The First Workshop on Language Support for Privacy-Enhancing Technologies (PETShop'13)

Martin Franz
Deutsche Bank

Andreas Holzer
Vienna University of Technology

Rupak Majumdar
MPI SWS Kaiserslautern

Bryan Parno
Microsoft Research

Helmut Veith
Vienna University of Technology

ABSTRACT

The Workshop on Language Support for Privacy-Enhancing Technologies (PETShop'13) aims at bringing together researchers from the areas of security, programming languages, compiler construction, and program verification to exchange ideas and research results to improve the practicality of state of the art cryptographic privacy-enhancing technologies.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*security and protection*

General Terms

Security, Languages

Keywords

Secure Multi-Party Computations; Zero-Knowledge Protocols; Programming Languages; Compiler Construction; Verification

1. BACKGROUND & MOTIVATION

Privacy enhancing technologies (PETs) are necessary when untrusted platforms compute on sensitive data, for example in a distributed setting or in cloud computing. Cryptography offers a rich set of privacy-enhancing technologies for such privacy-preserving computations, including secure multi-party computation (SMC) and zero-knowledge (ZK) protocols. These systems enable distrusting parties to collectively compute over their private inputs without revealing their data to the other parties. With the wide availability of distributed systems, social media, and cloud computing, there is a pressing need to make these technologies usable in practice. A key step towards practicality is the ability to compile from high-level languages, like C, into cryptographic protocols. Such cryptographic compilers have only recently begun to emerge, and they stand to benefit from decades of research in programming languages, compiler construction, and program verification. We believe that the concepts, methodologies, and tools developed in these areas of research can help to make cryptographic PETs practically available.

CCS'13, November 4–8, 2013, Berlin, Germany.
ACM 978-1-4503-2477-9/13/11.
http://dx.doi.org/10.1145/2508859.2509032.

2. GOALS & OBJECTIVES

PETShop is located at the crossroads of security, programming languages, compiler construction, and program verification and aims to bring together researchers from these different communities to exchange ideas and research results to improve the practicality of state of the art cryptographic PETs. In recent years, Europe has become a major center for research on verification and programming languages (e.g., as reflected by strong formal methods groups in Oxford, Cambridge, Munich, Kaiserslautern, Vienna, to name only a few), and we want to use the opportunity of having ACM CCS'13 in Berlin to bring together these researchers with the ACM CCS community.

3. TOPICS OF INTEREST

Topics of interest include (but are not limited to):

- Compiler optimizations for privacy-preserving computations, e.g., SMC or ZK protocols
- Programming language support for privacy-preserving computations
- Execution environments for privacy-preserving computations
- Experience reports, use cases, and implementations of privacy-preserving computations
- Tool demonstrations

4. FORMAT

The workshop features two invited talks, six short papers, and one invited paper covering several of the above mentioned topics. To emphasize the workshop character and the focus on the discussion of open challenges, the workshop

focuses on short work-in-progress/position papers/extended abstracts which describe applications, problems, and new ideas in the field of multi-party computation. Especially we want to encourage authors of such submissions to later publish extended versions of their submissions at other venues.

5. WORKSHOP ORGANIZERS

- **Martin Franz** holds Diploma degrees in Mathematics and Computer Science and received a Ph.D. degree from Technische Universität Darmstadt. His dissertation investigates different techniques for secure computations on non-integer values and shows how to use these techniques in real world scenarios. During a research visit at Philips Research in Eindhoven, Netherlands, he contributed to the European Research Project SPEED (Signal Processing in the Encrypted Domain). After that he worked at CASED, the Center for Advanced Security Research Darmstadt. Martin Franz is currently working as an expert for applied cryptography and IT-Security at Deutsche Bank.

- **Andreas Holzer** is a research assistant at the Faculty of Informatics of Vienna University of Technology (TU Vienna). He has a diploma in Computer Science from the University of Applied Sciences Landshut and a M.Sc. from TU Munich and received a Ph.D. degree from University of Technology Vienna. His current work is focusing on software testing and computer security.

- **Rupak Majumdar** received the B.Tech. degree in Computer Science from the Indian Institute of Technology at Kanpur in 1998 and the Ph.D. degree in Computer Science from the University of California at Berkeley in 2003. He is currently a Scientific Director at the Max Planck Institute for Software Systems. Previously, he was a professor in the Department of Computer Science at the University of California, Los Angeles. His research interests are in the verification and control of reactive, real-time, hybrid, and probabilistic systems, software verification and programming languages, game theoretic problems in verification, logic, and automata theory. Dr. Majumdar received the President's Gold Medal from IIT, Kanpur, the Leon O. Chua award from UC Berkeley, an NSF CAREER award, a Sloan Foundation Fellowship, a PLDI "Test of time" award, and several best paper awards. Rupak Majumdar served as program co-chair at GDV 2005, SPIN 2008, SCC 2009, TACAS 2010. He served as program committee member of CAV 2005, CAV 2008, TACAS 2009, TACAS 2011, CAV 2012, VMCAI 2012, CAV 2013, ICALP 2013, VMCAI 2013 etc.

- **Bryan Parno** works in the Security and Privacy Research Group at Microsoft Research. He completed his PhD at Carnegie Mellon University under the supervision of Adrian Perrig. Dr. Parno's dissertation, which won the 2010 ACM Doctoral Dissertation Award, studies the design, implementation, and evaluation of a combination of hardware, software, and cryptographic primitives for extending the trust one has in one service or device in order to allow one to trust other services and devices. His current work focuses on protocols for verifiable computation and zero-knowledge proofs, building practical, formally verified secure systems, and developing next-generation application models. He published a book on *Bootstrapping Trust in Modern Computers*, and he served on the program committee for Oakland 2013, TRUST 2012 & 2013, NDSS 2011,2012, & 2013, CCS 2012, CCSW 2012, MobiHoc 2012, CANS 2011, PKC 2011, MobiSys 2010, FC 2009, etc.

- **Helmut Veith** is a professor at the Faculty of Informatics of Vienna University of Technology (TU Vienna), and an adjunct professor at Carnegie Mellon University. He has a diploma in Computational Logic and a PhD sub auspiciis praesidentis in Computer Science, both from Vienna University of Technology. Prior to his appointment to Vienna, he was holding professor positions at TU Darmstadt and TU Munich. His current work is focusing on model checking, software verification and testing, embedded software and computer security. Helmut Veith is program committee co-chair of CAV 2013, CSL 2009, LPAR 2008, and tutorial chair of FMCAD 2010. He served as program committee member of ATVA 2010, CAV 2003, CAV 2005, CAV 2009, CAV 2010, CAV 2012, CSL 2009, CSL 2011, CSL 2012, CSR 2007-2009, DATE 2011, DATE 2012, EC2 2009-2012, FMCAD 2009, FMCAD 2010, FMCAD 2011, FMICS 2011, FSTTCS 2007, HVC 2010, HVC 2011, ICTAC 2009, ICTAC 2010, ICTERI 2011, ICTERI 2012, LICS 2004, SOFSEM 2012, SPIN 2012, SYNASC 2008-2011, TACAS SW Verification Competition 2012, TASE 2011, VMCAI 2012, WING 2009, WING 2010, WOLLIC 2011 etc.

6. ACKNOWLEDGMENTS

This workshop was partially supported by the Austrian National Research Network S11403 and S11405 (RiSE) of the Austrian Science Fund (FWF) and by the Vienna Science and Technology Fund (WWTF) through grant PROSEED.