Co-funded by the Erasmus+ Programme of the European Union

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

Exploitation Plan

Version 1.4

Author(s)/Organisation(s):

Igor Tartalja, Zarko Stanisavljevic / UB

Imre Lendak / UNS

Date of final release:

January 20th, 2018

Relevant Work Package(s):

WP1 – Preparation

Short Description:

ISSES course result exploitation plan

Keywords:

Exploitation Plan (EP)

Revision History:

Revision	Date	Author(s)	Status	Description
v1.0	Jan 20, 2018	Igor Tartalja	Working draft	First edition
v1.1	Jun 6, 2018	Imre Lendak	Release	v1.1 contains formatting changes only
v1.2	Jun 11, 2018	Imre Lendak	Release	List of authors updated
v1.3	Jan 29, 2020	Imre Lendak	Release	Study programs and KPIs added
v1.4	Feb 03, 2020	Dejan Simić, Žarko Stanisavljević, Igor Tartalja	Release	Added section 4.2 and revised several other sections

CONTENTS

Abbreviations

Abbreviation	Meaning	Comment
CI	Critical Infrastructure	
EP	Exploitation Plan	This document
ETF	Elektrotehnički fakultet	School of Electrical Engineering – Part of the University of Belgrade
FON	Fakultet organizacionih nauka	Faculty of Organization Sciences – Part of the University of Belgrade
HEI	Higher Education Institution	
N/A	Not Available	
UB	University of Belgrade	
UNI	University of Nis	
UNS	University of Novi Sad	
VTS	Visoka tehnička škola strukovnih studija Subotica	Subotica Tech - College of Applied Sciences

1 Introduction

The Exploitation Plan (EP) defines the specific activities necessary to maximize the exploitation potential of the project. The project team defined activities which will ensure that all relevant stakeholders are reached, especially among the students, teachers, public institutions, Non-Governmental Organizations (NGO) and in the industrial sectors which require and hire information security professionals. This document encompasses HEIs plans on the developed courses exploitation, plans on the implemented laboratories exploitation by partners' HEIs and industrial partners, and plans on usage of produced course materials, such as Power Point presentations by engineers in industry. Also, the EP contains a detailed plan of the annual information security roundtables organized by the project partners. These roundtables will be attended by key stakeholders, who will discuss the results achieved and possible ways of result exploitation in academia and industry.

It is planned that each higher education institution (HEI) in Serbia obtains an infrastructure security specialization during this project in the following manner:

- the University of Novi Sad will specialize in Critical Infrastructure Protection,
- the University of Belgrade – School of Electrical Engineering will specialize in network security,
- the University of Belgrade – Faculty of Organizational Sciences will specialize in digital forensics with a sub-specialization in data mining and mobile data forensics, and
- Subotica Tech will specialize in cloud security and Internet of Things (IoT) security.

The above specializations will allow the partner HEIs to diversify the skills gained during this project and to have complementary skills allowing them to invite guest lecturers from other institutions. Additionally, the specializations will allow the academic staff to have skills which make them the best specialists in their respective fields in Serbia. This will allow the academic staff to more easily market their skills, i.e. to provide consultancy services to various stakeholders in Serbia and outside the borders of Serbia.

2 Courses exploitation by HEIs

This chapter contains partners' HEIs plans on the developed courses exploitation. Students and teachers will be key users of the developed materials for target courses.

The table presents summary information on the planned courses exploitation by partners' HEIs.

Course Title	Developed & Used by	Used by
Critical Infrastructure Security	UNS	
Secure Software Development	UNS, UNI, ETF	VTS
Cloud Security – Integrated into 2.15	UNS, ETF (PhD-level)	VTS
Security and privacy in the Internet of Things	VTS, UNI	
Advanced Cryptography	UNS	ETF (partially)
Advanced Network Security	ETF, VTS	UNS, UNI, FON
Cyber Security Strategies	FON	UNS, UNI
Security in E-business Systems – Integrated into 2.5	UNS	
Risk Analysis and Threat Modelling	FON, UNS	
Cyber Incident Analysis and Response	FON, UNS	
Data Mining in Digital Forensics	FON	
Digital Forensics Tools and Techniques	FON, UNI	UNS, ETF (partially)
Mobile and Multimedia Forensics	FON, UNI	VTS
Security Data Science	UNS, UNI	
Computer Security	UNS	ETF

