

Table of Contents

Introduction	
<i>Bruce Christianson</i> (Transcript)	1
Keynote Address	
<i>Roger M. Needham</i>	2
Weak Authentication: How to Authenticate Unknown Principals without Trusted Parties	
<i>Jari Arkko* and Pekka Nikander</i>	5
Discussion	17
Is Entity Authentication Necessary?	
<i>Chris J. Mitchell* and Paulo S. Pagliusi</i>	20
Discussion	30
A Structured Operational Modelling of the Dolev-Yao Threat Model	
<i>Wenbo Mao</i>	34
Discussion	45
On Trust Establishment in Mobile <i>Ad-Hoc</i> Networks	
<i>Laurent Eschenauer*, Virgil D. Gligor*, and John Barras</i>	47
Discussion	63
Legally Authorized and Unauthorized Digital Evidence	
<i>Hiroshi Yoshiura*, Kunihiro Miyazaki, Shinji Itoh, Kazuo Takaragi,</i> <i>and Ryoichi Sasaki</i>	67
Discussion	71
Shrink-Wrapped Optimism: The DODA Approach to Distributed Document Processing	
<i>Bruce Christianson* and Jean F. Snook</i>	74
Discussion	87
Contractual Access Control	
<i>Babak Sadighi Firozabadi* and Marek Sergot</i>	96
Discussion	103
Confidentiality Levels and Deliberate/Indeliberate Protocol Attacks	
<i>Giampaolo Bella and Stefano Bistarelli*</i>	104
Discussion	119

VIII Table of Contents

Analyzing Delegation Properties	
<i>Giampaolo Bella and Lawrence C. Paulson*</i>	120
Discussion	126
Combinatorial Optimization of Countermeasures against Illegal Copying	
<i>Ryoichi Sasaki*, Hiroshi Yoshiura, and Shinji Itoh</i>	128
Discussion	144
Protocols with Certified-Transfer Servers	
<i>Raphael Yahalom</i>	145
Discussion	154
An Architecture for an Adaptive Intrusion-Tolerant Server	
<i>Alfonso Valdes, Magnus Almgren, Steven Cheung, Yves Deswarte,</i> <i>Bruno Dutertre, Joshua Levy, Hassen Saïdi, Victoria Stavridou*,</i> <i>and Tomás E. Uribe</i>	158
Discussion	178
Supporting Imprecise Delegation in KeyNote	
<i>Simon N. Foley</i>	179
Discussion	188
Modelling Protocols for Secure Group Communications in Ad Hoc Networks	
<i>Alec Yasinsac* and James A. Davis</i>	189
Discussion	202
Delegation of Signalling Rights	
<i>Pekka Nikander* and Jari Arkko</i>	203
Discussion	213
Mobile IPv6 Security	
<i>Tuomas Aura</i>	215
Discussion	229
Concluding Discussion: Accounting for Resources	
<i>All (Chair: Bruce Christianson) (Discussion)</i>	235
Back to the Beginning	
<i>Roger M. Needham</i>	242
Author Index	243

Security Protocols

10th International Workshop, Cambridge, UK, April

17-19, 2002, Revised Papers

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

2004, VIII, 248 p., Softcover

ISBN: 978-3-540-20830-3