Lecture Notes in Computer Science 10323

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7410

Michael Brenner · Kurt Rohloff
Joseph Bonneau · Andrew Miller
Peter Y.A. Ryan · Vanessa Teague
Andrea Bracciali · Massimiliano Sala
Federico Pintore · Markus Jakobsson (Eds.)

Financial Cryptography and Data Security

FC 2017 International Workshops
WAHC, BITCOIN, VOTING, WTSC, and TA
Sliema, Malta, April 7, 2017
Revised Selected Papers

Springer

Editors
Michael Brenner
Leibniz Universität Hannover
Hannover
Germany

Kurt Rohloff
New Jersey Institute of Technology
Newark, NJ
USA

Joseph Bonneau
New York University
New York, NY
USA

Andrew Miller
University of Illinois at Urbana-Champaign
Urbana, IL
USA

Peter Y.A. Ryan
University of Luxembourg
Luxembourg
Luxembourg

Vanessa Teague
University of Melbourne
Parkville, VIC
Australia

Andrea Bracciali
University of Stirling
Stirling
UK

Massimiliano Sala
University of Trento
Trento
Italy

Federico Pintore
University of Trento
Trento
Italy

Markus Jakobsson
Agari Inc.
San Mateo, CA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-70277-3 ISBN 978-3-319-70278-0 (eBook)
https://doi.org/10.1007/978-3-319-70278-0

Library of Congress Control Number: 2017959723

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

WAHC 2017: 5th Workshop on Encrypted Computing and Applied Homomorphic Cryptography

The hype over the cloud and recent disclosures show there is demand for secure and practical computing technologies. The WAHC workshop addresses the challenge in safely outsourcing data processing onto remote computing resources by protecting programs and data even during processing. This allows users to outsource computation over confidential information independently from the trustworthiness or the security level of the remote delegate. The workshop serviced these research needs by collecting and bringing together some of the top researchers and practitioners from academia, government, and industry to present, discuss, and share the latest progress in the field relevant to real-world problems with practical approaches and solutions. The workshop was uniformly attended by academia, government, and industry, with participants from previous years with experience in the domain and new attendees contributing and learning from the community for the first time. Specific encrypted computing technologies focused on homomorphic encryption and secure multiparty computation. The technologies and techniques discussed in this workshop are key to extending quality of implementation and the range of applications that can be securely and practically outsourced. Presentations and discussion at the workshop were of the high quality and deep insights we have come to expect from our community. Topics of conversation included insights and lessons learned from experience implementing encrypted computing schemes and experience reports on applying these technologies. Special thanks to the invited speakers: Kim Laine from Microsoft Research and Yuriy Polyakov from the New Jersey Institute of Technology, who shared their experiences implementing open-source homomorphic encryption libraries. The workshop received 19 submissions. All contained unique and interesting results. Each was reviewed by at least three Program Committee members. While all the papers were of high quality, only seven papers were accepted to the workshop. We thank the authors for all submissions, the members of the Program Committee for their effort, the workshop participants for attending, and the FC organizers for supporting us.

April 2017

Michael Brenner
Kurt Rohloff

WAHC 2017 Program Committee

Dan Bogdanov	Cybernetica, Estonia
Zvika Brakerski	Weizmann Institute, Israel
David Cash	Rutgers, USA
Hao Chen	Microsoft Research, USA
Rosario Gennaro	CUNY, USA
Seung Geol Choi	US Naval Academy, USA
David Cousins	BBN, USA
Marten van Dijk	UConn, USA
Dario Fiore	IMDEA, Spain
Sergey Gorbunov	University of Waterloo, USA
Debayan Gupta	MIT, USA
Vlad Kolesnikov	Bell Labs, USA
Kim Laine	Microsoft Research, USA
Tencrède Lepoint	SRI International, USA
Pascal Paillier	CryptoExperts, France
Benny Pinkas	Bar-Ilan University, Israel
Erkay Savas	Sabancı University, Turkey
Berk Sunar	WPI, USA
Mehdi Tibouchi	NTT, Japan
Fre Vercauteren	KU Leuven, Belgium
Adrian Waller	Thales, UK

