Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D9.7

CyberSec4Europe summer schools 1

Document Identification	
Due date	31/07/2020
Submission date	31/07/2020
Revision	1.0

Related WP	WP9	Dissemination Level	Public
Lead Participant	DTU	Lead Author	Alberto Lluch Lafuente Anders Schlichtkrull
Contributing Beneficiaries	AIT, BRNO, GUF, SIE, UMA	Related Deliverables	

Abstract: This document presents the deliverable “D9.7 CyberSec4Europe summer schools 1”. It describes the contributions made by the CyberSec4Europe project to summer schools in the first period of the project.

Executive Summary

Task 9.3 “Spreading of excellence” of the CyberSec4Europe project has as one of its main goals the dissemination of project results through several channels. This deliverable presents one of the key set of activities carried out to contribute to achieving this goal, in particular the dissemination among the new generations of researchers and professionals through summer schools. This deliverable provides a detailed overview of the summer schools that CyberSec4Europe partners used to disseminate about the project and its results in the first period of the project.

Goals. One of the main overall goals of CyberSec4Europe is to disseminate the latest research from the project and to provide training based on it. Project activities aimed at achieving such a goal are being conducted in several areas of the project and, especially, in WP9. Indeed, WP9 has, among others, the following objectives:

> [Obj. 9.1] Maximise dissemination of the project results to a wide audience of researchers and technologists within the relevant cybersecurity communities and initiatives. Run dissemination as a necessary step before and during exploitation
>
> [Obj. 9.2] Promote the project achievements and results taking strategic and targeted measures for communicating the education and training cybersecurity framework and the service infrastructure to all potential users, including the media.
>
> [Obj. 9.3] Spread excellence and guidance on best practices in next generation industrial and civilian cybersecurity technologies, applications and services

The project has several target groups for such dissemination and training efforts which includes, professionals, educators, students, researchers, both in the public and industrial sectors. A key target group are young professionals and researchers from the EU and beyond, who will form the basis of the new generations of experts in cybersecurity. Reaching them is fundamental to ensuring the widespread and long-term impact of the results of the project beyond the project’s lifetime. Indeed, summer schools often give rise to new international networks of professionals bound by a unique learning and social experience. Moreover, summer schools are an excellent vehicle to connect experienced researchers and professionals with the younger generation from all across the world, thereby ensuring knowledge transfer among the generations, worldwide. Overall, summer schools are a key instrument to meet the three objectives of WP9 mentioned above, as well as the general goal of spreading of excellence.

The summer schools. To ensure a successful dissemination of CyberSec4Europe’s results, the partners of the project decided to aim at getting actively involved in both well-established, reputed summer schools as well as in newly-created ones. Such efforts resulted in CyberSec4Europe partners providing significant contributions to a number of summer schools, ranging from active involvement in the organisation of the schools to teaching of individual lectures or modules. The set of summer schools, presented in this deliverable, is:

- NeCS PhD Winter School 2020
- ENISA NIS 2019 Summer School
- IFIP Summer School on Privacy and Identity Management 2019
- International School on Foundations of Security Analysis and Design 2019
- KYPO Summer School on Cybersecurity
- MISA DAAD Uni Passau IT-Security summer school
- SENSYBLE Graduate School
- Convite Ciclo De Palestras Internacionais UFBA

Details about how CyberSec4Europe partners contributed to the schools and about which particular CyberSec4Europe results were disseminated in the schools are described in detail in the deliverable. In particular, every summer school is described in a dedicated chapter where, for each summer school, we provide the following information:

- **Name of the school:** The full name of the summer school.
- **Website (URL):** The URL of the summer school.
- **Dates:** The dates when the summer school took place.
- **Location:** The location where the summer school took place.
- **Organiser:** Who was the main organiser of the summer school.
- **Main audience category:** Who the audience of the summer school primarily was.
- **Description:** A short description of the summer school.
- **Speakers, lecturers and topics:** Who the speakers and lecturers were and what topics they covered.
- **Teaching material:** Links to teaching material.
- **Picture:** Photograph taken at the event.
- **Number of attendees:** How many people attended the summer school.
- **CyberSec4Europe involvement:** How CyberSec4Europe was involved with the summer school.
- **Conclusion:** The main success and outcome of contributing to the summer school.

