Contents

Introduction: Information Security in Fiction and in Fact
(Transcript of Discussion) ..................................................... VII
  Bruce Christianson

The Dark Side of the Code .................................................... 1
  Olgierd Pieczul and Simon N. Foley

The Dark Side of the Code (Transcript of Discussion) ..................... 12
  Simon N. Foley and Olgierd Pieczul

Redesigning Secure Protocols to Compel Security Checks ................. 22
  Keith Irwin

Redesigning Secure Protocols to Compel Security Checks
(Transcript of Discussion) ..................................................... 30
  Keith Irwin

Derailing Attacks .............................................................. 41
  Saša Radomirović and Mohammad Torabi Dashti

Derailing Attacks (Transcript of Discussion) ................................ 47
  Mohammad Torabi Dashti

Establishing Software-Only Root of Trust on Embedded Systems:
Facts and Fiction ............................................................. 50
  Yanlin Li, Yueqiang Cheng, Virgil Gligor, and Adrian Perrig

Establishing Software-Only Root of Trust on Embedded Systems:
Facts and Fiction (Transcript of Discussion) ................................. 69
  Virgil Gligor

Mind Your $(R, \Phi)$s: Location-Based Privacy Controls for Consumer Drones . . . 80
  Tavish Vaidya and Micah Sherr

Mind Your $(R, \Phi)$s: Location-Based Privacy Controls for Consumer Drones
(Transcript of Discussion) ..................................................... 91
  Tavish Vaidya and Micah Sherr

Location-Private Interstellar Communication ................................ 105
  Hugo Jonker, Sjouke Mauw, and Saša Radomirović

Location-Private Interstellar Communication (Transcript of Discussion) ....... 116
  Sjouke Mauw
The Lifetime of Android API Vulnerabilities: Case Study on the 
JavaScript-to-Java Interface .................................................. 126
Daniel R. Thomas, Alastair R. Beresford, Thomas Coudray, 
Tom Sutcliffe, and Adrian Taylor

The Lifetime of Android API Vulnerabilities: Case Study on the 
JavaScript-to-Java Interface (Transcript of Discussion) ............... 139
Daniel R. Thomas

Challenges of Fiction in Network Security – Perspective of Virtualized 
Environments ............................................................................. 145
Vit Bukac, Radim Ostadal, Petr Svenda, Tatevik Bagdasaryan, 
and Vashek Matyas

Challenges of Fiction in Network Security – Perspective of Virtualised 
Environments (Transcript of Discussion) ..................................... 152
Radim Ostadal

Device Attacker Models: Fact and Fiction ................................... 158
Jiangshan Yu and Mark D. Ryan

Device Attacker Models: Fact and Fiction (Transcript of Discussion) .... 168
Mark Ryan

Smearing Fingerprints: Changing the Game of Web Tracking 
with Composite Privacy .............................................................. 178
Sandy Clark, Matt Blaze, and Jonathan M. Smith

Smearing Fingerprints: Changing the Game of Web Tracking 
and Differential Privacy (Transcript of Discussion) ...................... 183
Sandy Clark

Pico Without Public Keys ............................................................. 195
Frank Stajano, Bruce Christianson, Mark Lomas, Graeme Jenkinson, 
Jeunese Payne, Max Spencer, and Quentin Stafford-Fraser

Pico Without Public Keys (Transcript of Discussion) .................... 212
Frank Stajano

Do You Believe in Tinker Bell? The Social Externalities of Trust ........ 224
Khaled Baqer and Ross Anderson

Do You Believe in Tinker Bell? The Social Externalities of Trust 
(Transcript of Discussion) .......................................................... 237
Khaled Baqer and Ross Anderson

Security is Beautiful .................................................................. 247
Giampaolo Bella and Luca Viganò
Security is Beautiful (Transcript of Discussion) ........................................... 251
  Luca Viganò

On the Use of Security and Privacy Technology as a Plot Device ............. 261
  Joan Feigenbaum and Brad Rosen

On the Use of Security and Privacy Technology as a Plot Device
(Transcript of Discussion) ................................................................. 276
  Joan Feigenbaum

Bitcoin: Perils of an Unregulated Global P2P Currency ......................... 283
  Syed Taha Ali, Dylan Clarke, and Patrick McCorry

Bitcoin: Perils of an Unregulated Global P2P Currency
(Transcript of Discussion) ................................................................. 294
  Syed Taha Ali

Will Technology Make Information Security Impossible? And Must
Technology Be Invented Just Because We Can?: Thoughts Occasioned by
Brunner’s “The Productions of Time” and Asimov’s “The Dead Past” ...... 307
  Paul Wernick and Bruce Christianson

Will Technology Make Information Security Impossible? And Must
Technology Be Invented Just Because We Can? (Transcript of Discussion) . . 314
  Paul Wernick

Information Leakage Due to Revealing Randomly Selected Bits ............... 325
  Arash Atashpendar, A.W. Roscoe, and Peter Y.A. Ryan

Information Leakage Due to Revealing Randomly Selected Bits
(Transcript of Discussion) ................................................................. 342
  Arash Atashpendar

Efficient Data Intensive Secure Computation: Fictional or Real? ............... 350
  Changyu Dong

Efficient Data Intensive Secure Computations: Fictional or Real?
(Transcript of Discussion) ................................................................. 361
  Changyu Dong

Epilogue .............................................................................................. 365

Author Index ...................................................................................... 367
Security Protocols XXIII
23rd International Workshop, Cambridge, UK, March 31 - April 2, 2015, Revised Selected Papers
Christianson, B.; Švenda, P.; Matyáš, V.; Malcolm, J.; Stajano, F.; Anderson, J. (Eds.)
2015, XI, 367 p. 38 illus. in color., Softcover
ISBN: 978-3-319-26095-2