

ICCWS 2024

19th International Conference on Cyber Warfare and Security

26-27 March 2024, Johannesburg, South Africa

Mini Track on Security in Health Care: Innovations and Challenges for Trustworthy and Reliable Applications

Mini Track Chair: **Christoph Lipps & Jan Herbst**, German Research Center for Artificial Intelligence – Intelligent Networks Research Department, Germany



The acquisition, processing and exchange of (medical) information have always been the basis for sound diagnosis and effective therapy. The ability to share pathological findings and to collaborate in the process of developing solutions has led to significant advances in the field of medicine. This process is accelerated by the availability of huge amounts of data and the possibility to process and evaluate them accordingly. Recent innovations in mobile communication, such as Beyond 5G (B5G) and the Sixth Generation (6G) of wireless systems, are accelerating this trend even more. But, with the dependency and the increasing value of the transmitted (partly highly sensitive) information, however, comes the fact that systems are becoming increasingly attractive to attackers and saboteurs, entailing the need for technical solutions to detect, evolve, and protect the devices, the systems and above all the people.

Thus, the main challenge will be hardening the (communication) and the devices by addressing the entire cyber resilience lifecycle: Improving security, detecting attacks, responding to them and recovering from occurred ones. Therefore, this track focuses not only on security of medical devices and E-Health applications, but encompasses all aspects of system and device security, including but not limited to:

- Cyber Resilience, Biometrics and Biometric Security for E-Health Applications
- AI and Machine Learning for Health Data Security
- Security for Wearables and IoT-Devices
- Privacy, Risk Management and Regulatory Compliance in E-Health
- Ethical Considerations in E-Health Data Protection



Christoph Lipps, graduated in Electrical and Computer Engineering at the University of Kaiserslautern, where he meanwhile lectures as well. He is a Senior Researcher and Ph.D. candidate at the German Research Center for Artificial Intelligence (DFKI) in Kaiserslautern, Germany, heading the Cyber Resilience & Security Team of the Intelligent Networks Research Department. He is a member of the committee of the ICCWS and ECCWS, as well as a scientific committee member of various international conferences, and reviewer of several journals. His research focuses on Physical Layer Security (PhySec), Physically Unclonable Functions (PUFs) and Artificial Intelligence (AI).



Dipl.-Phys. **Jan Herbst** graduated with a Physics diploma from the Technical University of Kaiserslautern. He worked in the fields of laser physics, molecular beam epitaxy related to quantum dots, and photoluminescence spectroscopy. As a Researcher and Ph.D. candidate, he is working at the German Research Center for Artificial Intelligence (DFKI) in Kaiserslautern, Germany. His research includes Biometric Security, entity authentication, (Wireless) Body Area Networks, and Security Applications in Combination with Artificial Intelligence (AI).

Submission Details

In the first instance a 300-350 word abstract is required, to be received by the **4th September 2023**. Submissions must be made using the online submission form at <http://www.academic-conferences.org/conferences/iccws/iccws-abstract-submission/>

If you have any questions about this track please email: Christoph.Lipps@dfki.de Jan.Herbst@dfki.de

See more about ICCWS 2023 at <http://www.academic-conferences.org/conferences/iccws>