Summary. Overall, this set of summer schools constitutes a significant step towards the achievements of the above-mentioned goals of the project. In total, CyberSec4Europe reached out to, through these summer schools, more than 300 attendees in the scientific community, a main target group. The schools were spread among six countries, within the EU and beyond. Indeed, some of them were held in Madagascar and Brazil to spread European cybersecurity excellence internationally and strengthen partnerships beyond the EU. A particular interesting case is that of the NECS summer school, which was supported by the four EU Cybersecurity Competence Network pilots (CONCORDIA, CyberSec4Europe, ECHO and SPARTA). In addition to these strategically important partners, it is worth mentioning ENISA and IFIP as being two of the main organisers of some of the summer schools. Lastly, we think it is also worth mentioning that, in addition to spreading CyberSec4Europe results, some of the summer schools resulted in outcomes that are currently being integrated with the activities and results of the project.

Document information

Contributors

Name	Partner
Alberto Lluch Lafuente	DTU
Anders Schlichtkrull	DTU
Kai Rannenberg	GUF
Jorge Cuéllar	SIE
Javier López	UMA
Carmen Fernandez Gago	UMA
Stephan Krenn	AIT
Vaclav Matyas	BRNO
Jan Vykopal	BRNO
Sebastian Pape	GUF
David Goodman	TDL

Reviewers

Name	Partner
Lea Hemetsberger	OASC
Marco Angelini	ENG
Antonio Lioy	POLITO

History

Version	Date	Authors	Comment
0.01	2020-05-06	The Authors	1st Draft
0.02	2020-05-06	The Authors	Reorganized chapters and extended executive summary.
0.03	2020-05-11	The Authors	Minor fixes
0.04	2020-05-11	David Goodman	Comments and improvements.
0.05	2020-05-12	The Authors	Tables, figure headers and more
0.06	2020-05-12	The Authors	Merged several sections after suggestion from WP leader
0.07	2020-05-18	The Authors	Merged more sections after suggestion from WP leader
0.08	2020-06-02	The Authors	Addressed several comments from Lea Hemetsberger
0.09	2020-06-08	The Authors	Addressed several comments from the reviewers
0.10	2020-06-08	The Authors	Addressed several comments from the reviewers
0.11	2020-06-29	The Authors	Addressed comments from reviewers reply to rebuttal.
0.12	2020-07-11	David Goodman and The Authors	Various fixes and improvements
1.0	2020-07-31	Ahad Niknia	Preparation and submission process

Table of Contents

List of Figures

List of Tables

1 NeCS PhD Winter School 2020

1.1 Name of the school

NeCS PhD Winter School 2020.

1.2 Website (URL)

https://2020.necs-winterschool.disi.unitn.it

1.3 Dates

20 January 2020 - 24 January 2020.

1.4 Location

Fai della Paganella (Italy).

1.5 Organiser

University of Trento (UNITN)

1.6 Main audience category

Scientific community and young researchers (PhD and MSc students).

1.7 Description

The European Network for Cybersecurity (NeCS) PhD School was launched as part of the NeCS Marie Curie training network, in response to the increasing need for highly qualified experts in cybersecurity. The School addresses the issues of training and development of talented junior researchers as indicated in the European Cybersecurity strategy and highlighted in the EC's Digital Agenda.

For the edition of 2020, the school was supported by the four EU Cybersecurity Competence Networks pilots. The pilots launched in 2019, within the EU's H2020 framework, are **CONCORDIA**, **CyberSec4Europe**, **ECHO** and **SPARTA**. All of them emphasise the crucial role of education for cybersecurity, proposing new educational and training programmes and new methods of teaching.

1.8 Speakers, lecturers and topics

The full program is available at http://2020.necs-winterschool.disi.unitn.it/program/. CyberSec4Europe contributed with the following:

Lecturer (Partner)	Topic
Jorge Cuellar (SIE)	Distributed Workflow-driven access control for IoT
Simone Fischer-Hübner (KAU)	Usable Privacy – Eliciting Stakeholder Requirements
Kai Rannenberg (GUF)	CyberSec4Europe (in the slot devoted to presenting the pilots)

Table 1: CyberSec4Europe lectures at NeCS PhD Winter School 2020

1.9 Teaching material

Not publicly available. The material may be obtained by contacting the organisers.

