SecGen plenary meeting introduction

Pierre-François Gimenez
PIRAT team

March 6th, 2024

CentraleSupélec

What's SecGen?

SecGen

A 3-year collaboration between CISPA and Inria on AI and cybersecurity, started in 2023
Website: `https://files.inria.fr/secgen/`

Research axis 1

Security data pattern mining and generation

- identifying patterns in network and system data
- use these patterns to generate similar data

Research axis 2

Network anomaly detection, with a focus on:

- explainable alerts
- robustness against adversarial attacks

CentraleSupélec

What has been done in 2023

Kick-off meeting at Paris in June

Starting the collaboration with many insightful presentations

Stays of Joscha at Inria and Adrien at CISPA

- Joscha stayed at Inria in July and August to work on pattern mining in network flow descriptions
- Adrien stayed at CISPA from October to December to work on network flow generation

This collaboration has been successful and an article should be submitted in Spring 2024

Submitted article

An article by Pierre-François, Sarath and Mario on robustness against adversarial attacks

CentraleSupélec

In 2024: some replacement in the team

Some PhD are ending...

Hélène and Adrien will defend their PhD by the end of the year

... and we have some new members

- Matthieu, new PhD student on adversarial attacks against network IDS
- Fabien, new post-doc on reinforcement learning applied to supervision

We are still seeking new members!

If you or someone you know might be interested in joining SecGen, contact me!

CentraleSupélec

What to expect in 2024

A more few stays?

- Inria has renewed the budget for 2024
- We can fund two more two-months stays, or one longer stay
- It can be a great opportunity for PhD students to work abroad

The goal of this meeting

- Present some current work
- Share ideas we could explore together