Thematic CERN School of Computing on Security 2023

Report of Contributions

https://indico.cern.ch/e/sCSC-2023

Contribution ID: **73**

Type: **not specified**

Exam

Friday, 13 October 2023 14:15 (45 minutes)

Contribution ID: **74** Type: **not specified**

Announcements

Tuesday, 10 October 2023 10:45 (15 minutes)

Summary

Contribution ID: **75**

Type: **not specified**

Announcements

Wednesday, 11 October 2023 10:45 (15 minutes)

Summary

Contribution ID: **76** Type: **not specified**

Announcements

Summary

Contribution ID: **77** Type: **not specified**

Announcements

Thursday, 12 October 2023 10:45 (15 minutes)

Summary

Contribution ID: **78** Type: **not specified**

Announcements

Friday, 13 October 2023 11:45 (15 minutes)

Summary

Contribution ID: **79** Type: **not specified**

Opening Session

Monday, 9 October 2023 09:00 (45 minutes)

Summary

Presenters: PACE, Alberto (CERN); PULJAK, Ivica (Mayor of Split); DZELALIJA, Mile (University of Split)

Contribution ID: **80** Type: **not specified**

Closing Session

Friday, 13 October 2023 18:00 (45 minutes)

Summary

Presenter: PACE, Alberto (CERN)

Contribution ID: **81** Type: **not specified**

Student lightning talks

Tuesday, 10 October 2023 16:15 (1 hour)

Summary

Contribution ID: **82** Type: **not specified**

Guest lecture

Summary

Contribution ID: **84** Type: **not specified**

Special evening talk: Future of the Universe and of Humanity

Summary

Primary author: PULJAK, Ivica (University of Split. Fac.of Elect. Eng., Mech. Eng. and Nav.Architect. (HR))

Contribution ID: **87** Type: **not specified**

Scientific and computing challenges in fundamental physics

In this introductory lecture we will review the big picture of modern science, with the emphasis on biggest questions and challenges in fundamental physics. Higgs physics, neutrino experiments, dark matter, dark energy, multi messenger astronomy, physics beyond the standard model, gravitational waves and other scientific wanders will be presented, connecting great theoretical ideas and modern experiments trying to test them. Computing is now established as the crucial part of any present and future experiments. We will review and discuss the biggest challenges in computing for the next decades, including traditional increase of data throughput, data volume and data complexity, but also other emerging concepts like quantum computing, machine learning and artificial intelligence.

Summary

Primary author: PULJAK, Ivica (University of Split. Fac.of Elect. Eng., Mech. Eng. and Nav.Architect. (HR))

Contribution ID: **88** Type: **not specified**

Self-presentation: 1 minute per person

Sunday, 8 October 2023 16:00 (40 minutes)

Summary

Contribution ID: **92** Type: **not specified**

School photo

Tuesday, 10 October 2023 11:00 (5 minutes)

Summary

Contribution ID: **96** Type: **Lecture**

Guest lecture: Why is Higgs still a star?

The discovery of the Higgs boson particle in 2012 was an astonishing triumph of high energy physics. In this talk I will try to convince you that precision measurements of the Higgs boson properties are a very exciting prospect. Not only it will lead to a better understanding of our Universe but it is also one of our best windows in to the unknown.

Summary

Primary author: SCULAC, Toni (University of Split Faculty of Science (HR))

Contribution ID: **97** Type: **not specified**

Welcome to the CERN School of Computing

Sunday, 8 October 2023 16:40 (20 minutes)

Presenters: PACE, Alberto (CERN); SCULAC, Toni (University of Split)

Contribution ID: **99** Type: **not specified**

Announcements

Monday, 9 October 2023 10:45 (15 minutes)

Summary

Contribution ID: **100** Type: **not specified**

Photo contest

Summary

Primary author: TOLOMEO, Joelma (CERN)

Contribution ID: **101** Type: **Lecture**

Security in research and scientific computing

Monday, 9 October 2023 09:45 (1 hour)

- computer security: past, present and future
- current risk landscape
- most common threats and attack vectors
- “why are we here?”

