ESSENTIAL

H2020-MSCA-ITN-2016

Marie Skłodowska-Curie actions (MSCA)

Innovative Training Networks (ITN)

Grant Agreement Number 722482

ESSENTIAL

Evolving Security ScienE through Networked Technologies, Information policy And Law

EJD

WP 5: Training Programme

LEAD PARTNER – Norwegian University of Science and Technology

D5.8 - Fellows' Handbook for Introduction to Information 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".

ESSENTIAL

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 4

1.1. AIM OF THE HANDBOOK 4

1.2. USAGE OF THE MATERIAL 4

2. MASTER-LEVEL: INTRODUCTION TO INFORMATION SECURITY 5

2.1. INTRODUCTION TO CYBER AND INFORMATION SECURITY TECHNOLOGY (IMT4113) 5

2.2. INTRODUCTION TO DIGITAL FORENSICS (IMT4114) 8

2.3. INTRODUCTION TO INFORMATION SECURITY MANAGEMENT (IMT4115) 11

3. PHD-LEVEL: INTRODUCTION TO INFORMATION SECURITY 15

3.1. INTRODUCTION TO INFORMATION SECURITY (IMT 6011) 15

3.2. FOUNDATIONS OF INFORMATION SECURITY (IMT6201) 18

"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 easy introduction to Information Security primarily to the ESRs with a limited technical background. The aim is to assist the ESSENTIAL Early Stage Researchers and other students in the field of security science understand the basics of information-security aspects and to introduce them to accredited courses and key texts to assist their learning. 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 level 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 enroll in the courses, follow the entire course, 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 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 ESSENTAIL project are recommend to study Master (4xxx-level) courses in information security, while ESR with a technical education previously are strongly encouraged to follow PhD (6xxx-level) courses.

"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. Master-level: Introduction to Information Security

2.1. Introduction to Cyber and Information Security Technology (IMT4113)

Course content

- Bases of Crypto;
- Bases of Network Security;
- Authentication, Identification, and Biometrics;
- Access Control Models;
- Bases of Integrated System Security;
- Intrusion Detection;
- Introduction to Critical Infrastructure Security

Learning outcome

Knowledge:

- The candidate will have a thorough knowledge in the core concepts of cyber and information security technologies
- The candidate possesses thorough knowledge in the primitives of cryptology
- The candidate possesses knowledge about theory and scientific methods relevant to cryptology
- The candidate possesses basic knowledge in the theory and application of network security
- The candidate has thorough knowledge in the theory and methods in authentication and identification as well as general access control mechanisms
- The candidate will possess knowledge in the area of vulnerabilities and attack mechanisms and methods against cyber and information security systems
- The candidate possesses basic knowledge about integrated system 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".

Skills:

- The candidate is capable of finding and performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in any of the topics of this course
- The candidate is capable of analysing existing theories, methods, and interpretations in any of the fields in this course, and work independently on solving theoretical and practical problems.
- The candidate can plan and conduct a limited guided research exercise based on primary literature

General competence:

- The candidate is capable of independent working and are familiar with core concepts and problems in the area of cyber and information security technology
- The candidate is capable of discussing issues in the field of cyber and information security technology with specialists, decision makers and a general audience
- The candidate is capable to translate the concepts and ideas of cyber and information security technology to other fields, both inside and outside of general information security
- The candidate is able to identify advanced information security technology related problems and to contribute with approaches to solve these

Learning methods and activities

- Lectures
- Compulsory Assignments

"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".

Additional information:

The course will be made accessible for both campus (Gjøvik, NO) and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus (Gjøvik, NO) and are open for both categories of students. All the lectures will also be available on Internet through the university's learning management system.

Further on evaluation

Re-sit:

Possibility to retake written exam part of course in summer (August). If there is a re-sit examination, the examination form may be changed from written to oral.

Forms of assessment:

The overall grade is based on a grade for a final, written exam (3 hrs) as well as a grade for mandatory assignments.The final, written exam will count for 60% while the assignments count for 40% of the final grade. Both parts will be graded on a 0-100 scale and must be passed with at least 40 out of 100 points in order to pass the course. The final grade is the weighted average of the part scores and the 0-100 scale score of the final grade will be converted to the A-F scale according to recommended conversion table. In specific circumstances, can the course responsible slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale.

