



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

Steering Committee Meeting #7

Held on January 22nd, 2021

Author(s)/Organisation(s):
Imre Lendak / UNS
Date of meeting:
January 22nd, 2021
Relevant Work Package(s):
WP7 – Project Management
Short Description:
Minutes of the 7 th Steering Committee (SC) meeting
Keywords:
Steering Committee, minutes of the meeting, project status

The European Commission support for the production of this publication does not constitute endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Revision History:

Revision	Date	Author(s)	Status	Description
V1.0	Feb 2, 2021	Imre Lendak / UNS	Draft	

CONTENTS

1	Meeting agenda.....	4
1.1	Day #1: Student Workshop.....	4
1.2	Day #2: Project meetings and Lectures	4
2	Steering Committee meeting – Minutes of the Meeting.....	6
2.1	Attendees	6
2.2	Meeting Agenda	6
3	WP1 – Project Preparation	7
4	WP2 – Course Development	8
4.1	Books	8
5	WP3 – Laboratory Development	10
6	WP4 – Study Program Development.....	11
7	Supporting work packages WP5-WP7	12
7.1	WP5 – Quality	12
7.2	WP5 – Dissemination and Exploitation	12
7.3	WP7 – Management.....	13
8	Next actions and meetings.....	15

1 Meeting agenda

The Steering Committee (SC) meeting was organized as part of a 2-day project event consisting of a hackathon preparation workshop for students, lectures and meetings.

The detailed agenda is shown below.

1.1 Day #1: Student Workshop

January 21 st , 2021 (Thursday). Venue: Zoom	
10:00 – 11:00	Heap corruption Speaker(s): <ul style="list-style-type: none">CrySyS Lab, Budapest University of Technology and Economics, Hungary
11:00 – 12:00	Linux Binary Attack Mitigations - Security features of executables, compilers, and kernel (plus how to break them) Speaker(s): <ul style="list-style-type: none">Mario Polino, Politecnico di Milano, Italy
Zoom meeting details	Topic: ISSES workshop & meetings - Day #1: Hackathon prep workshop Time: Jan 21, 2021 10:00 AM Budapest https://us02web.zoom.us/j/81837643477?pwd=OTRXdnpCMzdNVTd3Tk5ZaHgrN1NOQT09 Meeting ID: 818 3764 3477 Passcode: isses

1.2 Day #2: Project meetings and Lectures

January 22 nd , 2021 (Friday). Venue: Zoom	
10:00 – 11:00	Lecture Speaker(s): <ul style="list-style-type: none">Prof. dr Tamás Holczer, CrySyS Lab, Budapest University of Technology and Economics, Hungary Zoom meeting details: <ul style="list-style-type: none">Topic: ISSES workshop & meetings - Day #2: LecturesTime: Jan 22, 2021 10:00 AM BudapestMeeting ID: 613 722 0349Passcode: isses
11:00 – 11:15	Break
11:15 – 13:00	Steering Committee (SC) meeting Moderated by: <ul style="list-style-type: none">Imre Lendák, University of Novi Sad, Serbia Note: private Zoom meeting details shared separately.

13:00 – 14:00	Lunch break
14:00 – 15:30	Quality Board (QB) meeting Moderated by: <ul style="list-style-type: none">• Stefano Zanero, Politecnico di Milano, Italy• Tamás Holczer, CrySyS Lab, Hungary• Stevan Gostojić, University of Novi Sad, Serbia• Pavle Vuletić, University of Belgrade, Serbia Note: private Zoom meeting details shared separately.

2 Steering Committee meeting – Minutes of the Meeting

The project Steering Committee (SC) meeting was held on January 22nd, 2021 on the Zoom platform.

2.1 Attendees

The Steering Committee had quorum for voting as the following SC members attended the meeting:

1. Imre Lendák / UNS (project coordinator)
2. Stefano Zanero / Polimi
3. Tamás Holczer / CrySys
4. Žarko Stanisavljević / UB-ETF
5. Dejan Simić / UB-FON
6. Dragan Stojanović / UNI
7. Dejan Rančić / ICUN
8. Igor Fuerstner / VTS

We were honored that Giulia Moro, the ISSES project officer from the EACEA also attended our meeting.

2.2 Meeting Agenda

The meeting had the following agenda:

- Work package status
- Financial status of the project
- Open issues
- Next steps

The status of work packages 1-7 are discussed in the next sections.

