

*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>

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

# Security Protocols XXIV

24th International Workshop  
Brno, Czech Republic, April 7–8, 2016  
Revised Selected Papers

*Editors*

Jonathan Anderson  
Memorial University  
St. John's, NL  
Canada

Vashek Matyáš  
Faculty of Informatics  
Masaryk University  
Brno  
Czech Republic

Bruce Christianson  
University of Hertfordshire  
Hertfordshire  
UK

Frank Stajano  
University of Cambridge  
Cambridge  
UK

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-62032-9              ISBN 978-3-319-62033-6 (eBook)  
DOI 10.1007/978-3-319-62033-6

Library of Congress Control Number: 2017945734

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

The 24th International Security Protocols Workshop was held in April 2016 at the Mendel Museum of Masaryk University in Brno, Czech Republic. This former Augustinian abbey is where Gregor Mendel presented his seminal *Versuche ber Pflanzenhybriden* (Experiments on Plant Hybridization); in keeping with this location, the theme of the workshop was “Evolving Security.”

Security protocols evolve with their changing requirements, their changing mechanisms, and attackers’ changing agendas and capabilities. We saw examples of this presented at the workshop: Llewellyn-Jones, Jenkinson, and Stajano described how the Pico authentication system is evolving to support more flexible delegation mechanisms, while Pieczul and Foley brought a qualitative approach to the workshop in their longitudinal consideration of how security-sensitive software has evolved over time in one open-source software project. Sometimes, however, the evolution we see is not in security software but in the attacks against it. Jonker, Mauw, and Trujillo-Rasua described for the workshop how middleperson attacks have evolved over the years but models of them have not, while Kang, Gligor, and Sekar showed us the evolution of DDoS attacks against core Internet infrastructure. With an even more explicit Mendel connection, Ošťádal, Švenda, and Matyáš made use of genetic algorithms in the context of ad hoc network protocols to better model wireless attackers.

As is often the case, many papers and discussions did not fit the theme but were challenging and thought-provoking. We hope that all of these papers and transcripts — edited both by authors and by ourselves — will provoke further debate as our protocols and our understanding of them continue to evolve.

April 2017

Jonathan Anderson  
Bruce Christianson  
Vashek Matyáš  
Frank Stajano

## 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:

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.

# **Introduction: Evolving Security (Transcript of Discussion)**

Vashek Matyáš

Masaryk University, Brno, Czech Republic

Good morning everybody, my name is Vashek Matyáš, I'm a local from Masaryk University and I'd like to welcome you to a monastery that does not belong to the University. [laughter]

Ground rules for the discussions: don't hesitate to ask questions. However, when you ask, you must say your name clearly. All discussions, including your names, will be recorded. Then, transcripts will follow. Of course, you will get audio and transcripts for your revision. For your revisions, you can edit them and give instructions accordingly. The transcription will actually happen in Canada, where in Newfoundland — and partly outsourced — the transcripts will be transformed from audio into text. The text and the audio you'll get to revise as soon as possible. So, anybody with any questions, first let everybody know who you are, especially for the recording. Raise your questions at any time you'd like, just raise your hand.

Now it's my pleasure to introduce the first speaker, Giampaolo Bella.

# Contents

Invisible Security . . . . .	1
<i>Giampaolo Bella, Bruce Christianson, and Luca Viganò</i>	
Invisible Security (Transcript of Discussion). . . . .	10
<i>Giampaolo Bella</i>	
Man-in-the-Middle Attacks Evolved... but Our Security Models Didn't . . . . .	19
<i>Hugo Jonker, Sjouke Mauw, and Rolando Trujillo-Rasua</i>	
Man-in-the-Middle Attacks Evolved... but Our Security Models Didn't (Transcript of Discussion) . . . . .	26
<i>Hugo Jonker</i>	
The Price of Belief: Insuring Credible Trust? . . . . .	35
<i>Paul Wernick and Bruce Christianson</i>	
The Price of Belief: Insuring Credible Trust? (Transcript of Discussion) . . . . .	39
<i>Bruce Christianson</i>	
Defending Against Evolving DDoS Attacks: A Case Study Using Link Flooding Incidents . . . . .	47
<i>Min Suk Kang, Virgil D. Gligor, and Vyas Sekar</i>	
Defending Against Evolving DDoS Attacks: A Case Study Using Link Flooding Incidents (Transcript of Discussion) . . . . .	58
<i>Virgil D. Gligor</i>	
The Evolution of a Security Control . . . . .	67
<i>Olgierd Pieczul and Simon N. Foley</i>	
The Evolution of a Security Control or <i>Why Do We Need More Qualitative Research of Software Vulnerabilities?</i> (Transcript of Discussion) . . . . .	85
<i>Olgierd Pieczul and Simon N. Foley</i>	
Novel Security and Privacy Perspectives of Camera Fingerprints. . . . .	90
<i>Jeff Yan</i>	
Novel Security and Privacy Perspectives of Camera Fingerprints (Transcript of Discussion) . . . . .	96
<i>Jeff Yan</i>	
Exploiting Autocorrect to Attack Privacy . . . . .	103
<i>Brian J. Kidney and Jonathan Anderson</i>	



Exploiting Autocorrect to Attack Privacy (Transcript of Discussion) . . . . . 110  
*Brian J. Kidney*

SMAPs: Short Message Authentication Protocols . . . . . 119  
*Khaled Baqer, Johann Bezuidenhout, Ross Anderson,  
and Markus Kuhn*

SMAPs: Short Message Authentication Protocols  
(Transcript of Discussion) . . . . . 133  
*Khaled Baqer and Ross Anderson*

Explicit Delegation Using Configurable Cookies . . . . . 141  
*David Llewellyn-Jones, Graeme Jenkinson, and Frank Stajano*

Explicit Delegation Using Configurable Cookies  
(Transcript of Discussion) . . . . . 153  
*David Llewellyn-Jones*

Red Button and Yellow Button: Usable Security  
for Lost Security Tokens . . . . . 165  
*Ian Goldberg, Graeme Jenkinson, David Llewellyn-Jones,  
and Frank Stajano*

Red Button and Yellow Button: Usable Security for Lost Security Tokens  
(Transcript of Discussion) . . . . . 172  
*Frank Stajano*

Detecting Failed Attacks on Human-Interactive Security Protocols . . . . . 181  
*A.W. Roscoe*

Detecting Failed Attacks on Human-Interactive Security Protocols  
(Transcript of Discussion) . . . . . 198  
*A.W. Roscoe*

Malicious Clients in Distributed Secret Sharing Based Storage Networks . . . . 206  
*Andreas Happe, Stephan Krenn, and Thomas Lorünser*

Malicious Clients in Distributed Secret Sharing Based Storage Networks  
(Transcript of Discussion) . . . . . 215  
*Andreas Happe*

Reconsidering Attacker Models in Ad-Hoc Networks . . . . . 219  
*Radim Ošádal, Petr Švenda, and Vashek Matyáš*

Reconsidering Attacker Models in Ad-Hoc Networks  
(Transcript of Discussion) . . . . . 228  
*Petr Švenda*

**Author Index** . . . . . 233