Lecture Notes in Computer Science 10674

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

Helger Lipmaa · Aikaterini Mitrokotsa
Raimundas Matulevičius (Eds.)

Secure IT Systems

22nd Nordic Conference, NordSec 2017
Tartu, Estonia, November 8–10, 2017
Proceedings

Springer

Editors
Helger Lipmaa
University of Tartu
Tartu
Estonia

Raimundas Matulevičius
University of Tartu
Tartu
Estonia

Aikaterini Mitrokotsa
Chalmers University of Technology
Gothenburg
Sweden

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-70289-6 ISBN 978-3-319-70290-2 (eBook)
https://doi.org/10.1007/978-3-319-70290-2

Library of Congress Control Number: 2017957852

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

This volume contains the papers presented at NordSec 2017, the 22nd Nordic Conference on Secure IT Systems. The conference was held during November 8–10, 2017, in Tartu, Estonia.

The NordSec conferences started in 1996 with the aim of bringing together researchers and practitioners in computer security in the Nordic countries, thereby establishing a forum for discussions and cooperation between universities, industry, and computer societies. NordSec addresses a broad range of topics within IT security and privacy and over the years it has developed into an international conference that takes place in the Nordic countries. NordSec is currently a key meeting venue for Nordic university teachers and students with research interests in information security and privacy.

NordSec 2017 received 42 submissions, with all valid submissions receiving three reviews by the Program Committee (PC). After the reviewing phase, 18 papers were accepted for publication and are all included in these proceedings. Furthermore, we had a poster session that encouraged discussions and brainstorming on current topics of information security and privacy.

We were honored to have had three brilliant invited speakers with talks on current topics in information security focusing on machine learning, blockchains, and verifiable computation. More precisely, Dr. Ananth Raghunathan from Google gave a talk on "Security and Privacy Challenges in Machine Learning," Prof. Aggelos Kiayias from the University of Edinburgh gave a talk on "Proof of Stake Blockchain Protocols," and Dr. Dario Fiore from IMDEA Software Institute gave a talk on "Homomorphic Authentication for Computing Securely on Untrusted Machines."

We sincerely thank everyone involved in making this year's instance a success including but not limited to: the authors who submitted their papers, the presenters who contributed to the NordSec program, and the PC members and the additional reviewers for their thorough and very helpful reviews. Last but not least, we sincerely thank the Cybernetica AS company for the support given to the NordSec 2017 conference.

November 2017

Helger Lipmaa
Aikaterini Mitrokotsa
Raimundas Matulevičius

Organization

General Chair

Helger Lipmaa	University of Tartu, Estonia

Program Committee Chairs

Helger Lipmaa	University of Tartu, Estonia
Aikaterini Mitrokotsa	Chalmers University of Technology, Sweden

Program Committee

Tuomas Aura	Aalto University, Finland
Musard Balliu	Chalmers University of Technology, Sweden
Céline Blondeau	Aalto University, Finland
Billy Brumley	Tampere University of Technology, Finland
Sonja Buchegger	KTH Royal Institute of Technology, Sweden
Ahto Buldas	Cybernetica AS, Estonia
Úlfar Erlingsson	Google Brain, Iceland
Simone Fischer-Hübner	Karlstad University, Sweden
Kristian Gjøsteen	Norwegian University of Science and Technology, Norway
Rene Rydhof Hansen	Aalborg University, Denmark
Camilla Hollanti	Aalto University, Finland
Thomas Johansson	Lund University, Sweden
Audun Jøsang	University of Oslo, Norway
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Martti Lehto	University of Jyväskylä, Finland
Ville Leppänen	University of Turku, Finland
Bei Liang	Chalmers University of Technology, Sweden
Olaf Maennel	Tallinn University of Technology, Estonia
Raimundas Matulevičius	University of Tartu, Estonia
Christian W. Probst	Technical University of Denmark, Denmark
Carla Ràfols	Universitat Pompeu Fabra, Spain
Alejandro Russo	Chalmers University of Technology, Sweden
Berry Schoenmakers	Technical University of Eindhoven, The Netherlands
Carsten Schuermann	IT University of Copenhagen, Denmark
Zheng Yan	Xidian University, China
Bingsheng Zhang	Lancaster University, UK