2.1 Critical Infrastructure Security

UNS. The Critical Infrastructure Security (CIS) course will be part of the newly-developed MSc in Information Security at the UNS. It will equip students with necessary skills to enter the information security workforce with advanced knowledge of CI-specific information security architectures (both traditional and modern), network theory and its application in CI protection, vulnerability and risk analysis, industry-specific standards, the latest tools and techniques used by both attackers and defenders of CIs. The expected number of students will be 13-16 in the first year and will be aligned with student and industry demands in the following years. Industrial partners from Novi Sad and Vojvodina will benefit from this course as it will train subject matter experts which are in high demand and whose specific CIS knowledge the company can then include in its professional services portfolio offered to their CI clients worldwide.

The course will prepare students for passing the following industry/infrastructure security certifications[1]:

- Certified SCADA Security Architect (CSSA)
- SANS Global Industrial Cyber Security Professional certification (GICSP)
- ISA99/IEC 62443 Cyber Security Certificate Program

[1] https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals/at_download/fullReport

2.2 Secure Software Development

UNS. The course will be offered to both students who enroll into the newly-developed MSc in Information Security at the UNS, and 4th-year BSc students of the Software Engineering and Information Technologies study program. Schneider Electric DMS Llc and other companies providing software development services or developing software intensive products in and around Novi Sad, Serbia will immediately benefit from the additional secure software development skills gained by students passing this course.

UNI. The course will be offered as an elective to students who enroll the Computer Science and Engineering master program at the UNI, particularly to those who enroll the Information Security and Digital Forensics module. Both information security engineers and software engineers that pass this course (10-20 per year) will gain knowledge related to design and implementation of secure software for the benefits of IT companies in which they will be employed.

ETF. The new course will be offered as an elective at the Software Engineering master degree program at the University of Belgrade-School of Electrical Engineering. The prerequisite for attending the course will be sucesfuly completed Computer Security course. The number of students that fulfil the prerequisite is around 200 per year, thus the expected number of students attending the new course will be between 10 and 50 per year. In that way software engineers will expand their knowledge to include secure software development issues.

VTS. The course will be offered to students who enroll into the MSc in Informatics at Subotica Tech – College of Applied Sciences . The number of students is expected to be between 20 and 35 per year. In this course students will gain an understanding of the software development life cycle and the security implications that may arise in order to ensure that the software their organization uses is well written and secure throughout its lifespan. The students will development their skills and knowledge to write secure code, and recognize the security shortcomings in any existing code.

Other stakeholders. The course content and selected exercises on the Avatao training platform will be offered to financial institutions and other relevant stakeholders with internal software development departments.

2.3 Cloud Security

Integrated into 2.15 Computer Security.

2.4 Security and privacy in the Internet of Things

VTS. This course will be offered to MSc students. The predicted number of students will be between 20 and 35 per year. In this course the students will learn how to adapt security and privacy mechanisms that allow them to reap the potential benefits of IoT, without endangering critical infrastructure or individual privacy.

UNI. The course will be offered as an elective to students who enroll the Computer Science and Engineering master program at the UNI, particularly to those who enroll the Information Security and Digital Forensics module. The course will provide software and systems engineers in the field of mobile and ubiquitous application development necessary knowledge for development of secure mobile, ubiquitous and IoT solutions preserving privacy of users.

UNS. Elements of this course will be integrated into 2.1 Critical Infrastructure Systems.

2.5 Advanced Cryptography

UNS. The course will equip students with both hands-on experience dealing with the latest cryptographic tools and techniques and theoretical depth in understanding them. Students excelling in this course will be capable to develop advanced data protection solutions in various systems. Elements of this course will be used to upgrade the existing introductory courses in information security at the Department of Power, Electronic and Telecommunication Engineering.

