

# 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
<i>Daniel R. Thomas and Alastair R. Beresford</i>	
Better Authentication Password Revolution by Evolution (Transcript of Discussion) . . . . .	146
<i>Daniel R. Thomas</i>	
Collaborating with the Enemy on Network Management . . . . .	154
<i>Chris Hall, Dongting Yu, Zhi-li Zhang, Jonathan Stout, Andrew Odlyzko, Andrew W. Moore, Jean Camp, Kevin Benton, and Ross Anderson</i>	
Collaborating with the Enemy on Network Management (Transcript of Discussion) . . . . .	163
<i>Ross Anderson and Chris Hall</i>	
Bootstrapping Adoption of the Pico Password Replacement System . . . . .	172
<i>Frank Stajano, Graeme Jenkinson, Jeunese Payne, Max Spencer, Quentin Stafford-Fraser, and Chris Warrington</i>	
Bootstrapping Adoption of the Pico Password Replacement System (Transcript of Discussion) . . . . .	187
<i>Frank Stajano</i>	
I Bought a New Security Token and All I Got Was This Lousy Phish—Relay Attacks on Visual Code Authentication Schemes. . . . .	197
<i>Graeme Jenkinson, Max Spencer, Chris Warrington, and Frank Stajano</i>	
Relay Attacks on Visual Code Authentication Schemes (Transcript of Discussion) . . . . .	216
<i>Max Spencer</i>	
Censorship Resistance as a Side-Effect . . . . .	221
<i>Henry Tan and Micah Sherr</i>	
Censorship Resistance as a Side-Effect (Transcript of Discussion). . . . .	227
<i>Henry Tan and Micah Sherr</i>	
On the Feasibility of a Technological Response to the Surveillance Morass. . . .	239
<i>Joan Feigenbaum and Jérémie Koenig</i>	
On the Feasibility of a Technological Response to the Surveillance Morass (Transcript of Discussion) . . . . .	253
<i>Joan Feigenbaum and Jérémie Koenig</i>	
Strange Bedfellows: How and When to Work with Your Enemy. . . . .	263
<i>Aaron D. Jagard and Rebecca N. Wright</i>	

Strange Bedfellows: How and When to Work with Your Enemy (Transcript of Discussion) . . . . .	268
<i>Rebecca N. Wright</i>	
On the Key Role Intelligence Agencies Can Play to Restore Our Democratic Institutions . . . . .	276
<i>Yvo Desmedt</i>	
On the Key Role Intelligence Agencies Can Play to Restore Our Democratic Institutions (Transcript of Discussion). . . . .	286
<i>Yvo Desmedt</i>	
On Node Capturing Attacker Strategies . . . . .	300
<i>Filip Jurnečka, Martin Stehlík, and Vashek Matyáš</i>	
On Node Capturing Attacker Strategies (Transcript of Discussion) . . . . .	316
<i>Filip Jurnečka</i>	
On the Reliability of Network Measurement Techniques Used for Malware Traffic Analysis. . . . .	321
<i>Joseph Gardiner and Shishir Nagaraja</i>	
On the Reliability of Network Measurement Techniques Used for Malware Traffic Analysis (Transcript of Discussion) . . . . .	334
<i>Shishir Nagaraja</i>	
Beyond Trust . . . . .	340
<i>Partha Das Chowdhury and Bruce Christianson</i>	
Beyond Trust (Transcript of Discussion) . . . . .	345
<i>Partha Das Chowdhury</i>	
FawkesCoin: A Cryptocurrency Without Public-Key Cryptography (Transcript of Discussion) . . . . .	350
<i>Joseph Bonneau and Andrew Miller</i>	
FawkesCoin: A Cryptocurrency Without Public-Key Cryptography (Transcript of Discussion) . . . . .	359
<i>Joseph Bonneau</i>	
The Final Word . . . . .	371
<b>Author Index</b> . . . . .	373

Security Protocols XXII

22nd International Workshop, Cambridge, UK, March

19-21, 2014, Revised Selected Papers

Christianson, B.; Malcolm, J.; Matyas, V.V.; #venda, P.;

Stajano, F.; Anderson, J. (Eds.)

2014, XI, 373 p. 40 illus., Softcover

ISBN: 978-3-319-12399-8