SAARLAND UNIVERSITY

ETAPS Daily

ETAPS 2011

The Newsletter of the European Joint Conferences on Theory and Practice of Software, ETAPS 2011

Thursday, March 31, 2011 Saarbrücken, Germany

Invited talk: Ross Anderson

Ross Anderson is Professor of Security Engineering at Cambridge University Computer Laboratory since 2003. He has been employed at Cambridge University since1992. From 1984 to 1991 he was self employed consultant working mostly in projects related to computer security. Between 1981 and 1983 he has worked on multilingual typesetting. From 1974 to 1975 he worked for Ferranti as a development engineer on avionics. Ross received his PhD from Cambridge University in 1995, a BA from Trinity College, Cambridge, in 1978.

The focus of his work in academia has been building security engineering into a discipline.

Over the last fifteen years his research ranged from hardware security to the uses of signal processing. He has written a reference book, 'Security Engineering – A Guide to Building Dependable Distributed Systems'. He has contributed to the design of a number of widely-deployed systems, from peer-to-peer systems through prepayment utility meters to the HomePlug standard for power-line communications. He chairs the Foundation for Information Policy Research, the UK's premier information thinktank. Ross is a Fellow of the Royal Society, the Royal Academy of Engineering, the Institution of Engineering and Technology, the Institute of Mathematics and its Applications, and the Institute of Physics.

The title of Ross' talk: The Dependability of Complex Socio-technical Systems

Abstract: The story of software engineering has been one of learning to cope with ever greater scale and complexity. We're now building systems with hundreds of millions of users, who belong to millions of firms and dozens of countries; the firms can be competitors and the countries might even be at war. Rather than having a central planner, we have to arrange things so that the desired behaviour emerges as a result of the self-interested action of many uncoordinated principals. Mechanism design and game theory are becoming as important to the system engineer as more conventional knowledge such as data structures and algorithms. This holds not just for systems no-one really controls, such as the Internet; it extends through systems controlled by small groups of firms, such as the future smart grid, to systems controlled by a single firm, such as Facebook. Once you have hundreds of millions of users, you have to set rules rather than micromanage outcomes. Other social sciences have a role to play too, especially the behavioural sciences; HCI testing has to be supplemented by a more principled understanding of psychology. And as software comes to pervade just about every aspect of society, software engineers cannot avoid engaging with policy. This has significant implications for academics: for how we educate our students, and for choosing research topics that are most likely to have some impact.

Ross Anderson

Today at 09:00

Invited talk: Michael Backes

Michael Backes

Michael Backes holds the chair of information security and cryptography at Saarland University, he is a fellow of the Max-Planck Institute for Software Systems (MPI-SWS), and he is the designated director of the IT-security center CISPA. Before joining Saarland University in 2006, he was a permanent research staff member at the IBM Zurich Research Lab. His research concentrates on theoretical foundations and applied aspects of information security and cryptography in a broad sense. Major research topics have been the design and verification of security protocols and implementations, linking formal methods and cryptography, privacy, and investigating novel side-channel attacks. For his work, he has been granted the Microsoft Award for Outstanding Research in Privacy Enhancing Technologies in 2003, the IBM Outstanding Achievement Awards for seminal contributions to privacy technologies in 2005, a Max Planck Fellowship in 2007, an IBM Faculty Award in 2008, as well as an ERC Starting grant and the TR35 award in 2009.

Today at 14:00

The title of Michael's talk: Automated Design and Verification of Security Protocols based on Zero-Knowledge Proofs

Abstract:

A central challenge in the analysis of large-scale security protocols is the expressiveness of the formalism used in the formal analysis and its capability to model complex cryptographic operations. While such protocols traditionally relied only on the basic cryp-