ETF (partially). The results from this course development will be used at the existing bachelor degree course Algorithms and Data Structures at the University of Belgrade-School of Electrical Engineering. The selected topics will be added to the course material. In that way computer and software engineers who attend the course will expand their knowledge to include advanced cryptographic algorithms.

VTS. The course will be offered to students of the MSc program. It will help students to better understand threats and attacks on web based e-business systems. Emphasis will be on security of transactions, secure web forms, secure data interchange and development of secure e-business systems. The course will upgrade the students' existing knowledge of web programming and computer networks.

Other stakeholders. Parts of the course and their specific extensions will be used as training materials for cybersecurity hackathons, especially the Serbian Cybersecurity Challenge organized by the ISSES team.

The course will prepare students for passing the following relevant cybersecurity and/or information security certifications[2]:

- Certified Information System Security Professional (CISSP) issued by the ISC[2].

2.6 Advanced Network Security

ETF. The new course will be offered as an elective at the Computer Engineering master degree program at the University of Belgrade-School of Electrical Engineering. The prerequisite for attending the course will be sucesfuly completed Computer Security course. The number of students that fulfil the prerequisite is around 200 per year, thus the expected number of students attending the new course will be between 10 and 50 per year. In that way computer engineers who attend the course will expand their knowledge to include advanced network security issues. The course will lean on the newly developed network security laboratory.

VTS. Students learn about typical risks and preventative measures for a variety of network configurations, including wireless networks, cloud-based networks, and different hardware/software setups. The Advanced Network Security program prepares students to enter this field by providing training in security risk assessment as well as in preventing, monitoring, and responding to common security breaches and hacks.

UNS. The course will equip students with knowledge to harden modern IP networks. The level of knowledge acquired will be sufficient to protect any IP network against both professional cybercriminal elements and state-funded attack vectors

[2] https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals/at_download/fullReport

UNI. The course will be offered as an elective to students who enroll the Computer Science and Engineering master program at the UNI, particularly to those who enroll the Information Security and Digital Forensics module. The course will provide insights into the network security weaknesses and enable students to obtain advanced knowledge how to enhance the security and how to apply advanced security techniques to computer networks.

FON. The results of development of this course will be used for refreshment and innovation of existing course "Security Techniques in Computer Networks" within the existing master program Information Systems and Technologies at the Faculty of organizational sciences. The expected number of students is between 25 and 35. Selected topics will be also used for existing course "Computer Systems Security" within the existing undergraduate academic program Information Systems and Technologies at the Faculty of organizational sciences. The expected number of students will be between 12 and 25.

The course will prepare students for passing the following relevant cybersecurity and/or information security certifications[3]:

- Systems Security Certified Practitioner (ISC[2])
- Certified Information System Security Professional (CISSP) issued by the ISC[2].
- CompTIA Security+

2.7 Cyber Security Strategies

FON. The course will be offered as an elective at the Information Systems and Technologies MSc program, Management and organization MSc program, as well as Information Security and Digital Forensics MSc program at the University of Belgrade-Faculty of Organizational Sciences. The total number of students enrolled in these programs is around 350 per year. The expected number of students who will attend this course could be between 20 and 35. The course develops the capabilities of students to understand cyber security in the context of risk and opportunities for the creation of national and organizational goals. The students evaluate the significance of multi-stakeholder collaboration, information sharing, building of appropriate cyber security structure for development of a sustainable and comprehensive national and organizational cyber security system. Students will be able to develop appropriate policies and strategies for strengthening of cyber power for the purpose of support to national goals and organizational missions.

UNS. The course will be an elective course on the MSc level. It will equip students with skills required for managerial and/or audit roles in information security.

UNI. The course will be offered as an elective to students who enroll the Computer Science and Engineering master program at the UNI, particularly to those who enroll the Information Security and Digital Forensics module. The course will provide advanced knowledge how to enhance cyber security and how to apply advanced security strategies and policies.

The course will prepare students for passing the following relevant cybersecurity and/or information security certifications[4]:

[3] https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals/at_download/fullReport

[4] https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals/at_download/fullReport

- Certified Information System Security Professional (CISSP) issued by the ISC[2].

