ESSENTIAL

H2020-MSCA-ITN-2016

Marie Skłodowska-Curie actions (MSCA)

Innovative Training Networks (ITN)

Grant Agreement Number 722482

ESSENTIAL

Evolving Security SciencE through Networked Technologies, Information policy And Law

EJD

WP 5: Training Programme

LEAD PARTNER – Norwegian University of Science and Technology

D5.9 - Fellows' Handbook for Trust and Security Technologies

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

Project co-funded by the European Commission within Marie Skłodowska-Curie actions (MSCA) Innovative Training Networks (ITN)		
Dissemination Level:		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	

Document Version Control:		
Version 0.1	Prepared by: Katrin Franke	20/March/2019

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482”.

Table of contents

1. INTRODUCTION 5

1.1. Aim of the Handbook 5

1.2. Usage of the Material 5

1.3. COINS - Research School of Computer and Information Security 5

2. MASTER-LEVEL: TRUST AND SECURITY TECHNOLOGY 6

2.1. System Security (IMT4123) 6

2.2. Critical Infrastructure Security(IMT4203) 7

2.3. Socio-technical Systems Enabled Crime (IMT4128) 9

2.4. Digital Economics (TTM4165) 11

2.5. Data Science for Security and Forensics (IMT4133) 12

2.6. Cybercrime Investigation (IMT4130) 14

2.7. Computational Forensics (IMT4210) 17

2.8. Reverse Engineering and Malware Analysis (IMT4116) 18

2.9. Further Master-level Courses and Readings 20

3. PHD-LEVEL: TRUST AND SECURITY TECHNOLOGY 21

3.1. Intrusion Detection and Prevention (IMT 6031) 21

3.2. Modern Cryptology (IMT6081) 24

3.3. Biometrics (IMT6071) 26

3.4. Behavioural Biometrics (IMT 6121) 29

3.5. Wireless Communication Security (IMT6051) 32

4. COINS: COURSES AND EVENTS 35

4.1. Brief Overview 35

4.2. Portfolio 35

4.3. COINS COURSE DESCRIPTION 36

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

1. Introduction

1.1. Aim of the Handbook

The aim of this handbook is to provide an overview on selected topics for Truss and Security Technologies primarily to the ESRs with a basic technical background. The aim is to assist the ESSENTIAL Early Stage Researchers and other students in the field of security science gain deeper understanding in selected topics of trust and security technologies. This Handbook is regularly updated on the Vergaderen platform (that is, the internal communication platform used within ESSENTIAL).

1.2. Usage of the Material

The material provided below is adopted from the accredited Master and PhD programs in information security at the Norwegian University of Science and Technology (NTNU). Course in Information Security at the NTNU are open for ESR in the ESSENTIAL project. ESR can choose to enrol in the courses, follow the entire course remotely or on campus, and being guided over the duration of the course, usually one semester. OR, acquire the learning outcomes, skills, and general competences, mentioned below, by studying the course materials entire individually.

Courses outline below are on the general Master and PhD level - course codes on 4xxx-level and 6xxx-level respectively. Non-technical ESR in the ESSENTIAL project are recommend to study Master (4xxx-level) courses, while ESR with a previous, technical education are strongly encouraged to follow PhD (6xxx-level) courses.

1.3. COINS - Research School of Computer and Information Security

ESR in ESSENTIAL project are encouraged to participate in the Norwegian Research school COINS that provides a vide portfolio of training activities that are accredited at PhD-level.For detail see course portfolio below.

2. Master-level: Trust and Security Technology

2.1. System Security (IMT4123)

Course content

- Access control and information flow (formal models and systems)
- System security analysis (attack-defense trees and covert channels)
- Secure software development (security assurance and evaluation)
- Vulnerabilities and attack patterns (analysis and detection)
- Operating systems security (hardware protection, privileges, I/O protection, virtualisation)

Learning outcome

Candidates who have successfully completed this course, should have achieved the following total learning outcome

Knowledge:

- Candidates are expected to possess in-depth knowledge of formal modelling techniques for secure computer systems
- Candidates have advanced knowledge of common vulnerabilities, attack mechanisms, and methods against computer and information systems
- Candidates have thorough knowledge on the theory and methods underlying access control and information flow policies
- Candidates have thorough knowledge on security techniques and methods applied in operating systems
- Candidates have thorough knowledge about secure software system assurance and evaluation

