## Contents

Multiple Objectives of Lawful-Surveillance Protocols .......................... 1  
   Joan Feigenbaum and Bryan Ford

Multiple Objectives of Lawful-Surveillance Protocols  
(Transcript of Discussion) ...................................................... 9  
   Joan Feigenbaum

Getting Security Objectives Wrong: A Cautionary Tale of an Industrial  
Control System ................................................................. 18  
   Simon N. Foley

Getting Security Objectives Wrong: A Cautionary Tale of an Industrial  
Control System (Transcript of Discussion) ................................ 30  
   Simon N. Foley

Assuring the Safety of Asymmetric Social Protocols .......................... 38  
   Virgil Gligor and Frank Stajano

Assuring the Safety of Asymmetric Social Protocols  
(Transcript of Discussion) ...................................................... 49  
   Frank Stajano

Simulating Perceptions of Security ............................................. 60  
   Paul Wernick, Bruce Christianson, and Joseph Spring

Simulating Perceptions of Security (Transcript of Discussion) .......... 69  
   Paul Wernick

Self Attestation of Things ...................................................... 76  
   Partha Das Chowdhury and Bruce Christianson

Self Attestation of Things (Transcript of Discussion) ...................... 85  
   Partha Das Chowdhury

Making Decryption Accountable ................................................ 93  
   Mark D. Ryan

Making Decryption Accountable (Transcript of Discussion) ............... 99  
   Mark D. Ryan

Extending Full Disk Encryption for the Future .............................. 109  
   Milan Brož
Extending Full Disk Encryption for the Future (Transcript of Discussion) . . . 116
   Milan Brož

Key Exchange with the Help of a Public Ledger . . . . . . . . . . . . . . . . . . . . 123
   Thanh Bui and Tuomas Aura

Key Exchange with the Help of a Public Ledger
(Transcript of Discussion) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 137
   Thanh Bui

Reconciling Multiple Objectives – Politics or Markets? . . . . . . . . . . . . . . . 144
   Ross Anderson and Khaled Baqer

Reconciling Multiple Objectives – Politics or Markets?
(Transcript of Discussion) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 157
   Ross Anderson

The Seconomics (Security-Economics) Vulnerabilities of Decentralized
Autonomous Organizations . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 171
   Fabio Massacci, Chan Nam Ngo, Jing Nie, Daniele Venturi,
   and Julian Williams

The Seconomics (Security-Economics) Vulnerabilities of Decentralized
Autonomous Organizations (Transcript of Discussion) . . . . . . . . . . . . . . . . . 180
   Chan Nam Ngo

A Security Perspective on Publication Metrics . . . . . . . . . . . . . . . . . . . . . 186
   Hugo Jonker and Sjouke Mauw

A Security Perspective on Publication Metrics (Transcript of Discussion) . . . 201
   Hugo Jonker

Controlling Your Neighbour’s Bandwidth for Fun and for Profit . . . . . . . . . . 214
   Jonathan Weekes and Shishir Nagaraja

Controlling Your Neighbour’s Bandwidth for Fun and for Profit
(Transcript of Discussion) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 224
   Jonathan Weekes

Permanent Reencryption: How to Survive Generations of Cryptanalysts
to Come . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 232
   Marcus Völп, Francisco Rocha, Jeremie Decouchant, Jiangshan Yu,
   and Paulo Esteves-Verissimo

Permanent Reencryption: How to Survive Generations of Cryptanalysts
to Come (Transcript of Discussion) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 238
   Marcus Völп
Contents XI

Security from Disjoint Paths: Is It Possible? ............................ 247
   Sergiu Costea, Marios O. Choudary, and Costin Raiciu

Security from Disjoint Paths: Is It Possible? (Transcript of Discussion) .... 254
   Marios O. Choudary

End to End Security is Not Enough ......................................... 260
   Dylan Clarke and Syed Taha Ali

End to End Security is Not Enough (Transcript of Discussion) ............ 268
   Dylan Clarke

Auditable PAKEs: Approaching Fair Exchange Without a TTP ............. 278
   A. W. Roscoe and Peter Y. A. Ryan

Auditable PAKEs: Approaching Fair Exchange Without a TTP
   (Transcript of Discussion) ............................................... 298
   Peter Y. A. Ryan

Author Index ................................................................. 307