Univerza v Mariboru

Fakulteta za varnostne vede

KATEDRA ZA INFORMACIJSKO VARNOST

Predstojnik katedre: prof. dr. Igor Bernik

Dan Inštituta za varstvoslovje 2022

10-11 NOVEMBER 2021

European Interdisciplinary Cybersecurity Conference

Targu Mures, Romania

CONFERENCE CHAIR

Martin Gilje Jaatun, University of Stavanger (Norway)

PROGRAM COMMITTEE CO-CHAIR

Geir Myrdahl Køien, University of South-eastern Norway (Norway)

DOCTORAL SYMPOSIUM CHAIR

Daniela Soares Cruzes, Norwegian university of science and technology (Norway)

ORGANIZING CHAIR

Bela Genge, University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures (Romania)

ORGANIZING CO-CHAIR

Piroska Haller, University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures (Romania)

ORGANIZING TEAM

Bogdan Crainicu, University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures (Romania)
Adam Gergely, University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures (Romania)
Teri Lenard, University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures (Romania)
Roland Bolboaca, University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures (Romania)

PROGRAM COMMITTEE

Rafael Asorey Cacheda, Universidad Politécnica de Cartagena (Spain)
Luca Caviglione, IMATI - CNR (Italy)
Michal Choras, University of Science and Technology (Poland)
Tobias Eggendorfer, University of Applied Sciences Ravensburg-Weingarten (Germany)
Virginia Franqueira, University of Kent (UK)
Petra Grd, University of Zagreb (Croatia)
Mordechai Guri, Ben-Gurion University of the Negev (Israel)
Piroska Haller, University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures (Romania)
Marko Hölbl, University of Maribor (Slovenia)
Pedro R. M. Inácio, University Beira Interior (Portugal)
Georgios Karopoulos, Joint Research Centre (Italy)
Stefan Katzenbeisser, University of Passau (Germany)
Peter Kieseberg, St. Pölten University of Applied Sciences (Austria)
Romain Laborde, University of Toulouse (France)
Jean-Francois Lalande, CentraleSupélec / Inria (France)
Shujun Li, University of Kent (UK)
Olaf Maennel, Tallinn University of Technology (Estonia)
Brad Malin, Vanderbilt University (USA)
Rodrigo Miani, Universidade Federal de Uberlândia (Brazil)
Aleksandra Mileva, University Goce Delcev (North Macedonia)
Pal-Stefan Murvay, Politehnica University of Timisoara (Romania)
Sebastian Pape, Goethe University Frankfurt (Germany)
Kaja Prislan, University of Maribor (Slovenia)
Peter Y. A. Ryan, University of Luxembourg (Luxembourg)
Gerardo Simari, Universidad Nacional del Sur in Bahía Blanca and CONICET (Argentina)
Daniel Spiekermann, Polizeiakademie Niedersachsen (Germany)
Edgar Weippl, SBA Research (Austria)
Steffen Wendzel, Worms University of Applied Sciences (Germany)
Christos Xenakis, University of Piraeus (Greece)
Nicola Zannone, Eindhoven University of Technology (Netherlands)
Aleš Završnik, Institute of Criminology at the Faculty of Law Ljubljana (Slovenia)

GARY MCGRAW

SECURITY ENGINEERING FOR MACHINE LEARNING

Machine Learning appears to have made impressive progress on many tasks including image classification, machine translation, autonomous vehicle control, playing complex games including chess, Go, and Atari video games, and more. This has led to much breathless popular press coverage of Artificial Intelligence, and has elevated deep learning to an almost magical status in the eyes of the public. ML, especially of the deep learning sort, is not magic, however. ML has become so popular that its application, though often poorly understood and partially motivated by hype, is exploding. In my view, this is not necessarily a good thing. I am concerned with the systematic risk invoked by adopting ML in a haphazard fashion. Our research at the Berryville Institute of Machine Learning (BIIML) is focused on understanding and categorizing security engineering risks introduced by ML at the design level. Though the idea of addressing security risk in ML is not a new one, most previous work has focused on either particular attacks against running ML systems (a kind of dynamic analysis) or on operational security issues surrounding ML. This talk focuses on the results of an architectural risk analysis (sometimes called a threat model) of ML systems in general. A list of the top five (of 78 known) ML security risks will be presented.