Additional Reviewers

Daniel Bosk
Alessandro Bruni
Prastudy Fauzi
Wei Feng
Rosario Giustolisi
Oliver Gnilke
Shohreh Hosseinzadeh
Xuyang Jing
Joona Kannisto
Xueqin Liang
Gao Liu
Samuel Marchal
Yoan Miche
Mads C. Olesen
Cesar Pereida Garcia
Sampsa Rauti
Jukka Ruohonen
Razane Tajeddine
Nicola Tuveri
Daren Tuzi
Thomas Zacharias
Daode Zhang

Organization Chair

Raimundas Matulevičius	University of Tartu, Estonia

Steering Committee

Tuomas Aura	Aalto University, Finland (Chair)
Karin Bernsmed	SINTEF ICT, NTNU, Norway
Billy Brumley	Tampere University of Technology, Finland
Bengt Carlsson	Blekinge Institute of Technology, Sweden
Úllfar Erlingsson	Google Inc., Mountain View, USA
Simone Fischer-Huebner	Karlstad University, Sweden
Dieter Gollmann	TUHH Technische Universität Hamburg-Harburg, Germany
Audun Jøsang	University of Oslo, Norway
Stewart Kowalski	Gjøvik University College, Norway
Peeter Laud	Cybernetica AS, Estonia
Helger Lipmaa	University of Tartu, Estonia
Hanne Riis Nielson	Technical University of Denmark, Denmark
Juha Röning	University of Oulu, Finland
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Simin Nadjm-Tehrani	Linköping University, Sweden
Magnus Almgren	Chalmers University of Technology, Sweden
Sonja Buchegger	KTH, Royal Institute of Technology, Sweden

Abstracts of Invited Talks

Homomorphic Authentication for Computing Securely on Untrusted Machines

Dario Fiore

IMDEA Software Institute, Madrid, Spain
dario.fiore@imdea.org

Abstract. Due to phenomena like the ubiquity of the Internet and cloud computing, it is increasingly common to store and process data on third-party machines. In spite of its attractive aspects, this trend raises a number of security concerns, including: how to ensure that the results computed by third parties are correct (integrity) and no unauthorized information is leaked (privacy)? This talk focuses on cryptographic solutions for integrity, and more specifically on the notion of homomorphic authentication. It presents this notion, gives an overview of the state of the art in this area, and covers some of the recent efficient constructions.

Introduction

Due to phenomena like the ubiquity of the Internet and cloud computing, it is increasingly common to store and process data on third-party machines. While this computing trend is undoubtedly successful for its attractive features, it also raises a number of security concerns, such as:

How to ensure that the results computed by third parties are correct (integrity) and no unauthorized information is leaked (privacy)?

Recent work in cryptography has shown a variety of new cryptographic means for protecting information processed on third-party, untrusted machines. For example, it is widely known that fully homomorphic encryption [6] can solve privacy by allowing one to compute on data that is encrypted. Here, we analyze the problem of guaranteeing the *authenticity of data during computation*, and more specifically we focus on the notion of *homomorphic authentication*.

Homomorphic Authenticators. Akin to standard authentication mechanisms (e.g., digital signatures or message authentication codes), homomorphic authenticators (HAs) allow a user Alice to authenticate a collection of data items $x_1, \ldots, x_n$ using her secret key. The distinguishing feature of HAs is that an untrusted party, without the need of any secret, can use the authenticators on $x_1, \ldots, x_n$ to generate a value $\sigma_{\mathcal{P},y}$ that vouches for the correctness of $y = \mathcal{P}(x_1, \ldots, x_n)$. Finally, a user Bob who is given the tuple $(\mathcal{P}, y, \sigma_{\mathcal{P},y})$ and Alice's verification key can verify the authenticity of y as output of the program $\mathcal{P}$ executed on data authenticated by Alice. In other words, Bob can verify that the server did not tamper with the computation's result and that it used the very same data authenticated by Alice. Alice's verification key can be either secret or public. In the former case, this primitive is known as *homomorphic MACs*, while in the latter case it is known as *homomorphic signatures*.