1.10 Picture

Figure 1: NeCS PhD Winter School 2020.
Picture from https://necs-winterschool.disi.unitn.it/pictures/necs2020-3/

1.11 Number of attendees

The summer school had around 30 attendees.

1.12 CyberSec4Europe involvement

CyberSec4Europe's involvement was as follows:

- UNITN was the organiser of the school.
- UMA was part of the steering committee
- KAU gave a lecture
- GUF presented CyberSec4Europe
- SIE gave a lecture

In short, project partners were involved in the organisation and gave lectures. For example, Jorge Cuellar (SIE) provided a detailed overview of the methods developed in CyberSec4Europe to secure workflows in cyber-physical systems and in particular in the supply chain of physical products and in collaborative

manufacturing or industrial plant construction. The main goal is to provide a distributed declarative workflow enforcement and a workflow-aware access control for IoT-based scenarios that enforce the order in which the physical objects and the documents and information are accessed by the authorized parties. This summer school contributed to successfully achieving some of the objectives of WP3, WP4, WP5, WP9 and WP10 – the tasks T9.2, T9.3, T10.3 and T5.2 in particular. For T5.2, the results presented – although also applicable to other distributed scenarios – are particularly tailored to securing the supply chain.

1.13 Conclusion

By being part of the organising committee we could include in the program of this school topics eliciting privacy requirements (WP3, WP4 and WP5) and distributed IoT. Also, Kai Rannenberg (GUF) presented the project to the participants of the summer school.

2 ENISA NIS 2019 Summer School

2.1 Name of the school

ENISA NIS 2019 Summer School

2.2 Website (URL)

https://nis-summer-school.enisa.europa.eu/2019/

2.3 Dates

16 September 2019 - 20 September 2019

2.4 Location

Heraklion, GR, Atlantis Aquila Hotel.

2.5 Organiser

European Union Agency for cybersecurity (ENISA) and Foundation for Research and Technology - Hellas (FORTH)

2.6 Main audience category

Most attendees were from industry, a smaller number were PhD students from Greek universities.

2.7 Description

All four pilots presented posters at the ENISA NIS 2019 Summer School. On Tuesday there was a dedicated time slot for the poster presentation at which Dr. Sebastian Pape presented the CyberSec4Europe poster and answered questions from the audience.

2.8 Speakers, lecturers and topics

The full programme is available at https://nis-summer-school.enisa.europa.eu/2019/index.html#program. CyberSec4Europe contributed with the following:

Lecturer (Partner)	Topic
Sebastian Pape (GUF, Social Engineering Academy)	Poster presentation of CyberSec4Europe
Sebastian Pape (GUF, Social Engineering Academy) (Organisation done with Kristian Beckers and Ludger Goeke of the Social Engineering Academy.)	Two two-hour tabletop security gaming sessions with the serious game HATCH.

Table 2: CyberSec4Europe presentation at ENISA NIS 2019 Summer School

2.9 Teaching material

No public material available.

2.10 Picture

Figure 2: Attendees playing HATCH.

2.11 Number of attendees

The summer school had around 50 attendees.

2.12 CyberSec4Europe involvement

GUF (in collaboration with the Social Engineering Academy) and FORTH were involved in the summer school. A tabletop security gaming session was held by GUF in collaboration with the Social Engineering Academy. CyberSec4Europe results were covered in the poster which mainly showed the goals and intended work plan of the project.

Social engineering threat analysis and awareness training was done with the serious game HATCH which was developed by the Social Engineering Academy in 2016. HATCH is a card game that is played by company employees, primarily with non-security experts. The game elicits domain-specific threats and teaches employees about the dangers of attacks and their consequences. At this event, an autonomous shipping scenario from the EU project, THREAT-ARREST (https://www.threat-arrest.eu/), was used as a scenario.

This summer school contributed to successfully achieving WP9 objectives. Presenting the poster contributed to promoting the project activities (T9.2). The tabletop security game sessions were part of the summer school (T9.3).

Work packages WP3 and WP5 were also relevant to the summer school. T3.10 deals among other things with the use of serious games for privacy and security awareness raising. HATCH is a game which exactly

fulfils this task. The scenario was about autonomous shipping which is related to T5.5 which is about maritime transport. WP10's task T10.3 was also relevant to the summer school.