Gary McGraw is co-founder of the Berryville Institute of Machine Learning. He is a globally recognized authority on software security and the author of eight best selling books on this topic. His titles include Software Security, Exploiting Software, Building Secure Software, Java Security, Exploiting Online Games, and 6 other books; and he is editor of the Addison-Wesley Software Security series. Dr. McGraw has also written over 100 peer-reviewed scientific publications. Gary serves on the Advisory Boards of Irius Risk, Maxmyinterest, Runsafe Security, and Secure Code Warrior. He has also served as a Board member of Cigital and Codiscope (acquired by Synopsys) and as Advisor to CodeDX (acquired by Synopsys), Black Duck (acquired by Synopsys), Dasient (acquired by Twitter), Fortify Software (acquired by HP), and Invotas (acquired by FireEye). Gary produced the monthly Silver Bullet Security Podcast for IEEE Security & Privacy magazine for thirteen years. His dual PhD is in Cognitive Science and Computer Science from Indiana University where he serves on the Dean's Advisory Council for the Luddy School of Informatics, Computing, and Engineering.

https://garymcgraw.com
https://berryvilleiml.com/
@cigitalgem

GEORGE EMIL PALADE UNIVERSITY OF MEDICINE, PHARMACY, SCIENCE, AND TECHNOLOGY OF TARGU MURES

University of Maribor
Faculty of Criminal Justice and Security

EICC: European Interdisciplinary Cybersecurity Conference

2021 Proceeding

Editors: Martin Gilje Jaatun, Geir M. Køien, Oksana Kulyk

Publisher: Association for Computing Machinery, New York, NY, United States

Conference: EICC '21: European Interdisciplinary Cybersecurity Conference • Virtual Event Romania • November 10 – 11, 2021

ISBN: 978-1-4503-9049-1

15-16 JUNE 2022

European Interdisciplinary Cybersecurity Conference

Internet Interdisciplinary Institute (IN3) / Universitat Oberta de Catalunya, Barcelona, Spain

CONFERENCE CHAIR

David Megías Jiménez, Internet Interdisciplinary Institute (IN3) / Universitat Oberta de Catalunya (Spain)

PROGRAM COMMITTEE CO-CHAIRS

Joaquín Garcia-Alfaro, Institut Polytechnique de Paris (France)
Roberto di Pietro, HBKU College of Science and Engineering (Qatar)

ORGANIZING CHAIR

Helena Rifà-Pous, Universitat Oberta de Catalunya (Spain)

STEERING COMMITTEE

Igor Bernik, University of Maribor (Slovenia)
Bela Genge, University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures (Romania)
Joerg Keller, FernUniversitaet in Hagen (Germany)
Blaž Markelj, University of Maribor (Slovenia)
Wojciech Mazurczyk, Warsaw University of Technology (Poland)
Simon Vrhovec, University of Maribor (Slovenia)

