Nicola d'Ambrosio

Attack-defense strategies in challenging cybersecurity environments

Tutor: Simon Pietro Romano

Cycle: XXXVII

Year: Second

My background

- MSc degree: Computer Engineering
- Second Year PhD: Academic Year 2022-2023
- PhD start date: 1/1/2022
- Laboratory: ArcLab
- Scholarship type: PON Dottorati di ricerca su tematiche dell'innovazione e green - Azione IV.4 (Innovazione)
- Period abroad:
  - Accenture Prague: 6 months (expected 6 months)
- Internship
  - Accenture Italia: 4 months (expected 6 months)

Research Activities

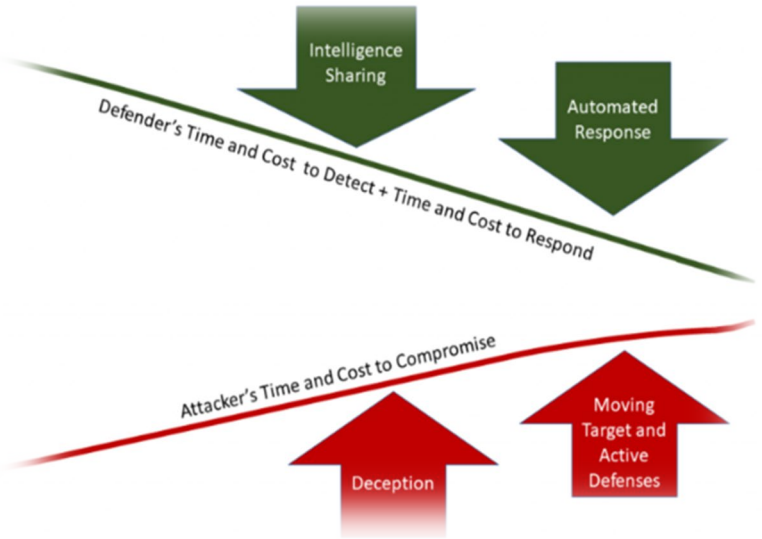
- Proactive strategies that work beyond traditional detect-then-prevent techniques and **block malicious activities** in the early stages of a cyber attack
- Development of a platform that collects, organizes, and analyzes information in order to **identify malicious entities** in a social network
- Integration of safety and cybersecurity threat frameworks to **model the hazard posed by specific malicious actions** and implement appropriate mitigation actions aimed at addressing and alleviating them

A Software-Defined Approach for Mitigating Insider and External Threats via Moving Target Defense

Problem - The aim is to empower defenders by providing them with more:

Time: ensure they enough time to either ***prevent*** or **react to** an attack before it is completed

Knowledge: allow them to examine the attacker's behaviour with the aim of ***anticipating*** their actions



… BUT HOW?

A Software-Defined Approach for Mitigating Insider and External Threats via Moving Target Defense

"Hold out baits to entice the enemy. Feign disorder and crush him."