2.13 Conclusion

By contributing to the program of the ENISA NIS 2019 Summer School, CyberSec4Europe could communicate the project's progress to policy makers from EU Member States and EU Institutions, decision makers from industry and members of the academic community.

3 IFIP Summer School on Privacy and Identity Management 2019

3.1 Name of the school

IFIP Summer School on Privacy and Identity Management

Data for Better Living: AI and Privacy

3.2 Website (URL)

https://2019edition.ifip-summerschool.org/

3.3 Dates

19 August 2019 - 23 August 2019

3.4 Location

Brugg/Windisch, Switzerland, in the canton of Aargau.

3.5 Organiser

University of Applied Sciences and Arts Northwestern Switzerland (FHNW), International Federation for Information Processing (IFIP), and International Association for Cryptologic Research (IACR)

3.6 Main audience category

The target audience of the IFIP Summer School series is twofold. Firstly, it offers a platform for early stage researchers to present their research goals, receive feedback from an experienced program committee, discuss ideas, and build an interdisciplinary network in the field of privacy and identity management. Secondly, the program is complemented by a series of keynote lectures and interactive workshops organised by experienced senior researchers.

3.7 Description

The 14th International IFIP Summer School on Privacy and Identity Management was held at the University of Applied Sciences and Arts Northwestern Switzerland (FHNW) in Brugg/Windisch, Switzerland, in the canton of Aargau. Specifically, the event was co-organised by the multidisciplinary Institute for Interactive Technologies. The IFIP Summer Schools take a holistic approach to society and technology and support interdisciplinary exchange through keynote and plenary lectures, tutorials, workshops, and research paper presentations. In particular, it aims to bring together early stage as well as senior researchers with technical, legal, regulatory, socio-economic, social or societal, political, ethical, anthropological, philosophical, or psychological backgrounds. This interdisciplinary character of the work is fundamental to the School.

3.8 Speakers, lecturers and topics

The full program is available at https://2019edition.ifip-summerschool.org/index.html%3Fp=291.html. CyberSec4Europe contributed with the following:

Lecturer (Partner)	Topic
Vaclav Matyas (BRNO)	Open tools for security case study on the ROCA vulnerability

Table 3: CyberSec4Europe lectures at IFIP Summer School on Privacy and Identity Management 2019

3.9 Teaching material

The post-event proceedings, including the student contributions, summaries of workshops, and tutorials, have been published by Springer: https://www.springer.com/gp/book/9783030425036

3.10 Picture

No pictures available.

3.11 Number of attendees

The summer school had around 80 attendees.

3.12 CyberSec4Europe involvement

AIT, KAU, GUF, BRNO were involved in the summer school. The IFIP Summer School series has a long tradition and strong links with several CyberSec4Europe participants. For the 2019 edition, Stephan Krenn (AIT) was one of the two general co-chairs, while Simone Fischer-Hübner (KAU) and Kai Rannenberg (GUF) are permanent members of the school's steering committee. Furthermore, team members from AIT, KAU, and GUF were part of the program committee responsible for the scientific evaluation of submissions. Vaclav Matyas (BRNO) contributed a keynote lecture on "Open tools for security case study on the ROCA vulnerability". A post-event proceedings was made based on the summer school including the student contributions, summaries of workshops, and tutorials. Submissions from multiple partners were included.

The IFIP Summer School is directly related to different ambitions of CyberSec4Europe. The school provides insights into up-to-date research in different domains (WP3). For WP3, the summer school is related to several tasks, e.g.,

- T3.2 (e.g., workshop on "Oblivious Identity Management for Private User-Friendly Services"),
- T3.4 (demonstrated by the special theme "Data for Better Living: AI and Privacy"),
- T3.5 (e.g., paper session on "Assessing Privacy Risks"), or
- T3.6 (e.g., workshop on "Interactive Focus Group GDPR-compliant Dynamic Consent Management" or paper session on "Users and Usability").

Given the main ambition of the summer school, there is also a strong relation to the topics covered by the demonstrators in WP5. The overall ambition of the summer school on privacy and identity management is directly related to the ambition of T5.3, underpinned, for example, by a paper session on "Identity Management".

