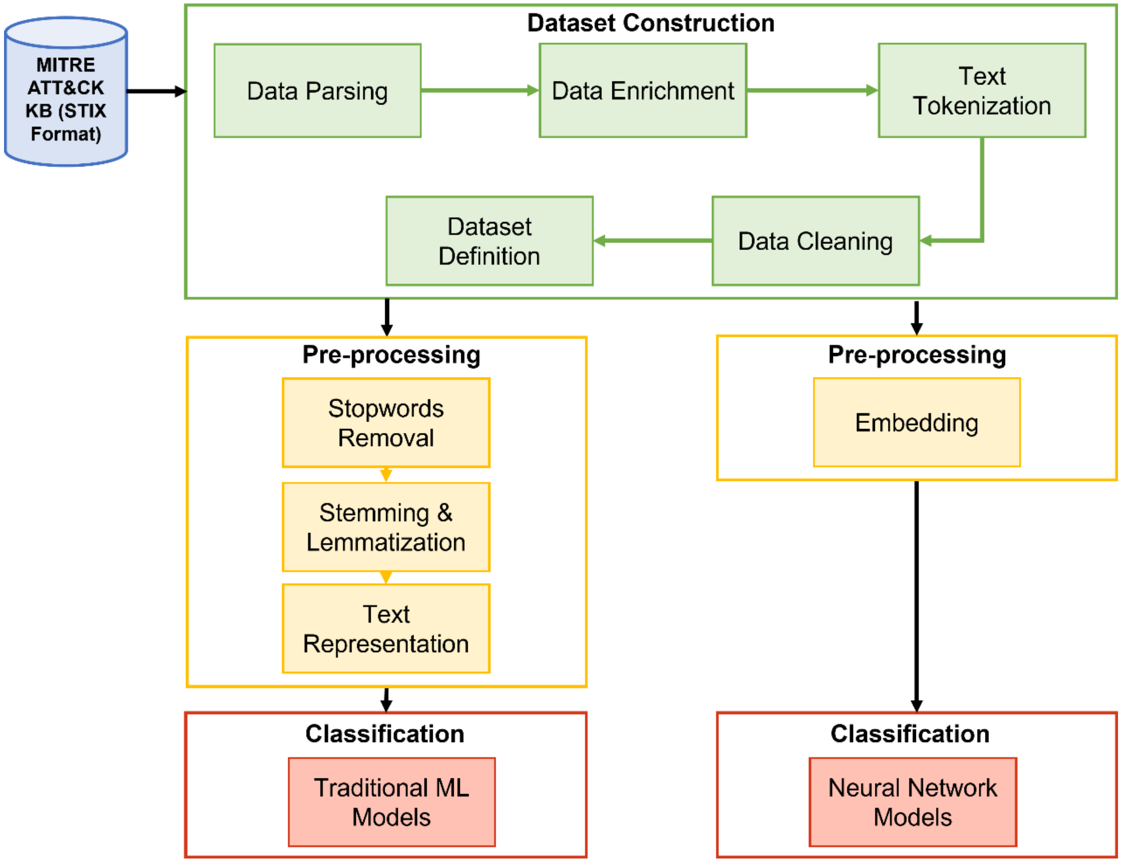
Research activity: Overview

My research activity was focused on addressing the two main problems of Adversary Emulation:

- Manual analysis of Cyber Threat Intelligence (CTI)
- Lack of anti-detection techniques in threat emulators