Course materials

"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".

W.Stallings & L. Brown: "Computer Security - Principles and practice", 4.edition (Global edition), ISBN-10:1-292-22061-9, ISBN-13:978-1-292-22091-1

2.2. Introduction to Digital Forensics (IMT4114)

Course content

- Digital investigations, stakeholders and their roles
- Digital evidence, e.g. acquisition, admissibility, authenticity
- Chain of custody, evidence integrity and forensic soundness
- File and live system forensics
- Timeline analysis
- Forensic reconstructions
- Internet and network forensics
- Automation and forensic tools
- Reporting and presenting evidence
- Expert witness and cyber crime law
- Computational forensics
- Forensic readiness
- Advanced topics if time permits

Learning outcome

Knowledge:

- Digital Forensics methodology with a solid understanding of requirements for handling digital evidence
- Requirements and impact on maintaining evidence integrity and chain of custody
- Principles, procedures, and the basic concepts of forensic standards and best practices, e.g. forensic tool testing
- The overall process for establishment and maintenance of a digital forensic lab environment
- The role of expert witnesses and digital evidence in the context of legal proceedings

"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 role of policies, standards and guidelines for controls and is capable of applying his/her knowledge in case studies
- Legal, privacy and ethical aspects of digital forensics investigations.

Skills:

- Forensic acquisition of digital evidence from computer and network media
- Live system forensics and evaluation of order of volatility
- Evidence analysis with timeline analysis and forensic reconstruction
- Scientific documentation of forensic acquisition and analysis
- Applying forensic principles on practical case-studies
- Performing stakeholder analysis, risk assessment and forensic triage on limited case-studies
- Evaluating the applicability of forensic methods and tools for various controls given a certain scope and policy for the control

General competence:

- Capability of analysing business, legal, ethical and case-specific requirements for planning and conducting a digital forensics investigation
- Understanding of forensic analysis and incident response processes
- Working independently and familiarity with digital forensics terminology
- Capability of discussing professional problems such as documentation, decision making processes, implementation plans, operations, reviews and corrective actions, with forensic experts, IT specialists and general managers
- Learning skills to continue acquiring new knowledge and skills in a largely self-directed manner
- Ability to contribute to innovative thinking and innovation processes

Learning methods and activities

- Lectures

"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".

- Group work
- Lab work
- E-learning
- Project work

Additional information:

This course is given on campus Gjøvik and will be accessible for off-campus/remote students (including Trondheim). The lectures will be live-streamed and made available as a recording for offline viewing through the university's learning management system. Each student is free to choose the pedagogic arrangement that best suits her/his own requirement. More information about this course will be provided on the first lecture and in our learning management systems.

Students should follow/attend the lab work sessions and complete all required hand-ins. The lab sessions will be live-streamed to remote students and be made available as recordings for offline viewing. More information about the lab sessions will be provided closer to its planned schedule.

Group-wise oral presentation of selected paper and project work must be approved for the group/project work as a whole to be approved.

Group projects, exercises and remote teaching assistance are guiding on demand.

Further on evaluation

Re-sit:

- Ordinary re-sit examination in August for the final written exam.

Forms of assessment:

"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".

- A group-wise oral presentation of a selected paper and project must be passed for the whole group/project work to pass.
- The final grade is an average of the project work and written exam, they count for 49% and 51% respectively, according to the recommended averaging process. Both parts must be completed to receive a final grade.
- The final written exam through Inspera

Course materials

- Course book (Digital Forensics, André Årnes ed.), lectures, other presentations/supplementary materials and selected papers.

2.3. Introduction to Information Security Management (IMT4115)

Course content

- Introduction to System Thinking and Scientific Management
- Cultural, Organisation and Behaviour theories used information security management organisation.
- Legal and Ethical Aspects of Information and Privacy Management.
- Overview of current information security management standards and practices
- Basic Micro and Macro Theory of Information Security
- Introduction to Risk, Threat and vulnerability Modelling
- Information Security Management and Security Awareness education and training
- Overview of Security Planning and Incident Management

