Table of Contents

Introduction: Brief Encounters (Transcript of Discussion) 1
Bruce Christianson

Evolutionary Design of Attack Strategies 3
Jiří Kůr, Václav Matyáš, and Petr Švenda

Evolutionary Design of Attack Strategies (Transcript of Discussion) 18
Petr Švenda

Below the Salt: The Dangers of Unfulfilled Physical Media Assumptions 24
Matt Blaze and Patrick McDaniel

Is the Honeymoon over? (Transcript of Discussion) 28
Matt Blaze

Below the Salt (Transcript of Discussion) 34
Matt Blaze

Attacking Each Other 41
Wihem Arsac, Giampaolo Bella, Xavier Chantry, and Luca Compagna

Attacking Each Other (Transcript of Discussion) 48
Xavier Chantry

Bringing Zero-Knowledge Proofs of Knowledge to Practice 51
Endre Bangerter, Stefania Barzan, Stephan Krenn, Ahmad-Reza Sadeghi, Thomas Schneider, and Joe-Kai Tsay

Bringing Zero-Knowledge Proofs of Knowledge to Practice (Transcript of Discussion) 63
Stephan Krenn

Towards a Verified Reference Implementation of a Trusted Platform Module 69
Aybek Mukhamedov, Andrew D. Gordon, and Mark Ryan

Towards a Verified Reference Implementation of a Trusted Platform Module (Transcript of Discussion) 82
Aybek Mukhamedov

The Least Privacy-Damaging Centralised Traffic Data Retention Architecture (Extended Abstract) 87
George Danezis

The Least Privacy-Damaging Centralised Traffic Data Retention Architecture (Transcript of Discussion) 93
George Danezis

Pretty Good Democracy 111
Peter Y.A. Ryan and Vanessa Teague

Pretty Good Democracy (Transcript of Discussion) 131
Peter Y.A. Ryan

Design and Verification of Anonymous Trust Protocols 143
Michael Backes and Matteo Maffei

Design and Verification of Anonymous Trust Protocols (Transcript of Discussion) 149
Michael Backes

Brief Encounters with a Random Key Graph 157
Virgil D. Gligor, Adrian Perrig, and Jun Zhao

Brief Encounters with a Random Key Graph (Transcript of Discussion) 162
Virgil D. Gligor

Trust*: Using Local Guarantees to Extend the Reach of Trust 171
Stephen Clarke, Bruce Christianson, and Hannan Xiao

Trust*: Using Local Guarantees to Extend the Reach of Trust (Transcript of Discussion) 179
Bruce Christianson

Alice and Bob in Love: Cryptographic Communication Using Shared Experiences 189
Joseph Bonneau

Alice and Bob in Love (Transcript of Discussion) 199
Joseph Bonneau

Why I'm Not an Entropist 213
Paul Syverson

Why I'm Not an Entropist (Transcript of Discussion) 231
Paul Syverson

Deriving Ephemeral Authentication Using Channel Axioms 240
Dusko Pavlovic and Catherine Meadows

Deriving Ephemeral Authentication Using Channel Axioms (Transcript of Discussion) 262
Catherine Meadows

A Novel Stateless Authentication Protocol 269
Chris J. Mitchell

A Novel Stateless Authentication Protocol (Transcript of Discussion) ... 275
Chris J. Mitchell

The Trust Economy of Brief Encounters 282
Ross Anderson

The Trust Economy of Brief Encounters (Transcript of Discussion) 285
Ross Anderson

Qualitative Analysis for Trust Management: Towards a Model of Photograph Sharing Indiscretion 298
Simon N. Foley and Vivien M. Rooney

Qualitative Analysis for Trust Management (Transcript of Discussion) 308
Simon N. Foley

Establishing Distributed Hidden Friendship Relations..... 321
Sören Preibusch and Alastair R. Beresford

Establishing Distributed Hidden Friendship Relations (Transcript of Discussion) 335
Sören Preibusch

Not That Kind of Friend: Misleading Divergences between Online Social Networks and Real-World Social Protocols 343
Jonathan Anderson and Frank Stajano

Not That Kind of Friend (Transcript of Discussion) 350
Jonathan Anderson

The Final Word 365

Author Index 367