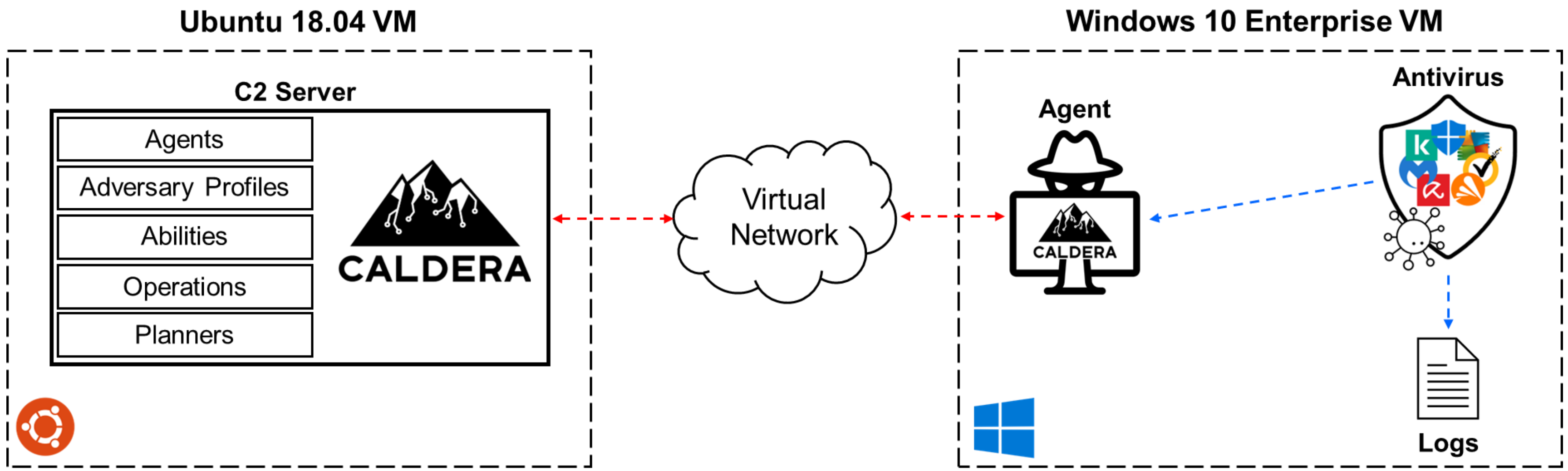
Research activity: Overview

A new approach was devised to automatically map unstructured CTI to attack techniques described by cybersecurity frameworks (e.g., MITRE ATT&CK).



Research activity: Overview

Study on the lack of anti-detection techniques in open-source Adversary Emulation tools. The results showed that their activities are easily identified by the most popular antiviruses (AV) and Endpoint Detection and Response (EDR).

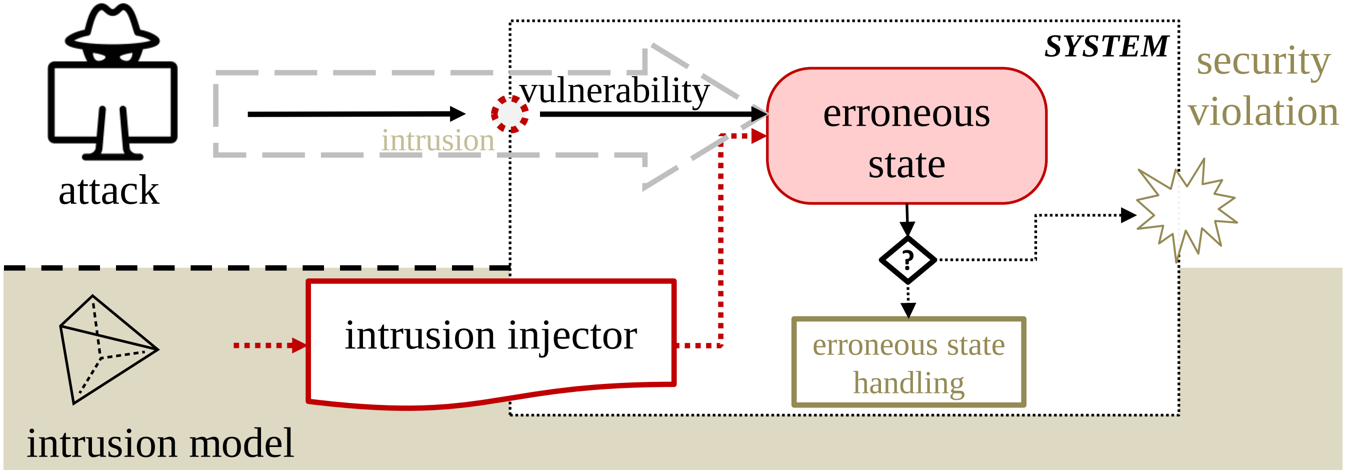


Research activity: Overview

Following the results of our study, we developed a new threat emulation tool for virtualized systems. The tool was tested against several AVs/EDRs, to demonstrate its effectiveness in evading detection solutions in comparison to state-of-the-art adversary emulation tools.

Research activity: Overview

During my abroad research period, currently taking place at the University of Coimbra (Portugal), I am working on the definition of **intrusion models** to assess the security of virtualized systems.



Products

[C1]	Orbinato, V.; Barbaraci, M.; Natella, R.; Cotroneo, D. *“Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study”* 33rd International Symposium on Software Reliability Engineering, ISSRE 2022, 2022

Thank you for your attention

Contact:
vittorio.orbinato@unina.it
Room 4.07 – building 3/A – via Claudio 21