2.8 Security in E-business Systems

Integrated into 2.5.

2.9 Risk Analysis and Threat Modelling

FON. The course will be offered as an elective at the Information Systems and Technologies MSc program and Bussiness Analytics MSc program at the University of Belgrade-Faculty of Organizational Sciences. It is planned also to introduce an elective course within planned new master program "Information Security and Digital Forensics" at the Faculty of organizational sciences. The total number of students enrolled in these programs is around 170 per year and the expected number of students who will attend this course will be between 15 and 35. The selected topics from the course will be incorporated into Risk assessment seminars in the Institute for Standardization of Serbia (ISS).

UNS. Selected elements of this course will be incorporated into the Critical Infrastructure Security course developed during this project.

2.10 Cyber Incident Analysis and Response

FON. It is planned to introduce an elective course within planned new master program "Information Security and Digital Forensics" at the Faculty of organizational sciences, University of Belgrade. The results of the project will be used for preparation and realization of the mentioned course. This course will provide a broad and sustainable set of knowledge necessary for detect-analyse-react cyber security resilient organizational environment from managerial and legal issues to necessary tools and techniques. The expected number of students is between 15 and 35.

UNS. Selected elements of this course will be incorporated into the Critical Infrastructure Security course developed during this project. It will be used as an elected courses in the strategic/managerial module of the MSc in Information Security program.

2.11 Data Mining in Digital Forensics

FON. It is planned to introduce an elective course within planned new master module “Information Technologies and Cyber Security” as a part of “Information Systems and Technologies” study program at the Faculty of organizational sciences, University of Belgrade. The results of the project will be used for preparation and realization of the mentioned course. The expected number of students is between 20 and 35.

UNS. Selected elements of this course will be incorporated into the digital forensics courses taught at the UNS.

2.12 Digital Forensics Tools and Techniques

FON. It is planned to introduce an elective course within planned new master module “Information Technologies and Cyber Security” as a part of “Information Systems and Technologies” study program at the Faculty of organizational sciences, University of Belgrade. The results of the project will be used for preparation and realization of the mentioned course. The expected number of students is from 20 to 35. This course will provide necessary knowledge in electronic evidence retrieval and how to collect the data without damaging or altering the original data. Digital forensics

is the practice of recovering and investigating information found on digital devices. This course will provide students with skills equal to an entry-level forensic examiner – ability to acquire, analyze and report information, with exposure to advanced topics, such as live system and mobile forensics. Students will learn how to perform the essential duties of a forensic examiner, prepare for and execute digital forensic investigations on Windows and Linux based systems, apply forensic methodologies to preserve, acquire, extract and analyze information of investigative importance, as well as to identify and analyze key artifacts of investigative importance.

UNI. The course will be offered as an elective to students who enroll the Computer Science and Engineering master program at the UNI, particularly to those who enroll the Information Security and Digital Forensics module. Students will obtain theoretical and practical knowledge of the process of identification, preservation and analysis of digital evidence, knowledge of software and hardware tools for digital forensics, knowledge of the legal components of digital forensics, knowledge of basic principles, policies and methodologies of digital forensics.

UNS. This course will be incorporated into the newly-developed MSc in Information Security program developed at the UNS, as well as the existing MSc in Software Engineering and Information Technologies. It will equip the students with necessary knowledge to perform post mortem investigations after failures or cyber attacks occurring in critical infrastructures. Elements of the Data Mining in Digital Forensics course will be incorporated into this course. Course pre-requisites: none.

ETF (partially). The results from the development of a new course will be used at the existing bachelor degree course Computer Security at the University of Belgrade-School of Electrical Engineering. The selected topics will be added to the course material. In that way computer and software engineers who attend the course will expand their knowledge to include digital forensics.

2.13 Mobile and Multimedia Forensics

FON. It is planned to introduce an elective course within the new master module “Information Technologies and Cyber Security” as a part of “Information Systems and Technologies” study program at the Faculty of organizational sciences, University of Belgrade. The results of the project will be used for preparation and realization of the mentioned course. The expected number of students is between 20 and 35.