The event directly contributes to the objectives of WP9 by raising awareness of cybersecurity, bringing together experts from different domains, and supporting CyberSec4Europe beyond the consortium. It is easy to see the relation to WP9 through the outreach achieved by the accepted publication of papers by CyberSec4Europe partners (T9.2) and the organisation of the overall summer school (T9.3).

3.13 Conclusion

The IFIP Summer School on Privacy and Identity Management was directly related to CyberSec4Europe's overall ambitions in several ways. Firstly, the summer school aims to bring together researchers from different fields, backgrounds, and seniority levels, thereby directly contributing to the objectives of strengthening Europe's cybersecurity capacities (Policy Objective 2), and establishing synergies between experts from different communities (Innovation Objective 2). Secondly, the contents of the summer school are directly linked to the project's vertical demonstrators, specifically T5.3 (Privacy-preserving identity management), but also to those dedicated, for example, to open banking (T5.1) or medical data exchange (T5.6), which have very strong privacy requirements. Thirdly and finally, the school was also related to

research activities from WP3, for example, regarding privacy-preserving technologies or blockchains (T3.2), or usable security (T3.6).

4 International School on Foundations of Security Analysis and Design 2019

4.1 Name of the school

19th International School on Foundations on Security Analysis and Design (FOSAD 2019)

4.2 Website (URL)

http://www.sti.uniurb.it/events/fosad19/

4.3 Dates

26 August 2019 - 30 August 2019.

4.4 Location

Bertinoro (Italy)

4.5 Organiser

University Residential Centre of Bertinoro

4.6 Main audience category

Scientific community and early stage researchers, mainly PhD students and MSc students.

4.7 Description

Security in computer systems and networks emerged as one of the most challenging research areas. The International School on Foundations of Security Analysis and Design (FOSAD) has been one of the foremost events established with the goal of disseminating knowledge in this critical area. The main aim of the FOSAD school is to offer a good spectrum of current research in the foundations of security - ranging from programming languages to the analysis of protocols, from cryptographic algorithms to access control policies and trust management - that can be of help to graduate students and young researchers from academia or industry who intend to specialise in the field.

FOSAD is held annually at the University Residential Centre of Bertinoro. Since the first event in 2000 until its 19th edition in 2019, FOSAD has attracted about 920 participants and 155 lecturers from all over the world. The school programme alternates monographic courses given by well-known experts in the security community. Moreover, FOSAD encourages presentations by those participants who intend to take advantage of the audience to discuss their current research topic. Many of the young speakers of the FOSAD open sessions are now appreciated researchers and professors.

4.8 Speakers, lecturers and topics

The full program is available at http://www.sti.uniurb.it/events/fosad19/Programme.html.
CyberSec4Europe contributed with the following:

Lecturer	Partner	Topic
Javier Lopez	UMA	Edge computing security (http://www.sti.uniurb.it/events/fosad19/FOSAD-Lopez.pdf)
Antonio Lioy	POLITO	Integrity verification of software-defined infrastructures (http://www.sti.uniurb.it/events/fosad19/Lioy_FOSAD_2019.pdf)

Table 4: CyberSec4Europe lectures at International School on Foundations of Security Analysis and Design 2019

4.9 Teaching material

http://www.sti.uniurb.it/events/fosad19/Programme.html

4.10 Picture

Figure 3: International School on Foundations of Security Analysis and Design 2019

4.11 Number of attendees

The summer school had around 30 attendees.

4.12 CyberSec4Europe involvement

UMA and POLITO were involved in the summer school. Javier Lopez (UMA) was a member of the Scientific Committee and also gave lectures. Antonio Lioy (POLITO) also gave lectures.

The following CyberSec4Europe topics and results were covered:

- Edge Computing Paradigms, including the ecosystem and security threats and mechanisms.
- Main Edge Architectures: OpenFog and MEC, and security issues in both of them, and research on Edge security mechanisms.
- Use of Edge computing as a security enabler and examples on how to use the Edge for enhanced security.
- Integrity monitoring in softwarised networks (SDN, NFV)

This summer school contributed to successfully achieving some of the objectives of WP3, WP5 and WP9. In particular the research issues presented are part of WP3 and WP5. WP9 is devoted to dissemination and outreach, therefore all activities that are carried out in order to reach certain audiences (young researchers in this case) are related to this WP – in particular tasks T9.2 and T9.3 which are devoted to outreach in general and summer schools in particular.