Skills:

- Candidates are capable of applying relevant methods for security modelling and analysis of software applications and information systems.
- Candidates are capable of analysing, evaluating and enhancing the security of information systems independently by identifying potential threats and propose possible countermeasures

General Competence:

- Candidates can analyse relevant professional and research ethical problems related to securing information system and software.
- Candidates are capable of applying their knowledge and skills in new fields, in order to carry out advanced tasks and projects.
- Candidates can work independently and are familiar with terminology of the field of software and system security.
- Candidates can communicate about academic issues related to system and software security both with specialists and public audience.
- Candidates can contribute to innovation and innovation processes in information security.

Course materials

- Bishop, M. (2018). Computer Security: Art and Science. Addison-Wesley Professional

2.2. Critical Infrastructure Security (IMT4203)

Course content

- Critical Infrastructures and Information Infrastructures
- Threat Actors and Agents in Critical Infrastructures
- Infrastructure Modelling, Robustness, and Dependencies

- Cyber-Physical Systems and their Security
- Control Systems Security
- Selected Aspects of Critical Telecommunications Infrastructure Security and Resilience
- Selected Aspects of Power Networks and Generation Infrastructure Security and Resilience
- Selected Aspects of Oil and Gas Infrastructure Security and Resilience
- Selected Aspects of Transportation Infrastructure Security and Resilience

Learning outcome

Knowledge:

- Advanced knowledge of core concepts of critical information infrastructures and general critical infrastructure as well as their dependencies
- Advanced understanding of infrastructure and infrastructure robustness models
- Advanced knowledge of cyber-physical systems and control systems security

Skills:

- Ability to analyse threat modelling approaches and to assess their suitability for a given set of threat sources and agents
- Ability to critically analyse existing theories and methods for the study of cyber-physical systems security and to independently apply such methods to related problems
- Ability to carry out research in selected areas of infrastructure security and resilience under guidance and supervision
- Ability to identify and critically analyse primary research literature on critical infrastructure security and to apply appropriate scientific reasoning

General competence:

- Ability to apply knowledge of concepts and methods of analysing security and resilience of infrastructures to new fields

- Capability to discuss academic and professional topics in the field of modelling and securing selected critical infrastructures both with a specialist and general audience
- Critical understanding of professional and ethical, including research ethics, issues in the field of critical infrastructure security

Course materials

- E.D. Knapp: Industrial Network Security
- Elsevier (2011)M. Newman: Networks
- Oxford University Press (2010)
- K. Stouffer, V. Pilliteri, S. Lightman, M. Abrams, A. Hahn: NIST SP800-82Rev2: Guide to Industrial Control Systems Security
- U.S. National Institute of Standards and Technology (2015)
- G. Sorelo, M. Echols: Smart Grid Security
- CRC Press, 2012
- Setola, Lopez, Wolthusen: Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defence
- Lecture Notes in Computer Science Vol. 7130, Springer-Verlag (2012)

2.3. Socio-technical Systems Enabled Crime (IMT4128)

Course content

- Historical Technology adoption and Information Security Problems and Solutions in Society Organisation and for individuals
- Technology enable crime in society and organisation
- Socio-technical metrics for cultural, and organisational changes.
- Introduction to Socio-technical Risk, Threat and vulnerability Modelling
- Root Cause Analysis - Society, Organisation, Individual.

Learning outcome

Knowledge:

- The students shall primarily understand the socio-technical ICT evolution that has taken place over the last thirty years that has led to a widening vulnerability gap between what we can do with ICT and what we can cost effective control with ICT.
- The students shall be given a broad systems theory perspective connected to practical cases so they will have the insight to implement a roadmap for information security in organisations and businesses.
- The candidate possess insight and understanding of technological enable crime
- The candidate possesses good understanding of the socio-technical risk analysis and reflect on the use appropriate security metrics for analysis.

Skills:

- The student can use relevant systems sciences and socio-technical theory in independent research and development in information security organisation and management
- The student is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning information security organisation and management.
- The student is capable of carrying out an independent limited research or development project in information security and management under supervision, following the applicable ethical rules.

