

CybAlliance WP2 Annual Mobility Report 2023

Habtamu Abie, Chief Research Scientist, Sandeep Pirbhulal, Senior Research Scientist,
Norwegian Computing Center/Norsk Regnesentral, November 30, 2023

Abstract

CybAlliance is centered around activities that promote excellence in both research and education in cybersecurity and privacy in the healthcare sector in Norway, USA, France, and Germany. To achieve this goal, one of the objectives is to arrange national and international mobility of students, researchers, and staffs. This objective will be performed under WP2 (“Research Cooperation”) Task 2.1 (“Mobility”) which aims to arrange 24 mobility stays of students, researchers, and staff at partner institution. This report presents the results of D2.1 (“Annual mobility report”) from this task performed in 2023.

1 Introduction

This report presents the progress and achievements of mobility (WP 2.1) whose main objective is to arrange 24 mobility stays of students, researchers, and staff at partner institutions during entire project duration. The progress includes two national mobilities and one international mobility. The latter has resulted in joint publication. Section 2 describes the two national mobilities. Section 3 presents the international mobility. Finally, Section 4 describes conclusion remarks and future work.

2 National Mobility

In 2023, NTNU were actively engaged in national mobility at OUS and NR to discuss potential collaboration in research, education and innovation for healthcare security and privacy.

Given below are reports produced by NTNU for their respective mobilities including details of visits, mobility duration, purpose of visit, hosting partners, key outcomes, and relevance to the CybAlliance, among others. The reports in this section were provided by Vasileios Gkioulos and Aida Akbarzadeh.

Research Visit Report

Duration: 1 week
Period: Across weeks 45 and 46
Hosting Partner: NR

I visited NR for several days across weeks 45 and 46, as part of the collaborative research project CybAlliance. The purpose of my visit was to exchange ideas with the researchers at NR, attend seminars and workshops, and seek opportunities for strengthening our collaboration.

During my visit:

- I delivered a presentation on “Enhancing cyber security preparedness through training and awareness”.
- We coordinated the organization of the workshop “SecUre aNd Resilient digital tranSformation of healthcarE (SUNRISE)” in conjunction with the 35th Norwegian ICT Conference for Research and Education.
- We coordinated the submission of a proposal towards the Marie Skłodowska-Curie Actions 2023.
- We discussed and proceeded with the participation of Telenor Norge to NESIOT, which is a community of interest of CybAlliance qualifying project SFI-NORCICS.
- We had several discussions on enhancing the collaboration between NTNU and NR both within ongoing activities (such as the SFI-NORCICS and CybAlliance), as well as on future opportunities beyond these projects.

Overall, my visit to NR was very productive and enjoyable. I gained valuable insights and perspectives and advanced my research goals. I also established strong relationships with the researchers at NR, and we plan to continue our collaboration in the future. I would like to thank NR for hosting me and providing me with excellent facilities and support, and particularly Dr. Habtamu Abie and Dr. Sandeep Pirbhulal.

Vasileios Gkioulos, Ph.D.

Associate Professor – Secure Systems Engineering
Critical Infrastructure Security and Resilience group

Phone: (+47)61135162,
Skype: vgkioulos,
Office: T413 (NTNU in Gjøvik)
www.ntnu.no



Faculty of Information Technology
and Electrical Engineering
Department of Information Security
and Communication Technology

Product Manager for OT Security Services

Telenor Norge AS
+47 91829887
Snarøyveien 30
N-1360 Fornebu
www.telenor.com



Research Visit Report

Dr. Aida Akbarzadeh

Researcher at Information Security and Communication Technology Department, CISaR group, NTNU

Title of the Visit: "Enhancing Security in Healthcare domain"

Duration of the visit: 1 week (from November 30, 2023)

Hosting Partner: OUS

Planned and Executed Activities:

During my research visit, Professor Balasingham and his team provided an overview of the different project they are currently working on, including:

- Ultra-low power wireless transceiver design
- Algorithms for localization and tracking intra body sensors
- Signal processing for implant communications
- Sensor networks
- Algorithms for colonoscopy and capsule endoscope videos for anomaly detection
- Nanomachine-to-neuron communications and networks (graphene, molecular, THz band, etc.)

I had the opportunity to attend three different group meetings, each focusing on a different aspects of healthcare technology. It was informative to learn about their approach to research and to see how they plan and collaborate.

I also had a short visit to the operational rooms, which provided me with a better overview of the technologies and devices in use.

My Presentation Delivery:

Title: "Dependency Based Risk Analysis"

Focus: I emphasized the importance of security and risk analysis in Cyber Physical Systems, showcasing its application in the healthcare domain, discussing current challenges, and potential solutions. This was followed by questions, identifying similarities in the approaches both partners, OUS and NTNU, are applying and how we can help each other. Additionally, the presentation led to discussions about potential collaboration and future work in considering security in the health domain.

Research Visit Report

Dr. Aida Akbarzadeh

Researcher at Information Security and Communication Technology Department, CISaR group, NTNU

Title of the Visit: "Enhancing Security in Healthcare domain"

Duration of the visit: 1 week (from November 30, 2023)

Hosting Partner: OUS

Planned and Executed Activities:

During my research visit, Professor Balasingham and his team provided an overview of the different project they are currently working on, including:

- Ultra-low power wireless transceiver design
- Algorithms for localization and tracking intra body sensors
- Signal processing for implant communications
- Sensor networks
- Algorithms for colonoscopy and capsule endoscope videos for anomaly detection
- Nanomachine-to-neuron communications and networks (graphene, molecular, THz band, etc.)

