

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, Zürich, 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, Saarbruecken, Germany

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

Bruce Christianson · James Malcolm
Vashek Matyáš · Petr Švenda
Frank Stajano · Jonathan Anderson (Eds.)

Security Protocols XXII

22nd International Workshop
Cambridge, UK, March 19–21, 2014
Revised Selected Papers

Editors

Bruce Christianson
James Malcolm
University of Hertfordshire
Hertfordshire
UK

Vashek Matyáš
Petr Švenda
Faculty of Informatics
Masaryk University
Brno
Czech Republic

Frank Stajano
University of Cambridge
Cambridge
UK

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

ISSN 0302-9743

ISBN 978-3-319-12399-8

DOI 10.1007/978-3-319-12400-1

ISSN 1611-3349 (electronic)

ISBN 978-3-319-12400-1 (eBook)

Library of Congress Control Number: 2014953266

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

© Springer International Publishing Switzerland 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

Printed on acid-free paper

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

Preface

This volume collects the revised proceedings of the 22nd International Security Protocols Workshop, held at Sidney Sussex College, Cambridge, England, from March 19 to 21, 2014.

The theme of this workshop was “Collaborating with the Enemy.” There is an ambiguity about collaboration, as the dictionary definition¹ reveals:

col-lab-o-rate:

1. To work together, especially in a joint intellectual effort.
2. To cooperate treasonably, as with an enemy occupation force in one’s country.

It has always been tricky to understand who is the enemy of Alice, under what circumstances that animosity might change, or what happens when Bob declares his stance (either toward Alice or her enemy). But we have certainly seen all our paranoid dreams of the last 20 years come true. And so the question becomes – what shall we wish for next?

“Attackers” now control so much of our infrastructure that we cannot achieve any serious distributed service without their cooperation. Interestingly, this remains true even if we interchange our view about whom we regard as the service provider, and whom as the protocol hacker subverting the (supposed) legitimate service. Spies have no privacy now either. Is this a zero-sum game, resulting in a straightforward shoving match, or are there security innovations that both parties have a positive incentive to support?

As with previous workshops in this series, each paper was revised by the authors to incorporate ideas that emerged during the workshop. These revised papers are followed by a revised transcript of the presentation and ensuing discussion.

Our thanks to Lori Klimaszewska for the initial transcription of the recorded workshop discussions, and to all but two of the authors for their kind and timely collaboration with revising these transcripts and their position paper. Particular thanks to Simon Foley and Virgil Gligor for joining us on the Program Committee. Last but not least, we thank GCHQ for providing us, perhaps appropriately, with financial support.

We hope that reading these proceedings will encourage you to join in the debate yourselves, and perhaps even to send us a position paper for the next workshop.

September 2014

Bruce Christianson
James Malcolm
Vashek Matyáš
Petr Švenda
Frank Stajano
Jonathan Anderson

¹ <http://www.thefreedictionary.com/collaborate>, accessed September 2, 2014

Previous Proceedings in this Series

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

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	In preparation
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: Collaborating with the Enemy (Transcript of Discussion)

Bruce Christianson

University of Hertfordshire

Hello everybody, and welcome to the 22nd Security Protocols Workshop. Every year we have a theme, and it has become customary to announce this prior to the start of the workshop. This year's theme is Collaborating with the Enemy, which immediately gives rise to a number of questions: why do we want to collaborate? who is the enemy? might they be us? and would it matter if they were?

As academics we collaborate all the time, we tend not to be fussy who we're collaborating with, and we think collaboration is a good thing. Unless it turns out that the people with whom we're collaborating go on to lose the war, in which case we rapidly discover that history is written by the winners. There's a fine line between being a freedom fighter and being a terrorist, I guess George Washington being a case in point, but when the BBC aren't sure which side is going to win they usually refer to them as guerillas. So maybe we're all still guerillas.

I had a look at the MI6 handbook section covering collaboration on my way here, and it said the four motives for collaboration are greed, fear, ideology and egotism, and I guess most of the work to this point on . . .