UNI. The course will be offered as an elective to students who enroll the Computer Science and Engineering master program at the UNI, particularly to those who enroll the Information Security and Digital Forensics module. Students will obtain knowledge of the process of identification, preservation and analysis of digital evidence related to mobile and multimedia data/software/devices and knowledge of software and hardware tools for mobile and multimedia forensics, as well as legal components of mobile and multimedia forensics.

VTS. The students will learn how to forensically preserve, acquire, and examine data stored on mobile devices and utilize the results. Also, this course prepares students to conduct digital forensic examinations on multimedia evidence, specifically images, videos and audio files. The course builds student knowledge starting from the basics of multimedia types to being able to recognize anomalies in files and identify file creation attributes. The projected number of students will be between 10 and 20 per year.

2.14 Security Data Science

UNS & UNI. The course will equip students with both the theoretical and practical skills necessary to fill in Security Analyst Level 1 and 2 roles, which are highly sought after in Security Operations Centers (SOC) worldwide. The key topics covered by this course will lie at the intersections of data science, network security monitoring (NSM) and malware analysis. The inclusion of this course will increase the overall appeal of the MSc in Information Security and Computer System Security module at the institutions, as it lies at the intersection of two hot topics, namely data science and cybersecurity.

2.15 Computer Security

UNS. The course will be offered to students who enroll into the newly-developed MSc in Information Security at the UNS. It will equip the students with necessary skills and knowledge in the hardware-, operating system- and cloud security domains.

ETF. Elements of the course concerning the coud security domain will be included in a newly developed elective course at the Software Engineering PhD degree program at the University of Belgrade-School of Electrical Engineering, called Cloud Security. The existing Computer Security course at the bachelor degree will be updated.

The course will prepare students for passing the following relevant cybersecurity and/or information security certifications[5]:

- Systems Security Certified Practitioner (ISC[2])
- Certified Cloud Security Professional (CCSP)

2.16 Key performance indicators (KPI)

The exploitation goals of the curricula (i.e. course content in lectures and exercises) developed and updated as part of the ISSES project will be measured by the following key performance indicators:

- Number of study programs in which the courses are included – measured on a course-by-course level.
- Number of industry-grade certification programs incorporated and covered by the course content. Measured as a number of certification programs per course.
- Number of students enrolled into each of the courses.
- Number of extra-HEI courses taught. For example, it is envisaged that parts of 2.2. Secure Software Development will be delivered in companies and other legal entities outside the project consortium. Measured as the number of trainings and trainees per training.
- Number of additional trainings prepared as part of the courses and towards training the participant of the Serbian Cybersecurity Challenge program, i.e. number of course content created/updated to be used as training material for the hackathons.

[5] https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals/at_download/fullReport

3 Laboratories exploitation by HEIs and industrial partners

This chapter contains plans on the developed laboratories exploitation. The laboratories will be used for students education, especially for their practice in information security, network security, and digital forensics domains. Also, the laboratories will be used for research of interest in the above mentioned domains. Industrial partners will be motivated to participate in the research & development of interest, together with teachers and students, by using specific equipment in the implemented laboratories.

The following laboratories will be designed:

- Critical Infrastructure Security Laboratory (CIS Lab), by UNS
- Digital Forensics Laboratory (DF Lab), by FON & UNI
- Network Security Laboratory (NS Lab), by ETF
- Cloud Security Laboratory (CS Lab), by UNS

The table presents summary information on the planned implementation and usage of laboratories by appropriate partners' HEI.

