

Contents

| | |
|--|-----|
| Multiple Objectives of Lawful-Surveillance Protocols | 1 |
| <i>Joan Feigenbaum and Bryan Ford</i> | |
| Multiple Objectives of Lawful-Surveillance Protocols (Transcript of Discussion) | 9 |
| <i>Joan Feigenbaum</i> | |
| Getting Security Objectives Wrong: A Cautionary Tale of an Industrial Control System. | 18 |
| <i>Simon N. Foley</i> | |
| Getting Security Objectives Wrong: A Cautionary Tale of an Industrial Control System (Transcript of Discussion) | 30 |
| <i>Simon N. Foley</i> | |
| Assuring the Safety of Asymmetric Social Protocols | 38 |
| <i>Virgil Gligor and Frank Stajano</i> | |
| Assuring the Safety of Asymmetric Social Protocols (Transcript of Discussion) | 49 |
| <i>Frank Stajano</i> | |
| Simulating Perceptions of Security | 60 |
| <i>Paul Wernick, Bruce Christianson, and Joseph Spring</i> | |
| Simulating Perceptions of Security (Transcript of Discussion). | 69 |
| <i>Paul Wernick</i> | |
| Self Attestation of Things | 76 |
| <i>Partha Das Chowdhury and Bruce Christianson</i> | |
| Self Attestation of Things (Transcript of Discussion). | 85 |
| <i>Partha Das Chowdhury</i> | |
| Making Decryption Accountable | 93 |
| <i>Mark D. Ryan</i> | |
| Making Decryption Accountable (Transcript of Discussion) | 99 |
| <i>Mark D. Ryan</i> | |
| Extending Full Disk Encryption for the Future | 109 |
| <i>Milan Brož</i> | |

| | |
|---|-----|
| Extending Full Disk Encryption for the Future (Transcript of Discussion) . . . | 116 |
| <i>Milan Brož</i> | |
| Key Exchange with the Help of a Public Ledger. | 123 |
| <i>Thanh Bui and Tuomas Aura</i> | |
| Key Exchange with the Help of a Public Ledger (Transcript of Discussion) | 137 |
| <i>Thanh Bui</i> | |
| Reconciling Multiple Objectives – Politics or Markets? | 144 |
| <i>Ross Anderson and Khaled Baqer</i> | |
| Reconciling Multiple Objectives – Politics or Markets? (Transcript of Discussion) | 157 |
| <i>Ross Anderson</i> | |
| The Seconomics (Security-Economics) Vulnerabilities of Decentralized Autonomous Organizations. | 171 |
| <i>Fabio Massacci, Chan Nam Ngo, Jing Nie, Daniele Venturi, and Julian Williams</i> | |
| The Seconomics (Security-Economics) Vulnerabilities of Decentralized Autonomous Organizations (Transcript of Discussion) | 180 |
| <i>Chan Nam Ngo</i> | |
| A Security Perspective on Publication Metrics | 186 |
| <i>Hugo Jonker and Sjouke Mauw</i> | |
| A Security Perspective on Publication Metrics (Transcript of Discussion). . . . | 201 |
| <i>Hugo Jonker</i> | |
| Controlling Your Neighbour’s Bandwidth for Fun and for Profit. | 214 |
| <i>Jonathan Weekes and Shishir Nagaraja</i> | |
| Controlling Your Neighbour’s Bandwidth for Fun and for Profit (Transcript of Discussion) | 224 |
| <i>Jonathan Weekes</i> | |
| Permanent Reencryption: How to Survive Generations of Cryptanalysts to Come. | 232 |
| <i>Marcus Völz, Francisco Rocha, Jeremie Decouchant, Jiangshan Yu, and Paulo Esteves-Verissimo</i> | |
| Permanent Reencryption: How to Survive Generations of Cryptanalysts to Come (Transcript of Discussion) | 238 |
| <i>Marcus Völz</i> | |

| | |
|--|-----|
| Security from Disjoint Paths: Is It Possible? | 247 |
| <i>Sergiu Costea, Marios O. Choudary, and Costin Raiciu</i> | |
| Security from Disjoint Paths: Is It Possible? (Transcript of Discussion) | 254 |
| <i>Marios O. Choudary</i> | |
| End to End Security is Not Enough. | 260 |
| <i>Dylan Clarke and Syed Taha Ali</i> | |
| End to End Security is Not Enough (Transcript of Discussion) | 268 |
| <i>Dylan Clarke</i> | |
| Auditable PAKEs: Approaching Fair Exchange Without a TTP. | 278 |
| <i>A. W. Roscoe and Peter Y. A. Ryan</i> | |
| Auditable PAKEs: Approaching Fair Exchange Without a TTP (Transcript of Discussion) | 298 |
| <i>Peter Y. A. Ryan</i> | |
| Author Index | 307 |

<http://www.springer.com/978-3-319-71074-7>

Security Protocols XXV

25th International Workshop, Cambridge, UK, March

20–22, 2017, Revised Selected Papers

Stajano, F.; Anderson, J.; Christianson, B.; Matyáš, V.

(Eds.)

2017, XI, 307 p. 19 illus., Softcover

ISBN: 978-3-319-71074-7