4.13 Conclusion

By being part of the organising committee and also lecturing at this school, the school focused on some CyberSec4Europe topics such as Edge computing and IoT (WP3 and WP5).

5 KYPO Summer School on Cybersecurity

5.1 Name of the school

KYPO Summer School on Cybersecurity

5.2 Website (URL)

https://twitter.com/csirtmu/status/1164493198389055490?s=20

5.3 Dates

13 August 2019 - 15 August 2019

5.4 Location

Brno, Czech Republic

5.5 Organiser

Masaryk University (BRNO)

5.6 Main audience category

Finalists of the 2019 Czech Secondary School Cyber Security Competition who are representing the Czech Republic in the European Cybersecurity Challenge. The finalists are top young talents selected in several rounds from about 3,000 students from various high schools in the Czech Republic.

5.7 Description

Masaryk University, founded in 1919, is the second largest university in the Czech Republic. More than 30,000 students study there in nine faculties. The Faculty of Informatics was founded in 1994 as the first Faculty of Informatics in the Czech Republic. Since 2017, the KYPO Summer School on Cybersecurity is held there for the finalists of the Czech Secondary School Cyber Security Competition who represent the Czech Republic in the European Cybersecurity Challenge (https://ecsc.eu).

Participants in the summer school were involved in hands-on tutorials and played cybersecurity games to develop and exercise cybersecurity skills needed for the European finals of the European Cybersecurity Challenge.

5.8 Speakers, lecturers and topics

The CyberSec4Europe partner BRNO contributed with the following programme:

Lecturer (Partner)	Topic
Milan Čermák (BRNO)	Hands-on tutorial on deep packet inspection
Andrej Tomči (BRNO)	Hands-on tutorial on web security
Daniel Kouřil (BRNO)	Hands-on tutorial and game on forensic analysis
Jakub Batortolomej Košuth (BRNO)	Game on steganography, cryptoanalysis and reverse engineering

Martin Laštovička and Valdemar Švábenský (BRNO)	Game on penetration testing
Benjamil Král (BRNO)	Game on forensic analysis
Milan Čermák and Jan Vykopal (BRNO)	Attack-defense cybersecurity game

Table 5: CyberSec4Europe lectures at KYPO Summer School on Cybersecurity

5.9 Teaching material

No public material available.

5.10 Picture

Figure 4: KYPO Summer School on Cybersecurity

5.11 Number of attendees

The summer school had 19 attendees.

5.12 CyberSec4Europe involvement

Masaryk University (BRNO) was involved in the summer school. The summer school was organised by Jan Vykopal and Valdemar Švábenský (both BRNO) who also served as instructors. The development and testing of the hands-on tutorials and cybersecurity games were done using the ideas and techniques which are now incorporated in the architecture and the first prototype of the open, virtual lab delivered by CyberSec4Europe. The summer school provided invaluable feedback for the design and development of the lab.

The CyberSec4Europe involvement was directly related to WP7 “Open Tools and Infrastructures for Certification and Validation”. The summer school provided the input for the Task 7.1 open tools and common portable virtual lab and a technical report detailing the selection of existing modern proven software technologies as building blocks for virtual lab development.

5.13 Conclusion

With this summer school, CyberSec4Europe communicated to the target group of talented high-school students interested in cybersecurity. In addition, the school enabled the first testing of the ideas and techniques which are now incorporated in the open source software being delivered by CyberSec4Europe.

6 MISA DAAD Uni Passau IT-Security summer school

6.1 Name of the school

MISA DAAD Uni Passau IT-Security summer school

6.2 Website (URL)

http://summerschool.misa-madagascar.com/

6.3 Dates

16 September 2019 - 17 September 2019

6.4 Location

Antananarivo, Madagascar.

6.5 Organiser

University of Passau's Chair of Security in Information Systems, and the University of Antananarivo's MISA.

6.6 Main audience category

Scientific community.

Master and PhD students, some local professors.

Research talks and lectures during the first week were open to the public, but places were limited.