Laboratory Title	**Used by**
Hybrid CIS, CS and NS Lab implementation	UNS
Hybrid NS and Crypto Lab Implementation (P5)	ETF
NS Lab implementation (P6)	UNI
DF Lab Implementation (P5)	FON, UNI, UNS
Hybrid CS and IoT Lab Implementation (P9)	VTS

3.1 Hybrid CIS, CS and NS Lab implementation

UNS. The lab will be used to support the Critical Infrastructure Security, Computer Security, Security Data Science, Advanced Network Security and Advanced Cryptography courses developed during this Erasmus+ CBHE project. It will allow the students to obtain hands-on experience in an environment equipped similarly to real-life infrastructure control centers. It will also allow the students to familiarize themselves with modern technologies just entering the CI sector, e.g. security in cloud computing, secure versions of well-known industrial protocols. The lab will allow researchers at the UNS to investigate various information security architectures which might be later practically implemented in industrial or critical infrastructure settings.

3.2 Hybrid NS and Crypto Lab Implementation

ETF. During the project a laboratory design for the NS laboratory will be made together with the EU partners. After that the appropriate equipment will be purchased and the NS laboratory will be implemented at the University of Belgrade-School of Electrical Engineering. Together with the NS laboratory, a cryptography laboratory will also be implemented using software systems implemented at the University of Belgrade-School of Electrical Engineering. This new hybrid laboratory will be used at the existing Computer Security course, and also on the newly developed Advanced Network Security course. This will enable students who attend these courses to have a higher degree of practical work during their studies.

3.3 NS & IoTS Lab implementation

UNI. The lab will be used to support the Network Security (Basic and Advanced), IoT Security and Privacy, and Secure Software Development courses. The lab will be designed and implemented jointly with national and EU partners. The state-of-the-art network and IoT equipment and infrastructure prurshased during project and advanced network and IoT software will enable students who attend these courses to have a higher degree of practical work and knowledge in protection and preserving network and IoT security and privacy.

3.4 DF Lab implementation

FON. Design of the DF Lab will be made together with EU partners during the project. The DF Lab will allow students to learn foundations of digital forensics and to obtain necessary practical skills such as identifying and finding digital evidence, analysis of digital evidence, securing and presenting digital evidence, analysis and preparation of legal frameworks and normative instruments necessary for the use of digital evidence. The DF Lab will be used for practical work for many courses within planned new master module “Information Technologies and Cyber Security” as a part of “Information Systems and Technologies" study program at the Faculty of organizational sciences, University of Belgrade. Staff members of Faculty of organizational sciences will cooperate within the DF Lab with: judicial authorities, state administration bodies, research institutions, professionals and professional bodies in this field as well as partner faculties on the project in order to solve incidents in cyberspace.

UNI. The DF Lab will provide students necessary knowledge and hands-on experience in state-of-the-art equipment and software used in digital forensic investigations. It will allow UNI staff members to further improve their knowledge and skills in digital forensics and apply the acquired knowhow in investigating cyber incidents for companies and the judicial sector (as court experts).

UNS. The DF Lab will allow students to familiarize themselves with state-of-the-art equipment and software used in digital forensic investigations. It will allow UNS staff members to further their knowledge in digital forensics and apply the acquired knowhow in investigating cyber incidents for companies and the judicial sector (as court experts).

3.5 Hybrid CS and IoT Lab implementation

VTS. Hybrid CS implementation will help students to get better understanding, knowledge, pros and cons about the system structure (hardware and software). Students will be able to make whole implementations of IoT devices, they will need to make the devices communicate with each other or/and with a server in a lab environment, this way learning about the logic and the vast world of IoT.

3.6 Key performance indicators (KPI)

The exploitation goals of the study laboratories developed and updated as part of the ISSES project will be measured by the following key performance indicators:

- Number of research papers published by the members and/or users of the project laboratories.
- Number of BSc, MSc and PhD students involved in the research and development activities supported by the laboratories.
- Number of professors and researchers involved in the research and development activities supported by the laboratories.

- Number of ISSES project courses taught or supported by the laboratory.
- Number of research collaborations between laboratories inside the partner HEIs, as well as with external entities, e.g. companies, NGOs, government institutions. Measured in the number of signed MoUs.
- Number of investigated court cases, especially for the Digital Forensics laboratories.
- Number of projects and contracts signed with external legal entities, e.g. companies.

