AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

TU WIEN

# INVITATION

## CYBERSECURITY LECTURE SERIES 2016

The Digital Safety & Security Department
of the AIT Austrian Institute of Technology and the TU Vienna
invites you to the Cybersecurity Lecture Series 2016

STEFAN RASS

Universität Klagenfurt, Austria

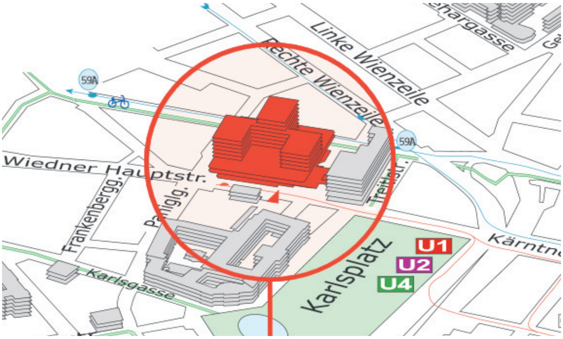
# » PRIVATE FUNCTION EVALUATION – ON THE GAP BETWEEN THEORY AND PRACTICE«

Private function evaluation is traditionally achieved in one of three ways: by fully homomorphic encryption, by garbled circuits or by multiparty computation. While all these have been studied for years and seen sophisticated implementations, their practical usefulness is so far still quite limited, either due to high computational complexity, high communication overhead, or similar. By exploring a fourth recent approach to secure function evaluation, we will demonstrate the crucial relevance of (logical) side-channel attacks for private function evaluation. Using a hypothetical (idealized) computing architecture that is assumed to process encrypted data (no matter how this is technically done), we will demonstrate how to break the underlying encryption (no matter how it looks like), using the computing platform only (thus needing no cryptanalysis).

Based on these findings, we argue for a broader view on security that explicitly accounts for the context and environment in which the processing happens. This gap is still widely open and will receive attention in the talk.  The presentation concludes by drawing the audience's attention to the wide range of security precautions beyond pure cryptography and access control, pointing out directions of security risk diversion by decision theory – a seemingly powerful yet widely unexplored route to security.

**Date** **24th February 4.30 pm**

**Venue** **Technische Universität Wien**
**Freihausgebäude, HS 5, Turm A (2nd Floor)**
Wiedner Hauptstr. 8, 1040 Vienna



**Prof Stefan Rass** Stefan Rass is currently an associate professor at the Universität Klagenfurt. He owns a double master degree in computer science and technical mathematics, and has a PhD in technical mathematics, with a dissertation related to game theory, security infrastructures and information-theoretic security. His research interests are security, applied cryptography, statistics, decision- and game-theory for security, and security infrastructures. He led many security-related projects, as well as being an active consultant and researcher in several EU projects.

**Organised by**

TU WIEN

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

**Registration** Please register by sending an E-mail to: cybersecurity-lectures@ait.ac.at
For addional information about the series please contact
Paul Smith (phone: +43 (0)664 883 90031)
Web: www.ait.ac.at/cybersecurity-lectures

AIT Austrian Institute of Technology GmbH
Donau-City-Straße 1 | 1220 Wien, Austria
T +43 (0) 50550-0 | F +43 (0) 50550-2201
office@ait.ac.at | www.ait.ac.at