General competence:

- The student is capable of analysing relevant professional and research ethical problems in information security organisation and management.
- The student is capable of applying his/her information security knowledge and skills in new fields, in order to accomplish advanced tasks and projects.

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482”.

- The student is capable of discussing professional problems, analyses and conclusions in the information security organisation and management, both with specialists and with general audience.
- The student is capable of contributing to innovation and innovation processes in information security and socio-technical modelling and analysis for information security management.

Course materials

- Books/standards, conference/journal papers and web resources.
- Optional: Marie A. Wright: John S Kakalik , Information Security: Contemporary CasesInformation Security: Contemporary Cases , Jones and Bartlett Publishers, Inc. , USA ©2006 ISBN:0763738190

2.4. Digital Economics (TTM4165)

Course content

The digitisation of the economy is one of the most critical issues of our time. Digital technologies has transformed businesses and peoples life, and will continue to do so in the future. This course is about digital economics and how the digital economy influences markets, the society and organisations. We learn about how the Internet, mobile communications, the sharing economy, social media, and cryptocurrencies impact global businesses.

The course consists of two parts:

1. Basic theory in digital economics, including: network effects, value creation models, digital business models and market modelling.
2. How the digital economy influences societies, environment, regulations, privacy, strategy, and financial operations.

Learning outcome

Knowledge:

- To get broad knowledge in digital economics.
- To get broad knowledge on how the digital economy impacts its surroundings.

Skills:

- To perform network effect analysis of a value network.
- To analysis and construct a business model.

Course materials

To be announced at the beginning of the term.

2.5. Data Science for Security and Forensics (IMT4133)

Course content

- Learning, Intelligence, and Machine learning basics: principles, measures, performance evaluation, method combinations.
- Knowledge representations: discriminant and regression functions, probability distributions, Bayesian classifier.
- Learning as search: Exhaustive search, heuristic search, genetic algorithms.
- Attribute quality measures: measures for classification, measures for regression, application of feature-selection measures.
- Data preprocessing: Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA).
- Supervised symbolic and statistical learning, basics of artificial neural networks.
- Unsupervised Learning and cluster analysis: hierarchical and partial clustering.
- Data classification: Bayesian classifier, k-NN classifier, multi-layered perceptron (MBPN), support vector machine (SVM), and Random Forrest.

- Data clustering: k-means clustering, Self-Organising map (SOM).
- Classification and clustering validity testing: leave-one-out, ground truth.
- Practical tasks may include to realise some search methods, classification methods, and some clustering methods

Learning outcome

Knowledge:

- Understand principles how multidimensional statistical methods differ from one dimensional methods.
- Understand the distribution of information in statistical analysis and meaning in data representation.
- Extract features from raw, measured values of data to be analysed.
- Program some basic classification and clustering methods and test their validity.
- Program some basic Neural networks methods and test their validity.
- To apply basic statistical and data analysis methods to data relevant in information security, forensics and/or colour/media technology

Skills:

- The students can use relevant scientific methods in independent research and development in machine learning and pattern recognition.
- The students are capable of carrying out an independent limited research or development project in machine learning and pattern recognition under supervision, following the applicable ethical rules.

General competence:

- The students can work independently and are familiar with terminology of machine learning and pattern recognition as well as their application in the security and forensics domain.

Course materials

Books/standards, conference/journal papers and web resources, such as:

- Kononenko, M. Kukar, Machine Learning and Data Mining: Introduction to Principles and Algorithms, Horwood Publishing, Chichester, U.K., 2007, ISBN 1-904275-21-4

Recommended further reading:

- T. Mitchell, Machine Learning, McGraw Hill, 1997.
- R.O.Duda, P.E. Hart, and D.G. Stork: Pattern Classification. 2nd edition., Wiley, 2001.
- S. Theodoridis, and K. Koutroumbas. Pattern Recognition, 3rd edition. Academic Press.