4 Study programs

This section contains the exploitation plan for each of the new or updated study programs which benefit from the Information Security Services Education in Serbia (ISSES) project. The following programs will be listed and analyzed:

- MSc in Information Security at the University of Novi Sad (P1).
- Joint MSc Master 4.0 at the University of Belgrade (P5).
- MSc module Computer System Security at the University of Nis (P6).
- Master in Computer Science at the Subotica Tech – College of Applied Sciences (P9).

Wherever applicable, the roles and involvement of other partners will be listed as well.

4.1 MSc in Information Security (P1)

The MSc in Information Security will be introduced at the University of Novi Sad, Faculty of Technical Sciences (FTN). It will be an inter-disciplinary study program created by three relevant departments, namely the:

- Computing and Control Department (RA),
- Department of Power, Electronic and Telecommunication Engineering (DEET), and
- Department of Industrial Engineering and Engineering Management (DIIM).

The program will be accredited in 2020 according to the project plan. The program will consist of two separate modules inside one master study program. Namely, one module will deal with the more technical aspects of cybersecurity, while the other will consist of training on the strategic, legal and managerial aspects of cybersecurity.

The following courses will be included in the technical module – if the courses are developed or updated as part of the ISSES project then task identifiers are included in parenthesis for easier reference:

- Applied Cryptography and Cryptanalysis (2.5) – mandatory for both modules
- Secure Software Development (2.2)
- Computer Security (2.15)
- Advanced Network and Systems Security (2.6)
- Digital Forensics Tools and Techniques (2.12)
- Critical Infrastructure Security (2.1)
- Security Data Science (2.14)

The following coursed will be included in the managerial-strategical module:

- Applied Cryptography and Cryptanalysis (2.5) – mandatory for both modules
- Cybersecurity Strategies (2.7)
- Risk Analysis and Threat Modeling (2.9) – partially
- Project Management in Information Security
- Information Security Management Systems

The first students will enroll in September – October 2020. It is expected that at least one group of 12-16 students will enroll in the 2020/2021 school year.

It is envisaged that the representatives of the MSc in Information Security program will sign memorandums of understandings with at least 3 companies in and around Novi Sad, including the associated partners listed in the original project proposal. These MoUs will outline the collaboration activities between the MSc program and the companies, e.g. internships, partnerships of joint events.

4.2 MSc Module "Information Technologies and Cyber Security" (P5 – UB-FON)

The new module "Information Technologies and Cyber Security" as a part of "Information Systems and Technologies" study program will be introduced at the University of Belgrade, Faculty of organizational sciences.

The new module will be accredited in 2020.

The following ISSES courses will be included as elective courses:

- Cyber Security Strategies (2.7)
- Risk Analysis and Threat Modeling (2.9)
- Cyber Incident Analysis and Response (2.10)
- Data Mining in Digital Forensics (2.11)
- Digital Forensics Tools and Techniques (2.12)
- Mobile and Multimedia Forensics (2.13)

The first students will enroll in September-October 2020. It is expected that at least 20-25 students will enroll in the 2020/2021 school year.

4.3 Master 4.0 (P5, P6)

The Serbian Government held consultations with Digital Serbia Initiative (non-profit non-governmental organization, founded by 9 leading ICT companies in Serbia and constituted of more than 30 ICT member companies in Serbia) and the technical universities in 2018-2019, and based on those discussions the Master 4.0 was envisaged and created as a joint, national master program in 2019. The following faculties and/or universities participate in the four master programs:

- Faculty of Organization Sciences (FON) & School of Electrical Engineering (ETF), University of Belgrade, i.e. both faculties which participate in the ISSES project.
- University of Niš (UNI), which participate in the ISSES project.
- Faculty of Matematics and Faculty of Mechanical Engineering, University of Belgrade.
- University of Kragujevac (UK).

M4.0 contains the following selection of cybersecurity courses:

- Cryptography (ETF/FON)
- Cyber Security (ETF/FON)
- Cyber Incident Analysis and Response (ETF/FON)
- Information Security and Personal Data Protection (ETF/FON)
- Distributed Systems Based on Blockchain Technology (ETF/FON)
- Compression and Data Protection (UNI)

- Computer Systems Security (UK)

The M4.0 study programs were accredited in 2019 and joint FON/ETF master program "Advanced Information Technologies in Digital Transformation" already started in the winter term of the 2019/2020 school year. In the first school year 22 students has been enrolled.

