

# Table of Contents

Keynote Address: Mobile Computing versus Immobile Security . . . . .	1
<i>Roger Needham</i>	
Experiences of Mobile IP Security (Transcript of Discussion) . . . . .	4
<i>Michael Roe</i>	
Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World . . . . .	12
<i>Pekka Nikander</i>	
Denial of Service, Address Ownership, and Early Authentication in the IPv6 World (Transcript of Discussion) . . . . .	22
<i>Pekka Nikander</i>	
Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols . . . . .	27
<i>William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, Omer Reingold</i>	
Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols (Transcript of Discussion) . . . . .	40
<i>Matt Blaze</i>	
Thwarting Timing Attacks Using ATM Networks . . . . .	49
<i>Geraint Price</i>	
Thwarting Timing Attacks Using ATM Networks (Transcript of Discussion) . . . . .	59
<i>Geraint Price</i>	
Towards a Survivable Security Architecture for Ad-Hoc Networks . . . . .	63
<i>Tuomas Aura, Silja Mäki</i>	
Towards a Survivable Security Architecture for Ad-Hoc Networks (Transcript of Discussion) . . . . .	74
<i>Silja Mäki</i>	
PIM Security . . . . .	80
<i>Dieter Gollmann</i>	
PIM Security (Transcript of Discussion) . . . . .	82
<i>Dieter Gollmann</i>	
Merkle Puzzles Revisited – Finding Matching Elements between Lists . . . . .	87
<i>Bruce Christianson, David Wheeler</i>	

Merkle Puzzles Revisited (Transcript of Discussion) . . . . .	91
<i>Bruce Christianson</i>	
Encapsulating Rules of Prudent Security Engineering (Position Paper) . . . . .	95
<i>Jan Jürjens</i>	
Encapsulating Rules of Prudent Security Engineering (Transcript of Discussion) . . . . .	102
<i>Jan Jürjens</i>	
A Multi-OS Approach to Trusted Computer Systems . . . . .	107
<i>Hiroshi Yoshiura, Kunihiko Miyazaki, Shinji Itoh, Kazuo Takaragi, Ryoichi Sasaki</i>	
A Multi-OS Approach to Trusted Computer Systems (Transcript of Discussion) . . . . .	115
<i>Hiroshi Yoshiura</i>	
A Proof of Non-repudiation . . . . .	119
<i>Giampaolo Bella, Lawrence C. Paulson</i>	
A Proof of Non-repudiation (Transcript of Discussion) . . . . .	126
<i>Larry Paulson</i>	
Using Authority Certificates to Create Management Structures . . . . .	134
<i>Babak Sadighi Firozabadi, Marek Sergot, Olav Bandmann</i>	
Using Attribute Certificates for Creating Management Structures (Transcript of Discussion) . . . . .	146
<i>Babak Sadighi Firozabadi</i>	
Trust Management and Whether to Delegate . . . . .	151
<i>Simon N. Foley</i>	
Trust Management and Whether to Delegate (Transcript of Discussion) . . . . .	158
<i>Simon N. Foley</i>	
You Can't Take It with You (Transcript of Discussion) . . . . .	166
<i>Mark Lomas</i>	
Protocols Using Keys from Faulty Data . . . . .	170
<i>David Wheeler</i>	
Protocols Using Keys from Faulty Data (Transcript of Discussion) . . . . .	180
<i>David Wheeler</i>	

On the Negotiation of Access Control Policies . . . . .	188
<i>Virgil D. Gligor, Himanshu Khurana, Radostina K. Koleva,</i> <i>Vijay G. Bharadwaj, John S. Baras</i>	
Negotiation of Access Control Policies (Transcript of Discussion) . . . . .	202
<i>Virgil D. Gligor</i>	
Intrusion-Tolerant Group Management in Enclaves (Transcript of Discussion) . . . . .	213
<i>Hassen Saïdi</i>	
Lightweight Authentication in a Mobile Network (Transcript of Discussion) . . . . .	217
<i>James Malcolm</i>	
Bluetooth Security — Fact or Fiction? (Transcript of Discussion) . . . . .	221
<i>Peter Drabwell</i>	
Concluding Discussion When Does Confidentiality Harm Security? . . . . .	229
<i>Chair: Bruce Christianson</i>	
The Last Word . . . . .	239
<i>Thucydides</i>	
<b>Author Index</b> . . . . .	241



<http://www.springer.com/978-3-540-44263-9>

Security Protocols

9th International Workshop, Cambridge, UK, April 25-27,

2001 Revised Papers

Christianson, B.; Crispo, B.; Malcolm, J.A.; Roe, M. (Eds.)

2002, X, 246 p., Softcover

ISBN: 978-3-540-44263-9