6.7 Description

The **IT-Security summer school** is organised through the collaboration between the University of Passau's Chair of Security in Information Systems (https://www.uni-passau.de/sis/), and the University of Antananarivo's MISA (http://misa-madagascar.com). The summer school is funded by the German Academic Exchange Service DAAD (https://www.daad.de) and is the first collaboration of its kind to strengthen the cybersecurity discipline in Madagascar at both research and industry levels.

In this second edition, topics in privacy, Internet of Things, CPS security, mobile communication, authorisation in the web, and automotive security were addressed in an interactive setting with multi-disciplinary researchers. During the first week, participants attended research talks by experts from German universities and leading tech companies. The second week consisted of a hands-on lab during which selected participants worked on practical implementations of several security concepts.

6.8 Speakers, lecturers and topics

The full program is available at http://summerschool.misa-madagascar.com/#services. CyberSec4Europe contributed with the following:

Lecturer (Partner)	Topic
Kai Rannenberg (GUF)	Security and privacy in the IoT age Home - Business - Public life & Governance
Kai Rannenberg (GUF)	Security and Authentication in Mobile Communication and Wireless Networks
Kai Rannenberg (GUF)	Assessing and appraising apps and policies (A4). What app markets and software can contribute to privacy and personal data protection

Table 6: CyberSec4Europe lectures at MISA DAAD Uni Passau IT-Security summer school

6.9 Teaching material

No public material available.

6.10 Picture

Figure 5: MISA DAAD Uni Passau IT-Security summer school.
Picture from http://summerschool.misa-madagascar.com

6.11 Number of attendees

The summer school had around 80 attendees.

6.12 CyberSec4Europe involvement

Kai Rannenberg (GUF) gave an overview on CyberSec4Europe as part of his talk “Security and privacy in the IoT age Home - Business - Public life & Governance” (90 minutes including discussion) covering, for example, the vertical use case demonstrators and the context of the four pilots.

Participating in the summer school contributed to successfully achieving some of WP9’s objectives – in particular the tasks T9.2 and T9.3 were relevant to the summer school as the school general communicates with international young talent and leading German researchers (the other lecturers).

6.13 Conclusion

With this woman-driven summer school, CyberSec4Europe communicated to young people in a developing country (Madagascar), especially an unusually large number of female students. Moreover as DAAD was funding this exercise, the message of CyberSec4Europe’s existence reached the DAAD, and of course the other high-ranking speakers.

7 SENSYBLE Graduate School

7.1 Name of the school

SENSYBLE Graduate School

7.2 Website (URL)

https://www.sensyble.org/en/

7.3 Dates

28 June 2019 - 29 June 2019

7.4 Location

Hetschbach, DE.

7.5 Organiser

Goethe University Frankfurt (GUF)

7.6 Main audience category

Scientific community. Approximately 15 professors and students of the Graduate School meeting.

7.7 Description

SENSYBLE Graduate School by GUF and RheinMain University of Applied Sciences Wiesbaden.

7.8 Speakers, lecturers and topics

The following lectures were given:

- Martin Gergeleit: Sicherheits-Modellierung und Automatic Deployment in Industrial Edge Cloud Systems
- Kai Rannenberg: Report on CyberSec4Europe (www.CyberSec4Europe.eu)
- Several presentations by PhD students

CyberSec4Europe contributed with the following:

Lecturer (Partner)	Topic
Kai Rannenberg (GUF)	Report on CyberSec4Europe (www.CyberSec4Europe.eu)

Table 7: CyberSec4Europe lectures at SENSYBLE Graduate School

7.9 Teaching material

No public material available.

7.10 Picture

No pictures available.

7.11 Number of attendees

The summer school had around 15 attendees.

7.12 CyberSec4Europe involvement

Kai Rannenberg (GUF) gave an overview on CyberSec4Europe and its relation to SENSYBLE (45 minutes including discussion) covering, for example, the vertical use case demonstrators. The title was “Report on CyberSec4Europe”.

Participating in the summer school contributed to successfully achieving some of WP9’s objectives – in particular tasks T9.2 and T9.3 were relevant to the summer school as the school communicates to international young talent.

7.13 Conclusion

With this summer school, CyberSec4Europe communicated to highly skilled PhD students and their advisors in the area of smart and sensing systems and contributed by raising and maintaining cybersecurity awareness. By being part of the organising committee, focus can be directed to issues of CyberSec4Europe.

