Lecture Notes in Computer Science 8813

Dimitris Gritzalis Aggelos Kiayias
Ioannis Askoxylakis (Eds.)

Cryptology and Network Security

13th International Conference, CANS 2014
Heraklion, Crete, Greece, October 22-24, 2014
Proceedings

Springer

Volume Editors

Dimitris Gritzalis
Athens University of Economics & Business
Department of Informatics
76, Patission Str., 10434 Athens, Greece
E-mail: dgrit@aueb.gr

Aggelos Kiayias
National and Kapodistrian University of Athens
Department of Informatics and Telecommunications
Panepistimiopolis, 15784 Athens, Greece
E-mail: aggelos@di.uoa.gr

Ioannis Askoxylakis
FORTH-ICS
Vassilika Vouton
P.O. Box 1385, 711 10 Heraklion, Crete, Greece
E-mail: asko@ics.forth.gr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-319-12279-3 e-ISBN 978-3-319-12280-9
DOI 10.1007/978-3-319-12280-9
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014950927

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 13th International Conference on Cryptology and Network Security (CANS) took place on Heraklion, on the island of Crete, Greece, during October 20–22, 2014, and was organized by the Institute of Computer Science of the Foundation for Research and Technology - Hellas (FORTH-ICS).

The conference received 86 submissions, four of which were withdrawn. The Program Committee (PC) decided to accept 25 papers for presentation at the conference. Most submitted papers were reviewed by at least three PC members, while submissions co-authored by a PC member received at least one additional review. In addition to the PC members, a number of external reviewers joined the review process in their particular areas of expertise. The initial reviewing period was followed by a lively discussion phase that enabled the committee to converge on the final program. There were six papers that were conditionally accepted and shepherded by assigned PC members in a second round of reviewing. All conditionally accepted papers were included in the program. The paper submission, reviewing, discussion, and the preparation of proceedings were facilitated by the Web-based system EasyChair.

The objective of the CANS conference is to support excellent research in cryptology and network security and promote the interaction between researchers working in these areas. The PC strived to broaden the program and include papers covering diverse areas such as encryption, cryptanalysis, malware analysis, privacy and identification systems as well as various types of network protocol design and analysis work. The program also featured three keynote speakers, Sotiris Ioannidis from FORTH, Moni Naor from Weizmann Institute of Science, and Dawn Song from the University of California, Berkeley, who gave lectures on cutting-edge research on cryptology and network security. The titles and abstracts of their talks can be found in this proceedings volume.

Finally, we would like to thank all the authors who submitted their research work to the conference, the members of the Organizing Committee, who worked very hard for the success and smooth operation of the event, and the members of the Steering Committee and particularly Yvo Desmedt whose guidance during various stages of the PC work was invaluable. Last but not least, we thank all the attendees who participated and contributed to the stimulating discussions after the talks and during the breaks and social events that took place as part of the conference program.

October 2014

Dimitris Gritzalis
Aggelos Kiayias
Ioannis Askoxylakis

Organization

Program Committee

Isaac Agudo	University of Malaga, Spain
Giuseppe Ateniese	University of Rome, Italy
Mike Burmester	Florida State University, USA
Dario Catalano	University of Catania, Italy
George Danezis	Microsoft Research, UK
Ed Dawson	University of Queensland, Australia
Sabrina De Capitani Di Vimercati	Università degli Studi di Milano, Italy
Roberto Di Pietro	University of Rome Tre, Italy
Itai Dinur	ENS, France
Sara Foresti	Università degli Studi di Milano, Italy
Joaquin Garcia-Alfaro	TELECOM SudParis, France
Dieter Gollmann	TU Hamburg, Germany
Sushil Jajodia	George Mason University, USA
Stanislaw Jarecki	University of California Irvine, USA
Vassilios Katos	Democritus University of Thrace, Greece
Panos Kotzanikolaou	University of Piraeus, Greece
Helger Lipmaa	University of Tartu, Estonia
Javier Lopez	University of Malaga, Spain
Evangelos Markatos	University of Crete, Greece
Adam O'Neil	Georgetown University, USA
Kenny Paterson	RH - University of London, UK
Siani Pearson	HP Laboratories
Rene Peralta	NIST, USA
Christian Rechberger	DTU, Denmark
Kui Ren	SUNY Buffalo, USA
Panagiotis Rizomiliotis	University of the Aegean, Greece
Ahmad-Reza Sadeghi	University of Darmstadt, Germany
Reihaneh Safavi-Naini	University of Calgary, Canada
Pierangela Samarati	Università degli Studi di Milano, Italy
Nitesh Saxena	University of Alabama, USA
George Spanoudakis	City University, UK
Ioannis Stamatiou	University of Patras, Greece
Francois-Xavier Standaert	University of Louvain, Belgium
Willie Susilo	University of Wollongong, Australia

