JOHANNES KEPLER UNIVERSITY LINZ | JKU

Univ.-Prof. Dr. Alois FERSCHA
Fachbereich Informatik

Altenberger Straße 69
A-4040 Linz
Tel.: +43 (732) 2468 4762
Fax: +43 (732) 2468 4765

fercha@pervasive.jku.at
http://www.pervasive.jku.at

Dr. Matteo Maffei

Universität des Saarlandes

Computer-aided design of security and privacy preserving systems

The digital ecosystem is rapidly evolving towards a network of computing devices and open-ended services, in which independently developed nodes share information, access each other's functionalities via powerful APIs, rely on personal data to offer a personalized web experience, and all together provide an integrated and multimodal workflow. This concept, known as the Internet of Things and Services (ITS), has rapidly become part of our daily life.

The swift integration of web services and interconnection among devices, however, has initially pushed into the background a number of severe security and privacy issues, which traditional security mechanisms and cryptographic solutions rapidly proved to be inadequate to deal with.

In this talk, I will present a framework for the declarative design and automated synthesis of security and privacy preserving distributed systems. The core component of our framework is a logic-based, declarative API for data processing. This API is integrated in mainstream programming languages and allows system developers, even those lacking a background in cryptography, to conveniently specify privacy properties as well as a variety of seemingly conflicting security requirements, such as authorization policies, linkability, and accountability.

The cryptographic realization is hidden to the programmer and relies on a powerful combination of digital signatures, non-interactive zero-knowledge proofs of knowledge, pseudonyms, and reputation lists. We formally proved that the cryptographic realization enforces the security properties expressed in the declarative specification.

A central feature of our framework is that the resulting systems can be easily extended to offer new services (open-endedness) and independently developed systems can interoperate and share data with each other (interoperability), which is a crucial aspect in the ITS.

We successfully employed our framework to design an anonymous lecture evaluation system, a security API for social networks, anonymous webs of trust, and a privacy-preserving e-health system.

This work is part of a larger research agenda on formal methods and privacy-enhancing technologies for the ITS, which I will briefly overview in the final part of the talk.

Zeit: Mittwoch, 6. Februar 2013, 13:00 Uhr

Ort: Johannes Kepler Universität Linz
Mechatronik-Gebäude, SCP 1, MT 127

Kurzbiographie

Matteo Maffei is the head of the Language-based Security group at Saarland University. The Language-based Security group is affiliated to the Cluster of Excellence on Multimodal Computing and Interaction and is supported by the Emmy Noether fellowship of the German Research Foundation, which he was granted in 2009. Matteo Maffei joined Saarland University after having received the Ph.D. degree in Computer Science at the Ca'Foscari University of Venice in March 2006, under the supervision of prof. Riccardo Focardi. His research interests include privacy enhancing technologies (e.g., privacy in social networks, anonymous and censorship-resistant content sharing, privacy-preserving authorization systems, privacy-preserving online behavioral advertising, and electronic voting), applied cryptography (e.g., zero-knowledge proofs, anonymous credentials, oblivious RAM, and private information retrieval), semantics of programming languages (e.g., theory of concurrency, functional and object-oriented languages, type systems, and abstract interpretation), and language-based security (e.g., formal analysis of cryptographic protocols, static analysis of cryptographic code, and verification of mobile applications).