NTNU

Kunnskap for en bedre verden

CybAlliance WP3 Report Course Material Report 2023

Author:
Lama Amro
Vasileios Gkioulos

November 2023

Executive Summary

The report provides a summary of the progress and achievements of WP3.4, which includes the Course Material component. This year, there has been a significant amount of effort invested in achieving the set deliverables, which involved the introduction of new courses to enhance the knowledge provided to students.

Contents

1 Introduction

In the context of WP3, the objective of TP3.4 is to improve cyber security and privacy education in the healthcare sector. Our strategy to accomplish this involves the development of educational courses that place a strong emphasis on healthcare security, thereby fostering the emergence of a well-trained and specialized workforce. Throughout this process, every partner contributes by sharing the courses that are presently on offer in their specific fields, thereby giving others a chance to discover what they might be lacking. An enhanced quality of education is achieved by providing a diverse selection of courses.

In this report, we provide a detailed explanation of the process we undertook to gather course ideas and content. Additionally, we present the proposed courses submitted by each partner. Finally, we conclude with an overview of the resulting proposed courses that are scheduled for implementation in the later stages of the project.

2 Process

The partners were requested to compile a list of the courses they offer, and the tables below display the lists provided by NTNU and GUF.

2.1 NTNU

Code	Course name	Location	Study level	Semester
TM8105	Advanced Discrete Event Simulation Methodology	Trondheim	PhD	Spring 2024
IMT6171	Artificial Intelligence and Machine Learning for Information Security Applications	Gjøvik	PhD	Spring 2024
IMT6121	Behavioural Biometrics	Gjøvik	PhD	Autumn2023
IMT6071	Biometrics	Gjøvik	PhD	Spring 2024
IMT6091	Computational Forensics	Gjøvik	PhD	Autumn2023
IMT6101	Computational Intelligence(Exam only, no teaching)	Gjøvik	PhD	Spring 2024
IMT6271	Critical Thinking	Gjøvik	PhD	Spring 2024
TM8107	Cryptographic Protocols and Their Applications	Trondheim	PhD	Spring 2024
IIK8010	Cyber Physical Systems Security	Gjøvik	PhD	Spring 2024
TM8101	Dependability Analysis of Information and Communication Systems	Trondheim	PhD	Spring 2024
TM8103	Formal Methods	Trondheim	PhD	Spring 2024
IIK8001	Human factor methods for Information Security Research	Gjøvik	PhD	Autumn2023
IMT6003	IIK Summer School	Gjøvik	PhD	Spring 2024
TM8111	Identity-Based Cryptography	Trondheim	PhD	Spring 2024
IMT6011	Introduction to Information Security	Gjøvik	PhD	Autumn2023
IMT6031	Intrusion Detection and Prevention	Gjøvik	PhD	Autumn2023
IMT6081	Modern Cryptology	Gjøvik	PhD	Autumn2023
TM8106	Optical Networking	Trondheim	PhD	Spring 2024
IMT6251	Quality in Academic Research	Gjøvik	PhD	Spring 2024
IMT6261	Scientific Communication	Gjøvik	PhD	Spring 2024
IMT6041	Selected Topics in Cryptology	Gjøvik	PhD	Autumn2023
TM8102	Traffic Analysis of Communication Networks	Trondheim	PhD	Spring 2024
IMT6051	Wireless Communication Security	Gjøvik	PhD	Autumn2023

2.2 GUF

Code	Course name	Location	Study level	Semester
MOB1	Mobile Business I - Technology, Markets, Platforms, and Business Models	Frankfurt am Main	Master	Winter 23/24
PWIN	Wirtschaftsinformatik 2	Frankfurt am Main	Bachelor	Winter 23/24
RAN1:W24	Data Privacy Analysis in Cloud Services	Frankfurt am Main	Master	Winter 23/24
MOB2	Mobile Business II - Application Design, Applications, Infrastructures and Security	Frankfurt am Main	Master	Summer 2024
RAN1:S24	A Seminar with and about ChatGPT and Large Language Models (LLMs)	Frankfurt am Main	Master	Summer 2024
PDBM	Privacy vs. Data: Business Models in the digital, mobile Economy	Frankfurt am Main	Master	Summer 2024
INKO	Informations- und Kommunikationssicherheit: Infrastrukturen, Technologien und Geschäftsmodelle (Information and Communication Security)	Frankfurt am Main	Master	Summer 2024

2.3 NR and OUS

NR is a research institute; therefore, it does not offer any courses. Most of the registered PhD students at NR take courses from NTNU or UiO. OUS is a healthcare institution that does not offer security and privacy courses, so it does not have any courses relevant to CybAlliance.

2.4 IMT and UCCS

IMT and UCCS have been internally identifying which courses are relevant to CybAlliance's visions and objectives. However, they will assist in identifying new material for new courses.

2.5 Potential courses

Once the partners had compiled the previously mentioned course lists, they engaged in a discussion to propose additional courses, resulting in the compilation of the following potential new courses. The presented courses are tentative, and the partners will begin in 2024 a quality assurance process prior to finalizing the proposed courses and course descriptions, the purpose of this process is to ensure the quality of the proposed courses and to maximize the impact to the community. This will be followed by establishing a strategy for the development and delivery of the courses, in the second half of 2024:

- Health informatics-Data protection and security: Protecting data and ensuring security is crucial in health informatics, as it safeguards the privacy, confidentiality, and integrity of health information. The course will cover the concepts, principles, and standards of data protection and security in health informatics, along with implementation challenges and best practices. The course will include subjects like data governance, data quality, data sharing, data encryption, data anonymization, data breach prevention and response, and data ethics.
- Ethics in eHealth: The course will analyze the ethical impact of using digital technologies in healthcare. The course will address various subjects, including privacy, consent, data protection, social justice, and human dignity in relation to eHealth applications and services. The course's goal is to provide students with the knowledge and skills needed to address ethical issues in eHealth practice and research.

- Medical technology cyber hygiene/ Cyber hygiene for Health sector: The goal of Cyber hygiene for the Health sector is to equip health professionals with the necessary knowledge and skills to safeguard their digital assets and data against cyber threats. Topics covered in the course include cyber security basics, best practices, policies and standards, risk assessment and management, incident response and recovery, and ethical and legal issues. In addition, the course will feature small scale hands-on exercises and case studies to showcase the practical implications of cyber hygiene in the health sector.
- Digital Literacy for Healthcare Professionals: The course aims to equip students with the skills and knowledge to use digital technologies effectively and ethically in their healthcare practice. The course will cover topics such as digital communication, data management, information literacy, online collaboration, and digital health applications. The course will also explore the challenges and opportunities of digital transformation in the healthcare sector, such as privacy, security, quality, and innovation.

3 Conclusion and Future work

Working on WP.3.4 aided the partners in evaluating their cybersecurity offerings, related to cybersecurity education in health care. This will have an impact on the quality of education by having a new variety of courses. Next year, the partners will work together to design course materials based on course levels and determine institutional responsibilities.