PROGRAM COMMITTEE

Kevin Allix, University of Luxembourg (Luxembourg)
Rafael Asorey Cacheda, Universidad Politécnica de Cartagena (Spain)
Laurent Aufrechter, Thales, (France)
Jurlind Budurushi, Cloudical Deutschland GmbH (Germany)
Krzysztof Cabaj, Warsaw University of Technology (Poland)
Luca Caviglione, IMATI - CNR (Italy)
Michal Choras, ITTI Ltd. (Poland)
Mehdi Chourib, FernUni Hagen (Germany)
Michele Colajanni, University of Modena (Italy)
Igino Corona, Pluribus One (Italy)
Salvatore D'Antonio, University of Naples "Parthenope" (Italy)
Bottjan Delak, Faculty of Information studies in Novo mesto (Slovenia)
Pavlos Efraimidis, Democritus University of Thrace (Greece)
Tobias Eggendorfer, University of Applied Sciences Ravensburg-Weingarten (Germany)
Virginia Franqueira, University of Kent (UK)
Dieter Gollmann, Hamburg University of Technology (Germany)
Mordechai Guri, Ben-Gurion University (Israel)
Piroska Haller, University of Medicine, Pharmacy, Sciences and Technology of Tg. Mures (Romania)
Marko Hölbl, University of Maribor (Slovenia)
Xinyi Huang, Fujian Normal University (China)
Pedro Inácio, Universidade da Beira Interior (Portugal)
Martin Gilje Jaatun, SINTEF Digital (Norway)
Petra Grd, University of Zagreb (Croatia)
Georgios Karopoulos, European Commission, Joint Research Centre (Greece)
Stefan Katzenbeisser, University of Passau (Germany)
Peter Kieseberg, St. Pölten University of Applied Sciences (Austria)
Oksana Kulyk, ITU Copenhagen (Denmark)
Romain Laborde, University Paul Sabatier Toulouse III (France)
Jean-Francois Lalande, CentraleSupélec / Inria (France)
Gabriele Lenzini, SnT/University of Luxembourg (Luxembourg)
Albert Levi, Sabanci University (Turkey)
Shujun Li, University of Kent (UK)
Olaf Maennel, Tallinn University of Technology (Estonia)
Brad Malin, Vanderbilt University (US)
Rodrigo Miani, Universidade Federal de Uberlândia (Brazil)
Anže Mihelič, University of Maribor (Slovenia)
Aleksandra Mileva, University Goce Delcev (North Macedonia)
Caroline Moeckel, Royal Holloway, University of London (UK)
Pal-Stefan Murvay, Politehnica University of Timisoara (Romania)
Sebastian Pape, Goethe University Frankfurt (Germany)
Marek Pawlicki, UTP Bydgoszcz, (Poland)
Fernando Pérez-González, Universidade de Vigo (Spain)
Kaja Prislan, University of Maribor (Slovenia)
Helena Rifà-Pous, Universitat Oberta de Catalunya (Spain)
Anderson Santana De Oliveira, SAP (Germany)
Lynsay Shepherd, Abertay University (UK)
Gerardo Simari, Universidad Nacional del Sur and CONICET (Argentina)
Kai Simon, Fraunhofer-Gesellschaft (Germany)
Florian Skopik, AIT Austrian Institute of Technology (Austria)
Daniel Spiekermann, Polizeiakademie Niedersachsen (Germany)
Mark Strembeck, WU Wien (Austria)
Hung-Min Sun, National Tsing Hua University (Taiwan)
Yuqiong Sun, Facebook (US)
Igor Tomičić, University of Zagreb (Croatia)
Damian Weber, HTW Saarland (Germany)
Edgar Weippl, University of Vienna (Austria)
Steffen Wendzel, Worms University of Applied Sciences (Germany)
Dirk Westhoff, Offenburg University of Applied Sciences (Germany)
Christos Xenakis, University of Piraeus (Greece)
Nicola Zannone, Eindhoven University of Technology (Netherlands)
Aleš Završnik, Institute of Criminology at the Faculty of Law Ljubljana (Slovenia)

Security and Communication Networks

Q2

SPECIAL SESSION ON ADVANCED AND RELIABLE SOLUTIONS TO COUNTER MALWARE AND STEGOMALWARE - DETONATOR 2022

Details

SECURITY IN OPEN CLOUD INFRASTRUCTURES - SOCI 2022

Details

COMPLEX NETWORK ANALYSIS FOR CYBERSECURITY - CNACYS 2022

Details

University of Maribor

Faculty of Criminal Justice and Security

KONFERENCA

Informacijska varnost

Zaupanje v človeka in tehnologijo

5. november 2021 \ on-line

Vodja organizacijskega in programskega odbora:
doc. dr. Blaž Markelj

Blaž Markelj sodelovanje z GV Založbo

izr. prod. dr. Blaž Markelj idejni in programski vodja konferenc prava v informacijski varnosti 2020, 2021 in 2022.

Akademske aktivnosti

Tematske številke znanstvenih revij

IEEE Security & Privacy
- Special Issue on Security and Privacy Issues of Home Globalization
- Simon Vrhovec, gostujoči urednik

Q1 Scopus

Scopus Q2 **Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (2x)**
- Special Issue on Multidisciplinary Solutions to Modern Cybersecurity Challenges
- Special Issue on Interdisciplinary Cybersecurity
- Simon Vrhovec, gostujoči urednik

Recenzent za znanstvene revije

Simon Vrhovec
- International Journal of Project Managemen
- Online Information Review
- Sensors
- Energy Research & Social Science
- IEEE Transactions on Engineering Management
- Aslib Journal of Information Management
- PLOS ONE
- Energies
- Journal of Cyber Security and Mobility
- International Journal of Advanced Computer Science and Applications
- Smart Cities
- Frontiers in Computer Science
- International Journal of Cyber Forensics and Advanced Threat Investigations

Blaž Markelj
- Revija za kriminalistiko in kriminologijo

Anže Mihelič
- Aslib Journal of information Management
- IEEE Access
- PLOS ONE
- Journal of Universal Computer Science

Igor Bernik
- Behaviour & Information Technology
- PlosONE
- IET Information Security

Uredniški odbor znanstvenih revij

Scopus Q4

Journal of Cyber Security and Mobility
- Simon Vrhovec

Frontiers in computer science
- Simon Vrhovec

International Journal of Cyber Forensics and Advanced Threat Investigations
- Simon Vrhovec

