Lecture Notes in Computer Science 8501

David Naccache   Damien Sauveron (Eds.)

Information Security Theory and Practice

Securing the Internet of Things

8th IFIP WG 11.2 International Workshop, WISTP 2014
Heraklion, Crete, Greece, June 30 – July 2, 2014
Proceedings

Springer

Volume Editors

David Naccache
École Normale Supérieure
Département d'Informatique
45, rue d'Ulm, 75230 Paris, France
E-mail: david.naccache@ens.fr

Damien Sauveron
Université de Limoges
XLIM (UMR CNRS 7252)
123 avenue Albert Thomas, 87060 Limoges Cedex, France
E-mail: damien.sauveron@unilim.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-662-43825-1 e-ISBN 978-3-662-43826-8
DOI 10.1007/978-3-662-43826-8
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014940797

LNCS Sublibrary: SL 4 – Security and Cryptology

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

Future ICT technologies, such as the concepts of ambient intelligence, cyber-physical systems and Internet of Things, provide a vision of the information society in which: people and physical systems are surrounded with intelligent interactive interfaces and objects, and environments are capable of recognising and reacting to the presence of different individuals or events in a seamless, unobtrusive and invisible manner. The success of future ICT technologies will depend on how secure these systems may be, to what extent they will protect the privacy of individuals and how individuals will come to trust them.

The 8th Workshop in Information Security Theory and Practice (WISTP 2014) addressed security and privacy issues of smart devices, networks, architectures, protocols, policies, systems, and applications related to the Internet of Things, along with evaluating their impact on business, individuals, and society. WISTP 2014 was organized by the FORTH-ICS during June 30 – July 2, 2014, in Heraklion, Greece.

The workshop received 33 submissions. Each submission was reviewed by at least three reviewers. This long and rigorous process was only possible thanks to the hard work of the Program Committee members and additional reviewers, listed on the following pages.

This volume contains the eight full papers and six short papers that were selected for presentation at WISTP 2014. Furthermore, the proceedings include the two keynotes given by Bart Preneel and Timo Kasper, to whom we are grateful.

WISTP 2014 was collocated with the 7th International Conference on Trust and Trustworthy Computing (TRUST), and keynote talks of each event were delivered to both, with the attendees having the possibility to attend sessions of both events.

We wish to thank all the people who invested time and energy to make WISTP 2014 a success: first and foremost all the authors who submitted papers to WISTP and presented them at the workshop. The members of the Program Committee together with all the external reviewers worked hard in evaluating the submissions. The WISTP Steering Committee helped us graciously in all critical decisions. Thanks also go to the 2014 General Chairs Ioannis Askoxylakis, the local organizer Nikolaos Petroulakis and their respective teams for handling the local arrangements, to the Trusted Computing Group, Intel, and Microsoft for financial cosponsoring WISTP 2014, IFIP WG 11.2 Pervasive Systems Security for scientific cosponsoring of WISTP 2014, and to Sara Foresti and Cheng-Kang Chu for their efforts as publicity chairs.

April 2014

David Naccache
Damien Sauveron

Organization

WISTP 2014 was organized by FORTH-ICS.

General Chair

Ioannis Askoxylakis	FORTH-ICS, Greece

Local Organizers

Nikolaos Petroulakis	FORTH-ICS, Greece

Workshop/Panel/Tutorial Chair

Konstantinos Markantonakis	ISG-SCC, Royal Holloway University of London, UK

Publicity Chairs

Sara Foresti	Università degli Studi di Milano, Italy
Cheng-Kang Chu	Huawei, Singapore

Program Chairs

David Naccache	Ecole Normale Supérieure, France
Damien Sauveron	XLIM, University of Limoges, France

Program Committee

Raja Naeem Akram	University of Waikato, New Zealand
Claudio A. Ardagna	Università degli Studi di Milano, Italy
Ioannis Askoxylakis	FORTH-ICS, Greece
Gildas Avoine	INSA de Rennes, France
Lejla Batina	Radboud University Nijmegen, The Netherlands
Lorenzo Cavallaro	Royal Holloway, University of London, UK

