Position Description

1. General Information

Name of the position	**Towards the fusion of heterogeneous information in-to security operations centres**
Foreseen enrolment date	January 2025
Position is funded by	• COFUND, Marie Skłodowska-Curie Actions (MSCA), Horizon Europe, European Union • Université Savoie Mont Blanc (USMB) • University of Adelaide (UoA) • French Institute of Geopolitics (IFG)
Research Host	Université Savoie Mont Blanc
PhD awarding institutions	Université Savoie Mont Blanc & University of Adelaide
Locations	Primary: Chambéry, France Secondary: Adelaide, Australia
Supervisors	Kavé Salamatian (Université Savoie Mont Blanc) Kaie Maennel and Olaf Maennel (University of Adelaide)
Group of discipline	Computer Science

2. Research topics (only one of these projects will be funded)

Project 1: *Graph-based fusion of Heterogenous Data for Cybersecurity*

Cybersecurity landscape is characterized the heterogeneity of information sources that are at the core of the decision process. Information might come in periodic intervals from signal samplers, like in OT systems, or be event based, like in from Intrusion Detection Systems (IDS), be structured, in JSON like format, or simply textual, like in IT logs. Moreover, information sources might be analytical, like in thread intelligence reports, or factual, like in logs reporting. The integration of these heterogenous data sources into a coherent and actionable cybersecurity system remains critical challenge. This research aims to develop tools that fusion these heterogeneous data through graph-based methodologies to integrate heterogeneous data like threat intelligence reports, logs/Endpoint data, SIEMs, etc. Representing this data in multi-graph form, *i.e,* a graph for each consistent source of information, enable the application of graph mining techniques, along with multi-criteria semi-convex optimization, to fusion relevant information into a comprehensive decision. Moreover, it enhances the visualization capabilities crucial for rapid decision making and threat mitigation. Potentially enhancing advanced visualization tools such as 3D glasses (e.g., see prior work from K. Kullman on „Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity ").

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement № 101081465

A particular motivating use-case to consider could be highly automated maritime vessel with minimal crew. The onboard technical systems detect anomalies indicating that critical navigation or operational systems might be compromised by an attacker. The challenge lies in effectively communicating and visualizing these threats to the seafarers, who are not trained to interpret raw IDS output data. The proposed graph-based system would aggregate and transform these inputs into an intuitive visual format, enabling quick understanding and response even under communication-restricted conditions, where communication to shore facilities is jammed by adversarial actions. Such a system could increase the security posture of semi-automated maritime operations.

This research project aims to:

- Create a system that integrates heterogeneous data sources, such as IDS, threat intelligence reports, logs/endpoint data, and SIEMs, to provide timely alerts and warnings of potential cybersecurity threats.
- Represent the integrated data in graph form, improve visualization capabilities and enabling rapid decision-making and threat mitigation.
- Evaluate effectiveness of threat communication methods to non-technical users that enable improved situational awareness, such as seafarers in the maritime use case.

The research will be performed with the support of the French Institute for Geopolitics.

Supervisors: Kavé Salamatian (Université Savoie Mont Blanc) ; Kaie Maennel and Olaf Maennel (UoA)

Research Fields: Computer science, cyber security, heterogenous data, data visualisation, human in the loop

Project 2: *Synthesizing Heterogeneous Intelligence for Enhanced Threat Landscape Detection*

The exponential growth in data complexity and volume within cybersecurity domains necessitates the development of advanced processing capabilities to effectively manage and derive meaningful insights from vast amounts of information. This research topic proposes the utilization of generative neural networks, large language models (LLMs), and graph clustering techniques to conduct a comprehensive meta-analysis of heterogeneous cybersecurity information sources, encompassing intrusion detection systems (IDS), social media feeds, and taking geo-political threat models into account.

The primary objective is to investigate the potential of integrating these cutting-edge artificial intelligence (AI) methodologies to refine raw data into strategically actionable intelligence, thereby enhancing the decision-making process and enabling proactive threat mitigation. More specifically, the research questions include how large language models (LLMs) can be effectively integrated into cybersecurity security operations to optimize the processing and maximize the utility of heterogeneous information sources? While the potential of AI-driven analysis has been demonstrated, the aim is providing a more nuanced understanding of cybersecurity threats by leveraging the advanced capabilities techniques.

Furthermore, this research is also to comprehensively understand the attack vectors that could target AI-driven systems within SOCs, with a specific emphasis on the manipulation of data inputs. By identifying these potential threats, the research seeks to contribute to the design and development of robust AI systems that exhibit resilience against manipulation and maintain reliable operation even under adversarial conditions. This encompasses the development of advanced detection algorithms capable of identifying poisoned data and the formulation of strategies to ensure the integrity of data utilized by AI in cybersecurity contexts. The research will employ a multi-faceted approach, leveraging techniques from machine learning, data science, and cybersecurity.

This research project aims to:

- Explore how the integration of AI technologies can refine raw data from various sources into strategically actionable intelligence.
- Contribute to the creation of cybersecurity early warning systems that can proactively identify and respond to emerging threats.
- Investigate offensive methodologies and attack vectors targeting AI systems.
- Ethically develop advanced methods for poisoning data in AI-driven cybersecurity systems and provide

This project has received funding from the European Union’s Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement № 101081465

countermeasures and safeguards to mitigate the associated risks.

