Lecture Notes in Computer Science 10476

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

Editorial Board

David Hutchison
Lancaster University, Lancaster, UK
Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA
Josef Kittler
University of Surrey, Guildford, UK
Jon M. Kleinberg
Cornell University, Ithaca, NY, USA
Friedemann Mattern
ETH Zurich, Zurich, Switzerland
John C. Mitchell
Stanford University, Stanford, CA, USA
Moni Naor
Weizmann Institute of Science, Rehovot, Israel
C. Pandu Rangan
Indian Institute of Technology, Madras, India
Bernhard Steffen
TU Dortmund University, Dortmund, Germany
Demetri Terzopoulos
University of California, Los Angeles, CA, USA
Doug Tygar
University of California, Berkeley, CA, USA
Gerhard Weikum
Max Planck Institute for Informatics, Saarbrücken, Germany

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

Frank Stajano · Jonathan Anderson
Bruce Christianson · Vashek Matyáš (Eds.)

Security Protocols XXV

25th International Workshop
Cambridge, UK, March 20–22, 2017
Revised Selected Papers

Springer

Editors

Frank Stajano
University of Cambridge
Cambridge
UK

Bruce Christianson
University of Hertfordshire
Hatfield
UK

Jonathan Anderson
Memorial University of Newfoundland
St. John’s, NL
Canada

Vashek Matyáš
Masaryk University
Brno
Czech Republic

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-71074-7 ISBN 978-3-319-71075-4 (eBook)
https://doi.org/10.1007/978-3-319-71075-4

Library of Congress Control Number: 2017960873

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
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.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

In 2017, for its 25th edition, the International Security Protocols Workshop returned to Cambridge, UK, but moved from charming Sidney Sussex to the majestic grounds of Trinity College, where it will remain for the foreseeable future as one of us is now a Fellow there.

Our theme this year was "multi-objective security". Security protocols often have more than one objective. For example, entity authentication holds only during the protocol run, but data implicitly authenticated by the session persists long afterwards. When are such temporal disparities essential and when are they inadvertent? Protocols may also have multiple objectives because they have multiple stakeholders with potentially-competing interests. Alice's access may be Bob's risk: how do we design protocols to satisfy both? How do we detect protocols serving one master better than the other? Do we even know where the protocol came from and what its authors' objectives are? How do they interact with the policies of resource owners? What about data provenance?

As usual, the workshop theme at SPW is not prescriptive. It is not intended to restrict the topic of the paper, but to help provide a particular perspective and focus to the discussions. Our intention is to stimulate discussion likely to lead to conceptual advances, or to promising new lines of investigation, rather than to consider finished work. If you are considering participating in a future SPW, and we hope you do, please consider the year's theme as a springboard rather than a fence.

An initial draft of each position paper was circulated informally at the workshop. The post-proceedings volume you hold in your hands contains revised versions that were edited and updated by the authors to reflect the discussions and contributions triggered by the lively discussions accompanying the workshop presentations. Following SPW tradition, for each paper we also present a curated transcript of the ensuing discussion. Wherever possible we have excised the initial monologue in which the presenter said the same things that can be found in more polished form in the post-proceedings paper.

The SPW admits participants by invitation only. To be considered for invitation, please send us a short, indicative submission by the announced deadline. The call for papers for the next available workshop, while not yet out at the time of writing, is widely distributed: with a modest amount of luck you will be able to find it on the web using your favourite search engine.

August 2017

Frank Stajano
Jonathan Anderson
Bruce Christianson
Vashek Matyáš

Previous Proceedings in This Series

The proceedings of previous International Security Protocols Workshops are also published by Springer as *Lecture Notes in Computer Science* and are occasionally referred to in the text:

24th Workshop (2016)	LNCS 10368	ISBN 978-3-319-62033-6
23rd Workshop (2015)	LNCS 9379	ISBN 978-3-319-26096-9
22nd Workshop (2014)	LNCS 8809	ISBN 978-3-319-12399-8
21st Workshop (2013)	LNCS 8263	ISBN 978-3-642-41716-0
20th Workshop (2012)	LNCS 7622	ISBN 978-3-642-35693-3
19th Workshop (2011)	LNCS 7114	ISBN 978-3-642-25866-4
18th Workshop (2010)	LNCS 7061	ISBN 978-3-662-45920-1
17th Workshop (2009)	LNCS 7028	ISBN 978-3-642-36212-5
16th Workshop (2008)	LNCS 6615	ISBN 978-3-642-22136-1
15th Workshop (2007)	LNCS 5964	ISBN 978-3-642-17772-9
14th Workshop (2006)	LNCS 5087	ISBN 978-3-642-04903-3
13th Workshop (2005)	LNCS 4631	ISBN 3-540-77155-7
12th Workshop (2004)	LNCS 3957	ISBN 3-540-40925-4
11th Workshop (2003)	LNCS 3364	ISBN 3-540-28389-7
10th Workshop (2002)	LNCS 2845	ISBN 3-540-20830-5
9th Workshop (2001)	LNCS 2467	ISBN 3-540-44263-4
8th Workshop (2000)	LNCS 2133	ISBN 3-540-42566-7
7th Workshop (1999)	LNCS 1796	ISBN 3-540-67381-4
6th Workshop (1998)	LNCS 1550	ISBN 3-540-65663-4
5th Workshop (1997)	LNCS 1361	ISBN 3-540-64040-1
4th Workshop (1996)	LNCS 1189	ISBN 3-540-63494-5