Hervé Chabanne	Morpho, France
Serge Chaumette	LaBRI, University Bordeaux 1, France
Mauro Conti	University of Padua, Italy
Manuel Egele	Carnegie Mellon University, USA
Flavio Garcia	University of Birmingham, UK
Dieter Gollmann	Hamburg University of Technology, Germany
Johann Groszschädl	Universität Luxemburg, Luxembourg
Yong Guan	Iowa State University, USA
Gerhard Hancke	City University of Hong Kong, Hong Kong
Süleyman Kardas	TUBITAK BILGEM UEKAE, Turkey
Issa Mohammad Khalil	Qatar Fondation, Qatar
Ioannis Krontiris	Goethe University Frankfurt, Germany
Andrea Lanzi	Università degli Studi di Milano, Italy
Corrado Leita	Lastline, UK
Albert Levi	Sabanci University, Turkey
Peng Liu	Pennsylvania State University, USA
Javier Lopez	University of Malaga, Spain
Federico Maggi	Politecnico di Milano, Italy
Vashek Matyas	Masaryk University, Czech Republic
Sjouke Mauw	University of Luxembourg, Luxembourg
Aikaterini Mitrokotsa	Chalmers University of Technology, Sweden
Flemming Nielson	Technical University of Denmark, Denmark
Vladimir A. Oleshchuk	University of Agder, Norway
Frank Piessens	Katholieke Universiteit Leuven, Belgium
Wolter Pieters	TU Delft and University of Twente, The Netherlands
David Pointcheval	Ecole Normale Supérieure, France
Axel York Poschmann	Nanyang Technological University, Singapore
Henrich C. Pöhls	Institute of IT Security and Security Law at the University of Passau, Germany
Christina Pöpper	Ruhr University Bochum, Germany
Jean-Jacques Quisquater	UCL Crypto Group, Louvain-la-Neuve, Belgium
Kui Ren	State University of New York at Buffalo, USA
Vincent Rijmen	University of Leuven, Belgium
Reihaneh Safavi-Naini	University of Calgary, Canada
Kouichi Sakurai	Kyushu University, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Seungwon Shin	KAIST, Korea
Jose Maria Sierra	Carlos III University of Madrid, Spain
Asia Slowinska	Vrije Universiteit Amsterdam, The Netherlands
Willy Susilo	University of Wollongong, Australia
Michael Tunstall	Cryptography Research Inc, USA
Umut Uludag	TUBITAK BILGEM UEKAE, Turkey
Stefano Zanero	Politecnico di Milano, Italy
Jianying Zhou	Institute for Infocomm Research, Singapore

Additional Reviewers

Ahmadi, Ahmad
Alcaraz, Cristina
Ambrosin, Moreno
Autefage, Vincent
Barenghi, Alessandro
Ben Jaballah, Wafa
Bingol, Muhammed Ali
Cai, Shaoying
Dahan, Xavier
Dayioğlu, Ziynet Nesibe
Ege, Baris
Emura, Keita
Jafari, Mohammad
Noorman, Job
Ouoba, Jonathan
Perrin, Léo
Picek, Stjepan
Riha, Zdenek
Rios, Ruben
Riou, Sebastien
Stöttinger, Marc
Yan, Jingbo

WISTP Steering Committee

Angelos Bilas	FORTH-ICS and University of Crete, Greece
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Dieter Gollmann	Hamburg University of Technology, Germany
Konstantinos Markantonakis	ISG-SCC, Royal Holloway University of London, UK
Jean-Jacques Quisquater	DICE, Catholic University of Louvain, Belgium
Damien Sauveron	XLIM, University of Limoges, France

Scientific Support

IFIP WG 11.2 Pervasive Systems Security

Main Sponsors

Since the early stages of the workshop inception the workshop organizers received positive feedback from a number of high profile organizations. With the development of a strong program and organizing committee, this was further capitalised into direct financial support. This enabled the workshop organizers to strengthen significantly their main objective for proposing a high standard academic workshop. The support helped significantly to keep the workshop registration costs as low as possible and as the same time offer a number of best paper awards. Therefore, we would like to express our gratitude and thank every single organization. We are also looking forward to work together in future WISTP events.

TRUSTED COMPUTING GROUP™

intel®

Microsoft

Abstracts of Invited Papers

Lightweight and Secure Cryptographic Implementations for the Internet of Things (Extended Abstract)

Bart Preneel

KU Leuven and iMinds
Dept. Electrical Engineering-ESAT/COSIC,
Kasteelpark Arenberg 10 Bus 2452, B-3001 Leuven, Belgium
bart.preneel@esat.kuleuven.be

Abstract. There is a growing insight that if we build Internet functionality into every object, it will be essential for broad acceptability that security and privacy features are protected from day one. The old approach of first rolling out the system and thinking about security and privacy later will no longer work. Cryptographic algorithms form an essential element to protect the Internet of Things; moreover, this environment will impose ever higher requirements for the algorithms in terms of performance, security, and cost. For many settings algorithms tradeoffs are expected that offer an improvement of one order of magnitude compared to existing standards. This extended abstract presents a brief overview of the issues that need to be addressed for such an optimization to be successful.