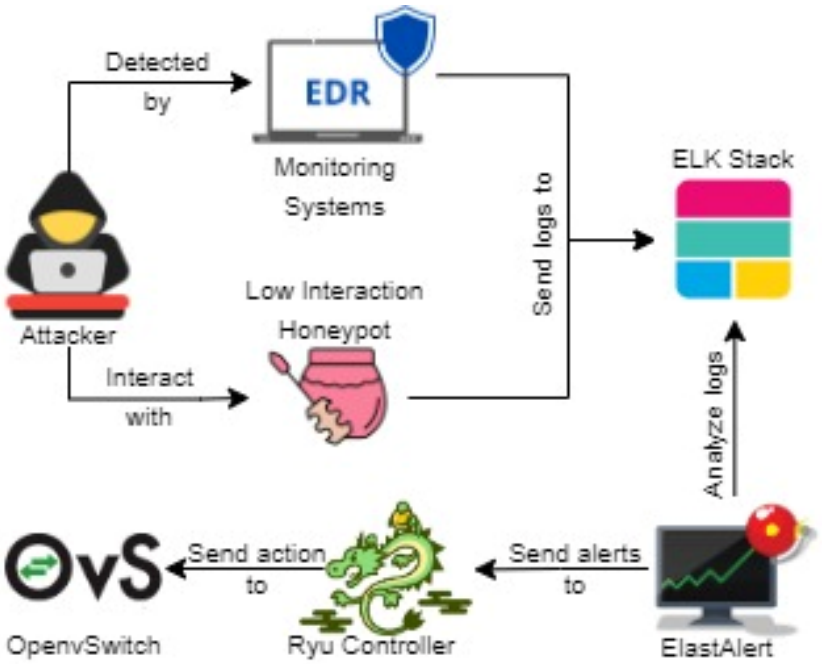
Sun Tzu, The Art of the War

MOVING TARGET DEFENSE	***HONEYPOTS***
Dynamic and continuous change of the attack surface exposed by vulnerable systems	*Decoy that expose intentionally vulnerable services in order to attract attackers.*
• **Time-Based and Event-Based** • **Shuffling, Diversity and Redundancy**	• **Low-Interaction** • **Medium and High-Interaction**

A Software-Defined Approach for Mitigating Insider and External Threats via Moving Target Defense

Objective: Implementation, in a typical business network, of Active Deception Techniques, like Moving Target Defense (MTD) and Honeypots, as an added benefit to traditional approaches, in order to overcome their shortcomings

Approach: The architectural design of the project incorporates the Software Defined Networking (SDN) paradigm and provides a comprehensive approach for integrating honeynets with MTD, Security orchestration, automation and response (SOAR), and Security information and event management (SIEM) platform.



Threat Scenarios to Attack Emulation

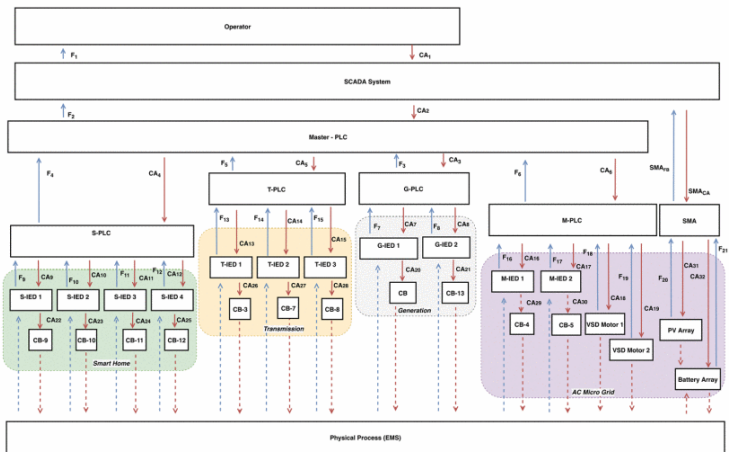
Problem - Safety and security are intricately linked and can not be considered stand-alone anymore.

Objective: We integrate safety models (STAMP/STPA) with cybersecurity models (STRIDE and MITRE) to identify the safety consequences of safety hazard events that may be raised by exploiting specific vulnerabilities.

Threat Scenarios to Attack Emulation

Approach - Our proposed methodology is composed of three stages:

1. we integrate STPA-Sec with STRIDE and formal verification to enumerate safety critical threat scenarios;
2. we leverage the integration of the safety model with the architecture of the deployed system to generate the attack graph (AG) leading to the privileges that the adversary needs to acquire to exploit a threat scenario;
3. we use a systematic and semi-automated procedure to build an attacker agent which is capable of exploiting safety critical attack paths, thus triggering threat scenarios.