3 WP1 – Project Preparation

Task statuses are shown in the table below

ID	Title	Deadline	Status	LFM KPI
1.1	Baseline Curricula Report	M1-M3		3/1 report – Instead of 1 BCP, the consortium produced one report for each school year since the start of the project
1.2	Repository of Information Security Concepts	M1-M4		0.5/1 Repository – roughly 50% complete, limited work remaining, numerous existing glossaries can be and/or were already referenced
1.3	Course Development Plan (CDP)	M3-M5		1/1 CDP – The CDP was extended and amended as the project progressed.
1.4	Laboratory Development Plan (LDP)	M4-M6		1/1 LDP – The LDP was extended multiple times during the project.

4 WP2 – Course Development

Part 1 of WP2 status is shown in the table below

ID	Title	Interval	LFM KPI:			
			Curricula	textbook	accredited	taught
2.1	Critical Infrastructure Security	M13-M21	4	1	1	0
2.2	Secure Software Development	M6-M12	12+7	0	2	2*
2.3	Cloud Security		Note: Merged into 2.15			
2.4	Security and privacy in the Internet of Things	M16-M24	3	1	1	0
2.5	Advanced Cryptography	M16-M24	9+6	1	2	1
2.6	Advanced Network Security	M7-M15	13+9	1	2	2*
2.7	Cyber Security Strategies	M7-M15	13+2	0	2	0
2.8	Security in E-business Systems		Note: Substituted by 2.14			

Part 2 of the WP2 status overview is shown in the table below.

ID	Title	Interval	LFM KPI:			
			Curricula	textbook	accredited	taught
2.9	Risk Analysis and Threat Modelling	M25-M33	13	1	2	0
2.10	Cyber Incident Analysis and Response	M9-M17	13+7	0	3	2
2.11	Data Mining in Digital Forensics	M17-M24	12+12	0	2	0
2.12	Digital Forensics Tools and Techniques	M13-M21	12+11	0	3	2
2.13	Mobile and Multimedia Forensics	M22-M30	0	0	2	0
2.14	Security Data Science	M20-M34	2+1	0	1	0
2.15	Computer Security	M19-M33	2	0	2	0

NOTE: The above tables contain the 13 courses from the original project proposal, plus the two additional courses, which will be used as substitutes/extensions of one or more courses from the original 13 courses.

4.1 Books

We discussed the book projects in more detail. We listed the following complete or nearly complete book projects:

- 1 Zarko Stanisljevic, Pavle Vuletic, "Network and Systems Security Lab Manual" (P5 – UB/ETF).

- 2 Bojan Jovanovic, "Cyber Incident Analysis and Response Lab Manual" (P5 – UB/FON).
- 3 Milija Suknović, Boris Delibašić, Miloš Jovanović, Milan Vukićević, Sandro Radovanović, "Decision Making Theory" (P5 – UB/FON)
- 4 Daniela Rosic et al, "Applied Cryptography" (P1 – UNS).
- 5 Imre Lendak, "Critical Infrastructure and Industrial Control System Security" (P1 – UNS).
- 6 Sanja Maravić, Róber Pintér, „IoT Security Lab Manual" (P9 – VTŠ).

The representatives of the various project institutions explained that there are numerous relevant textbooks and that the courses developed in the ISSES project are quite new and therefore the content is not stabilized and tested, and thereby it is too soon to start writing new textbooks.

5 WP3 – Laboratory Development

We concluded that all (originally) planned public procurements were completed and that the equipment was deployed. The digital forensics equipment requires physical interaction and is not fully available due to the covid pandemic.

ID	Title	Deadline	Status	LFM KPI
3.1	Lab Design: Critical Infrastructure Security Laboratory (CIS Lab)	M13		Documentation incomplete
3.2	Lab Design: Digital Forensics Laboratory (DF Lab)	M13		Documentation incomplete
3.3	Lab Design: Network Security Laboratory (NS Lab)	M13		
3.4	Lab Design: Cloud Security Laboratory (CS Lab)	M14		Merged into 3.3, but agreed to keep as separate document
3.5	Hybrid CIS, CS and NS Lab implementation (P1)	M14-M24		Documentation incomplete
3.6	Hybrid NS and Crypto Lab Implementation (P5)	M14-M21		
3.7	Hybrid NS and IoT Lab implementation (P6)	M18-M24		Documentation incomplete
3.8	DF Lab Implementation – Belgrade (P5)	M13-M24		Documentation incomplete
3.9	DF Lab Implementation – Nis (P6)	M25-M30		Documentation incomplete
3.10	DF Lab Implementation – Novi Sad (P1)	M31-M36		Documentation incomplete
3.11	Hybrid CS and IoT Lab Implementation (P9)	M15-M24		Documentation incomplete