8 Convite Ciclo De Palestras Internacionais UFBA

8.1 Name of the school

Convite Ciclo de Palestras Internacionais UFBA, LaSiD/DCC/IME

8.2 Website (URL)

http://www.lasid.ufba.br/ (of the institution)

https://www.youtube.com/watch?v=1_Y7bcbGfvs

8.3 Dates

28 March 2019

8.4 Location

Salvador da Bahia, BR

8.5 Organiser

The Distributed Systems Laboratory (LaSiD) of the Computer Science Department at the Federal University of Bahia (UFBA)

8.6 Main audience category

Scientific Community.

Talks were attended by about 70 professors and students of UFBA and other universities from Salvador; they were also transmitted to the Brazilian Computer Society community (via its YouTube channel)

8.7 Description

The Distributed Systems Laboratory (LaSiD) is a research laboratory within the Computer Science Department at the Federal University of Bahia (UFBA). It involves faculty members of the Computer Science Department, research assistants, and research students (Ph.D., MSc. and BSc.). The mission of LaSiD is to develop methods, techniques and tools that help in the design of correct and dependable distributed systems, preparing the next generation of researchers and developers in these areas by investigating challenging problems.

Members of IFIP give open and free lectures to the community of UFBA and the region. The speakers are volunteer scientists of great international prestige. The lectures, organised by Professor Raimundo Macêdo, LaSiD/DCC/IME, chairmain of IFIP and director of SBC (Brazilian Society of Computing), take place in the Auditorium “Maria José Zezé de Oliveira” of the Institute of Statistics and Mathematics (IME) at UFBA.

8.8 Speakers, lecturers and topics

The following talks were given:

- Professor Mike Hinchey, University of Limerick (Ireland), IFIP President, former Director of the Software Engineering Laboratory at NASA: A Brief Introduction to IFIP International Federation for Information Processing
- Professor Franz J. Rammig, Paderborn University (Germany), IFIP Councillor: Digital Twins for Designing and Operating Adaptive IoT Applications

- Professor Gabriela Marín Raventós, Costa Rica University, IFIP Vice President, Latin America: ICT challenges and perspectives from the UN Sustainable Development Goals
- Professor Kai Rannenberg, Goethe University (Germany), IFIP Vice President CyberSec4Europe: Moving Europe forward in the field of Cybersecurity
- Professor Yuko SJ Murayama, Tsuda University (Japan), IFIP Vice President and Chair of IFIP Domain Committee on IT in Disaster Risk Reduction. The use of IT for disaster management
- Professor Jee In Kim, Konkuk University (Korea), IFIP Councillor, Director of Digital Content Research Center and Eco Tech Institute, UX (User eXperience): What, Why and How?

CyberSec4Europe contributed with the following:

Lecturer (Partner)	Topic
Kai Rannenberg (GUF)	Moving Europe forward in the field of Cybersecurity

Table 8: CyberSec4Europe lectures at Convite Ciclo De Palestras Internacionais Ufba

8.9 Teaching material

https://www.youtube.com/watch?v=1_Y7bcbGfvs

8.10 Picture

Figure 6: Kai Rannenberg introducing CyberSec4Europe.

8.11 Number of attendees

The event had more than 70 attendees.

8.12 CyberSec4Europe involvement

Prof. Kai Rannenberg (GUF) gave an overview on CyberSec4Europe and its relations to Brazil (30 minutes + discussion later) covering for example the vertical use case demonstrators. The title was “Moving Europe forward in the field of Cybersecurity”.

Participating in the summer school contributed to successfully achieving some of WP9’s objectives – in particular the tasks T9.2 and T9.3 were relevant to the summer school as the school contributes general dissemination of the project to an international audience.

8.13 Conclusion

With this international seminar, CyberSec4Europe communicated to a highly skilled audience in Northern Brazil, also demonstrating and supporting the relationship of CyberSec4Europe partners to Brazil and especially UFBA. As this was a seminar with the leaders of IFIP (www.ifip.org) also speaking and attending full time (on the occasion of an IFIP Board meeting), the message about CyberSec4Europe and the European Strategy for Cybersecurity also reached the top executives of IFIP including the president and two vice presidents.