BITCOIN 2017: 4th Workshop on Bitcoin and Blockchain Research

The past year leading up to the 4th Bitcoin and Blockchain Workshop in 2017 has seen a continued booming trend: increased adoption and development in cryptocurrencies like Bitcoin, Ethereum, Zcash, and many more, as well as investment in blockchain - related technologies from industry broadly. Cryptocurrency and blockchain technology are emerging as a significant and productive research topic in computer security.

Much like the price of Bitcoin and the market capitalization of the cryptocurrency ecosystem, our workshop has also grown year by year. This year we received a record number of submissions (38), and after our peer-review process we accepted a record number of papers (14), and yet increased in selectivity (37% acceptance rate). We were very happy to convene an outstanding Program Committee (listed here) comprising not just leading academics, but also top PhD students and prominent developers.

From our strong technical program emerged several themes of focus, including privacy analysis and privacy-preserving enhancements; smart contract scripting functionality and applications in both Bitcoin and Ethereum; game theoretic analysis of consensus protocols; and scalability improvements for cryptocurrency transactions. We note also that our host conference accepted five papers on blockchain technology to its main track, and also featured a keynote talk on a new cryptocurrency protocol from Turing Award winner Silvio Micali. A new workshop dedicated to smart contract security hosted in parallel also featured 11 talks and a keynote from Vitalik Buterin.

We would like to thank our Program Committee for the hard work they put into producing high-quality and useful reviews, and the authors and speakers for contributing to our program. We especially thank Nicolas Christin for once again hosting the conference management server, and the organizers and sponsors of Financial Cryptography for guiding us through a successful event.

April 2017

Andrew Miller
Joseph Bonneau

BITCOIN 2017 Program Committee

Elli Androulaki	IBM Zürich, Switzerland
Foteini Baldimtsi	George Mason University, USA
Iddo Bentov	Cornell University, USA
Rainer Böhme	University of Innsbruck, Austria
Melissa Chase	Microsoft Research, USA
Nicolas Christin	Carnegie Mellon University, USA
Jeremy Clark	Concordia University, Canada
George Danezis	University College London, UK
Christian Decker	Blockstream, USA
Tadge Dryja	MIT Digital Currency Initiative
Ittay Eyal	Cornell University, USA
Bryan Ford	EPFL, Switzerland
Juan Garay	Yahoo! Research, USA
Christina Garman	Johns Hopkins University, USA
Arthur Gervais	ETH Zürich, Switzerland
Garrick Hilemen	University of Cambridge, UK
Ethan Heilman	Boston University, USA
Ari Juels	Cornell Tech, USA
Stefan Dziembowski	University of Warsaw, Poland
Aniket Kate	Purdue University, USA
Ian Miers	Johns Hopkins University, USA
Patrick McCorry	Newcastle University, UK
Malte Möser	Princeton University, USA
Andrew Poelstra	Blockstream, USA
Christian Reitwießner	Ethereum Foundation, Switzerland
Yonatan Sompolinsky	Hebrew University, Israel
Eran Tromer	Tel Aviv University, Israel
Peter Van Valkenburgh	Coin Center, USA
Luke Valenta	University of Pennsylvania, USA
Nathan Wilcox	Zcash, USA
Pieter Wuille	Blockstream, USA

VOTING 2017: Second Workshop on Advances in Secure Electronic Voting Schemes

Voting 2017 was the second of what looks like turning into an ongoing series of workshops on verifiable voting systems associated with Financial Crypto.

Voting 2017 occurred at a time of hightened global interest in election security. Attacks, attributed to Russia, deliberately interfered with the politics of the US presidential election. Much remains murky about what exactly occurred, but it is clear that hackers breached the Democratic campaign system and selectively leaked material. It is also clear that various registration systems were hacked, although the resulting damage is unclear.