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 possess through knowledge of the fundamental theories , models practices of information security management for both large and small organisation.
- The candidate possess insight and understanding of ethical and legal aspect information security management and privacy management
- The candidate possesses good understanding of the risk management processes
- The candidate possesses good understanding of security planning and incident management process
- The candidate possess insight and good understand of security awareness and security escalations issues in information security management work
- The candidate possess insight and good understand of both macro and micro economics issues in information security management.
- The candidate possess insight of the technological innovation process in IT security and its effect on security management.
- The candidate possess basic knowledge of the standards in information security management

Skills:

- The candidate is capable of analysing existing theory , models and methods in the field of information security management and work independently on solving theatrical and practical problems.
- The candidate is capable of applying his/her knowledge to both modelling the potential problems and the solutions in information security management and be able to communicate this problems and solutions using basic rhetorical skills.
- The candidate is capable of using and the basic terminology and is aware of the basic standards used in the area.

General competence:

"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".

- Can participate in group work and manage different organisation roles of information security management.

Learning methods and activities

- Lectures
- Group work
- E-learning
- Assignments
- Project work
- Reflection
- Seminar(s)

Additional information:

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus Gjøvik, and are open for both categories of students. All the lectures will also be available on Internet through the NTNU Gjøvik lecture recording system and integrated in the learning management system.

Mandatory:

Each group must:

- Present and get approval on their mini case work s/case.
- Get group concept approval of the term paper
- Deliver an individual commented PPT

Compulsory assignments

"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".

- SOHO Risk Analysis

Further on evaluation

Re-sit:

- Ordinary re-sit examination for the written exam in August.
- A new, written assignment must also be completed for failed project report.

Forms of assessment:

- Project reports (49%)
- 3-hours written individual exam (51%).
- A mandatory assignment to perform SOHO risk analysis needs to be complete in order be eligible to write the written exam
- Each part must be passed to pass the course.

Course materials

- Management of Information Security newest (5th) Edition by Michael E. Whitman (Author), Herbert J. Mattord (Author) ISBN for 2016: ISBN-13: 978-1305501256 / ISBN-10: 130550125X
- Course Material provided on / Blackboard

"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".

3. PhD-level: Introduction to Information Security

3.1. Introduction to Information Security (IMT 6011)

Course content

- Key results in the theory and modelling of information security
- Network security
- Operating system security
- Human factors in security
- Security engineering and assurance
- Cyber-physical systems security
- Cryptography and cryptanalysis
- Database security
- Information security management
- Anonymity and privacy

Learning outcome

The module (mandatory for doctoral students in the programme) is intended to provide additional insights into the information security domain for doctoral students in Information Security beyond their immediate area of specialisation.To this end two areas of information security that are distinct from the candidate's specialisation are to be identified, where the two areas should normally also not overlap. For each area (including but not limited to those identified below), a sub-area is to be chosen, and primary and secondary literature to be studied to elaborate a seminar paper. In one of the areas, the sub-area chosen should be such that a reasonable overview of the state of the art in the research specialisation can be achieved and described, whilst a second area may follow a somewhat wider remit and rely more on secondary literature. The results will be a synopsis and survey of the two respective sub-areas, combined with individual perspective and reflection by the candidate.

"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".

Skills:

On concluding the module, candidates

- can identify relevant primary and secondary research literature in the respective areas chosen by the candidate, forming an insight into the state of the art in an unfamiliar area
- can synthesise the state of the art and articulate key research problems and methods in the respective areas chosen by the candidate
- are able to evaluate the merits and contributions of research articles in the respective areas chosen by the candidate

Knowledge:

On concluding the module, candidates

- will be able to summarise the state of the art in the respective areas chosen by the candidate
- can outline key methods employed by research in the respective areas chosen by the candidate and state relative merits
- can identify main strands of inquiry and key results in the respective areas chosen by the candidate

General Competence:

On concluding the module, candidates

- can appraise the merit of research methods and quality of research in the sub-areas studied also in relation to the candidate's own specialisation area
- is able to cogently discuss the state of the art in the chosen areas for the seminar papers
- is able to identify gaps in the state of the art in the respective areas chosen by the candidate

Learning methods and activities

- Lectures
- Individual discussions

"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".

- Seminars
- Literature study

Compulsory requirements:

- Students are required to prepare a term paper on one of the subject areas covered in the course in coordination with and approved by the lecturer and must provide a presentation of results and findings in a seminar.
- The delivery date for the term paper is arranged individually to match the seminar schedule.

Further on evaluation

Re-sit:

- New seminar papers must be provided.

