Central European
Cybersecurity Conference
2018

Conference program

15–16 November 2018

Ljubljana, Slovenia

Organized by

University of Maribor

Faculty of
Criminal Justice and Security

Sponsors

https://www.a1.si/
A1

http://www.siq.si/
SIQ

http://genlan.si/
GenLan

https://en.posta.si/
Pošta Slovenije

https://www.telekom.si/en
Telekom Slovenije

https://www.siemens.com/global/en/home.html
Siemens

https://www.biokoda.com/home
Biokoda

https://www.informatika.si/?lang=en
Informatika

http://www.smartis.si/
SmartIS

https://www.abakus.si/
Abakus Plus

Supporting partners

http://www.isaca.si/

ISACA Slovenia Chapter

https://chapters.cloudsecurityalliance.org/sloven
ia/

CSA Slovenia Chapter

http://www.akos-rs.si/

Agency for Communication
Networks and Services of the
Republic of Slovenia

https://www.amzs.si/en
AMZS

https://www.gzs.si/
Chamber of Commerce and Industry
of Slovenia

http://www.amcham.si/
AmCham Slovenia

https://www.cert.si/
SI-CERT

Media partners

http://www.mdpi.com/journal/computers
Computers

http://www.mdpi.com/journal/futureinternet
Future Internet

About the Conference

The second Central European Cybersecurity Conference – CECC 2018 aims at establishing a venue for the exchange of information on cybersecurity and its many aspects in central Europe. CECC 2018 encourages the dialogue between researchers of technical and social aspects of cybersecurity, both crucial in attaining adequate levels of cybersecurity. Complementary contributions dealing with its economic aspects as well as any legal, investigation or other issues related to cybersecurity are welcome, too.

Program

Thursday, 15 November 2018

9:00 – 18:00   **Registration**

10:00 – 10:30   **Opening**
Andrej Sotlar
Dean of the Faculty of Criminal Justice and Security, University of Maribor

Andrej Tomšič
Deputy Information Commissioner of the Republic of Slovenia

Jörg Keller
CECC 2017 Co-Chair, FernUniversität Hagen

10:30 – 11:00   **Invited talk**
An introduction into car forensics with an example of a car2infrastructure application
Christian Hummert (Mittweida University of Applied Sciences)

11:00 – 11:30   **Coffee break**

11:30 – 12:00   **Professional presentations**
Artificial intelligence in cyber security
Primož Vogrinec (A1)

Security assessment in industrial control systems and IEC 62443 standards certification process
Miha Ozimek (SIQ)

12:00 – 13:00   **Research papers**
One countermeasure, multiple patterns: Countermeasure variation for covert channels
Steffen Wendzel, Daniela Eller and Wojciech Mazurczyk

Virtual honeypots and detecion of telnet botnets
Tomáš Bajtoš, Pavol Sokol and Terézia Mézešová

Hack my company: An empirical assessment of post-exploitation behavior and lateral movement in cloud environments
Daniel Fraunholz, Daniel Schneider, Janis Zemitis and Hans Dieter Schotten

13:00 – 15:00   **Lunch break & Career marketplace**

15:00 − 15:30 **Invited talk**
Gorazd Božič (SI-CERT)

15:30 − 16:30 **Research papers**
Security analysis of key acquiring strategies used by cryptographic ransomware
Ziya A. Genc, Gabriele Lenzini and P. Y. A. Ryan

Improving lawful interception in virtual datacenters
Daniel Spiekermann, Jörg Keller and Tobias Eggendorfer

Structural limitations of B+-tree forensics
Peter Kieseberg, Sebastian Schrittwieser and Edgar Weippl

16:30 − 17:00 **Coffee break**

17:00 − 17:15 **Professional presentations**
Deja-Vu: Added value of keeping your data safe
Urh Srečnik (Abakus Plus)

17:15 − 17:30 **Invited talk**
Safety and security of cyberspace users – criminological, victimological and preventative aspects
Gorazd Meško, Kaja Prislan, Rok Hacin, Blaž Markelj, Simon Vrhovec, Igor Bernik

17:30 − 18:30 **Research papers**
Coping with access control requirements in the context of mutual dependencies between business and IT
Roman Pilipchuk

