

Table of Contents

Putting the Human Back in the Protocol (Transcript of Discussion) <i>Bruce Christianson</i>	1
Composing Security Metrics (Transcript of Discussion) <i>Matt Blaze</i>	3
Putting the Human Back in Voting Protocols <i>Peter Y.A. Ryan and Thea Peacock</i>	13
Putting the Human Back in Voting Protocols (Transcript of Discussion) <i>Peter Y.A. Ryan</i>	20
Towards a Secure Application-Semantic Aware Policy Enforcement Architecture <i>Srijith K. Nair, Bruno Crispo, and Andrew S. Tanenbaum</i>	26
Towards a Secure Application-Semantic Aware Policy Enforcement Architecture (Transcript of Discussion) <i>Srijith K. Nair</i>	32
Phish and Chips: Traditional and New Recipes for Attacking EMV <i>Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Steven Murdoch, Ross Anderson, and Ron Rivest</i>	40
Phish and Chips (Transcript of Discussion) <i>Mike Bond</i>	49
Where Next for Formal Methods? <i>James Heather and Kun Wei</i>	52
Where Next for Formal Methods? (Transcript of Discussion) <i>James Heather</i>	59
Cordial Security Protocol Programming: The Obol Protocol Language <i>Per Harald Myrvang and Torgeir Stabell-Kulø</i>	62
Cordial Security Protocol Programming (Transcript of Discussion) <i>Torgeir Stabell-Kulø</i>	85
Privacy-Sensitive Congestion Charging <i>Alastair R. Beresford, Jonathan J. Davies, and Robert K. Harle</i>	97

Privacy-Sensitive Congestion Charging (Transcript of Discussion)	105
<i>Alastair R. Beresford</i>	
The Value of Location Information: A European-Wide Study	112
<i>Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis</i>	
The Value of Location Information (Transcript of Discussion)	122
<i>Vashek Matyas</i>	
Update on PIN or Signature (Transcript of Discussion)	128
<i>Vashek Matyas</i>	
Innovations for Grid Security from Trusted Computing: Protocol Solutions to Sharing of Security Resource	132
<i>Wenbo Mao, Andrew Martin, Hai Jin, and Huanguo Zhang</i>	
Innovations for Grid Security from Trusted Computing (Transcript of Discussion)	150
<i>Wenbo Mao</i>	
The Man-in-the-Middle Defence	153
<i>Ross Anderson and Mike Bond</i>	
The Man-in-the-Middle Defence (Transcript of Discussion)	157
<i>Ross Anderson</i>	
Using Human Interactive Proofs to Secure Human-Machine Interactions via Untrusted Intermediaries	164
<i>Chris J. Mitchell</i>	
Using Human Interactive Proofs to Secure Human-Machine Interactions via Untrusted Intermediaries (Transcript of Discussion)	171
<i>Chris J. Mitchell</i>	
Secure Distributed Human Computation (Extended Abstract)	177
<i>Craig Gentry, Zulfikar Ramzan, and Stuart Stubblebine</i>	
Secure Distributed Human Computation (Transcript of Discussion)	181
<i>Craig Gentry</i>	
Bot, Cyborg and Automated Turing Test (Or “Putting the Humanoid in the Protocol”)	190
<i>Jeff Yan</i>	
Bot, Cyborg and Automated Turing Test (Transcript of Discussion)	198
<i>Jeff Yan</i>	
A 2-Round Anonymous Veto Protocol	202
<i>Feng Hao and Piotr Zieliński</i>	

A 2-Round Anonymous Veto Protocol (Transcript of Discussion)	212
<i>Feng Hao</i>	
How to Speak an Authentication Secret Securely from an Eavesdropper	215
<i>Lawrence O’Gorman, Lynne Brotman, and Michael Sammon</i>	
How to Speak an Authentication Secret Securely from an Eavesdropper (Transcript of Discussion)	230
<i>Lawrence O’Gorman</i>	
Secret Public Key Protocols Revisited	237
<i>Hoon Wei Lim and Kenneth G. Paterson</i>	
Secret Public Key Protocols Revisited (Transcript of Discussion)	257
<i>Hoon Wei Lim</i>	
Vintage Bit Cryptography	261
<i>Bruce Christianson and Alex Shafarenko</i>	
Vintage Bit Cryptography (Transcript of Discussion)	266
<i>Alex Shafarenko</i>	
Usability of Security Management: Defining the Permissions of Guests	276
<i>Matthew Johnson and Frank Stajano</i>	
Usability of Security Management: Defining the Permissions of Guests (Transcript of Discussion)	284
<i>Matthew Johnson</i>	
The Last Word	286
<i>Eve</i>	
Author Index	287