Summary

Presenter: LUEDERS, Stefan (CERN)

Contribution ID: **102** Type: **Lecture**

Security management

- security principles
- threat modeling, risk assessment, risk management
- security standards
- security policies
- the human factor, security culture

Summary

Contribution ID: **103** Type: **Lecture**

Security operations - lecture 1

Monday, 9 October 2023 16:15 (1 hour)

- security operations: history, CERT vs. CSIRT
- CSIRT organisation and provided services
- preparations: asset management, security monitoring etc.
- incident response readiness
- lessons learned from past incidents

Summary

Presenter: GABRIEL, Sven

Contribution ID: **104** Type: **Lecture**

Security operations - lecture 2

Monday, 9 October 2023 17:15 (1 hour)

- security operations: history, CERT vs. CSIRT
- CSIRT organisation and provided services
- preparations: asset management, security monitoring etc.
- incident response readiness
- lessons learned from past incidents

Summary

Presenter: GABRIEL, Sven

Contribution ID: **105** Type: **Lecture**

Identity, authentication, authorisation

Monday, 9 October 2023 11:30 (1 hour)

- An introduction to the concepts of Identity, Authentication, and Authorization
- Authentication and authorisation for distributed research
- Methods for communicating authentication and authorization: Certificates, SAML, OAuth
- How these technologies fit within research infrastructures

Summary

Presenter: Mr DACK, Tom (Science and Technology Facilities Council STFC (GB))

Contribution ID: **106** Type: **Lecture**

Security architecture fundamentals

Monday, 9 October 2023 14:45 (1 hour)

Security architecture fundamentals
- fundamental security principles
- develop skills to be a security architect
- how to design and provide secure computing infrastructure
- security standards and frameworks
- physical security
- network security: segmentation, firewalls, VPNs

Summary

Presenter: KRAŠOVEC, Barbara (IJS)

Contribution ID: **107** Type: **Exercise**

Network design - exercise

Monday, 9 October 2023 18:15 (1 hour)

Summary

Presenter: KRAŠOVEC, Barbara (ISJ)

Contribution ID: **108** Type: **Lecture**

Virtualisation and cloud security

Tuesday, 10 October 2023 08:45 (1 hour)

Virtualisation and cloud security
- virtualisation security fundamentals
- cloud service models
- authentication and key management
- data security in the cloud
- DevSecOps
- security in private and public cloud
- common threats in the cloud
- security tools

Summary

Presenter: KRAŠOVEC, Barbara (IJS)

Contribution ID: **109** Type: **Lecture**

Container security

Wednesday, 11 October 2023 08:45 (1 hour)

- key concepts of containers (namespaces, cgroups etc.) and Docker
- container security, threat landscape
- vulnerability and patch management

Summary

Presenter: KOUŘIL, Daniel (CESNET)

Contribution ID: **110** Type: **Exercise**

Container security - exercises

Wednesday, 11 October 2023 09:45 (1 hour)

Summary

Presenter: KOUŘIL, Daniel (CESNET)

Contribution ID: **111** Type: **Lecture**

Risk and vulnerability management

Tuesday, 10 October 2023 09:45 (1 hour)

- risk analysis and risk mitigation
- vulnerability lifecycle, monitoring, scanning
- CVE, CVSS, CPE, CWE and related standards
- special cases: vulnerable hardware, EOL systems etc.

Summary

Presenter: GABRIEL, Sven

Contribution ID: **112** Type: **Lecture**

Introduction to web penetration testing

Tuesday, 10 October 2023 17:15 (1 hour)

- web application security, typical web vulnerabilities
- ethical hacking
- introduction to pentesting

Summary

Presenter: LOPIENSKI, Sebastian (CERN)

Contribution ID: **113** Type: **Exercise**

Penetration testing - exercises

Tuesday, 10 October 2023 18:15 (1 hour)

Summary

Presenter: LOPIENSKI, Sebastian (CERN)

Contribution ID: **114** Type: **Lecture**

Logging and traceability

Tuesday, 10 October 2023 11:30 (1 hour)

- host-based logs (system and application level), network monitoring
- the importance of central logging
- tools and technologies
- data privacy, dealing with personal and sensitive data, log retention
- traceability challenges

Summary

Presenter: CROOKS, David (UKRI STFC)

Contribution ID: **115** Type: **Lecture**

Intrusion detection with SOC: threat intelligence, monitoring, integration and processes

Tuesday, 10 October 2023 14:45 (1 hour)

- indicators of compromise (IoCs), threat intelligence sharing, TLP protocol
- tools and technologies: MISP, Zeek, OpenSearch etc.
- deploying a Security Operation Center
- security incidents: detecting and alerting

Summary

Presenter: CROOKS, David (UKRI STFC)

Contribution ID: **116** Type: **Lecture**

Intrusion detection with SOC: deployment and operation

Wednesday, 11 October 2023 11:30 (1 hour)