2.6. Cybercrime Investigation (IMT4130)

Course content

- Digital Forensics Ontology
- File carving and reconstruction
- Multi-media forensics
- Malware Forensics: static, dynamic, content
- Memory Forensics
- Fraud detection and analysis
- Open source Intelligence and Internet forensics
- Cloud forensics
- Search for digital evidence
- Selected topics, as for example: Identity Theft, Bitcoin and Dark Net investigation
- Guest lectures, as for example: Cooperate Forensics, Embedded device forensics,
- Laboratory to forensic case scenarios, investigation report and mock trail

Learning outcome

Knowledge:

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482”.

- Candidates develop deep understanding in the methodology, technology and application of digital forensics in cybercrime investigation.
- Candidates are expected to reach an advanced level of knowledge in the broad spectrum of digital evidence, analysis methods and tools.
- The course is oriented towards profound theoretical background, where the students learn contemporary techniques, best practices, and advanced topics.

Skills:

- Candidates are capable of analysing existing theories, methods and interpretations in the field of digital forensics and working independently on solving theoretical and practical problems related to cybercrime investigation.
- Candidates can use relevant methods in independent studies and development in digital forensics.
- Candidates are capable of performing critical analysis of various literature sources and applying them in structuring and formulating problem-oriented reasoning in cybercrime investigation.
- Candidates are capable of carrying out an independent limited study or development project in cybercrime investigation under supervision, following the applicable ethical rules.

General competence:

- Candidates are capable of analysing relevant professional and research ethical problems in cybercrime investigation.
- Candidates are capable of applying their knowledge and skills in new fields, in order to accomplish advanced tasks and projects in cybercrime investigation.
- Candidates can work independently and are familiar with terminology of cybercrime investigation.
- Candidates are capable of discussing professional problems, analyses and conclusions in the field of digital forensics, both with specialists and with general audience.

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

- Candidates are capable of contributing to innovation and innovation processes.

Course materials

The following textbook is the primary reference. Additional sources, e.g. presentation material and 10 selected papers will be provided during the course.

- M.Ligh, S.Adair, B.Hartstein and M.Richard (2010). Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code.

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482”.

2.7. Computational Forensics (IMT4210)

Course content

Deepening of knowledge and skills in computer-assisted digital investigations and forensics using specific methods to realistic case scenarios. Methods may include yet are not limited to:

- Forensic Statistics
- Forensics Data Science
- Pattern Recognition
- Machine Learning
- Predictive Analytics
- Information Retrieval
- Data Mining
- Signal and Video Processing
- Computer Visualisation

A selection of possible case scenarios will be made available at the beginning of the course.

Learning outcome

Knowledge:

Understanding of cutting-edge problems in computational and forensic sciences as well as their applications specific domains, as for example threat intelligence, automation of malware analysis, biometric identification, network intrusion detection, internet investigation, deep-package mining and multimedia-content analysis in forensics.

Skills:

- The students can use relevant scientific methods in independent research and development in computational forensics.

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

- The students are capable of carrying out an independent limited research or development project in computational forensics under supervision, following the applicable ethical rules.

General competence:

- The students can work independently and are familiar with computational forensic terminology.

Required previous knowledge

Candidates should have read IMT4133 Data Science for Security and Forensics.

Course materials

- Scientific Articles related to the field of Specialisation.

2.8. Reverse Engineering and Malware Analysis (IMT4116)

Course content

- Malware methodology
- Basic analysis
- Advanced static analysis
- Advanced Dynamic analysis
- Anonymous and stealthy analysis
- Malware classification and functionality
- Anti Reverse-engineering
- Malware lab

Learning outcome

Knowledge:

The candidate possess

- knowledge of methodology, technology and application of malware analysis and reverse engineering
- thorough knowledge of anonymous analysis
- advanced knowledge of static malware analysis
- advanced knowledge of dynamic malware analysis
- thorough knowledge of malware classification and functionality
- knowledge of anti-reverse engineering techniques
- thorough knowledge of building and using a malware lab

Skills:

The candidate is capable to

- apply malware analysis methodology and technology
- apply advanced static malware analysis
- apply advanced dynamic malware analysis
- identify basic and some advanced malware functionality
- identify known anti-reverse engineering techniques
- conduct an analysis without revealing that the investigation is taking place and/or revealing their identity.

General competence:

The candidate is

- capable of analysing relevant professional and research problems in malware analysis
- capable of applying their knowledge and skills in new fields, in order to accomplish advanced task and projects in malware analysis
- capable of working independently as a malware analyst and is familiar with terminology.

