Thematic CERN School of Computing on Security 2023

https://indico.cern.ch/event/1297500/

Sebastian Lopienski, Kristina Gunne and David Crooks
On behalf of the school organisers

GDB meeting, 8 November 2023
https://indico.cern.ch/event/1225118/

Introduction to CERN School of Computing

A school with a long history

- The school was created in 1970
  - 43rd edition in 2022

- 2900 students of ~80 different nationalities have followed the school
  - usually 60-80 per year
  - alumni web site: https://cern.ch/CSC/history/alumni/

- The school has visited 22 countries
  - https://cern.ch/CSC/history/past-schools/
  - recent: France, Romania, Croatia, Israel, Spain, Belgium, Greece, Portugal, Cyprus

Bridging science and computing

- Technological evolution in computing empowers science
  - especially in data-intensive domains such as High Energy Physics
  - computing is the main strategy for many scientific fields to do research efficiently on a large scale

- It is nowadays essential that:
  - scientists master computing technologies as a main tool for their research
  - computer engineers understand the scientific needs in order to deliver computing services to research projects

Academic dimension

CERN School of Computing…

- is not a conference
  - lecturers do not present their work or promote their projects
- is not a training session
  - not a replication of training courses available at home institutes or online
  - focus on persistent knowledge, less on know-how

Thematic CSC on Security 2023

CERN Organizers

New Technical Manager! Welcome

Kristina Gunne
Administrator

Andrzej Nowicki
Technical Manager

Alberto Pace
Director

Local Organizers

Toni Šćulac

… and the MEDILS staff

- No more support for external activities
- All bookings, payments etc directly handled with the service providers (restaurants,transport excursions etc)

Security CSC 2023

- **Applications → student selection**
- **October 8-14, 2023** (Sunday to Saturday) at MEDILS institute, **Split, Croatia**
  - **Sunday afternoon:** arrival and informal welcome, visit of Split city
  - **Monday to Friday:** official opening, lectures and exercises
  - **Wednesday afternoon**: excursion / outdoor acitivty
  - **Saturday morning:** departure
- **Lectures and hands-on exercises:** ~30 hours in total
  - including student lightning talks etc.
- **Exam → diploma**
- **Optional social and sport activities**
- **Registration fee**: covers acommodation, meals, tuition, activities
  - depending on the accommodation (twin vs. single rooms, places)

Programme committee

https://indico.cern.ch/event/1297500/page/30008-programme-committee

- Ian Collier — UKRI-STFC
- David Crooks — UKRI-STFC / EGI CSIRT / IRIS CSIRT
- Sven Gabriel — Nikhef / EGI CSIRT
- David Groep — Nikhef
- David Kelsey — UKRI-STFC
- Sebastian Lopienski — CERN / CSC
- Hannah Short — CERN / GÉANT GN4-3
- Romain Wartel — CERN / WLCG
- Ralph Niederberger — Forschungszentrum Jülich

Topic and target audience

CERN School of Computing "**Security of research computing infrastructures**"

The programme of this school is targeted at **people working in academia and research institutes**, who as part of their job need to **ensure security and resilience of computing resources** they manage, and want to be prepared to **detect and handle possible security incidents**:

- **service managers and service providers** of distributed scientific computing infrastructures, both from IT departments and from experiments,
- **people in charge of deploying cloud services** used by scientists,
- **security professionals**, who would like to expand their knowledge in a more holistic fashion.

Lecturers

https://indico.cern.ch/event/1297500/page/30668-lecturers

Stefan Lüders
CERN

Sebastian Łopieński
CERN

Sven Gabriel
Nikhef, the Netherlands

Tom Dack
UKRI-STFC, UK

Barbara Krašovec
IJS, Slovenia

Daniel Kouřil
CESNET, Czech Republic

David Crooks
UKRI-STFC, UK

Programme

https://indico.cern.ch/event/1297500/page/30007-academic-programme

Introduction	Security in research and scientific computing Security operations
Track 1: Protection and prevention	Identity, authentication, authorisation Defensible security architecture Vulnerability management Application security and penetration testing
Track 2: Detection	Logging and traceability Intrusion detection with SOC
Track 3: Response	Introduction to forensics Incident response Coordination of security incidents

30 class hours

Lectures and **exercises,** but also **group discussions** and **role-playing**

Programme

https://indico.cern.ch/event/1297500/page/30007-academic-programme

- Programme predominantly the same as last year
  - Some small tweaks including new tutors taking over where appropriate
- Allows for a gradual evolution of the programme over time