Forms of assessment:

- Two seminar papers are to be provided by the candidate and are marked separately by the examiner on a Pass/Fail scale.
- Both papers must be completed successfully to secure an overall Pass grade.

Course materials

The textbooks, monographs, and research articles are determined by the respective sub-area chosen for the seminar papers and will normally need to reflect the state of the art in the area. The following identifies a small number of seminal papers and texts in selected areas only.
Suggested textbooks:

- O. Goldreich: Foundations of Cryptography (2 vols.), Cambridge University Press, 2001-2004

"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".

- W. Diffie and M. Hellman: New Directions in Cryptography. IEEE Transactions on Information Theory 22(6):644-654 (1976)
- R. L. Rivest, A. Shamir,, and L. Adleman: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2):120-126 (1978)
- E. Bertino and R. Sandhu: Database Security - Concepts, Approaches, and Challenges. IEEE Transactions on Dependable and Secure Computing 2(1):2-19 (2005)
- J. Vaidya and C. Clifton: Privacy-Preserving Decision Trees over Vertically Partitioned Data. ACM Transactions on Knowledge Discovery from Data 2(3):14 (2008)
- K. Thompson: Reflections on Trusting Trust Communications of the ACM 27(8):761-763 (1984)
- J. Feigenbaum, A. Johnson, and P. Syverson: A Model of Onion Routing with Provable Anonymity" Proceedings of the 11th International Conference Financial Cryptography and Data Security (FC 2007), Vol. 4886 of Lecture Notes in Computer Science. Trinidad/Tobago, Feb. 2007, Springer-Verlag.
- E. Peeters, F.-X. Standaert, and J.-J. Quisquater: Power and Electromagnetic Analysis: Improved Model, Consequences, and Comparisons Integration: The VLSI Journal 40(1):52-60 (2007)
- D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi: The EM Side-Channel(s) Proceedings of Cryptographic Hardware and Embedded Systems (CHES 2002), Vol. 2523 of Lecture Notes in Computer Science, Lausanne, Switzerland, Sep. 2002, Springer-Verlag.
- A. Mishra: Security and Quality of Service in Ad Hoc Wireless Networks, Cambridge University Press, 2010
- S.K. Das, K. Kant, N. Zhang: Handbook on Securing Cyber-Physical Critical Infrastructure. Elsevier, 2012

3.2. Foundations of Information Security (IMT6201)

Course content

- Security Analysis Models and Methods
- Foundations of Identification and Authentication

"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".

- Trust and Reputation Models
- Access Control Models and Foundational Results
- Security and Information Flow Models
- Developmental Assurance

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.

Skills:

On concluding the module, candidates

- are able to analyse an information system's security relying on formal and semi-formal methods
- can identify appropriate formal security and information flow models consistent with threat and risk analyses as well as security policies
- are able to evaluate and conduct developmental assurance processes

Knowledge:

On concluding the module, candidates

- will have an in-depth understanding of formal security models, particularly access control and information flow models

"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".

- will be able to synthesise or analyse a formal or semi-formal system security analysis with emphasis on attack tree variant models
- can articulate constraints and risks for identification and authentication mechanisms serving as a pre-requisite for formal security model

General Competence:

On concluding the module, candidates

- are able to assess formal and informal security models
- have formed an overview of the foundations of information security allowing to contextualise and frame discussions in the area
- will have developed the ability to link disjoint areas of information security, synthesising security models and realisations

Learning methods and activities

- Lectures
- Literature study and term paper

Further on evaluation

Re-site:

- Failing one part requires a re-sit of both parts, a new term paper must be provided.

Evaluation forms:

Assessment consists of two parts; both parts must be passed to secure an overall 'Pass' grade:

"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".

- Part I is a written examination (3 hours), accounting for 33% of grade. Candidates must achieve an 'A' or 'B' grade to gain the equivalent 'Pass' Grade in Part I. The written exam evaluated by internal and external examiners.
- Part II is a term paper, accounting for 67% of grade. The term paper is evaluated by the lecturer on a Pass/Fail scale.

Course materials

The following textbooks are the primary references; further recommended reading is provided in the course syllabus.

- D. Gollmann: Computer Security, 3rd edition Wiley, 2011
- M. Bishop: Computer Security: Art and Science. Addison-Wesley, 2003.

"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".