The M4.0 program website is available here: https://www.dsi.rs/master40/

4.4 Computer System Security module (P6)

The Computer System Security (CSS) module of the MSc in Computer Science program of the Electronic Faculty of the University of Nis (P6) was accredited in 2019.

It consists of the following courses – where applicable the related project task is included in parenthesis:

- Network Security (2.6)
- Secure Software Development (2.2)
- Digital Forensics (2.12)
- Cloud Security – elements of 2.15
- Virtualization
- System Administration
- Cryptography – elements of 2.5
- High Performance Computing

The project results will be exploited by updating existing courses and adding new courses from the ISSES project. The Security Data Science (2.14) course will be developed jointly and the colleagues at P6 plan to include it in their existing CSS module.

4.5 Master in Computer Science (P9)

Subotica Tech – College of Applied Sciences (P9) submitted a 3-semester study program for accreditation. It includes the following ISSES courses:

- Secure Software Development (2.2)
- Advanced Network and System Security (2.6)
- Mobile and Multimedia Forensics (2.13)
- Course "Security in e-Business Systems" will incorporated the majority of topics from 2.5.
- Course "Cloud Security" will incorporate topics from 2.15.

Considering the fact that their size is limited, the management of the college decided to accredit the new MSc program under a more general title.

4.6 Key performance indicators

The exploitation goals of the study programs developed and updated as part of the ISSES project will be measured by the following key performance indicators:

- Number of students enrolled in the new/updated study programs.
- Number of professors involved in the teaching activities.
- Number of teaching assistants involved in the teaching activities.

- Number of chairs, departments and faculties participating in the teaching activities.
- Number of laboratory assistants involved.
- Number of complete ISSES courses included.
- Number of partial ISSES courses included.
- Number of ISSES laboratories utilized as part of the study program execution.
- Number of other laboratories utilized as part of the study program execution.

5 Annual information security roundtables

The project team will organize at least three roundtables and/or panel discussions with both state-owned and private companies, which might be interested in the services and knowhow built in this project. These events might lead to the creation of start-ups for finding novel ways of utilising the knowledge acquired. The roundtables will be attended by information security experts both from within the consortium and outside it. They will not be open to the wider public. Roundtable attendance will be recorded via attendance sheets.

These events will be organized jointly with the annual workshops, thereby boosting attendance and lowering the travel and stay costs.

5.1 First Project Information Security Roundtable

Organization: UB-ETF

Planned dates: September 2018

Planned place: Belgrade

Planned Roundtable topics:

- Secure Software Development
- Advanced Network Security and Vulnerability Analysis
- Cyber Security Strategies
- Cyber Incident Analysis and Response

5.2 Second Project Information Security Roundtable

Organization: NI

Planned dates: September 2019

Planned place: Niš

Planned Roundtable topics:

- Cyber Incident Analysis and Response
- Data Mining in Digital Forensics
- Digital Forensics Tools and Techniques

5.3 Third Project Annual Workshop and Information Security Roundtable

Organization: UNS

Planned dates: September 2020

Planned place: Novi Sad

Planned Roundtable topics:

- Critical Infrastructure Security
- Security and privacy in the Internet of Things
- Cloud Security

5.4 Key performance indicators (KPI)

The exploitation goals of the roundtables and workshops organized during the ISSES project will be measured by the following key performance indicators:

- Number of different stakeholders represented, e.g. HEIs, NGOs, government institutions and companies.
- Number of people attending the events.

6 Summary

This documents contains the exploitation plan (EP) specifically developed for the Information Security Services Education in Serbia (ISSES) project co-funded by the Erasmus+ program of the European Union. The EP was developed to maximize the benefits gained from the project by different stakeholders, first of all by students and the industrial sector employing the professionals trained at the higher education institutions (HEIs) involved in the project.