The research will be performed with the support of the French Institute for Geopolitics.

Supervisors: Kavé Salamatian (Université Savoie Mont Blanc) ; Kaie Maennel and Olaf Maennel (UoA)

Research Fields: Computer science, cyber security, artificial intelligence, machine learning

Project 3: *Mapping the logical layer of Internet to its physical layer: fusioning routing information sources*

Internet is a large-scale system that is built over a physical infrastructure consisting of routers, servers and hosts that are positioned in the physical space. Over this infrastructure, several layers of logical structures, *e.g.*, cable trunks, ethernet VLANs, intradomain routing, BGP, overlays, *etc.*, are built that provide connectivity between networked applications. In other terms, while internet might seem a nebulous and virtual structure, it is strongly rooted in concrete fundaments of the physical infrastructure. Nonetheless, the physical infrastructure is the concrete element of Internet where real-world constraints, *i.e.,* economic, (geo)political or technical, might be imposed. The real path followed by data from source to destination, crosses different physical infrastructures, likely in different countries with various level of interference risks. Localizing these infrastructures in the geographical space is of utmost importance, for understanding geopolitics of cyberspace, the security of information, and the resilience of the vital Internet infrastructures. Unfortunately, the layered architecture of the Internet is hiding the localization of infrastructure, and some Internet actors consider this information as sensitive privileged information. But Internet actors have fortunately to uncover a large part of these hidden information to enable connectivity. There are therefore several source of information, BGP level information, Traceroutes, delay measurements, PeeringDB databases, maritime cable maps, commercial information, *etc.*, that can be exploited to uncover the hidden dimension of infrastructures. However, these sources of information are heterogeneous, diverse, sometime uncertain and we need to develop methods for gathering and fusing these information's in to attain a consistent and coherent vision. The thesis will combine deep knowledge of how Internet infrastructures work with advanced mathematical and statistical knowledge to develop new methods for matching the logical level of the Internet to its physical level. This project will come as a follow-up to several previous research efforts in this direction.

The research project aims to:

- Enhance the understanding of the geopolitical situation on Internet Stability
- Improve security and resilience under cyberattacks on the Internet infrastructure
- Develop more comprehensive data collection and integration methods

The research will be performed with the support of the French Institute for Geopolitics.

Supervisors: Kavé Salamatian (Université Savoie Mont Blanc) ; Kaie Maennel and Olaf Maennel (UoA)

Research Fields: Computer science, cyber security, offensive security, adversarial ML/AI.

3. Employment Benefits and Conditions

Université Savoie Mont Blanc offers a 36-months full-time work contract (with the option to extend up to a maximum of 42 months). There is a 6-months probation period and the total working hours per week is 37h30.

The remuneration, in line with the European Commission rules for Marie Skłodowska-Curie grant holders, will consist of a gross annual salary of 28,817.28€ EUR. Of this amount, the estimated net salary to be perceived by the Researcher is 1,930 EUR per month. However, the definite amount to be received by the Researcher is subject to national tax legislation.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement № 101081465

Benefits include

- Becoming a Marie Skłodowska-Curie fellow and be invited to join the Marie Curie Alumni Association
- Access to all the necessary facilities and laboratories at USMB and UNSW, as well as Solar Graduate School research facilities and laboratories.
- Tuition fee waiver at both PhD awarding institutions.
- Yearly travel allowance to cover flights and accommodation for participating in AUFRANDE events.
- 10,000 EUR allowance to cover flights and living expenses for 12 months in Australia.
- 25 days paid holiday leave.
- Sick leave.
- Parental leave.

4. PhD enrolment

Successful candidates for this position will be enrolled by the following institutions and must comply with their specific entry requirements, in addition to AUFRANDE's conditions.

Applicants must hold a Master of Science or Master of Engineering or another similar world-class master's degree (officially recognized as equivalent by the French Higher Education and Research authorities) containing a significant research component.

If English is not your first language, you will be required to demonstrate English language proficiency in the form of an English test that has been taken within the two years preceding the date of commencement. The following test types are accepted:

- IELTS (International English Language Testing System) Academic
- TOEFL (Test of English as a Foreign Language) Internet Based Test
- PTE (Pearson Test of English) Academic
- C1 Advanced (formerly CAE - Cambridge English: Advanced)

Université Savoie Mont Blanc

Applicants from foreign countries may have to be evaluated by French Authorities before being allowed to be hosted by University Savoie Mont Blanc. USMB may refuse to sign or interrupt a work contract in the event of an unfavourable assessment of the Applicant.

More information: https://www.univ-smb.fr/college-doctoral/en/doctorat/sinscrire/

University of Adelaide

Short-listed applicants will need to demonstrate their suitability for entry to the program. More information: https://www.adelaide.edu.au/graduate-research/future-students/how-to-apply#step-4-apply-online

More information: https://www.adelaide.edu.au/degree-finder/2023/hdrdoctor_philosophy.html

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement № 101081465