The members of the SC concluded that the documentation is complete for tasks 3.3 and 3.6 and not yet completed for the rest of the WP3 tasks (marked with blue status).

We noted that the project team members at P1 were able to enter the new building of the Faculty of Technical Sciences, University of Novi Sad, i.e. the Science and Technology Park in July-August 2020, i.e. after the last SC meeting. The P1 equipment is partially deployed there, and partially in the main server room of the University.

As mentioned elsewhere in the document, partners P5, P6 & P9 requested from the project coordinator and project office to organize one additional, small public procurement and acquire additional books necessary to complete WP2 & WP5 activities.

6 WP4 – Study Program Development

We discussed WP4 – Study Program Development in detail. Imre Lendak reported that the study program documentation of P1 was just submitted to the NEAQA on January 22nd, 2021. The accreditation costs were paid by the Faculty of technical sciences, University of Novi Sad and will be re-funded from the ISSES subcontracting budget line – this cost was already approved by the EACEA as there were necessary savings in that budget line.

We also noted that the study program of P9 (Subotica Tech) was re-submitted in June 2020 and that there was no response from the NEAQA yet. This re-submission was extended and aligned with the comments received from the NEAQA in late 2019.

The overview of WP4 is shown in the table below.

ID	Title	Deadline	Status	LFM KPI
4.1	MSc Program: Information Security	M31		Master implemented 10 students enrolled
4.2	MSc Program: Information Security and Digital Forensics	M27		Master implemented 10 students enrolled
4.3	MSc Program: Security in the Cloud and Internet of Things	M31		Master implemented 10 students enrolled

Additional notes and comments related to the study program development which was originally planned in the ISSES project plan:

- 4.2 was transformed into an MSc module
- 4.3 re-submitted in June 2020

Additional study program developments, which were implemented but were not originally planned in the ISSES project proposal:

- MSc module in Computer Systems Security accredited at UNI (P6) accredited in October 2019
- Master 4.0 “Digital Serbia”, Joint MSc program with the P5 & P6 aAccredited in September 2019. Requested by the government, consumes P5 & P6 resources. Includes the following ISSES courses:
 - 2.5 Advanced Cryptography (P5)
 - 2.10 Cyber Incident Analysis and Response (P5)

7 Supporting work packages WP5-WP7

7.1 WP5 – Quality

We started the quality-related discussion by re-visiting the agenda and explaining that there will be a Quality Board meeting following the SC meeting (in the afternoon). We briefly touched the external quality review, which is necessary to be procured in February to be able to complete the quality process on time and within the timeframe of the project.

WP5 status was discussed in detail based on the tabular overview shown below.

ID	Title	Deadline	Status	LFM KPI
5.1	Quality Plan	M3		1/1 QP
5.2	Annual Course Quality Report			4/13 course quality reports
5.3	Annual Laboratory Build Report			0/7 lab quality reports
5.4	Quality Board Meeting			4/5 QB meetings meetings
5.5	External Quality Assessment			0/1 external quality assessment

We agreed that we are behind with lab reports, which are due as the procurements were finished in 2020. We also concluded that the number of course quality reports completed is also slightly delayed and should be addressed in detail in the QB meeting.

7.2 WP5 – Dissemination and Exploitation

We discussed WP5 status based on the tabular task status overview shown below.