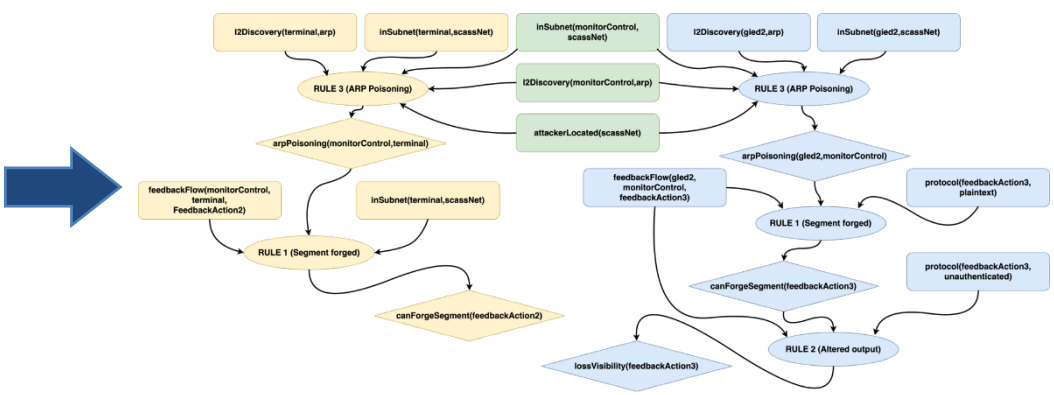
Attack Step	Description	HCA
a_1	$\{(spoof, CA_{12}, cmd)\}$	$4, 5, 6$
a_2	$\{(tamper, CA_{12}, cmd)\}$	$4, 5, 6$
a_3	$\{(spoof, CA_4, cmd)\}$	$4, 5, 6$
a_4	$\{(tamper, CA_4, cmd)\}$	$4, 5, 6$
a_5	$\{(spoof, CA_2, cmd)\}$	$1-10$
a_6	$\{(tamper, CA_2, cmd)\}$	$1-10$
a_7	$\{(spoof, CA_2, cmd)\}$	$1-10$
a_8	$\{(tamper, CA_2, cmd)\}$	$1-10$
a_9	$\{(tamper, sPLC, memory)\}$	$4, 5, 6$
a_{10}	$\{(tamper, Master-PLC, memory)\}$	$1-10$
a_{11}	$\{(tamper, SCADA, memory)\}$	$1-10$
a_{12}	$\{(spoof, F_{12}, \bar{v})\}$	$4, 5, 6, 11$
a_{13}	$\{(tamper, F_{12}, \bar{v})\}$	$4, 5, 6, 11$
a_{14}	$\{(spoof, F_4, \bar{v})\}$	$4, 5, 6, 11$
a_{15}	$\{(tamper, F_4, \bar{v})\}$	$4, 5, 6, 11$
a_{14}	$\{(spoof, F_2, \bar{v})\}$	$1-11$
a_{15}	$\{(tamper, F_2, \bar{v})\}$	$1-11$
a_{16}	$\{(spoof, F_1, \bar{v})\}$	$1-11$
a_{17}	$\{(tamper, F_1, \bar{v})\}$	$1-11$

Threat Scenarios to Attack Emulation

Approach - Our proposed methodology is composed of three stages:

1. we integrate STPA-Sec with STRIDE and formal verification to enumerate safety critical threat scenarios;
2. we leverage the integration of the safety model with the architecture of the deployed system to generate the attack graph (AG) leading to the privileges that the adversary needs to acquire to exploit a threat scenario;
3. we use a systematic and semi-automated procedure to build an attacker agent which is capable of exploiting safety critical attack paths, thus triggering threat scenarios.