Joan Feigenbaum: Isn't love supposed to be in there?

Reply: Well maybe it's in the CIA handbook, it's not in the MI6 handbook. I think it's buried under ego in the MI6 handbook.

But the work we've done so far on security protocols for collaboration is mainly I guess in the ideology chapter, except we tend to refer to it as security policy, rather than as ideology. The idea is that there's this security policy, which we all agree that we're going to act as if we believed. But it's clear that when you're collaborating with an enemy, which is almost by definition somebody who isn't on the same page of the security policy as you are, then a lot of what I'd loosely describe as the trust-management type approaches to collaboration need a radical reinterpretation, at the very least.

On the other hand, even in the familiar Alice and Bob scenario, it's never clear that Alice and Bob actually have the same agenda, and we seem to be able to work around that OK. It's quite unusual for security objectives to be diametrically opposed, so can we not somehow use the triangle of forces to allow greed, fear, egotism, and love¹, to do the heavy lifting for us? Maybe if we just thought more carefully about how we design our security infrastructure we'd be more easily able to tack against the wind.

¹ Thank-you, Joan.

There's a nice mix here of people who have been before, and people who haven't, so I'll just go quickly through the rules of engagement. This is supposed to be a workshop and not a conference, so if everybody listens politely until you've got to the end of your presentation, then you've failed. The idea is to get as rapidly as possible from presenting your position paper to leading a discussion about it, and the only rule about interrupting is please try and make sure that what you're about to say, if you interrupt, is at least as interesting as what the person you're interrupting would have said if you hadn't interrupted them. That's true regardless of whether you're the speaker or not.

The discussions are being recorded, and we will publish both the position papers and a transcript of the discussion that follows them. Don't panic, this isn't Hansard, both are very heavily edited before they see the light of day. This is a safe environment in which to speculate and try out new ideas, because we will not let you say anything egregiously stupid on the record. So if you feel the urge to have a punt and see where a line of argument goes, feel free, and if it turns out it didn't go anywhere good we'll just take it out. The other rule is, if you break somebody's protocol during their talk then it's expected that you will help them fix it at the tea break afterwards. We've had several rather good publications come out of that over the years.

If at any point you feel the urge just to tell somebody how wonderful the workshop is, and how well everything is going, then feel free to interrupt me regardless of what I'm doing. Conversely, if you have a problem, however large, James is just over there, and we do collaborate. In the spirit of the workshop, the organising committee has approached GCHQ who have agreed to pay for some, but not all, of your dinners, and we will be revealing more about that as the workshop proceeds².

Ockham's Razor says that we should start with the model that has the smallest number of moving parts, and only when we can prove that that doesn't work are we justified in using a more complicated model. The simplest model of security is not to have any, and so to put us in the correct boot state, Dieter Gollmann has kindly agreed to be the first speaker and talk about, why bother securing DNS?

² Philippe Golle and Ari Juels, Dining Cryptographers Revisited, EUROCRYPT 2004, LNCS 3027, pp. 456–473.

Contents

Introduction: Collaborating with the Enemy (Transcript of Discussion)	VII
Why Bother Securing DNS? <i>Dieter Gollmann</i>	1
Why Bother Securing DNS? (Transcript of Discussion) <i>Dieter Gollmann</i>	9
Collaborating as Normal: Detecting Systemic Anomalies in Your Partner. <i>Olgierd Pieczul and Simon N. Foley</i>	18
Collaborating as Normal: Detecting Systemic Anomalies in Your Partner (Transcript of Discussion) <i>Simon N. Foley</i>	28
<i>Remark!</i> : A Secure Protocol for Remote Exams <i>Rosario Giustolisi, Gabriele Lenzini, and Peter Y.A. Ryan</i>	38
<i>Remark!</i> : A Secure Protocol for Remote Exams (Transcript of Discussion). <i>Rosario Giustolisi</i>	49
Red Queen's Race: APT Win-Win Game. <i>Vit Bukac, Vaclav Lorenc, and Vashek Matyáš</i>	55
Red Queen's Race: APT Win-Win Game (Transcript of Discussion) <i>Vit Bukac</i>	62
Non-collaborative Attackers and How and Where to Defend Flawed Security Protocols (Extended Version) <i>Michele Peroli, Luca Viganò, and Matteo Zavatteri</i>	69
Non-collaborative Attackers and How and Where to Defend Vulnerable Security Protocols (Transcript of Discussion) <i>Luca Viganò</i>	91
Dancing with the Adversary: A Tale of Wimps and Giants <i>Virgil Gligor</i>	100
Dancing with the Adversary: A Tale of Wimps and Giants (Transcript of Discussion) <i>Virgil Gligor</i>	116