CERN School of Computing

Monday, 9 October 2023	
08:00	**Opening Session** - Alberto Pace (CERN) Mile Dzelalija (University of Split) Ivica Puljak (Mayor of [illegible])
08:45	**Security in research and scientific computing** - Stefan Lueders (CERN)
09:45	**Announcements**
10:00	**Coffee break**
10:30	**Identity, authentication, authorisation** - Tom Dack (Science and Technology Facilities Council STFC (GB))
11:30	**Lunch**
12:15	**Study time and/or daily sports**
13:45	**Security architecture fundamentals** - Barbara Krašovec (IJS)
15:00	**Coffee break**
15:15	**Security operations - lecture 1** - Sven Gabriel
16:15	**Security operations - lecture 2** - Sven Gabriel
17:15	**Network design - exercise** - Barbara Krašovec (ISJ)
18:15	**Dinner at MEDILS**

Tuesday, 10 October 2023	
07:45	**Virtualisation and cloud security** - Barbara Krašovec (IJS)
08:45	**Risk and vulnerability management** - Sven Gabriel
09:45	**Announcements**
10:00	**School photo**
10:05	**Coffee break**
10:30	**Logging and traceability** - David Crooks (UKRI STFC)
11:30	**Lunch**
12:15	**Study time and/or daily sports**
13:45	**Intrusion detection with SOC: threat intelligence, monitoring, integration and processes** - David Crooks (UKRI STFC)
14:45	**Coffee break**
15:15	**Student lightning talks**
16:15	**Introduction to web penetration testing** - Sebastian Lopienski (CERN)
17:15	**Penetration testing - exercises** - Sebastian Lopienski (CERN)
18:15	**Dinner at MEDILS**

Wednesday, 11 October 2023	
07:45	**Container security** - Daniel Kouřil (CESNET)
08:45	**Container security - exercises** - Daniel Kouřil (CESNET)
09:45	**Announcements**
10:00	**Coffee break**
10:30	**Intrusion detection with SOC: deployment and operation** - David Crooks (UKRI STFC)
11:30	**Lunch**
12:15	**Outdoor excursion**
17:45	**Outside dinner at Kastil Slanica, Omis**

Thursday, 12 October 2023	
07:45	**Digital forensics: essentials and data acquisition** - Daniel Kouřil (CESNET)
08:45	**Defensible security architecture: how to implement security principles** - Barbara Krašovec (IJS)
09:45	**Announcements**
10:00	**Coffee break**
10:30	**Digital forensics: data analysis** - Daniel Kouřil (CESNET)
11:30	**Lunch**
12:15	**Study time and/or daily sports**
13:45	**Incident response management** - Barbara Krašovec (IJS)
14:45	**Coffee break**
15:15	**Intrusion detection with SOC and AAI - exercises** - David Crooks (UKRI STFC) Tom Dack (Science and Technology Facilities Council STFC (GB))
18:15	**Dinner at MEDILS**

Friday, 13 October 2023	
07:45	**Digital forensics - exercises** - Daniel Kouřil (CESNET)
09:15	**Coffee break**
09:30	**Introduction to forensics - exercises** - Daniel Kouřil
10:45	**Announcements**
11:00	**Penetration testing - exercise debriefing** - Sebastian Lopienski (CERN)
11:30	**Lunch**
12:15	**Study time**
13:15	**Exam**
14:00	**Incident response - exercise** - David Crooks (UKRI STFC) Sebastian Lopienski (CERN) Tom Dack (Science and Technology Facilities Council STFC (GB)) Romain Wartel (CERN)
15:30	**Coffee break**
15:45	**Incident response - exercise** - Tom Dack (Science and Technology Facilities Council STFC (GB)) Sebastian Lopienski (CERN) Romain Wartel (CERN) David Crooks (UKRI STFC)
17:00	**Closing Session** - Alberto Pace (CERN)
18:00	**Walk to the restaurant**
18:30	**Outside Closing Dinner at Kavanazona (Zona restaurant)**

Participants

https://indico.cern.ch/event/1297500/page/30975-student-participants

26 students invited out of 29 applicants

- 6 female participants
- 11 different institutes,
- 13 nationalities (Belgium, Bulgaria, Canada, Estonia, Germany, Greece, India, Italy, Portugal, Romania, Spain, Ukraine, United Kingdom)
  - One sponsored student cancelled due to travel funds

Diverse, talented, passionate about science and technology

Istituto Nazionale di Fisica Nucleare
Centro Nazionale per la Ricerca e lo Sviluppo nelle Tecnologie Informatiche e Telematiche