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

- capable of discussing professional problems, analysis and conclusions in the field of malware analysis, both with professionals and with general audience
- has the learning skills to continue acquiring new knowledge and skills in a largely self-directed manner
- capable of contributing to innovation and innovation processes

Required previous knowledge

Laboratory activities will involve analysing and handling malicious code on your computer system. Virtual machines and due caution will be used, but it is nevertheless not recommended to use your organisations laptop in laboratory activity.

Course materials

Books/standards, conference/journal papers and web resources, such as

- M.Sikorski and A. Honig: Practical Malware Analysis, The hands on guide to dissecting Malicious Software
- M. Ligh, S Adair, B Hartstein and M.Richard: Malware Analyst¿s Cookbook and DVD: Tools and Techniques for Fighting Malicious Code.

2.9. Further Master-level Courses and Readings

For an extended list of courses and detailed descriptions see https://tinyurl.com/y2z3bhkz

3. PhD-level: Trust and Security Technology

3.1. Intrusion Detection and Prevention (IMT 6031)

Course content

- IDS/IPS definition and classification
- Basic elements of attacks and their detection
- Misuse detection systems (search algorithms and applications in IDS)
- Anomaly detection systems (machine learning basics: principles, measures, performance evaluation, method combinations, basics of artificial neural networks, clustering (hierarchical and partitional) and supervised learning in IDS)
- Testing IDS and measuring their performances
- Computational complexity-theoretic and information-theoretic IDS models and quality criteria
- Intrusion detection in virtual networks.

Learning outcome

Skills:

- The candidate is capable of formulating problems, planning and completing research projects in the field of intrusion detection and prevention.
- The candidate is capable of doing research and development at a high international level.
- The candidate is capable of handling complex academic tasks. The candidate can challenge established knowledge and practice in the field of intrusion detection and prevention.

Knowledge:

- The candidate possesses knowledge at the most advanced frontier in the field of intrusion detection and prevention. The candidate has mastered academic theory and scientific methods in intrusion detection and prevention.

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482”.

- The candidate is capable of considering suitability and use of different methods and processes in research in the field of intrusion detection and prevention.
- The candidate is capable of contributing to development of new knowledge, theories, methods, interpretations and forms of documentation in the field of intrusion detection and prevention.

General Competence:

- The candidate is capable of identifying relevant - and possibly new - ethical problems and exercising research in the field of intrusion detection and prevention with academic integrity.
- The candidate is capable of managing complex interdisciplinary tasks and projects.
- The candidate is capable of disseminating the results of research and development in the field of intrusion detection and prevention through approved national and international publication channels.
- The candidate is capable of taking part in debates in international forums within the field of intrusion detection and prevention.
- The candidate is capable of considering the need for, taking initiative to and engaging in innovation in the field of intrusion detection and prevention.

Learning methods and activities

- Lectures
- Lab.work
- Assignments
- Project work

- The course is taught on the individual basis - reading the literature and consulting the teacher.

Further on evaluation

Re-sit:

- The whole course must be repeated.

Forms of assessment:

- Oral exam
- Project evaluation
- Both parts must be passed

Course materials

- Rebecca Gurley Bace, Intrusion Detection, Macmillan, 2000.
- Jack Koziol, Intrusion Detection with SNORT, SAMS, 2003.
- David J. Marchette, Computer Intrusion Detection and Network Monitoring - A Statistical Viewpoint, Springer Verlag, 2001.
- Richard Bejtlich, Extrusion Detection - Security Monitoring for Internal Intrusions, Addison-Wesley, 2005.
- Stephen Northcutt, Judy Novak, Network Intrusion Detection, 3rd edition, New Riders, 2003.Various papers (available on-line)

3.2. Modern Cryptology (IMT6081)

Course content

- Introduction - elements of information theory, general cipher system theory
- Contemporary theory of randomness - randomness and indistinguishability
- Elements of modern symmetric ciphers theory - Galois fields, primitive polynomials, Boolean functions theory, block ciphers theory, hash functions theory
- Public key cryptography - RSA theory, digital signatures

Learning outcome

The module provides an overview over several foundational areas in information security. In doing so, the module seeks to provide a consistent narrative emphasising the need for thorough analysis of threats and vulnerabilities and the inclusion of assurance mechanisms and metrics over considering security mechanisms in isolation.The core of the module is given over to a rigorous discussion of security models and their relation to access control models with selected issues in identification and authentication and their required trust and reputation models also covered.