tographic operations such as encryption and digital signatures, modern cryptography has invented more sophisticated primitives with unique security features that go far beyond the traditional understanding of cryptography to solely offer secrecy and authenticity of a communication. Zero-knowledge proofs constitute the most prominent and arguably most amazing such primitive. A zero-knowledge proof consists of a message or a sequence of messages that combines two seemingly contradictory properties: First, it constitutes a proof of a statement that cannot be forged, i.e., it is impossible, or at least computationally infeasible, to prod-uce a zero-knowledge proof of a wrong statement. Second, a zero-knowledge proof does not reveal any information besides the bare validity of the statement. This primitive's unique security features, combined with the recent advent of efficient cryptographic implementations of zero-knowledge proofs for special classes of problems, have paved the way for its deploymentin modern applications, such as e-voting systems and anonymity protocols.In this talk, I will present a framework for the verification and design of security protocols based on zero-knowledge proofs. The framework comprises a symbolic representation of the cryptographic semantics of zero-knowledge proofs that is suitable to automated verification, a type system for the static enforcement of authorization policies, a corresponding cryptographic soundness result against arbitrary active attacks, and a general methodology for designing security protocols that are resistant to principal compromise.

Lunch options on Thursday

Menu A:
Meatball with a creamy sauce, side dish, seasonal salad, dessert

Menu B:
Green pasta with sauce of soya and tomatoes, grated cheese, seasonal salad, dessert

Free Flow:
- Potato wedges with a chili dip and garlic mayonaise
- Turkey breast with vegetables
- Rigatoni with sauce of prawns, vegetables and cream

What's in this building?

The Saarland University Department of Computer Science has celebrated its 40th anniversary in fall 2009. It emerged out of the Department of Applied Mathematics and owes its origin to Günter Hotz, one of the pioneers of computer science in Germany. Today 19 chairs cover a broad range of research fields and form the core of the computer science activities that have grown on the university premises during the last two decades. In October 2007, Saarbrücken Computer Science was awarded two major grants in the framework of the Initiative for Excellence of the German government: the Cluster of Excellence on "Multimodal Computing and Interaction" (already introduced to you in the ETAPS Daily on Monday) and the "Saarbrücken Graduate School of Computer Science". Saarbrücken is the only German site with Excellence funding for both a Cluster of Excellence and a Graduate School in computer science.
Currently more than 320 PhD students are enrolled in the Saarbrücken Graduate School of Computer Science. They profit from the optimal environment for pursuing their doctoral studies in computer science at an internationally competitive level. Student obtain research-oriented training and experience a stimulating and scientifically challenging atmosphere. Advised by internationally renowned scientists, they participate in one of the many research groups and find their way into first-class research.

The Saarbrücken Graduate School of Computer Science

Theory of Security and Applications

TOSCA (Theory of Security and Applications) is the 2011 edition of an annual series of events formerly known as ARSPA-WITS, which itself combined a workshop on issues in the theory of security and one on using automated reasoning for security protocols. Information security has in recent years been an important consumer of theoretical computer science. System designers need clean models to predict behavior in different environments, and to appraise the effects of broad types of adversary actions. Consequently, security has motivated new work in many areas of theory, including type systems and program analysis; on process algebras and models of distributed systems; on information flow, both qualitative and quantitative; and on connections between logical models and computational (often cryptographic) models.

We hope that TOSCA 2011 will help to set the stage for an annual ETAPS event on security. The aim is, on the one hand, to bring information security researchers in closer contact with the ETAPS community, and to give ETAPS attendees an opportunity to respond to core problems of security. On the other hand, we hope to contribute to bridging the gap between logical foundations and security methods. Besides the regular presentations of the accepted papers, the program of TOSCA 2011 features invited talks by Michael Backes (ETAPS plenary speaker), on analysis and design of protocols using zero-knowledge proofs; Veronique Cortier, on secure protocol composition; Ueli Maurer, on new methods for defining and proving cryptographic properties; Sjouke Mauw, on extracting security information from audits and other large repositories of data; and David Sands, on programming with expressive information flow policies.

TOSCA runs on Thursday afternoon and Friday. It is held in E1.4/024. It is open to all participants of ETAPS.

What ETAPS can do to your Faculty

Organising ETAPS is an easy task. We guarantee. Here is the main reason why you should put in a bid for 201X.

The restrooms in one of the CS buildings (E1.1) had been in a mediocre state for long, to say it mildly. The urgently needed state changes were blocked by lacking financial resources for several years. ETAPS 2011 was the key reason for raising the priority level of this renovation. Indeed the renovation finished only last Friday evening. Feel free to visit the result.
If you proceed along the corridor a little further, you can also enjoy a fabulous indoor shower that the renovation activities brought to us for free!