- indicators of compromise (IoCs), threat intelligence sharing, TLP protocol
- tools and technologies: MISP, Zeek, OpenSearch etc.
- deploying a Security Operation Center
- security incidents: detecting and alerting

Summary

Presenter: CROOKS, David (UKRI STFC)

Contribution ID: **117** Type: **Exercise**

Intrusion detection with SOC and AAI - exercises

Thursday, 12 October 2023 16:15 (2h 45m)

- indicators of compromise, threat intelligence sharing, TLP protocol
- tools and technologies
- deploying a Security Operation Center
- detecting security incidents

Summary

Presenters: CROOKS, David (UKRI STFC); Mr DACK, Tom (Science and Technology Facilities Council STFC (GB))

Contribution ID: **118** Type: **Lecture**

Digital forensics: essentials and data acquisition

Thursday, 12 October 2023 08:45 (1 hour)

digital evidence handling
data acquisition (live systems, storage etc.)
data analysis (OS, file system, network, executables etc.)
reporting

Summary

Presenter: KOUŘIL, Daniel (CESNET)

Contribution ID: **119** Type: **Lecture**

Digital forensics: data analysis

Thursday, 12 October 2023 11:30 (1 hour)

Summary

Presenter: KOUŘIL, Daniel (CESNET)

Contribution ID: **120** Type: **Exercise**

Digital forensics - exercises

Friday, 13 October 2023 08:45 (1h 30m)

Summary

Presenter: KOUŘIL, Daniel (CESNET)

Contribution ID: **121** Type: **Lecture**

Defensible security architecture: how to implement security principles

Thursday, 12 October 2023 09:45 (1 hour)

- data security
- endpoint security: hardware, host, OS, BMC security, system hardening
- application security
- future security trends

Summary

Primary author: KRAŠOVEC, Barbara (IJS)

Presenter: KRAŠOVEC, Barbara (IJS)

Contribution ID: **122** Type: **Lecture**

Incident response management

Thursday, 12 October 2023 14:45 (1 hour)

- incident management and coordination
- incident analysis and investigation
- communication with stakeholders
- containment and eradiction
- recovery
- lessons learnt

Summary

Primary author: KRAŠOVEC, Barbara (IJS)

Presenter: KRAŠOVEC, Barbara (IJS)

Contribution ID: **123** Type: **Exercise**

Incident response - exercise

Friday, 13 October 2023 15:00 (1h 30m)

- incident management and coordination
- Sirtfi and trust frameworks
- communication with local users, external communities, and other stakeholders
- working with law enforcement
- privacy aspects

Summary

Presenters: Dr CROOKS, David (UKRI STFC); WARTEL, Romain (CERN); LOPIENSKI, Sebastian (CERN); Mr DACK, Tom (Science and Technology Facilities Council STFC (GB))

Contribution ID: **124** Type: **Lecture**

Penetration testing - exercise debriefing

Friday, 13 October 2023 12:00 (30 minutes)

Summary

Presenter: LOPIENSKI, Sebastian (CERN)

Contribution ID: **125** Type: **Lecture**

Special evening talk: Ransomware - and much more! TBC

This is not about ransomware. It's about (double) extortion!

Summary

Contribution ID: **126** Type: **Exercise**

Introduction to forensics - exercises

Friday, 13 October 2023 10:30 (1h 15m)

Summary

Presenter: KOUŘIL, Daniel

Contribution ID: **127** Type: **not specified**

Study time

Friday, 13 October 2023 13:15 (1 hour)

Contribution ID: **128** Type: **not specified**

Study time and/or daily sports

Thursday, 12 October 2023 13:15 (1h 30m)

Contribution ID: **129** Type: **not specified**

Study time and/or daily sports

Tuesday, 10 October 2023 13:15 (1h 30m)

Contribution ID: **130** Type: **not specified**

Study time and/or daily sports

Monday, 9 October 2023 13:15 (1h 30m)

Contribution ID: **131** Type: **Exercise**

Incident response - exercise

Friday, 13 October 2023 16:45 (1h 15m)

- incident management and coordination
- Sirtfi and trust frameworks
- communication with local users, external communities, and other stakeholders
- working with law enforcement
- privacy aspects

Summary

Presenters: Dr CROOKS, David (UKRI STFC); WARTEL, Romain (CERN); LOPIENSKI, Sebastian (CERN); Mr DACK, Tom (Science and Technology Facilities Council STFC (GB))