Knowledge:

- The candidate possesses knowledge at the most advanced frontier in the field of cryptology. The candidate has mastered academic theory and scientific methods in cryptology.
- The candidate is capable of considering suitability and use of different methods and processes in research in the field of cryptology.
- The candidate is capable of contributing to development of new knowledge, theories, methods, interpretations and forms of documentation in cryptology.
-

Skills:

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482”.

- The candidate is capable of formulating problems, planning and completing research projects in cryptology.
- The candidate is capable of doing research and development at a high international level.
- The candidate is capable of handling complex academic tasks. The candidate can challenge established knowledge and practice in cryptology.

General Competence:

- The candidate is capable of identifying relevant - and possibly new - ethical problems and exercising research in cryptology with academic integrity.
- The candidate is capable of managing complex interdisciplinary tasks and projects.
- The candidate is capable of disseminating the results of research and development in cryptology through approved national and international publication channels.
- The candidate is capable of taking part in debates in international forums within the field of cryptology.
- The candidate is capable of considering the need for, taking initiative to and engaging in innovation in the field of cryptology.

Learning methods and activities

- Lectures
- Project work
- Tasks

Further on evaluation

Re-site:

- The whole course must be repeated.

Forms of assessment:

- Oral exam
- Project evaluation of one project
- Both parts must be passed

Course materials

- Introduction to Cryptography and Coding Theory, 2. edition, Trappe W., Washington L., Prentice Hall, 2006, ISBN: 0131981994.
- Handbook of Applied Cryptography, Menezes A., http://www.cacr.math.uwaterloo.ca/hac
- Introduction to modern cryptography, Katz J., Lindell Y., Chapman&Hall/CRC, 2008, ISBN: 1-58488-551-3Various papers (available on-line)

3.3. Biometrics (IMT6071)

Course content

- Fingerprint recognition
- Vein recognition
- Face recognition specifically focused on three dimensional data
- Iris recognition
- Multimodal biometrics
- Score Normalisation
- Attack mechanisms
- Privacy Enhancing Technologies
- Revocable biometric references

Learning outcome

Knowledge:

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

- The candidate possesses knowledge at the most advanced frontier in the field of biometrics.
- The candidate has mastered academic theory and scientific methods in biometrics.
- The candidate is capable of considering suitability and use of different methods and processes in research in the field of biometrics.
- The candidate is capable of contributing to development of new knowledge, theories, methods, interpretations and forms of documentation in biometrics.

Skills:

- The candidate is capable of formulating problems, planning and completing research projects in biometrics.
- The candidate is capable of doing research and development at a high international level.
- The candidate is capable of handling complex academic tasks.
- The candidate can challenge established knowledge and practice in biometrics. More specifically after the course, the candidate should have the following capabilities:
    - developed a systematic understanding of biometric systems and their capabilities
    - mastered multiple modality-specific feature extraction and have the ability to evaluate their suitability for given acquisition characteristics
    - developed in-depth insights into statistical methods and tools for biometrics and their performance evaluation
    - the ability to synthesise multi-modal analysis methods and solve score normalisation problems in fusion systems
    - the ability to appraise and differentiate threats to biometric reference data, judging and realising adequate protection mechanisms accordingly
    - the ability to perform in-depth assessment of biometric component placement within a security system
    - demonstrated the ability to design and defend a biometric security system when provided with a threat scenario

General competence:

- The candidate is capable of identifying relevant - and possibly new - ethical problems and exercising research in biometrics with academic integrity.
- The candidate is capable of managing complex interdisciplinary tasks and projects.
- The candidate is capable of disseminating the results of research and development in biometrics through approved national and international publication channels.
- The candidate is capable of taking part in debates in international forums within the field of biometrics.
- The candidate is capable of considering the need for, taking initiative to and engaging in innovation in the field of biometrics. More specifically the candidate will have the competence to
  - demonstrate the ability to design a biometric system suitable for a given scenario
  - judge the relevance of ethical and privacy issues
  - investigate for a given scenario technical solutions and evaluate them in a critical analysis.
  - synthesise new ideas during evaluation phase
  - communicate with peers in the biometric community in terms of reviewing research topics
  - manage team work

Learning methods and activities

- Lectures
- Assignments
- Seminar(s)

Additional information: Seminar with term paper presentation

Further on evaluation

Re-site:

- The whole course must be repeated.