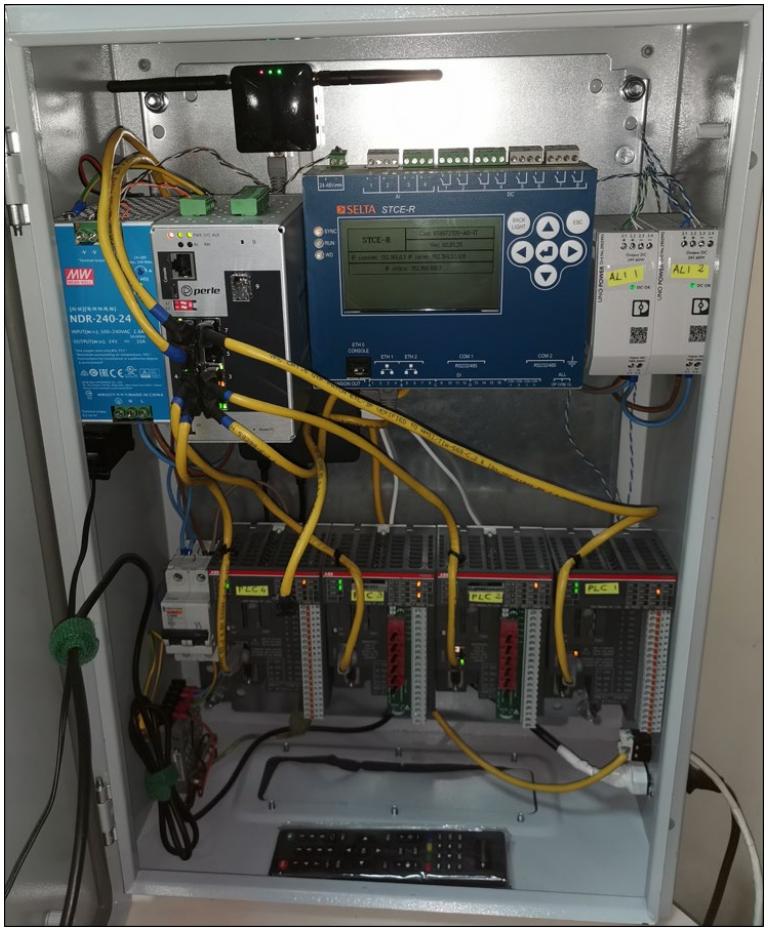
Attack Step	Description	HCA
a_1	$\{(spoof, CA_{12}, cmd)\}$	$4, 5, 6$
a_2	$\{(tamper, CA_{12}, cmd)\}$	$4, 5, 6$
a_3	$\{(spoof, CA_4, cmd)\}$	$4, 5, 6$
a_4	$\{(tamper, CA_4, cmd)\}$	$4, 5, 6$
a_5	$\{(spoof, CA_2, cmd)\}$	$1 - 10$
a_6	$\{(tamper, CA_2, cmd)\}$	$1 - 10$
a_7	$\{(spoof, CA_2, cmd)\}$	$1 - 10$
a_8	$\{(tamper, CA_2, cmd)\}$	$1 - 10$
a_9	$\{(tamper, sPLC, memory)\}$	$4, 5, 6$
a_{10}	$\{(tamper, Master - PLC, memory)\}$	$1 - 10$
a_{11}	$\{(tamper, SCADA, memory)\}$	$1 - 10$
a_{12}	$\{(spoof, F_{12}, \bar{v})\}$	$4, 5, 6, 11$
a_{13}	$\{(tamper, F_{12}, \bar{v})\}$	$4, 5, 6, 11$
a_{14}	$\{(spoof, F_4, \bar{v})\}$	$4, 5, 6, 11$
a_{15}	$\{(tamper, F_4, \bar{v})\}$	$4, 5, 6, 11$
a_{14}	$\{(spoof, F_2, \bar{v})\}$	$1 - 11$
a_{15}	$\{(tamper, F_2, \bar{v})\}$	$1 - 11$
a_{16}	$\{(spoof, F_1, \bar{v})\}$	$1 - 11$
a_{17}	$\{(tamper, F_1, \bar{v})\}$	$1 - 11$



Threat Scenarios to Attack Emulation

Testbed – To demonstrate the effectiveness of our approach, we implemented SCASS (SCADA Systems Security):
– a hybrid and modular testbed
– the hybrid nature of our testbed allows us to work with a scalable and maintainable environment

Future Work – We aim to apply a similar approach in different contexts, specifically in the fields of aerospace and automotive sectors.

