Lecture Notes in Computer Science 10311

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

Raphael C.-W. Phan · Moti Yung (Eds.)

Paradigms in Cryptology – Mycrypt 2016

Malicious and Exploratory Cryptology

Second International Conference, Mycrypt 2016
Kuala Lumpur, Malaysia, December 1–2, 2016
Revised Selected Papers

Springer

Editors

Raphael C.-W. Phan
Multimedia University, MMU
Cyberjaya
Malaysia

Moti Yung
Snap and Columbia University
New York, NY
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-61272-0 ISBN 978-3-319-61273-7 (eBook)
DOI 10.1007/978-3-319-61273-7

Library of Congress Control Number: 2017944355

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

The first and only Mycrypt up to 2015 was Mycrypt 2005, wherein an unconventional cryptography session featured papers with ideas that were beyond the norm. Since Mycrypt 2005, substantial breakthroughs have been made in crypto and security in the past decade, including notions pertaining to malicious security, i.e., where security is no longer simply against bad guys but where good guys who are conventionally viewed as mostly defensive can equally be adversarial. These align well with recent trends wherein trusted parties need not necessarily be trustworthy, and where insiders can potentially be malicious.

Mycrypt 2016 was a rejuvenation of the Mycrypt series with a particular focus on paradigm-shifting crypto research and thinking outside the current box. Jointly organized by the Multimedia University and Cyber Security Malaysia in cooperation with the International Association for Cryptologic Research (IACR), it was held in Kuala Lumpur, Malaysia, during December 1–2, 2016, at the Pullman Kuala Lumpur City Centre Hotel, just before Asiacrypt 2016 took place in Hanoi.

The technical Program Committee (PC) comprised 41 experts from 19 countries with an additional 51 external reviewers. We adopted a hybrid journal-like style where there were two separate and independent calls each with its own review process. Each submission was put through two stages, where after stage one some papers without major issues were accepted or those without scientific merit rejected, while others were put through to stage two for a further review after obtaining rebuttals from authors. Every worthwhile submission was reviewed by at least two reviewers, and up to six reviewers for some submissions requiring substantial deliberations. The server handling the submissions, reviews, and discussions was hosted by Microsoft via its Conference Management Toolkit (CMT). We thank all the PC members and external reviewers for their passion and commitment to see this through. Note that in defying convention, we have listed the PC and external reviewers in alphabetical order based on first name first! This is not a new paradigm, but is somewhat unusual in the West.

A total of 51 complete submissions were processed through the review phases after filtering checks, from which 21 papers were finally accepted for inclusion in the technical program, with authors spanning 14 countries. Of these submissions, three paradigm-revisiting papers that garnered a significant number of positive comments and interest from PC members and external reviewers are listed in these proceedings under the “Revisiting Tradition” category. Papers under “Different Paradigms” touch on alternative or new perspectives on doing cryptography, while the “Cryptofication” papers aim to bridge the gap between the physical world and the cryptographic world. “Malicious Crypto” papers deal with the issues of backdoors, malware, and leakages, while papers under “Advances in Cryptanalysis” aim to revisit existing cryptanalytic techniques toward new formulations or measures. The “Primitives and Features” papers are those that propose new variants of cryptographic primitives or new features. Finally, the “Cryptanalysis Correspondence” section presents two concise papers that had the unique feature of being able to obtain rebuttals from the authors of the attacked schemes as part of an extended review process.

After much deliberation and considering the points made by PC members and external reviewers, the paper "Another Look at Tightness II: Practical Issues in Cryptography" by Sanjit Chatterjee, Neal Koblitz, Alfred Menezes and Palash Sarkar was awarded Best Paper.

Mycrypt 2016 had the pleasure of two keynote talks, namely, Xavier Boyen of QUT speaking on human primacy in crypto and Neal Koblitz of the University of Washington discussing paradigm shifts in our disciplinary culture. There was also an IEICE invited talk sponsored by the IEICE Malaysia Section, by Goichiro Hanaoka on user-friendly crypto.

As an additional twist to an otherwise conventionally structured program, several Insight Papers were solicited for presentation at Mycrypt 2016 and/or inclusion in the proceedings. Insight Papers were invited from researchers on their celebrated or recent breakthrough results: these were notably on multi-prover interactive proofs, human encryption, algebraic cryptanalysis, watermarking programs, polytopic cryptanalysis, and the division property. Authors of such papers had the option of presenting at Mycrypt 2016 physically or pre-recording a video clip to be shown during Mycrypt 2016 to the audience.

We thank the general chairs, Wei-Chuen Yau and Geong-Sen Poh, as well as the local secretariat led by Cyber Security Malaysia for supporting the venue logistics and outreach. We are also grateful to Tourism Malaysia for sponsoring the cultural dance performance during the banquet dinner.