Forms of assessment:

Candidates must provide a research report (term paper) on a topic that is chosen by the candidate in coordination with the lecturer. The term paper should preferably not focus on a survey of methods but rather address original research and be submitted to a scientific conference (e.g. NISK, BIOSIG)

Required previous knowledge

None - however the course content will be complementary to the course "Behavioural Biometrics". The course Machine Learning is recommended as an accompanying module for this course; although some concepts of applied statistics and decision theory are revisited in this course, candidates will benefit from the more rigorous treatment of the subject matter in IMT4612 and IMT 4632.

Course materials

- LI , S . Z. , AND JAIN, A. K. , Eds. Handbook of Face Recognition. Springer, 2011.
- MALTONI , D. , MAIO, D. , JAIN, A. K. , AND PRABHAKAR , S . Handbook of Fingerprint Recognition. Springer, 2009.
- WAYMAN, J . , JAIN, A. , MALTONI , D. , AND MAI O, D. , Biometric Systems. Springer, 2005.
- JAIN, L.C. , HALICI, U. , HAYASHI, I. ; LEE, S.B., TSUTSUI, S. Intelligent Biometric Techniques in Fingerprint and Face Recognition. CRC Press, 1999.
- TUYLS, P., SKROIC, B., KEVENAAR, T. Security with Noisy Data. Springer, 2007

3.4. Behavioural Biometrics (IMT 6121)

Course content

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

- Authentication methods in general
- Password Security
- Behavioural biometric system evaluation
- Gait recognition
- Keystroke Dynamics
- Signature verification
- Mouse Dynamics
- Continuous Authentication Systems
- Evaluation of Continuous Authentication Systems

Learning outcome

Objectives:

Give the candidates an improved understanding of

- Different general authentication mechanisms
-
- Selected authentication methods: passwords/PIN, gait, signature, keystroke dynamics, mouse dynamics
- The concept of Continuous Authentication
- Technics to test authentication methods

Knowledge:

- The candidate possesses thorough knowledge of the security of knowledge based authentication systems.
- The candidate possesses advanced knowledge in the theory, design and evaluation of Behavioural Biometric Systems.
- The candidate possesses advanced knowledge in the theory, design, and evaluation of Continuous Authentication Systems.
- The candidate is capable of applying his/her knowledge in the field of IT-security.

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

- The candidate is capable of updating his/her own knowledge in authentication related topics.

Skills:

- The candidate is capable of using relevant scientific methods in independent research and analysis in biometrics.
- The candidate is capable of performing critical analysis of various literature sources on authentication methods.
- The candidate know relevant authentication methods and terminology.

General competence:

- The candidate is capable of taking part in debates in national and international fora within the field of authentication and behavioural biometrics.
- The candidate is capable of working independently in the field of biometrics and is familiar with biometric terminology.
- The candidate is capable of analysing relevant professional and research publications in behavioural biometrics.

Learning methods and activities

- Lectures
- Project work
- Tutoring

Additional information: This course will be mainly self-study with some supervision of the lecturer.

Further on evaluation

Re-site:

The whole course needs to be repeated

Evaluation forms:

- The final grade is based upon written report and an oral examination.
- The student must provide a report on a topic that is chosen by the lecturer.
- The oral exam will focus on both the report and the course content.

Course materials

A reader written by the lecturer is handed out to the candidates at the beginning of the course. Additional course material is available in Blackboard.

3.5. Wireless Communication Security (IMT6051)

Course content

- Introduction - elements of radio frequency theory, elements of information security with applications in the wireless environment, elements of physical layer security (the wiretap channel).
- Elements of RFID systems security analysis with case studies: the electronic passport
- Elements of WLAN security analysis
- Bluetooth system security
- Security in mobile telephony systems with case studies: the 2G, the 3G and the 4G, opportunities in 5G.