The design of cryptographic algorithms corresponds to finding a tradeoff between performance, cost, and security. It is rather easy to obtain any two of these, while giving up the third one. As an example, it is easy to develop a highly secure and very fast algorithm if the implementation can be expensive.

- Performance is typically thought of as speed or throughput: how many cycles or seconds are needed to process a single byte or message. It is difficult to express performance in a single number, as the performance depends on the hardware platform (even performance numbers on two hardware platforms with the same cost can be very different) and the time to process one byte varies depending on the length of the message (there are typically setup costs). Moreover, parallelism is playing a more important role (for high end systems).
- Security can typically be expressed in number of bits of the effective key length; a more accurate but harder to estimate measure is the monetary cost for the opponent. The difficulty with estimating security is that there are a range of attacks that assume different access of the opponent to the device and that achieve difference goals. As an example, cryptographers typically consider only attackers that try to break a single instance of a cryptographic scheme, while attacking multiple instances frequently brings

economies of scales, e.g. through time-memory tradeoffs. Moreover, in the past two decades the insight has grown that implementation attacks (also known as grey box attacks), that exploit physical properties of the implementation, can be much more effective than black box attacks that only exploit the input-output behavior. Finding low-cost protections against such attacks is notoriously difficult.

- The third element is the cost: ideally, cost can be expressed in financial terms. Hardware cost depends on the gate count or chip area, but for small devices packaging costs can play a very large role. Moreover, in environments such as the Internet of Things money or hardware may not be the only constraint: devices such as passive RFID tags that receive power from the reader or devices that harvest their energy from the environment will have power constraints. Other devices are battery operated, and the challenge is to minimize energy to maximize the life time. Note that energy is the product of power and time, so an algorithm that minimizes power does not necessarily minimize energy.

The interest in lightweight cryptography has grown in the last decade. Many algorithms have been published, including block ciphers, streams ciphers, MAC algorithms, hash functions, authenticated encryption and public key algorithms. For symmetric cryptography, the focus was initially on reducing the area or gate count, but the attention has shifted to reducing energy consumption, to algorithms for low-end micro-controllers and to resistance against implementation attacks. For public-key cryptography, research has concentrated on demonstrating that it is indeed possible to implement current algorithms such as ECC (Elliptic Curve Cryptography) and NTRU on low-end platforms.

The main conclusion so far is that there is no such thing as a cryptographic algorithm suited for the Internet of Things. If one wants to push the boundaries by an order of magnitude and also resist implementation attacks, it will be essential to optimize both the algorithm and the implementation for a specific environment. At this stage it is not clear how many algorithms will be needed to satisfy the demand, but one can expect that a set of – perhaps tunable – standard algorithms will emerge. Next to the algorithm, the cryptographic protocol in which it is used plays a central role: the protocol should not use too many cryptographic algorithms and should again be optimized for a specific setting; the optimization should consider the algorithm(s), but also the communication and storage costs.

Sweet Dreams and Nightmares: Security in the Internet of Things

Timo Kasper, David Oswald, and Christof Paar

Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany
{timo.kasper,david.oswald,christof.paar}@rub.de

Abstract. Wireless embedded devices are predominant in the Internet of Things: Objects tagged with Radio Frequency IDentification and Near Field Communication technology, smartphones, and other embedded tokens interact from device to device and thereby often process information that is security or privacy relevant for humans. For protecting sensitive data and preventing attacks, many embedded devices employ cryptographic algorithms and authentication schemes. In the past years, various vulnerabilities have been found in commercial products that enable to bypass the security mechanisms. Since a large number of the devices in the field are in the hands of potential adversaries, implementation attacks (such as side-channel analysis and reverse engineering) can play a critical role for the overall security of a system. At hand of several examples of assailable commercial products we demonstrate the potential impact of the found security weaknesses and illustrate "how to not do it".

Table of Contents

Invited Paper

Cryptography and Cryptanalysis

Smart Cards and Embedded Devices

Privacy

Short Papers