I had the opportunity to attend three different group meetings, each focusing on a different aspects of healthcare technology. It was informative to learn about their approach to research and to see how they plan and collaborate.

I also had a short visit to the operational rooms, which provided me with a better overview of the technologies and devices in use.

My Presentation Delivery:

Title: "Dependency Based Risk Analysis"

Focus: I emphasized the importance of security and risk analysis in Cyber Physical Systems, showcasing its application in the healthcare domain, discussing current challenges, and potential solutions. This was followed by questions, identifying similarities in the approaches both partners, OUS and NTNU, are applying and how we can help each other. Additionally, the presentation led to discussions about potential collaboration and future work in considering security in the health domain.

3 International Mobility

The report in this section was provided by Alessio Baiocco of NTNU.

Research Visit Report

Dr. Alessio Baiocco

Researcher at Information Security and Communication Technology Department, CISaR group, NTNU

Title of the Visit: "Enhancing Security in Healthcare domain"

Duration of the visit: September 10th to September 22nd (12 days)

Hosting Partner: UCCS, University of Colorado at Colorado Springs

Planned and Executed Activities:

During my stay at UCCS - University of Colorado, Colorado Springs – Professor Shouhuai Xu and his research team provided an overview of the projects they are working on which are briefly **reported** hereafter:

1. Space Cybersecurity
2. Moving-Target Defense and Deception and Human Factors
3. Adversarial Machine Learning, especially Adversarial Malware Detection
4. Bio- and Immune System-inspired Cyber Defense
5. Security for, and by, Blockchain
6. IoT and CPS Security
7. Trustworthy Cloud and Edge Computing (Cryptographic Multi-Party Computing, Storage, Systems)

I had the opportunity to attend a meeting with the Dr. Xu and his team on which each of held a presentation with regarding of their research topic(s), in particular space cybersecurity, IoT and CSP security and Bio- and Immune System-inspired Cyber Defense

Meeting with the research group to discuss of an eventual research topic to work at during my visit.

Dr Xu organized a series of meetings to integrate me in the drafting of two scientific publications to be developed during my stay at UCCS.

Networking and Professional Interactions:

New contacts: I had the chance to connect with some of fellow researchers, which has let to a productive collaboration on writing a publication and, in the future, will lead to more collaborations.

Obtained Results and Visit Outcomes:

The visit enriched my scientific knowledge in the field of IoMT. Furthermore, a scientific publication I contributed to during my visit to UCCS was submitted to the SUNRISE 2023 conference to be held in Stavanger at the end of November. The publication has been accepted and will be presented on November 30th.

The title of the paper: Characterizing Privacy Risks in Healthcare IoT Systems

Authors: Shuai Li, Alessio Baiocco and Shouhuai Xu

Abstract: The advancement in Internet of Things (IoT) technology has been having a huge societal and economic impact, effectively changing the paradigms in doing various kinds of business, including the healthcare industry. While citizens now can enjoy the convenience brought up by healthcare IoT systems, such as wearable healthcare IoT devices, the privacy risks incurred by these systems and devices are far from being understood, let alone adequately addressed. In this paper we systematically characterize the privacy risks in healthcare IoT systems, by considering a range of privacy attack vectors such as those that can be imposed by healthcare IoT device fingerprinting and semi-honest Internet Service Providers. Then, we leverage these characteristics to guide us in exploring countermeasures for mitigating privacy risks in healthcare IoT systems. We hope the present study will serve as a baseline for designing a systematic solution to protect citizen's privacy in the healthcare IoT systems domain.

Reflections and Future Steps:

Personal Reflections: This visit turned out to be a great opportunity to broaden my knowledge of the Medical IoT (IoMT) sector. Dr. Xu and his research group are very active in the IoMT sector research and related cybersecurity at all levels.

My knowledge in cybersecurity and my engineering background helped me understand the topics covered and quickly settle into the research group.

Future Collaboration: The prospect of future collaborations is truly exciting, a real opportunity for mutual professional growth for both parties.

The drafting of one of the scientific publications was not completed because it required more time than expected for submission of the manuscript to the SUNRISE 2023 conference (Stavanger, Norway, November 2023). However, this remains as a promise of a collaboration in the short term.

4 Conclusion and Future Work

This CybAlliance WP2 ("Research Cooperation") Annual Mobility Report 2023 presented the CybAlliance Task 2.1 ("Mobility") progress and achievements D2.1 ("Annual mobility report") in 2023. The achievements include NTNU's two national mobilities and one international mobility.

The first NTNU's national mobility was at NR for several days across weeks 45 and 46, to exchange ideas with the researchers to NR to attend seminars and workshops and seek opportunities for strengthening collaboration. The second NTNU's national mobility was to OUS with the visit title "Enhancing Security in Healthcare domain" for 1 week (from November 30, 2023). This visit provided the opportunity to engage in meaningful conversations with all members of the hosting group, exchanging ideas and perspectives on healthcare technology security, understand the current trends and challenges in this field, and identify potential areas for future collaboration, especially in integrating security from the design phase in healthcare technologies and conducting specialized risk assessments in the healthcare domain.

The international mobility to UCCS which provided the opportunity to attend meetings with presentations space cybersecurity, IoT and CSP security and Bio- and Immune System-inspired Cyber Defense and to discuss of an eventual research topic to work on during the visit including the drafting of two scientific publications to be developed during the stay. One of the

papers titled Characterizing Privacy Risks in Healthcare IoT Systems has been presented at the SUNRISE 2023 conference (Stavanger, Norway, November 30, 2023) and will be published in springer CCIS proceedings.

In our future work in 2024 NR plans two international mobilities to UCCS and IMT and two national mobilities to NTNU and OUS.