Katsuyuki Takashima	Mitsubishi Electric
Marianthi Theoharidou	Joint Research Center, Italy
Nikos Triandopoulos	EMC RSA Labs, USA
Huaxiong Wang	NTU, Singapore
Moti Yung	Google
Hong-Sheng Zhou	VCU, USA
Vasilis Zikas	UCLA, USA

Additional Reviewers

Alderman, James
Anand, S Abhishek
Baldimtsi, Foteini
Bartlett, Harry
Blanc, Gregory
D'Errico, Michela
Di Raimondo, Mario
Dmitrienko, Alexandra
Donida Labati, Ruggero
Fernandez, Carmen
Garg, Sanjam
Gaspar, Lubos
Gentry, Craig
Guo, Fuchun
Han, Jinguang
Heuser, Stephan
Huang, Qiong
Jhawar, Mahavir
Jiang, Shaoquan
Jost, Daniel
Koelbl, Stefan
Koeune, François
Krotofil, Marina
Latsiou, Aikaterina
Lauridsen, Martin M.
Liang, Kaitai
Matsuda, Takahiro
Mitelbach, Arno
Mohamed, Manar
Moody, Dustin
Moyano, Francisco
Mukhopadhyay, Dibya
Nieto, Ana
Nishide, Takashi
Onete, Cristina
Pan, Jiaxin
Papadopoulos, Dimitrios
Perlner, Ray
Peters, Thomas
Poettering, Bertram
Procter, Gordon
Puglisi, Orazio
Rios, Ruben
Schmidt, Desmond
Shahandashti, Siamak
Shirvanian, Maliheh
Shrestha, Babins
Smart, Nigel
Sugawara, Takeshi
Tackmann, Björn
Tang, Qiang
Tiessen, Tyge
Xiao, Weijun
Yang, Guomin
Yasuda, Takanori
Zhang, Bingsheng
Zhang, Liangfeng

Invited Talks

Invited Talk 1: Primary-Secondary-Resolvers Membership Proof Systems and their Application to DNSSEC

Moni Naor

Weizmann Institute of Science
Rehovot, Israel
moni.naor@weizmann.ac.il

Abstract. We consider Primary-Secondary-Resolver Membership Proof Systems (PSR for short) that enable a secondary to convince a resolver whether or not a given a element is in a set defined by the primary without revealing more information about the set.

The main motivation is studying the problem of zone enumeration in DNSSEC. DNSSEC is designed to prevent network attackers from tampering with domain name system (DNS) messages. The cryptographic machinery used in DNSSEC, however, also creates a new vulnerability - Zone Enumeration, where an adversary launches a small number of online DNSSEC queries and then uses offline dictionary attacks to learn which domain names are present or absent in a DNS zone.

We explain why current DNSSEC (NSEC3) suffers from the problem of zone enumeration: we use cryptographic lower bounds to prove that in a PSR system the secondary must perform non trivial online computation and in particular under certain circumstances signatures. This implies that the three design goals of DNSSEC — high performance, security against network attackers, and privacy against zone enumeration — cannot be satisfied simultaneously.

We provide PSR constructions matching our lower bound and in particular suggest NSEC5, a protocol that solves the problem of DNSSEC zone enumeration while remaining faithful to the operational realities of DNSSEC. The scheme can be seen as a variant of NSEC3, where the hash function is replaced with an RSA based hashing scheme. Other constructions we have are based on the BonehLynnShacham signature scheme, Verifiable Random and Unpredictable Functions and Hierarchical Identity Based Encryption.

The talk is based on the papers "NSEC5: Provably Preventing DNSSEC Zone Enumeration" by Sharon Goldberg, Moni Naor, Dimitrios Papadopoulos, Leonid Reyzin, Sachin Vasant and Asaf Ziv and "PSR Membership Proof Systems" by Moni Naor and Asaf Ziv.