ID	Title	Deadline	Status	LFM KPI
6.1	Dissemination Plan (DP)	M2		1/1 DP
6.2	Exploitation Plan (EP)	M3		1/1 EP
6.3	Annual Project Workshop	M11, M23, M35		3/3 project workshops 3/3 attendance lists & Zoom-shots
6.4	Mass Media Dissemination	M1-M36		~10/36 mass media disseminations ~50/72 disseminations via social media
6.5	Security Services Roundtable	M11, M23, M35		2/3 roundtables
6.6	Web portal setup and maintenance	M1-M36		1/1 web portal set up & regularly maintained
6.7	Sustainability Plan (SP)	M24-M36		1/1 SP

We re-iterated that the Sustainability Plan was published on the project website, but requires updates caused by external changes, e.g. the setup of the Cybersecurity Network Foundation as the formal continuation of the Petnica Group informal public-private partnership in cybersecurity on the national (Serbian) level. Task 6.7 was not in the original LFM, i.e. extra work, but useful.

Additionally, we identified the small number of mass media appearances as a potential problem. Giulia Moro suggested that the consortium spend part of the Travel/Accommodation funds for short promotional video preparation about the project. This idea was well-received and will be further evaluated by the representatives of P5 (University of Belgrade).

We also discussed the role of our Associated Partners, who became dormant during the project. Fortunately, other partners were identified, e.g. Avatao, CRDF Global, Cybersecurity Network, EC-Council, Enlight IT, Erste bank Serbia, Ingram Micro, ISACA, Silensec. Partners P1, P5 and P9 already signed Memorandums of Understanding (MoU) with one or more of the listed, newly acquainted partners.

7.3 WP7 – Management

We discussed the status of WP7 tasks with the support of the tabular task overview below.

ID	Title	Deadline	Status	LFM KPI
7.1	Brussels Kick-of Meeting	M2		1/1 meeting + attendance lists
7.2	Project Kick-off Meeting	M3		1/1 meeting + attendance lists
7.3	Project Steering Committee Meeting	6 pcs		7/6 meetings + attendance lists
7.4	Project Coordination	M1 – M36		Work in progress
7.5	Financial Plan	M3		1/1 Financial Plan (document) 0/1 external financial report – contracted, underway
7.6	Interim and Final Report	M18, M36		1/1 Interim Report (IR) 0/1 Final Report (FR)

We concluded that since the last SC meeting (in June 2020) the project was extended by one year and thanked the EACEA for making this possible. We also identified the Interim Report as a weak point, as it was poorly graded by the EACEA as it was incomplete when submitted. It was subsequently extended and we hope that Final Report (FR) will be well-received. Giulia Moro stated that there were online trainings made available for project coordinators and specifically focusing on the preparation of the FR.

Giulia Moro emphasized that each project activity has to be implemented within the timeframe of the project.

We reviewed the project budget status as well and asked the partners who are behind with their project documentation submissions to submit asap. The budget status overview is shown below.

#	Partner	1 of 1	2 of 1	1 of 2	2 of 2	Equipment	Remaining 10%
P2	University of Zagreb	9525,25	9525,25	7620,20	7620,20	0,00	3810,10
P3	CrySys Lab/BME	12507,50	12507,50	10006,00	10006,00	0,00	5003,00
P4	Politecnico di Milano	21332,00	21332,00	17065,60	17065,60	0,00	8532,80
P5	University of Belgrade	10248,25	10248,25	38198,60	38198,60	75000,00	19099,30
P6	University of Nis	1564,00	1564,00	23149,7	23149,7	50730,00	11128,6
P8	Unicom-Telecom Ltd	3792,00	3792,00	3033,60	3033,60	0,00	1516,80
P9	Subotica Tech	1632,50	1632,50	16706,00	16706,00	38500,00	8353,00
P10	Innovation center of the University of Nis (ICUN)	3300,50	3300,50	2640,40	2640,40	0,00	1320,20

The representatives of P5 raised the questions of remaining funds in the Equipment vertical. We proposed that we would like to use these funds to acquire additional books. Giulia Moro mentioned that the EACEA usually does not approve procurements during the last year of the project. The representatives of the interested institutions (P5, P6 & P9) explained that the books would aid the development of the final courses (WP2) and their quality improvements (WP5).

8 Next actions and meetings

We proposed the next action items:

- Define strict deadline for the quality process during the Quality Board meeting on the same day.
- Organize the Serbian Cybersecurity Challenge 2021 as a key dissemination activity towards student and industry stakeholders. The first group participates, the latter act as sponsors.
- Organize one additional SC meeting in May or June.
- Collocate another SC meeting with a conference, workshop and hackathon event during the 2nd week of September 2021.
- Organize a larger training event at Polimi in July (if able).
- Organize additional training events online.