COST Action CA22104 BEiNG-WISE

Behavioral Next Generation in Wireless Networks for Cyber Security

Cybersecurity and the human factor in the era of evolved communication technologies

Training School

26-27 June 2024

University Ss Cyril and Methodius in Skopje, Faculty for Computer Science and Engineering

Venue: Faculty for Computer Science and Engineering (FINKI), ul.Rudzer Boshkovikj 16, Skopje, Republic of North Macedonia

Google Maps: https://maps.app.goo.gl/FLeRMiwnZkwJYqgk8

Room: (**TMF Amphitheater –** Amphitheater of the Faculty of Technology and Metallurgy, UKIM)

AGENDA

DAY 1 (26.06)

09.00   Arrival of the participants

09.15   **Welcoming remarks by organizers**

09.30-11.30   **Isabella Corradini**

Title and description

Understanding the human factor in cybersecurity: psychological aspects

Cybersecurity is typically associated with experts in IT, because the concept calls on technical aspect. However, cybersecurity is above all a human problem, because it concerns the relation between people and digital technologies. The human factor has always been considered the weakest link in the security chain. Using a psychological and a social approach, the lecture will be focused on how human errors, people's attitude and behavior can affect the success of a cyberattack (e.g. social engineering). Therefore, managing cybersecurity effectively requires the knowledge of the human nature and the development of a new mindset.

Bio: Isabella Corradini is a social psychologist and criminologist. She is the director of Themis Research Center, an interdisciplinary research organization focused on psychological and criminological issues, and co-founder of the Link&Think Research Lab, which provides information, education and socio-technical analysis of information technologies.

She served as a Professor of Social Psychology at various Italian universities for many years, and currently she is a lecturer in academic master's and industrial training programmes. She is also author of numerous articles, chapters and books on her expertise areas (e.g.

"Building a Cybersecurity Culture in organizations", published by Springer).

As a recognized expert in the field of human factors in safety and cybersecurity, she is member of several scientific and technical committees. She is also in charge of the area "Digital citizenship" of a national project in education for schools, promoted by the Italian Ministry of Education.

11.30-12.00 Coffee break

12.00-14.00 Aleksandar Jevremovic

Title: Technological Sovereignty, Cybersecurity, and Cybercrime

Abstract: Today, only the strongest states and companies can afford technological sovereignty, capable of independently developing cybersecurity solutions for their needs or securing custom solutions through specific contracts with control over the entire production process. Typical solutions available on the market today contain closed components whose operating principles end users are not familiar with. The security of such solutions, as well as the systems that use them, cannot be adequately determined. This lecture presented the problem of technological sovereignty, as well as possible ways to ensure it.

Short bio: Aleksandar Jevremovic is currently a Full Professor with the Faculty of Informatics and Computing, Singidunum University, Belgrade, Serbia; a guest lecturer with Harvard University, USA; a Visiting Professor at the Faculty of Computer Science and Engineering (FCSE) in Skopje; a Visiting Scholar with Cyprus Interaction Laboratory, Limassol, Cyprus; a post-doc researcher at the HCI Group at the Tallinn University in Tallinn, Estonia. He is also recognized as an Expert Level Instructor at Cisco Networking Academy Program. So far, he has authored/co-authored a number of research articles and made contributions to three books about computer networks, computer network security, and web development. Since 2018, he has been

serving as a Serbian Representative at the Technical Committee on Human–Computer Interaction, UNESCO International Federation for Information Processing (IFIP).

14.00-15.00 Lunch break

15.00-17.00 Marcel Moritz

European cybersecurity law: from data security to digital sovereignty

Short abstract :

The decade 2010 was characterized by a desire to develop cybersecurity requirements within European legislation, for personal data with the RGPD and beyond this with the NIS Directive. Today, the growing challenge is that of global digital sovereignty in the face of increasing threats.

Short bio :

Marcel Moritz is senior public law lecturer at Lille University. He heads the master's degree in cyberspace law and the digital law research team at Ceraps lab, involved in many funded projects. Marcel also practices in these areas as a lawyer.