Better Authentication: Password Revolution by Evolution 130
Daniel R. Thomas and Alastair R. Beresford

Better Authentication Password Revolution by Evolution
(Transcript of Discussion) 146
Daniel R. Thomas

Collaborating with the Enemy on Network Management 154
*Chris Hall, Dongting Yu, Zhi-li Zhang, Jonathan Stout, Andrew Odlyzko,
Andrew W. Moore, Jean Camp, Kevin Benton, and Ross Anderson*

Collaborating with the Enemy on Network Management
(Transcript of Discussion) 163
Ross Anderson and Chris Hall

Bootstrapping Adoption of the Pico Password Replacement System 172
*Frank Stajano, Graeme Jenkinson, Jeunese Payne, Max Spencer,
Quentin Stafford-Fraser, and Chris Warrington*

Bootstrapping Adoption of the Pico Password Replacement System
(Transcript of Discussion) 187
Frank Stajano

I Bought a New Security Token and All I Got Was This Lousy
Phish—Relay Attacks on Visual Code Authentication Schemes. 197
Graeme Jenkinson, Max Spencer, Chris Warrington, and Frank Stajano

Relay Attacks on Visual Code Authentication Schemes
(Transcript of Discussion) 216
Max Spencer

Censorship Resistance as a Side-Effect 221
Henry Tan and Micah Sherr

Censorship Resistance as a Side-Effect (Transcript of Discussion). 227
Henry Tan and Micah Sherr

On the Feasibility of a Technological Response to the Surveillance Morass. 239
Joan Feigenbaum and Jérémie Koenig

On the Feasibility of a Technological Response to the Surveillance Morass
(Transcript of Discussion) 253
Joan Feigenbaum and Jérémie Koenig

Strange Bedfellows: How and When to Work with Your Enemy. 263
Aaron D. Jagard and Rebecca N. Wright

Strange Bedfellows: How and When to Work with Your Enemy
(Transcript of Discussion) 268
Rebecca N. Wright

On the Key Role Intelligence Agencies Can Play to Restore
Our Democratic Institutions 276
Yvo Desmedt

On the Key Role Intelligence Agencies Can Play to Restore
Our Democratic Institutions (Transcript of Discussion). 286
Yvo Desmedt

On Node Capturing Attacker Strategies 300
Filip Jurnečka, Martin Stehlík, and Vashek Matyáš

On Node Capturing Attacker Strategies (Transcript of Discussion) 316
Filip Jurnečka

On the Reliability of Network Measurement Techniques Used for
Malware Traffic Analysis. 321
Joseph Gardiner and Shishir Nagaraja

On the Reliability of Network Measurement Techniques Used for
Malware Traffic Analysis (Transcript of Discussion) 334
Shishir Nagaraja

Beyond Trust 340
Partha Das Chowdhury and Bruce Christianson

Beyond Trust (Transcript of Discussion) 345
Partha Das Chowdhury

Fawkescoin: A Cryptocurrency Without Public-Key Cryptography 350
Joseph Bonneau and Andrew Miller

FawkesCoin: A Cryptocurrency Without Public-Key Cryptography
(Transcript of Discussion) 359
Joseph Bonneau

The Final Word 371

Author Index 373