In the wake of this, many European countries discontinued Internet voting or electronic counting plans over fears that their elections would also be targeted.

In France we witnessed similar attempts to meddle with the democratic process, although in this case the Kremlin's favored candidate did not carry the day. Interestingly in this case it appears that the Macron team were forewarned and detected the attempted meddling, and indeed staged some counter-meddling of their own: injecting fake items for the hackers to uncover.

The most interesting statement about US election security came from Former CIA Acting Director Michael Morell, who said of Russian interference: "They tried, and they were not successful, but they still tried, to get access to voting machines and vote counting software, to play with the results."

This raises the obvious question, "How does he know they were not successful?"

This is what Voting 2017 was about: the quest to design election systems that produce evidence of an accurate election result, or a clear indication of a problem.

We began with an inspiring keynote by Prof. Philip Stark from The University of California at Berkeley, who explained that the absence of meaningful post-election audits implies that we will never know who truly deserved to be elected US president in 2016. Efforts to perform recounts in Pennsylvania, Michigan, and Wisconsin were thwarted by either technical obstacles, e.g., absence of a paper audit trail, or legal, e.g., judges using absurd "Catch 22" style arguments that to justify a recount required evidence of fraud. He explained how routine post-election risk-limiting audits would allow us to be confident, every election, that the result was correct.

In "BatchVote: Voting Rules Designed for Auditability," Perumal, Rivest, and Stark investigated voting schemes that were designed for efficient auditability. First-past-the-post elections (the most common style in the USA) are very easy to audit, but can suffer from the spoiler effect and other distortions. Other, more expressive, voting systems such as IRV and STV are very difficult to audit, or even to find the winning margin for. This paper considers both democratic qualities and ease of auditing to design voting systems that meet both criteria.

In "Existential Assertions for Voting Protocols," by Ramanujam, Sundararajan, and Suresh, a new type of formal verification of e-voting protocols is introduced. The

term-based model of e-voting protocols is replaced with assertions, e.g., signatures or zero-knowledge proofs are replaced with assertions idealizing their desired behavior. This firstly makes the model quite intuitive to read, but more importantly allows us to model how the adversary can logically infer based on the assertions he has seen, and capture if this gives new attacks. The main novelty from the authors is an existential quantifier that allows the authors to give an equivalence-based notion of privacy in e-voting protocols and check privacy for FOO and Helios 2.0.

In "A Roadmap to Fully Homomorphic Elections," Gjøsteen and Strand describe how to use fully homomorphic encryption to provide universal verifiability while protecting privacy for Norway's complex ballots. Norway's current system requires the verification process to be restricted to a few auditors due to privacy concerns. The main challenge is that a Norwegian ballot has so many possible values that a voter may choose to identify herself by choosing a unique vote. If individual votes are exposed, this can result in bribery or coercion. Fully homomorphic encryption would allow for universal verification, although at present it is not fast enough to run on real elections.

The next paper considers the voter's end of verifiable Internet voting. In "Using Selene to Verify Your Vote in JCJ," Rial, Iovino, Roenne, and Ryan describe how the transparent voter verification techniques of the Selene scheme can be combined with the rather strong coercion resistance mechanisms of JCJ (Juels, Catalano, and Jakobsson).

In "Enabling Vote Delegation for Boardroom Voting," Kulyk, Neumann, Marky, and Volkamer consider the privacy and verifiability of vote delegation, in which a voter may choose to nominate someone else to determine his vote. In their setting there are a relatively small number of voters, who all participate actively in the protocol.
We had a valuable tutorial on complex proofs for mixnet verification. Haenni, Locher, Koenig, and Dubuis wrote "Pseudocode Algorithms for Verifiable Re-encryption Mixnets" to explain to a general audience how these sophisticated proofs work and facilitate implementations.