17.00-17.20 Coffee break

17.20-18.30 Boro Jakimovski

Title: Digital Trust and Services

Abstract:

Short Bio:

Boro Jakimovski, Professor, Faculty of Computer Science and Engineering at UKIM (male) – obtained his PhD in Computer Science in 2010. His main interests and activities include Trust and Identity, Cloud, Grid, and HPC infrastructures, mainly in the deployment of federated identity management services, cloud services, core Grid services, regional Grid operations, deployment of operational tools,

application development support, dissemination activities and training. His research area is distributed computing (Cloud, Grid, HPC), security and software engineering. He is co-author of over 48 scientific papers published in international journals and proceedings of conferences. He was involved in 25 international and national application and research projects funded by TEMPUS, PHARE, DAAD, FP7, H2020 and Horizon Europe such as GN3, GN3+, GN4-1, GN4-2, GN4-3, EGI-InSPIRE, HP-SEE, SEE-GRID-SCI, NI4OS Europe, EGI-ACE and many more. Currently he is involved in Trust and Identity activities in GEANT, WP leader for the North Macedonian work package within the EuroCC project, as well as the head of the National competence center for HPC. He is a member of the board of the national NREN, MARNET, member of the EuroHPC GB as well as member of the EGI Council.

DAY 2 (27.06)

09.00-09.15 Welcoming participants and Networking

09.15-11.00 Pardeep Kumar

The Always-Connected Paradigm – Cyber Security Issues and Best Practices

Abstract: Recent technological evolution and advancements in wireless communication systems are enabling millions of innovative cyberspace applications to connect to the Internet by anyone, anywhere. These applications are becoming an integral part of our daily life, in different sectors spanning from transport, health, energy, to deliver education, critical infrastructures, etc. The proliferation of disruptive technologies allows several opportunities to be (inter)connected and exchange significant amounts of data, by enabling the always-online-paradigm.

In this always-connected heterogeneous paradigm, it is difficult to understand how to trust technologies/tools and where to define the boundaries, which enable several concerns including security and privacy. Therefore, privacy and security management have become very intricate, and often tools used for guaranteeing security/privacy are very complex to be used and hinder the user's engagement instead of supporting it. The challenge is compounded by the fact that developers or users are neither experts nor typically have enough training, tools, support and guidance to design for the diverse security needs of the always-connected paradigm.

This talk will explore security/privacy issues (at various levels) from an ongoing multi-year of research and highlight a research agenda for the user's engagement (e.g., developer community, and so on).

11.00-11.30 Coffee break

11.30-13.30 Nuno Garcia

Cybersecurity and Machine Learning.

13.30-14.30 Lunch break

14.30-16.00 Bozidar Spirovski and Anja Ivanovska

Session title: "The day the network stood still - an incident management exercise of an ICS network compromise"

Session abstract: The session is an extensive exercise in the incident management process of an incident in which an ICS network infrastructure is compromised. The session will have the following sections:

Brief review of incident management process and key elements

Incident scenario overview

Tabletop Incident exercise, with roles of the incident handling roles assigned to the audience.

Incident post-mortem and mutual feedback

Wrap up and discussion

The objective of the session is to immerse the participants in the crisis environment of an incident, so they can have a better grasp of the process and be better equipped to conduct their own exercises and preparation for incidents in their own environment.

Technical skills are not required, although basic understanding of computer networking and mobile telephony is helpful. Laptops are needed for accessing the exercise materials and for being able to draft tasks/responses. Users should be able to use Slack to access the environment used for the exercise.

Session presenters: Anja Ivanovska, Information Security Officer of EVN and Bozidar Spirovski, Chief Information Security Officer of Blue dot and Sourcico.

16.00-16.30 Coffee Break

16.30-17.30   Bozidar Spirovski and Anja Ivanovska (continued)

Incident management exercise on compromised IoT modems

17.30-18.00   Panel Discussion and Concluding remarks.

Hybrid event, online option:

Microsoft Teams meeting

Microsoft Teams Need help?

Join the meeting now

Meeting ID: **322 030 749 137**

Passcode: **9RctnY**

https://teams.microsoft.com/l/meetup-join/19%3ameeting_NGY3NGQwM2EtN2Q0MS00MDUwLWFjNGUtY2I3YTU4OTE0YWY4%40thread.v2/0?context=%7b%22Tid%22%3a%22f0cac47b-e2b3-4e1b-a52f-487d2d996288%22%2c%22Oid%22%3a%225b6d8b7a-78ac-403c-ab69-252efc2b9970%22%7d