Invited Talk 2: Ask Us before you download: Lessons from Analyzing 3 Million Android Apps

Dawn Song

University of California, Berkeley
Berekely, CA, USA
dawnsong@cs.berkeley.edu

Abstract. Android is the most popular mobile platform currently, with over 1 billion devices activated. Millions of Android Apps have been downloaded billions of times. What are the security and privacy issues in these millions of apps? What lessons can we learn to ensure better app security and mobile security? In this talk, I will share our insights and lessons learned from analyzing over 3 million apps.

Invited Talk 3: Security applications of GPUs

Sotiris Ioannidis

Institute of Computer Science
Foundation for Research & Technology Hellas, Greece
sotiris@ics.forth.gr

Abstract. Modern graphics processors have been traditionally used for gaming, but in the last few years they have been used more and more in the area of high performance computing. In this talk we will explore alternate uses of graphics processors, in the area of security. We will discuss how a defender can use graphics hardware to bolster system defenses, and how miscreants can exploit them to build better and stealthier malware.

Table of Contents

Bootstrappable Identity-Based Fully Homomorphic Encryption 1
Michael Clear and Ciarán McGoldrick

Proxy Re-encryption with Unforgeable Re-encryption Keys 20
Hui Guo, Zhenfeng Zhang, and Jiang Zhang

On the Lossiness of 2^k-th Power and the Instantiability of Rabin-OAEP 34
Haiyang Xue, Bao Li, Xianhui Lu, Kunpeng Wang, and Yamin Liu

Breaking and Fixing Cryptophia's Short Combiner 50
Bart Mennink and Bart Preneel

FFT Key Recovery for Integral Attack 64
Yosuke Todo and Kazumaro Aoki

Message Extension Attack against Authenticated Encryptions: Application to PANDA 82
Yu Sasaki and Lei Wang

New Second Preimage Attack Variants against the MD-Structure 98
Tuomas Kortelainen and Juha Kortelainen

Negotiating DNSSEC Algorithms over Legacy Proxies 111
Amir Herzberg and Haya Shulman

A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System 127
Matthias Wachs, Martin Schanzenbach, and Christian Grothoff

Universally Composable Oblivious Transfer Based on a Variant of LPN 143
Bernardo David, Rafael Dowsley, and Anderson C.A. Nascimento

Converting PKI-Based Authenticated Key Exchange to Identity-Based 159
Koutarou Suzuki and Kazuki Yoneyama

Proving Correctness and Security of Two-Party Computation Implemented in Java in Presence of a Semi-honest Sender 175
Florian Böhl, Simon Greiner, and Patrik Scheidecker

Mining API Calls and Permissions for Android Malware Detection 191
Akanksha Sharma and Subrat Kumar Dash

Direct Anonymous Attestations with Dependent Basename Opening 206
Nicolas Desmoulins, Roch Lescuyer, Olivier Sanders, and Jacques Traoré

A Storage-Efficient and Robust Private Information Retrieval Scheme Allowing Few Servers 222
Daniel Augot, Françoise Levy-dit-Vehel, and Abdullatif Shikfa

Should Silence be Heard? Fair Rational Secret Sharing with Silent and Non-silent Players 240
Sourya Joyee De, Sushmita Ruj, and Asim K. Pal

Attribute-Based Signatures with User-Controlled Linkability 256
Ali El Kaafarani, Liqun Chen, Essam Ghadafi, and James Davenport

Towards a Full-Featured Implementation of Attribute Based Credentials on Smart Cards 270
Antonio de la Piedra, Jaap-Henk Hoepman, and Pim Vullers

Security of a Privacy-Preserving Biometric Authentication Protocol Revisited 290
Aysajan Abidin, Kanta Matsuura, and Aikaterini Mitrokotsa

Private and Dynamic Time-Series Data Aggregation with Trust Relaxation 305
Iraklis Leontiadis, Kaoutar Elkhiyaoui, and Refik Molva

Privacy-Enhanced Participatory Sensing with Collusion Resistance and Data Aggregation 321
Felix Günther, Mark Manulis, and Andreas Peter

Short Comparable Encryption 337
Jun Furukawa

Decentralized Distributed Data Usage Control 353
Florian Kelbert and Alexander Pretschner

Efficient Signatures with Tight Real World Security in the Random-Oracle Model 370
Christoph Bader

More Sparse Families of Pairing-Friendly Elliptic Curves 384
Georgios Fotiadis and Elisavet Konstantinou

Author Index 401