Starting with Mycrypt 2016, the Mycrypt series will continue to focus on beyond-norm, paradigm-shifting, unconventional cryptography as we firmly believe that a field can only advance if its research community revisits conventional paradigms, rocks the crypto boat, questions the status quo, and raises controversial issues. Mycrypt will thus henceforth be known as the International Conference on ***M***alicious and Explorator***y*** ***Crypt***ology, and be co-located with major crypto/security conferences to maximize the impact of its frontier-stretching theme.

April 2017

Raphaël C.-W. Phan
Moti Yung

Organization

Program Chairs

Raphaël C.-W. Phan	MMU, Malaysia
Moti Yung	Snap and Columbia University, USA

General Chairs

Wei-Chuen Yau	Xiamen University, Malaysia
Geong-Sen Poh	MIMOS, Malaysia

Program Committee

Adam Young	Cryptovirology Labs, USA
Aggelos Kiayas	National and Kapodistrian University of Athens, Greece
Ahmad-Reza Sadeghi	Technische Universität (TU) Darmstadt, Germany
Alfred Menezes	University of Waterloo, Canada
Andrew Odlyzko	University of Minnesota, USA
Angela Sasse	University College London (UCL), UK
Arjen Lenstra	EPFL, Switzerland
Bart Preneel	University of Leuven (KU Leuven), Belgium
Catherine Meadows	Naval Research Lab, USA
Chris Mitchell	Royal Holloway, University of London (RHUL), UK
David Naccache	Université Paris II, France
Ed Dawson	Queensland University of Technology (QUT), Australia
Elisa Bertino	Purdue University, USA
Graham Steel	Inria, France
Gregory Neven	IBM Research–Zurich, Switzerland
Helena Handschuh	Cryptography Research Inc., USA
Ivan Visconti	Università degli Studi di Salerno, Italy
Jean-Philippe Aumasson	Kudelski Security, Switzerland
Jonathan Katz	University of Maryland, USA
Josef Pieprzyk	QUT, Australia
Kaoru Kurosawa	Ibaraki University, Japan
Kristian Gjøsteen	NTNU, Norway
Lars Knudsen	Danmarks Tekniske Universitet (DTU), Denmark
Marine Minier	LORIA, France
Markus Dürmuth	Ruhr-Universität Bochum (RUB), Germany
Markus Jakobsson	Agari and ZapFraud, USA
Moti Yung (Chair)	Snap and Columbia University, USA

Nasir Memon	New York University, USA
Neal Koblitz	University of Washington, USA
Orr Dunkelman	University of Haifa, Israel
Peter Y.A. Ryan	Université du Luxembourg
Phillip Rogaway	University of California (UC) Davis, USA
Raphaël C.-W. Phan (Chair)	Multimedia University (MMU), Malaysia
Reihaneh Safavi-Naini	University of Calgary, Canada
Ronald Cramer	CWI and Universiteit Leiden, The Netherlands
San Ling	Nanyang Technological University (NTU), Singapore
Sherman S.M. Chow	Chinese University of Hong Kong
Shiho Moriai	NICT, Japan
Tatsuaki Okamoto	Nippon Telegraph and Telephone (NTT), Japan
Vincent Rijmen	KU Leuven and iMinds, Belgium
Yvo Desmedt	University of Texas at Dallas, USA and UCL, UK

External Reviewers

Alexander Koch
Alfredo Rial Duran
Anton Stiglic
Benjamin Wesolowski
Cristina Onete
Daniel Masny
Duane Wilson
Edoardo Persichetti
Frédérique Elise Oggier
Gäetan Leurent
Guomin Yang
Hossein Siadati
Huaxiong Wang
Hyung Tae Lee
Irene Giacomelli
Jae Hong Seo
Jean-Pierre Tillich
Jens Zumbrägel
John Chan
Jonathan Bootle
Jong Hwan Park
Kazuki Yoneyama
Keita Emura
Khoa Nguyen
Koutarou Suzuki
Laura Luzzi
Luisa Siniscalchi
Mark Marson
Michele Ciampi
Nicolas Sendrier
Palash Sarkar
Peng Jiang
Peter B. Rønne
Pierre-Louis Cayrel
Rafael Misoczki
Robert Granger
Russell W.F. Lai
Scott Ruoti
Sébastien Canard
Shiwei Zhang
Sigurd Eskeland
Subhamoy Maitra
Sylvain Ruhault
Tom Ristenpart
Vanishree Rao
Viet Tung Hoang
Wakaha Ogata
Yannick Seurin
Yu Sasaki
Yu Yu
Yusi James Zhang

In Cooperation with

The International Association for Cryptologic Research (IACR)

Sponsoring Institutions

Cyber Security Malaysia
IEICE Malaysia Section
Multimedia University (MMU)
Tourism Malaysia

Contents

Keynotes

Revisiting Tradition

Different Paradigms

Cryptofication

Malicious Cryptography

Advances in Cryptanalysis

Primitives and Features

Cryptanalysis Correspondence

Invited and Insight Papers