

Contents

Inductive Analysis of the Internet Protocol TLS	
<i>Lawrence C. Paulson</i>	1
Discussion	13
External Consistency and the Verification of Security Protocols	
<i>Simon N. Foley</i>	24
Discussion	28
The Trust Shell Game	
<i>Carl Ellison</i>	36
Discussion	41
Overview of the AT&T Labs Trust-Management Project	
<i>Joan Feigenbaum</i>	45
Discussion	51
KeyNote: Trust Management for Public-Key Infrastructures	
<i>Matt Blaze, Joan Feigenbaum, Angelos D. Keromytis*</i>	59
Discussion - Trust Management	64
Application-Oriented Security Policies and Their Composition	
<i>Virgil D. Gligor* and Serban I. Gavrila</i>	67
Discussion	75
Secure Fingerprinting Using Public-Key Cryptography	
<i>Hiroshi Yoshiura, Ryoichi Sasaki* and Kazuo Takaragi</i>	83
Discussion	90
Third Party Certification of HTTP Service Access Statistics	
<i>Francesco Bergadano* and Pancrazio De Mauro</i>	95
Discussion	100
Delegating Trust	
<i>William S. Harbison</i> (Discussion)	108
Delegation of Responsibility	
<i>Bruno Crispo</i>	118
Discussion	125
Abuse of Process	
<i>Mark Lomas</i> (Discussion)	131

A New Concept in Protocols: Verifiable Computational Delegation	
<i>Peter Landrock</i>	137
Discussion	146
Delegation and Not-So Smart Cards	
<i>Bruce Christianson* and James A. Malcolm</i>	154
Discussion	158
Certification and Delegation	
<i>Michael Roe</i> (Discussion)	168
Discussion - Differences Between Academic and Commercial Security	
<i>Virgil Gligor, Peter Landrock, Mark Lomas, Raphael Yahalom</i> <i>and John Warne</i>	177
Optimistic Trust with Realistic eNvestigators	
<i>Raphael Yahalom</i>	193
Discussion	203
Insider Fraud	
<i>Dieter Gollmann</i>	213
Discussion	220
Panel Session - Future Directions	
<i>Stewart Lee, Joan Feigenbaum, Virgil Gligor and Bruce Christianson</i> <i>Chair: Roger Needham</i>	227
Contributor Index	241

Security Protocols

6th International Workshop, Cambridge, UK, April 15-17,
1998, Proceedings

Christianson, B.; Crispo, B.; Harbison, W.S.; Roe, M.
(Eds.)

1999, VIII, 252 p., Softcover

ISBN: 978-3-540-65663-0