Learning outcome

Knowledge:

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

- The candidate possesses knowledge at the most advanced frontier in the field of wireless communication security. The candidate has mastered academic theory and scientific methods in wireless communication security.
- The candidate is capable of considering suitability and use of different methods and processes in research in the field of wireless communication security.
- The candidate is capable of contributing to development of new knowledge, theories, methods, interpretations and forms of documentation in the field of wireless communication security.

Skills:

- The candidate is capable of formulating problems, planning and completing research projects in the field of wireless communication security.
- The candidate is capable of doing research and development at a high international level.
- The candidate is capable of handling complex academic tasks. The candidate can challenge established knowledge and practice in the field of wireless communication security.

General competence:

- The candidate is capable of identifying relevant - and possibly new - ethical problems and exercising research in the field of wireless communication security with academic integrity.
- The candidate is capable of managing complex interdisciplinary tasks and projects.
- The candidate is capable of disseminating the results of research and development in the field of wireless communication security through approved national and international publication channels.
- The candidate is capable of taking part in debates in international forums within the field of wireless communication security.
- The candidate is capable of considering the need for, taking initiative to and engaging in innovation in the field of wireless communication security.

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482".

Learning methods and activities

- Lectures
- Project work

The course is taught on the individual basis - reading the literature and consulting the teacher.

Further on evaluation

Re-sit: The whole course must be repeated

Forms of assessment:

- Oral exam
- Project evaluation
- Both parts must be passed.

Course materials

- D. Forsberg, G. Horn, W. Moeller, V. Niemi, LTE Security, 2nd. edition, Wiley, 2013.Various papers (available on-line)

4. COINS: Courses and Events

4.1. Brief Overview

The Research School “COINS Research School of Computer and Information Security” integrates Norwegian research groups in Information Security to a larger entity by integrating the course portfolio for research school members, builds stronger relationships between doctoral students in the network, establishes more incentives to excel and increases student mobility through access to a larger network. COINS also increases Norway’s international student mobility, hosts internationally recognised researchers, and offers “free flow of goods and services” in Information Security Research in Norway. COINS expects to recruit 40 students at any given moment.

COINS is led by the Norwegian University of Science and technology (NTNU) in Gjøvik. Participants in the research school include University of Agder, University of Bergen, University of Oslo, University of Stavanger, University of Tromsø, and NTNU.

For more details see https://coinsrs.no/about-coins/

4.2. Portfolio

COINS offers a wide range of course and thematic portfolio on advanced topics in cyber and information security. the topics are related to emerging trends and ongoing research within the domain. Lecturers from academic, governmental, and private sector share new insights, experiences, now ongoing challenges with the audience.

Over the duration off their PhD research studies ERS and members of the research school can attend up to three COINS workshops, annual summer and winter schools. For more details see https://coinsrs.no/upcoming_events/ and https://coinsrs.no/events-phd-courses/

4.3. COINS Course description

Course content

A winter school, summer school, workshop and IT-security exercise (compare https://www.ntnu.edu/studies/phdis/programme-components) can span all aspects of information security, i.e.

- Foundations of information security and security models, e.g. authentication, access control, biometrics, identity management, cryptography, modelling
- Secure programming, e.g. development processes, vulnerability analysis, embedded & cyber-physical systems
- Computer crime, digital forensics, privacy and civil liberties, including legal aspects, privacy
- Network security and security operations, e.g. perimeter security, intrusion detection, critical infrastructure protection
- Risk assessment, human factors and security, e.g. risk analysis, security management, security economics, incident management, awareness

The exact choice and composition of topics in a given year may vary.

In addition, COINS events address cross-cutting concerns like peer review, presentation in the scientific community, and collaboration.

Learning outcome

After having successfully completed the course, students are expected to have mastered the following learning outcomes:

- Knowledge of advanced research in information security.

Learning methods and activities

- Block seminars, presentation

Further on evaluation

Re-sit: Whole course must be re-taken.

Forms of assessment: Passing a COINS workshop involves preparation and presentation of a research article and passing an oral examination.

Course materials

- Scientific articles and hand-outs provided by lecturers.

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 722482”.