Aligning business process access control policies with enterprise architecture
Roman Pilipchuk, Stephan Seifermann and Robert Heinrich

Privacy improvement model for biometric person recognition in ambient intelligence using perceptual hashing
Petra Grd, Igor Tomičić and Miroslav Bača

19:00 − 21:30 **Dinner**

Friday, 16 November 2018

9:00 − 18:00 **Registration**

10:00 − 10:30 **Invited talk**
Engineering edge security for the protection of critical infrastructures
Béla Genge (University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures)

10:30 – 11:30 **Research papers**
OpenSPA - An open and extensible protocol for single packet authorization
Gregor Robert Krmelj, Matjaž Pančur, Miha Grohar and Mojca Ciglarič

A brief look at the security of DeviceNet communication in industrial control systems
Pal-Stefan Murvay and Bogdan Groza

A testbed for performing security experiments with software-defined industrial control systems
Zoltán Szántó, Hunor Sándor and Béla Genge

11:30 – 12:00 **Coffee break**

12:00 – 12:30 **Professional presentations**
Cybersecurity operations, why and how
Metod Platiše (Telekom Slovenije)

Establishing SOC in energy sector - issues and obstacles
Ciril Kafol and Andrej Bregar (Informatika)

12:30 – 13:10 **Research papers**
It's all fun and games, and some legalese: Data protection implications for increasing cyber-skills of employees through games
Danaja Fabčič Povše

What drives the motivation to self-protect on social networks? The role of privacy concerns and perceived threats
Damjan Fujs, Simon Vrhovec and Anže Mihelič

13:10 – 15:00 **Lunch break**

15:00 – 15:15 **Professional presentations**
Secure communication and real-time protection
Denis Justinek (Biokoda)

15:15 – 16:15 **Research papers**
Application detection in anonymous communication networks
Mohammad Hajian Berenjestanaki and Mohammadali Akhaee

A framework for a forensically sound harvesting the dark web
Christian Valassi, Jesper Bergman and Oliver Popov

Do ut des: Disseminating online child sexual abuse material for investigative purposes?
Sabine Witting

16:15 – 16:45 **Coffee break**

16:45 – 17:15 **Professional presentations**
"Bouquet" of several information security survey results
Boštjan Delak (Faculty of Information Studies in Novo mesto)

It is easy to be DPO with SmartDPO
Jana Češarek (SmartIS)

17:15 – 17:55   **Research papers**
Towards unambiguous IT risk definition
Maksim Goman

An ontology capturing the interdependence of the General Data Protection
Regulation (GDPR) and information security
Melisa Geko and Simon Tjoa

17:55 – 18:20   **Closing**
Igor Bernik
CECC 2018 Publication Chair, University of Maribor

Best paper award sponsored by Future Internet journal, MDPI

Venue

HOTEL LEV
HOTEL AND CONFERENCE CENTER
★★★★

Vošnjakova 1, Ljubljana, Slovenia
+386 1 308 1438
lev@union-hotels.eu
http://www.union-hotels.eu/en/hotel-lev/

Invited speakers

Christian Hummert
An introduction into car forensics with an example of a car2infrastructure application

Christian Hummert obtained his PhD in computer science from the Friedrich-Schiller University in Jena, Germany. He worked six years as a forensic expert for the Federal Police of Thuringia. In 2015 he was appointed as a Full Professor for IT-Security / Digital Forensics at the Mittweida University of Applied Science. In October 2018 he left university and became a director for digital forensics at the Central Office for Information Technology in the Security Sector (ZITiS) in Germany. He is a member of the Steering Committee of the Embedded World Conference. His research interests include digital forensics especially forensics of embedded systems and automotive forensics.

Béla Genge

Engineering edge security for the protection of critical infrastructures

Béla Genge obtained his PhD in 2009 in network security from the Technical University of Cluj-Napoca, Romania. After a 3-year Post-Doctoral research experience at the Joint Research Centre of the European Commission (Ispra, Italy), he was appointed as an Associate Professor at the Petru Maior University of Tg. Mures, Romania. He is a member of the Editorial Boards of the International Journal of Critical Infrastructure Protection (Elsevier), and of the Security and Communication Networks (Hindawi). His research interests include security and resilience of Industrial Control Systems, Software-Defined industrial network control, and anomaly detection systems.