Finally, Yang and Clark described a new protocol for "Practical Governmental Voting with Unconditional Integrity and Privacy." This scheme (probably inevitably) has to sacrifice universal verifiability, but it represents an interesting part of the solution space that deserves exploration, and may be appropriate for some elections.

The threat of electoral fraud is not new, and is not going away. Introducing computers expands the opportunity, possibly allowing for very large scale fraud from all over the world. We hope this volume has contributed to a global effort to ensure that our voting systems are robust, privacy-preserving, and not trusted until they provide meaningful evidence of having produced an accurate election result.

We would like to thank the Program Committee for their hard work and careful reviews of the papers.

April 2017

Peter Y.A. Ryan
Vanessa Teague

VOTING 2017 Program Committee

Roberto Araujo	Universidade Federal do Pará (UFPA), Brazil
Jeremy Clark	Concordia University, Canada
Chris Culnane	University of Melbourne, Australia
Jeremy Epstein	SRI International, USA
Aleksander Essex	Western University, Canada
David Galindo	University of Birmingham, UK
Kristian Gjøsteen	Norwegian University of Science and Technology, Norway
Rajeev Gore	The Australian National University, Australia
Jens Groth	University College London, UK
Rolf Haenni	Bern University of Applied Sciences, Switzerland
Reto Koenig	Berne University of Applied Sciences, Switzerland
Steve Kremer	Inria Nancy - Grand Est, France
Olivier Pereira	Universite catholique de Louvain, Belgium
Ron Rivest	MIT, USA
Peter Roenne	SnT, University of Luxembourg, Luxembourg
Alon Rosen	IDC Herzliya, Israel
Mark Ryan	University of Birmingham, UK
Steve Schneider	University of Surrey, UK
Berry Schoenmakers	Eindhoven University of Technology, The Netherlands
Carsten Schuermann	IT University of Copenhagen, Denmark
Philip Stark	University of California, Berkeley, USA
Melanie Volkamer	Karlstad University, Sweden
Poorvi Vora	The George Washington University, USA

WTSC 2017: First Workshop on Trusted Smart Contracts

These proceedings collect the papers and posters accepted at the First Workshop on Trusted Smart Contracts (WTSC 2017) associated to the Financial Cryptography and Data Security 2017 (FC 2017) conference held in Malta in April 2017.

WTSC 2017 focused on smart contracts, i.e., self-enforcing agreements in the form of executable programs and other decentralized applications that are deployed to and run on top of blockchains. These technologies introduce a novel programming framework and execution environment, which, together with the supporting blockchain technologies, carry unanswered and challenging research questions. Multidisciplinary and multifactorial aspects affect correctness, safety, privacy, authentication, efficiency, sustainability, resilience, and trust in smart contracts and decentralized applications.

WTSC 2017 aimed to address the scientific foundations of Trusted Smart Contract engineering, i.e., the development of contracts that enjoy some verifiable "correctness" properties, and to discuss open problems, proposed solutions, and the vision on future developments among a research community that is growing around these themes and brings together users, practitioners, industry, institutions, and academia. This was reflected in the Program Committee of this first edition of WTSC, comprising members from companies, universities, and research institutions from 11 countries worldwide, who kindly accepted to support the event. The association with FC 2017 provided an ideal context for our workshop to be run in. WTSC 2017 was partially supported by the University of Stirling, UK, the University of Trento, Italy, and FC 2017 IFCA-ICRA. This first edition of WTSC 2017 received 19 submissions by about 50 authors, of which nine were accepted after peer review as full papers and three as posters, and have been collected in the present volume. These analyzed the current state of the art, addressed aspects of privacy, models for contract composition and concurrency, incentives and penalties, taxonomies of smart contract applications, legal implications of smart contracts, theorem-proving-based verification for smart contracts, decentralized markets, and smart-contract-based consensus protocols.