In terms of security, HAs must be unforgeable. Intuitively, this means that an adversary must not be able to forge a valid authenticator on an incorrect computation's result $y^* \neq \mathcal{P}(x_1, \ldots, x_n)$. In addition to security, HAs are interesting because of two additional properties. The first one is *succinctness*, which says that the authenticators remain short, i.e., much shorter than $\mathcal{P}$'s input size: this means that one can convince Bob about the correctness of a program executed on a huge amount of data by sending him only a very short piece of information. The second interesting property is *composability*, which says that derived authenticators can be used further as inputs to new computations: this means that one can, for example, distribute different subtasks to several untrusted workers, ask each of them to produce a proof of its local task, and use these proofs to create another single proof for the final job (as in the MapReduce approach).

Thanks to these properties, homomorphic authenticators can provide a nice and elegant solution to the problem of ensuring authenticity and integrity of data during computation.

A glance at the state of the art.[1] The notion of homomorphic authentication was first introduced by Desmedt [4] and later reconsidered more formally by Johnson et al. [8]. A more formal definition, as the one depicted above, came only more recently starting with the works of Boneh et al. [1, 2]. Since then, research was mainly devoted towards two fundamental goals: (i) to broaden the class of functionalities that can be computed homomorphically, and (ii) to obtain efficient instantiations. With respect to (i), research has gone far up to the notable result of Gorbunov, Vaikuntanathan and Wichs who showed a scheme that supports boolean circuits of bounded polynomial depth [7]. Yet, the existence of truly fully homomorphic schemes remain an open problem. As far as (ii) is concerned, the problem is less settled as practically efficient instantiations essentially are confined to schemes supporting linear functions. The situation is slightly better in the symmetric-key setting: a fully homomorphic MAC that can deal with all circuits was proposed by Gennaro and Wichs [5] based on FHE, and a simpler, more efficient homomorphic MAC supporting only NC1 circuits has been shown by Catalano and Fiore [3] based on pseudorandom functions.

Talk Overview. This talk begins with an introduction to the notion of homomorphic authentication and an overview of the state of the art. Next, it covers some recent constructions, and finally concludes by discussing some of the main open problems in this research area.

[1] This is not meant to be an exhaustive analysis; we only mention a selection of milestones in the area.

Acknowledgements. I would like to thank the program chairs and the entire PC of NordSec 2017 for inviting me to give this talk. I am also grateful to Michael Backes, Manuel Barbosa, Dario Catalano, Rosario Gennaro, Katerina Mitrokotsa, Luca Nizzardo, Elena Pagnin, Valerio Pastro, Raphael Reischuk, Konstantinos Vamvourellis, and Bogdan Warinschi for their fruitful collaboration in this research area.

References

1. Boneh, D., Freeman, D.M.: Homomorphic signatures for polynomial functions. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 149–168. Springer, Berlin (2011)
2. Boneh, D., Freeman, D., Katz, J., Waters, B.: Signing a linear subspace: signature schemes for network coding. In: Jarecki,S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 68–87. Springer, Berlin (2009)
3. Catalano, D., Fiore, D.: Practical homomorphic MACs for arithmetic circuits. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 336–352. Springer, Berlin (2013)
4. Desmedt, Y.: Computer security by redefining what a computer is. NSPW (1993)
5. Gennaro, R., Wichs, D.: Fully homomorphic message authenticators. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 301–320. Springer, Berlin (2013)
6. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: 41st ACM STOC, pp. 169–178. ACM Press (2009)
7. Gorbunov, S., Vaikuntanathan, V., Wichs, D.: Leveled fully homomorphic signatures from standard lattices. In: 47th ACM STOC. ACM Press (2015)
8. Johnson, R., Molnar, D., Song, D.X., Wagner, D.: Homomorphic signature schemes. In: Preneel, B. (ed.) CT-RSA 2002. LNCS, vol. 2271, pp. 244–262. Springer, Cham (2002)

Security and Privacy Challenges in Machine Learning

Ananth Raghunathan

Google, Mountain View, CA, USA
pseudorandom@google.com

Abstract. This talk covers many of the security and privacy issues raised by the recent advances in machine learning. In particular, I'll present recent results in protecting the privacy of sensitive training data, and recent attacks enabled by semi-supervised learning and knowledge transfer.

Proof of Stake Blockchain Protocols

Aggelos Kiayias

University of Edinburgh, Edinburgh, UK
akiayias@inf.ed.ac.uk

Abstract. In this talk I will cover recent developments in the design of blockchain protocols focusing on proof of stake based solutions. The talk will overview design challenges and analysis approaches, from both a security and a high performance perspective.

Contents

Applications

Access Control

Emerging Security Areas