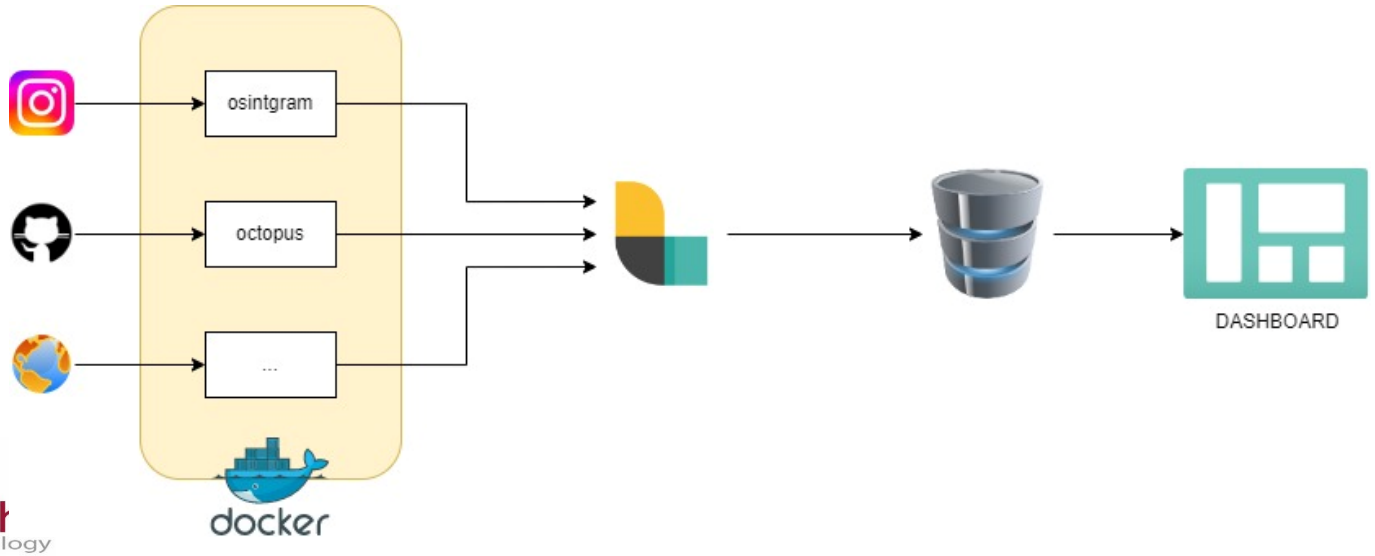


OSINT - Collector

We are developing a tool that helps users manage data from open sources. Our goal is to make it easy for users to collect, organize, and analyze information.

The project has three modules:

- the **Tool Classifier** is crucial because it suggests the best OSINT tools to use based on the user's needs. It uses an ontology-based approach to make automatic recommendations.
- The **Data Collector** module stores the data in a graph database, making it easy to organize and find connections
- The **Data Visualization** module provides an interface that presents the analyzed data in visual formats.



Products

[C1]	F. Caturano, N. d'Ambrosio, G. Perrone, L. Previdente and S. P. Romano, "ExploitWP2Docker: a Platform for Automating the Generation of Vulnerable WordPress Environments for Cyber Ranges," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2022, pp. 1-7, doi: 10.1109/ICECET55527.2022.9872859.
[C2]	N. d'Ambrosio, E. Melluso, G. Perrone and S. P. Romano, "A Software-Defined Approach for Mitigating Insider and External Threats via Moving Target Defense," 2023 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Dresden, Germany, 2023, pp. 213-219, doi: 10.1109/NFV-SDN59219.2023.10329613.
[J1]	Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano, "Including insider threats into risk management through Bayesian threat graph networks", Computers & Security, Volume 133, 2023, 103410, ISSN 0167-4048, doi: 10.1016/j.cose.2023.103410.

Thanks for your attention!