EUREKA: Social and Humanities
- Simon Vrhovec

Journal of forensic research and crime studies
- Igor Bernik

Varstvoslovje : revija za teorijo in prakso varstvoslovja
- Igor Bernik

Programski odbor znanstvenih konferenc

Simon Vrhovec
- Future Technologies Conference 2021 (**FTC 2021**)
- 4th International Workshop on Security Engineering for Cloud Computing (**IWSECC 2021**), 16th International Conference on Availability, Reliability and Security (**ARES 2021**)
- 3nd International Workshop on Information Security Methodology and Replication Studies (**IWSMR 2021**), 16th International Conference on Availability, Reliability and Security (**ARES 2021**)
- The 2021 Multidisciplinary International Conference of Research Applied to Defense and Security (**MICRADS´21**)
- The Sixth International Conference on Cyber-Technologies and Cyber-Systems (**CYBER 2021**)
- Computing Conference (**CC 2021**)
- Future of Information and Communication Conference 2021 (**FICC 2021**)

Anže Mihelič
- International Conference on Internet Monitoring and Protection (**ICIMP 2021**)
- European Interdisciplinary Cybersecurity Conference (**EICC 2021**)
- International Conference on Computer Science and Application Engineering (**CSAE 2021**)

Igor Bernik
- European Interdisciplinary Cybersecurity Conference (**EICC 2021**)
- European Conference on e-Learning (**ECEL 2021**)
- Knowledge Management and Intellectual Capital (**ECKM 2021**)
- European Conference on the Impact of Artificial Intelligence and Robotics (**ECIAIR 2021**)
- International Conference on Education and New Learning Technologies (**EduLEARN 2021**)

Raziskovalna področja in objave 2021 1/2

Človeški dejavniki kibernetske varnosti

Simon Vrhovec and Anže Mihelič. “Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation”. In: Computers & Security 106 (2021), 102309:1–22. doi: 10.1016/j.cose.2021.102309

Lara Klemenc, Simon Vrhovec, and Anže Mihelič. “Zaznavanje tveganj pri sprejemanju tehnoloških vsadkov”. In: Elektrotehniški vestnik / Electrotechnical Review 88.4 (2021), pp. 174–182

Zdravstvena informatika

Žiga Kodrič, Simon Vrhovec, and Luka Jelovčan. “Securing edge-enabled smart healthcare systems with blockchain: A systematic literature review”. In: Journal of Internet Services and Information Security 11.4 (2021), pp. 19–32. doi: 10.22667/JISIS.2021.11.30.019

Mihelič, Anže, Žvanut, Boštjan. (In)Secure smart device use among senior citizens. IEEE security & privacy : building confidence in a networked world, ISSN 1540-7993. [Print ed.], Jan./Feb. 2022, vol. 20, iss. 1, str. 62-71, ilustr., doi: 10.1109/MSEC.2021.3113726.

Razvoj varne programske opreme in sprejemanje novih tehnologij

Damjan Fujs, Simon Vrhovec, and Damjan Vavpotič. “Kategorizacija uporabnikov na podlagi njihovega z informacijsko varnostjo povezanega znanja, stališč in vedenja: pilotna študija”. In: Uporabna informatika 29.3 (2021), pp. 163–169

Simon Vrhovec and Blaž Markelj. “The relation between project team conflict and user resistance in software projects”. In: PLOS ONE 16.11 (2021), p. e0260059:1–11. doi: 10.1371/journal.pone.0260059

Damjan Fujs, Simon Vrhovec, and Damjan Vavpotič. “Know Your Enemy: User Segmentation Based on Human Aspects of Information Security”. In: IEEE Access 9 (2021), pp. 157306–157315. doi: 10.1109/ACCESS.2021.3130013

Raziskovalna področja in objave 2021 2/2

Simon Vrhovec and Blaž Markelj. “The relation between project team conflict and user resistance in software projects”. In: PLOS ONE 16.11 (2021), p. e0260059:1–11. doi: 10.1371/journal.pone.0260059

Novak, Primož, Bernik, Igor, Mihelič, Anže. Uvajanje nosljivih kamer v policijske postopke : vloga nadzora “od spodaj navzgor”. Varstvoslovje: revija za teorijo in prakso varstvoslovja, 2021, letn. 23, št. 2, str. 198-217

Metodologija

Simon Vrhovec, Luca Caviglione, and Steffen Wendzel. “Crème de la Crème: Lessons from Papers in Security Publications”. In: 16th International Conference on Availability, Reliability and Security (ARES 2021). Vienna, Austria: ACM, 2021, 75:1–9. doi: 10.1145/3465481.3470027