No published proceedings exist for the first three workshops.

Contents

Multiple Objectives of Lawful-Surveillance Protocols 1
Joan Feigenbaum and Bryan Ford

Multiple Objectives of Lawful-Surveillance Protocols (Transcript of Discussion) 9
Joan Feigenbaum

Getting Security Objectives Wrong: A Cautionary Tale of an Industrial Control System 18
Simon N. Foley

Getting Security Objectives Wrong: A Cautionary Tale of an Industrial Control System (Transcript of Discussion) 30
Simon N. Foley

Assuring the Safety of Asymmetric Social Protocols 38
Virgil Gligor and Frank Stajano

Assuring the Safety of Asymmetric Social Protocols (Transcript of Discussion) 49
Frank Stajano

Simulating Perceptions of Security 60
Paul Wernick, Bruce Christianson, and Joseph Spring

Simulating Perceptions of Security (Transcript of Discussion). 69
Paul Wernick

Self Attestation of Things 76
Partha Das Chowdhury and Bruce Christianson

Self Attestation of Things (Transcript of Discussion). 85
Partha Das Chowdhury

Making Decryption Accountable. 93
Mark D. Ryan

Making Decryption Accountable (Transcript of Discussion) 99
Mark D. Ryan

Extending Full Disk Encryption for the Future 109
Milan Brož

Extending Full Disk Encryption for the Future (Transcript of Discussion) . . . 116
Milan Brož

Key Exchange with the Help of a Public Ledger. 123
Thanh Bui and Tuomas Aura

Key Exchange with the Help of a Public Ledger
(Transcript of Discussion) 137
Thanh Bui

Reconciling Multiple Objectives – Politics or Markets? 144
Ross Anderson and Khaled Baqer

Reconciling Multiple Objectives – Politics or Markets?
(Transcript of Discussion) 157
Ross Anderson

The Seconomics (Security-Economics) Vulnerabilities of Decentralized
Autonomous Organizations. 171
Fabio Massacci, Chan Nam Ngo, Jing Nie, Daniele Venturi, and Julian Williams

The Seconomics (Security-Economics) Vulnerabilities of Decentralized
Autonomous Organizations (Transcript of Discussion) 180
Chan Nam Ngo

A Security Perspective on Publication Metrics 186
Hugo Jonker and Sjouke Mauw

A Security Perspective on Publication Metrics (Transcript of Discussion). . . . 201
Hugo Jonker

Controlling Your Neighbour's Bandwidth for Fun and for Profit. 214
Jonathan Weekes and Shishir Nagaraja

Controlling Your Neighbour's Bandwidth for Fun and for Profit
(Transcript of Discussion) 224
Jonathan Weekes

Permanent Reencryption: How to Survive Generations of Cryptanalysts
to Come. 232
Marcus Völp, Francisco Rocha, Jeremie Decouchant, Jiangshan Yu, and Paulo Esteves-Verissimo

Permanent Reencryption: How to Survive Generations of Cryptanalysts
to Come (Transcript of Discussion) 238
Marcus Völp

Security from Disjoint Paths: Is It Possible? 247
Sergiu Costea, Marios O. Choudary, and Costin Raiciu

Security from Disjoint Paths: Is It Possible? (Transcript of Discussion) 254
Marios O. Choudary

End to End Security is Not Enough 260
Dylan Clarke and Syed Taha Ali

End to End Security is Not Enough (Transcript of Discussion) 268
Dylan Clarke

Auditable PAKEs: Approaching Fair Exchange Without a TTP 278
A. W. Roscoe and Peter Y. A. Ryan

Auditable PAKEs: Approaching Fair Exchange Without a TTP (Transcript of Discussion) 298
Peter Y. A. Ryan

Author Index 307