WTSC 2017 also enjoyed Vitalik Buterin (Ethereum Foundation) as keynote speaker. Vitalik, a prominent contributor to the world of smart contracts, gave a talk on the challenging topic of the cryptoeconomics of smart contracts.

April 2017

Andrea Bracciali
Federico Pintore
Massimiliano Sala

WTSC 2017 Program Committee

Massimo Bartoletti	University of Cagliari, Italy
Andrea Bracciali	University of Stirling, UK (Chair)
Eimear Byrne	University College Dublin, Ireland
Martin Chapman	King's College London, UK
Tiziana Cimoli	University of Cagliari, Italy
Nicola Dimitri	University of Siena, Italy
Stuart Fraser	Wallet.Services, UK
Laetitia Gauvin	ISI Foundation, Italy
Davide Grossi	University of Liverpool, UK
Iain Henderson	Jlink Lab, UK
Yoichi Hirai	Ethereum DEV, Germany
Camilla Hollanti	Aalto University, Finland
Ioannis Kounelis	Joint Research Centre, European Commission
Loi Luu	National University of Singapore
Michele Marchesi	University of Cagliari, Italy
Peter McBurney	King's College London, UK
Neil Mclaren	Avaloq Innovation Ltd, UK
Philippe Meyer	Avaloq Innovation Ltd, UK
Mihail Mihaylov	Vrije Universiteit Brussel, Belgium
Sead Muftic	KTH Royal Institute of Technology, Sweden
Igor Nai Fovino	Joint Research Centre, European Commission
Daniela Paolotti	ISI Foundation, Italy
Federico Pintore	University of Trento, Italy
Massimiliano Sala	University of Trento, Italy (Chair)
Ilya Sergey	University College London, UK
Jason Teutsch	University of Chicago, USA
Roberto Tonelli	University of Cagliari, Italy
Yaron Velner	Hebrew University, Israel
Luca Vigano	King's College London, UK

TA 2017: First Workshop on Targeted Attacks

A targeted attack is one in which contextual information about the intended victim is used to configure the attack; for example, a spear phishing attack is targeted, while a typical spam blast is not. Targeting is performed in order to maximize yield and minimize detection. Being able to assess the yield of attacks enables efforts to predict the likely growth of these attacks, as soaring profits fuel more attacks. Similarly, it is important to understand how targeted attacks avoid detection in order to improve detection methods.

It is commonly believed that targeted attacks are enabled by data from account compromises, breaches, and public resources, but the risk associated with various types of data is poorly understood. It is also important to better understand new methods or communication media used for targeted attacks, and how attackers tailor targeted attacks to the media and to their goals whether this is to distribute malware, obtain data, or coerce a user to perform an action.

Targeted Attacks 2017 was the first workshop addressing this threat. Its success rested both on the insightful submissions we received and the excellent Program Committee that guided the selection.

April 2017 Markus Jakobsson

TA 2017 Program Committee

David Maimon	UMD
Damon McCoy	NYU
Angela Sasse	UCL
Hossein Siadati	NYU
Elaine Shi	Cornell
Gianluca Stringhini	UCL
Gary Warner	PhishMe
Moti Yung	Snap

Blockchain and Smart Contract Mechanism Design Challenges (WTSC17 Keynote Talk)

Vitalik Buterin
Ethereum Foundation

Abstract. Arguably, the true genius behind the success of Bitcoin, Ethereum and similar systems was not the specific design of their blockchain, or their use of algorithms that resemble forms of distributed consensus in order to maintain security; rather, it is the innovation of *cryptoeconomics* - the art of combining cryptographic techniques and economic incentives defined and administered inside a protocol in order to encourage users to (correctly) participate in certain roles in the protocol, and thereby preserve and maintain certain desired properties of the protocol. I describe the key ideas in the abstract, then apply them to Bitcoin proof of work, the Schellingcoin oracle, Casper, as well as describing several key open problems in blockchain-based system design.

Contents

Trusted Smart Contracts

Targeted Attacks

Poster Papers