

## INAUGURAL LECTURE



### **Univ.-Prof. Dr. Stefan Rass**

Professorship Secure Systems

Stefan Rass graduated with a double Master's degree in Mathematics and Computer Science from the University of Klagenfurt (AAU) in 2005. He received a Ph.D. degree in Mathematics in 2009 and became Associate Professor for Security at the University of Klagenfurt in 2014. His research interests cover decision theory and game-theory, with applications in system security, robotics security, as well as complexity theory, statistics and information-theoretic security. He has won several awards and authored almost 200 papers to date. He is co-author of books on cryptography, as well as game-theoretic security and risk management, published by Artech House and Springer. He was chair of the 2015 Central European Conference on Cryptography, the 8<sup>th</sup> Conference on Decision and Game Theory for Security in 2017 and the 2020 ICRA Workshop on Security in Robotics. As of September 1, 2021, he is a full Professor at the LIT Secure and Correct Systems Lab.

Wednesday, April 27 2022, 16:00  
Festsaal, Uni-Center, 1<sup>st</sup> Floor

### **The Devil takes the Hindmost: Security as a Battle of Wits**

Security is an endless competition of creativity about finding new defenses and overcoming them. Cryptography as a well-established technology of protection is becoming increasingly endangered by the evolution of quantum computers. Starting with quantum cryptography, the talk will introduce my two main areas of research: applied cryptography and security economics. We will look into how cryptographic mechanisms lend themselves to measurable and unconditional protection, by casting privacy breaching attacks into mathematical games to obtain optimal and quantifiable security. The evolution of black markets in the dark net, endowing cyber criminals with cheap and ready-to-use technology for attacking, calls for an economic re-definition of security: security is not the absence of threats, but rather a state where an attack is more expensive than what can be gained from it. The presented research has its roots in this "definition" and results in new perspectives and possibilities to protect information as the basic commodity of the 21<sup>st</sup> century.