COVID-19

Mihelič, Anže, Jelovčan, Luka, Prislan, Kaja. Internal and external drivers for compliance with the COVID-19 preventive measures in Slovenia : The view from general deterrence and protection motivation. PloS one, ISSN 1932-6203, 2021, no. 11, e0259675

Jelovčan, Luka, Prislan, Kaja, Mihelič, Anže. Self-protective behaviour among young adults during public health crisis. Varstvoslovje : revija za teorijo in prakso varstvoslovja, ISSN 1580-0253. [Tiskana izd.], 2020, letn. 22, št. 3, str. 239-254

Raziskovalna področja, objave 2021 in sodelovanje z gospodarstvom

Podpisani sporazumi o sodelovanju

Organizacije:
AmCham Slovenija (skrbnik sporazuma Blaž Markelj)
SmartCom (skrbnik sporazuma Blaž Markelj)
GenLan (skrbnik sporazuma Blaž Markelj)
Hit d.d. Nova Gorica (skrbnik sporazuma Blaž Markelj)
ISACA (skrbnik sporazuma Blaž Markelj)

Sodelovanje z študenti in njihov nadaljni razvoj kariere

Sara Tomše (etični heking), nadaljevanje kariere na Telekom Slovenija
Branko Miličević, nadaljevanje kariere SIQ, Deloitte Slovenija
Žan Babič, nadaljevanje kariere na GenLan
Gašper Školč (pametni avtomobili), nadaljevanje kariere na Telekom Slovenija
Maša Dreven, sodelovanje z Deloitte Slovenija
Ida Majerle, ISACA, SIQ, SETCCE
Suzana Kužnik, ISACA, SIQ, NIL
Živa Kristančič, SmartCom
Gašper Kopušar, Elektro Ljubljana

Sodelovanje z gospodarstvom (kombinacija akademskega in gospodarskega sveta)

Konferenca InfoSEK 2021
Predstavitev delovanja katedre in aktualnih raziskovanj – Igor Bernik
Sodelujočih več kot 200 organizacij in 600 udeležencev tako iz ponudbe IV rešitev, uporabnikov IV rešitev iz gospodarstva ter javne uprave.

Konferenca Informacijska varnost zaupanje v človeka in tehnologijo 2021
Predsednik organizacijskega in programskega odbora - Blaž Markelj
Sodelujoče zunanje organizacije: A1, AmCham Slovenija, CheckPoint, SmartCom, GenaLan, Telekom Slovenije,Telemach, GV Založba.

Sodelovanje z gospodarstvom
A1, Smartcom, Smartis, Informatika d.o.o., Telekom, Eles, Ingram, GenLan, Telemach, GV Založba, IUS Info, AmCham, RealSecurity, Elektro Ljubljana...

Raziskovalna področja in sodelovanja 2021

Raziskovalne metode
- Luca Caviglione, IMATI - CNR (Italija)
- Sašo Džeroski, IJS (Slovenija)
- Dragi Kocev, IJS (Slovenija)
- Anže Mihelič
- Simon Vrhovec
- Steffen Wendzel, Worms University of Applied Sciences (Nemčija)

Socialna omrežja
- Damjan Fujs, UL FRI
- Simon Vrhovec

Sprejemanje in uporaba tehnologij
- Damjan Fujs, UL FRI
- **Lara Klemenc**, študentka UM FVV
- **Primož Novak**, student UM FVV
- **Tilen Sladič**, študent UM FVV
- **Katja Turha**, študentka UM FVV
- Damjan Vavpotič, UL FRI
- Simon Vrhovec
- Boštjan Žvanut, UP FVZ
- Anže Mihelič

Razvoj varne programske opreme
- **Damjan Fujs**, doktorski študent UL FRI
- Tomaž Hovelja, UL FRI
- **Anže Mihelič**, doktorski študent UL FRI
- Damjan Vavpotič, UL FRI
- Simon Vrhovec

Človeški dejavniki kibernetske varnosti
- **Andraž Hovnik**, študent UM FVV
- **Luka Jelovčan**, študent UM FVV
- Anže Mihelič
- **Samanta Mikuletič**, doktorska študentka FZAB
- Simon Vrhovec
- Boštjan Žvanut, UP FVZ

Umetna inteligenca v kibernetski varnosti
- **Aljaž Berčič**, študent UM FVV
- Michal Choras, University of Science and Technology (UTP), Poljska
- **Zvonimir Cvetko Damnjanović**, doktorski študent FIŠ
- Anže Mihelič
- Joerg Keller, FernUniversität in Hagen (FUH), Nemčija
- Simon Vrhovec

Univerza v Mariboru

Fakulteta za varnostne vede

Hvala za pozornost!

Dan Inštituta za varstvoslovje 2022