Thematic CERN School of Computing on Security 2023

Sunday, 8 October 2023 - Saturday, 14 October 2023

MedILS, Split, Croatia

Book of Abstracts

Contents

73

Exam

74

Announcements

Summary:

75

Announcements

Summary:

76

Announcements

Summary:

77

Announcements

Summary:

78

Announcements

Summary:

79

Opening Session

Corresponding Authors: mile.dzelalija@cern.ch, alberto.pace@cern.ch

Summary:

80

Closing Session

Corresponding Author: alberto.pace@cern.ch

Summary:

81

Student lightning talks

Summary:

82

Guest lecture

Summary:

84

Special evening talk: Future of the Universe and of Humanity

Author: Ivica Puljak[1]

[1] *University of Split. Fac.of Elect. Eng., Mech. Eng. and Nav.Architect. (HR)*

Corresponding Author: ivica.puljak@fesb.hr

Summary:

87

Scientific and computing challenges in fundamental physics

Author: Ivica Puljak[1]

[1] *University of Split. Fac.of Elect. Eng., Mech. Eng. and Nav.Architect. (HR)*

Corresponding Author: ivica.puljak@fesb.hr

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:

88

Self-presentation: 1 minute per person

Summary:

92

School photo

Summary:

96

Guest lecture: Why is Higgs still a star?

Author: Toni Sculac[1]

[1] *University of Split Faculty of Science (HR)*

Corresponding Author: toni.sculac@cern.ch

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:

97

Welcome to the CERN School of Computing

Corresponding Author: alberto.pace@cern.ch

99

Announcements

Summary:

100

Photo contest

Author: Joelma Tolomeo[1]

[1] *CERN*

Corresponding Author: joelma.tolomeo@cern.ch

Summary:

101

Security in research and scientific computing

Corresponding Author: stefan.lueders@cern.ch

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

Summary:

102

Security management

- security principles
- threat modeling, risk assessment, risk management
- security standards
- security policies

- the human factor, security culture

Summary:

103

Security operations - lecture 1

Corresponding Author: sveng@nikhef.nl

- 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:

104

Security operations - lecture 2

Corresponding Author: sveng@nikhef.nl

- 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:

105

Identity, authentication, authorisation

Corresponding Author: tom.dack@cern.ch

- 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:

106

Security architecture fundamentals

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:

107

Network design - exercise

Summary:

108

Virtualisation and cloud security

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:

109

Container security

Corresponding Author: kouril@ics.muni.cz

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

Summary:

110

Container security - exercises

Corresponding Author: kouril@ics.muni.cz

Summary:

111

Risk and vulnerability management

Corresponding Author: sveng@nikhef.nl

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

Summary:

112

Introduction to web penetration testing

Corresponding Author: sebastian.lopienski@cern.ch

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

Summary:

113

Penetration testing - exercises

Corresponding Author: sebastian.lopienski@cern.ch

Summary:

114

Logging and traceability

Corresponding Author: david.crooks@cern.ch

- 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:

115

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

Corresponding Author: david.crooks@cern.ch

- 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:

116

Intrusion detection with SOC: deployment and operation

Corresponding Author: david.crooks@cern.ch

- 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:

117

Intrusion detection with SOC and AAI - exercises

Corresponding Authors: tom.dack@cern.ch, david.crooks@cern.ch

- indicators of compromise, threat intelligence sharing, TLP protocol
- tools and technologies

- deploying a Security Operation Center
- detecting security incidents

Summary:

118

Digital forensics: essentials and data acquisition

Corresponding Author: kouril@ics.muni.cz

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

Summary:

119

Digital forensics: data analysis

Corresponding Author: kouril@ics.muni.cz

Summary:

120

Digital forensics - exercises

Corresponding Author: kouril@ics.muni.cz

Summary:

121

Defensible security architecture: how to implement security principles

Author: Barbara Krašovec[1]

[1] *IJS*

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

Summary:

122

Incident response management

Author: Barbara Krašovec[1]

[1] *IJS*

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

Summary:

123

Incident response - exercise

Corresponding Authors: romain.wartel@cern.ch, david.crooks@cern.ch, tom.dack@cern.ch, sebastian.lopienski@cern.ch

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

Summary:

124

Penetration testing - exercise debriefing

Corresponding Author: sebastian.lopienski@cern.ch

Summary:

125

Special evening talk: Ransomware - and much more! TBC

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

Summary:

126

Introduction to forensics - exercises

Corresponding Author: daniel.kouril@cesnet.cz

Summary:

127

Study time

128

Study time and/or daily sports

129

Study time and/or daily sports

130

Study time and/or daily sports

131

Incident response - exercise

Corresponding Authors: sebastian.lopienski@cern.ch, tom.dack@cern.ch, david.crooks@cern.ch, romain.wartel@cern.ch

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

Summary: