Contents

Introduction: Collaborating with the Enemy (Transcript of Discussion) . . . . VII

Why Bother Securing DNS? ................................................................. 1
Dieter Gollmann

Why Bother Securing DNS? (Transcript of Discussion) ..................... 9
Dieter Gollmann

Collaborating as Normal: Detecting Systemic Anomalies in Your Partner . . 18
Olgierd Pieczul and Simon N. Foley

Collaborating as Normal: Detecting Systemic Anomalies in Your Partner
(Transcript of Discussion) ................................................................. 28
Simon N. Foley

Remark!: A Secure Protocol for Remote Exams .................................. 38
Rosario Giustolisi, Gabriele Lenzini, and Peter Y.A. Ryan

Remark!: A Secure Protocol for Remote Exams (Transcript of Discussion). . 49
Rosario Giustolisi

Red Queen’s Race: APT Win-Win Game ........................................... 55
Vit Bukac, Vaclav Lorenc, and Vashek Matyáš

Red Queen’s Race: APT Win-Win Game (Transcript of Discussion) ....... 62
Vit Bukac

Non-collaborative Attackers and How and Where to Defend Flawed
Security Protocols (Extended Version) ............................................. 69
Michele Peroli, Luca Viganò, and Matteo Zavatteri

Non-collaborative Attackers and How and Where to Defend
Vulnerable Security Protocols (Transcript of Discussion) ................... 91
Luca Viganò

Dancing with the Adversary: A Tale of Wimps and Giants ............ 100
Virgil Gligor

Dancing with the Adversary: A Tale of Wimps and Giants
(Transcript of Discussion) ............................................................... 116
Virgil Gligor
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. Jaggard 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
(Transcript of Discussion) ...................................................... 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
Security Protocols XXII
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