Central European Cybersecurity Conference CECC 2019

Conference program

14–15 November 2019

Munich, Germany

Organized by

University of Maribor

Faculty of
Criminal Justice and Security

ZITiS

Last update: 2019-11-12

We reserve the right to change the conference program

About the Conference

The third Central European Cybersecurity Conference – CECC 2019 aims at establishing a venue for the exchange of information on cybersecurity and its many aspects between academics and practitioners in central Europe. CECC 2019 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, 14 November 2019	
9:00 – 17:30	**Registration**
9:30 – 10:30	**Opening**
	Invited talk Digital Forensics vs. Due Process - Conflicting Standards or Complementary Approaches? *Uwe Ewald (International Justice Analysis Forum)*
10:30 – 11:00	**Coffee break**
11:00 – 12:30	**Session I** Forensic Investigations in Vehicle Data Stores *Nico Vinzenz and Tobias Eggendorfer*
	Accommodating Time-Triggered Authentication to FlexRay Demands *Pal-Stefan Murvay, Bogdan Groza and Lucian Popa*
	Discussing the Feasibility of Acoustic Sensors for Side Channel-aided Industrial Intrusion Detection: An Essay *Simon Duque Anton, Anna Pia Lohfink and Hans Dieter Schotten*
	Secure Logging for Industrial Control Systems Using Blockchain *Stefan Schorradt, Edita Bajramovic and Felix Freiling*
	Security in Process: Detecting Attacks in Industrial Process Data *Simon Duque Anton, Anna Pia Lohfink, Christoph Garth and Hans Dieter Schotten*

12:30 – 14:00 Lunch break

Poster session

Combined side-channels malware detection for NFV infrastructure
Andrew Sergeev, Eyal Ben-Sa'adon, Asi Saar and Elad Tannenbaum

Towards a delegation-type secure software development method
Anže Mihelič, Tomaž Hovelja and Simon Vrhovec

Approaching the Automation of Cyber Security Testing of Connected Vehicles
Stefan Marksteiner and Zhendong Ma

Integrating Threat Modeling and Automated Test Case Generation into Industrialized Software Security Testing
Stefan Marksteiner, Rudolf Ramler and Hannes Sochor

A practical view on IT risk management process
Maksim Goman

Cybercrime victimization and seeking help: A survey of students in Slovenia
Kaja Prislan, Igor Bernik, Gorazd Meško, Rok Hacin, Blaž Markelj and Simon Vrhovec

14:00 – 15:30 Session II
Achieving Consistency of Software Updates against Strong Attackers
Lamya Abdullah, Sebastian Hahn and Felix Freiling

How much does a zero-permission Android app know about us?
Antonios Dimitriadis, George Drosatos and Pavlos S. Efraimidis

Meizodon: Security Benchmarking Framework for Static Android Malware Detectors
Sebastiaan Alvarez Rodriguez and Erik van der Kouwe

Case Study: Analysis and Mitigation of a New Sandbox-Evasion Technique
Ziya A. Genc, Gabriele Lenzini and Daniele Sgandurra

15:30 – 16:00 Coffee break

16:00 – 16:30 Invited talk
Obfuscated Android Application Development
Jean-François Lalande (CentraleSupélec / Inria)

16:30 – 17:30 Session III
IPv6 Covert Channels in the Wild
Wojciech Mazurczyk, Krystian Powójski and Luca Caviglione

Simulating and Detecting Attacks of Untrusted Clients in OPC UA Networks
Charles Neu, Ina Schiering and Avelino Francisco Zorzo

Network Forensic Investigation in OpenContrail Environments
Alexander Heckel and Daniel Spiekermann

Friday, 15 November 2019

9:00 – 12:30 Registration

9:30 – 10:00 Invited talk
Fake news and digital manipulations at the age of modern technology
Tal Pavel (CyBureau)

10:00 – 11:00 Session IV
Multi-Platform Authorship Verification
Abdulaziz Altamimi, Nathan Clarke and Steven Furnell

The password literacy in North Macedonia: A case study
Andrej Cvetkovski and Flavio Esposito

Bitcoin adoption: Scams and anonymity may not matter but trust into Bitcoin security does
Aleksander Murko and Simon Vrhovec

Retrospective Tracking of Suspects in GDPR Conform Mobile Access Networks Datasets
Louis Tajan and Dirk Westhoff

11:00 – 11:30 Coffee break

11:30 – 12:30 Session V
A Secure String Class Compliant with PCI DSS
Katarína Amrichová and Terézia Mézešová

Determining Minimum Hash Width for Hash Chains
Martin Dietzfelbinger and Jörg Keller

SAT Solvers and their Limits with NFSR-based Stream Ciphers - an Example with Grain v1
Andreas Schaffhauser

12:30 – 12:40 Closing

Venue

ZITiS

ZITiS
Zamdorfer Straße 88
D-81677 Munich
Germany

Invited speakers

Tal Pavel

Fake news and digital manipulations at the age of modern technology

Tal Pavel is Founder and CEO of CyBureau – The Cyber Empowerment Center in Romania and Israel. He is also Head of Cybersecurity Studies – Information Systems Program, School of Economics and Management at the Academic College of Tel Aviv-Yaffo, Lecturer at several academic institutions in Israel, expert and researcher of the internet and cyber threats in the Middle East and the entire world. He holds a PhD in Middle Eastern Studies from Bar-Ilan University in Israel. He served as a keynote speaker at international conferences and has been interviewed as an expert cyber commentator on all major Israeli media outlets.

Jean-François Lalande

Obfuscated Android Application Development

Jean-François Lalande is Professor at CentraleSupélec, in the Inria project CIDRE of the IRISA laboratory. His areas of interest are the security of operating systems, the security of C embedded software (e.g. smart cards) and the security of Android applications. He works on malware analysis, access control policies, intrusion detection tools and software code analysis. He also actively develops tools for analyzing statically or dynamically Android applications that have malicious behaviors.

Uwe Ewald

Digital Forensics vs. Due Process - Conflicting Standards or Complementary Approaches?

Uwe Ewald is the founding Executive Director of the International Justice Analysis Forum (IJAF), focusing on the analysis of digital data in evidentiary criminal proceedings and the digitization of the (international) criminal justice process. He conducted criminological and legal research and held teaching positions at different universities, at Humboldt and Free University Berlin, Germany, at Simon Fraser University, Vancouver, Canada, and the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany. Between 2002 and 2018 he taught Security Governance in the European Union, and Critical Assessment of Applied Empirical Research Methods at the Ruhr-Universität Bochum, Department of Criminology and Police Science. From 2002 till 2009 he conducted computer-aided content analysis of digitized evidentiary mass data at the Office of the Prosecutor at the UN International Criminal Tribunal for the Former Yugoslavia. Due to his legal background (Dr. iur) he cooperates as an attorney and analyst at the law office Dost-Roxin and Marson, Berlin, and advises German parliamentarians regarding the implementation of European legislation at the Saxon State Parliament, Dresden, Germany with particular focus on digitation in the Area of Freedom, Security and Justice. As a Certified Expert for Digital Forensic Big Data Analysis he is a Member of the German Expert Association. He is trainer for content analysis Software Provalis.