CERN School of Computing

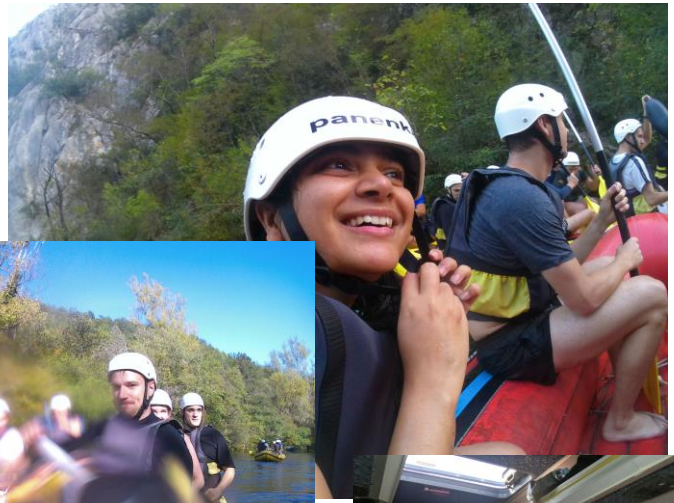
Science and Technology Facilities Council

Lectures and exercises

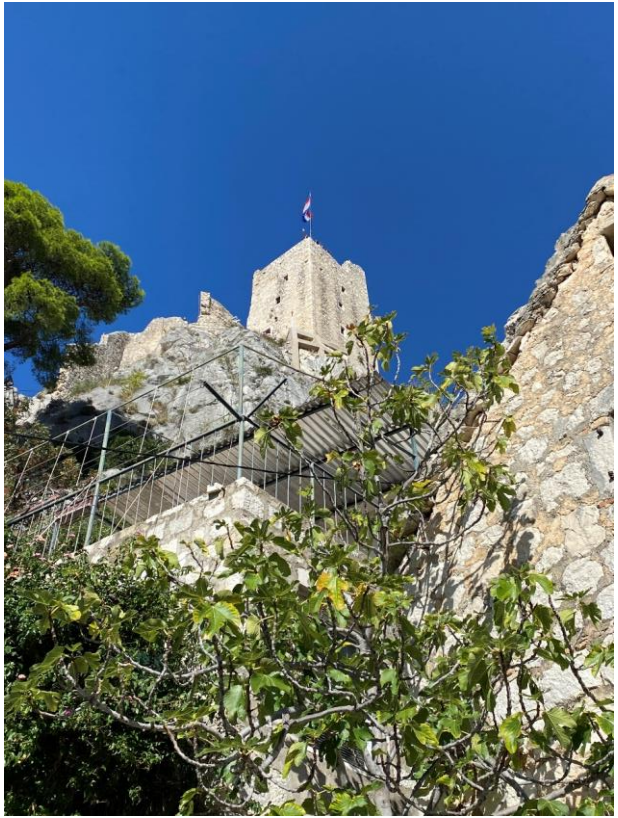
Exam

Evening activities….

Excursion on the Cetina river



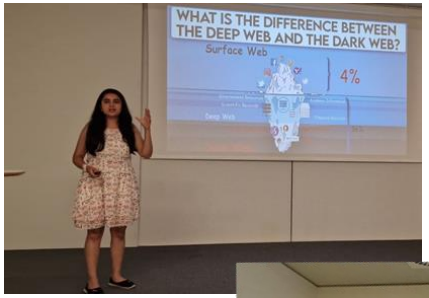
Excursion on the Cetina river – calm version



Security tCSC 2023 participants

tCSC on security 2023: Student lightning talks

- Benedikt Bieringer (University of Münster)
  "Reverse engineering USB drivers (with PyUSB)"
- Robin Hofsaess (Steinbuch Centre for Computing)
  "Nelson Mandela"
- Roberta Miccoli (INFN CNAF)
  "An overview of the INDIGO IAM service"
- Elizaveta Ragozina (CERN)
  "Quantum Computing and Cybersecurity: Preparing for Tomorrow"
- Diogo Santos (CERN)
  "Model Security in Federated Learning"
- Shrija Rajen Sheth (CERN)
  "Dark web and Cyber Security"
- Roman Sumailov (CERN)
  "OSINT: What you post online" + "Privacy in modern cars"
- Leon Welchert (WWU Münster)
  "Encrypting Secrets with SOPS"



Feedback and reflections

- Feedback from the students was very constructive and useful
- Overall feedback was very positive
  - Maintained level from first iteration
- Need to process as we work towards the next iteration
  - Planned for the same time next year
  - Feedback included interest in material on dev-sec-ops, secure coding, etc…

- Topics we're thinking about include the demographic of the cohort and how this factors into the evolution of the syllabus

Summary

- Second Thematic CSC on Security
- Predominantly similar programme with slight adjustments
- Lots of interactions, discussions and networking
  - between the students and with lecturers
- Maintained level of feedback from first time

- Next iteration planned for October 2024


CERN