

Table of Contents

Where Have All the Protocols Gone?	
<i>Bruce Christianson</i>	1
A Protocol's Life After Attacks...	
<i>Giampaolo Bella*, Stefano Bistarelli, Fabio Massacci</i>	3
Discussion	11
Towards Flexible Credential Negotiation Protocols	
<i>Piero A. Bonatti, Sabrina De Capitani di Vimercati, Pierangela Samarati*</i>	19
Discussion	24
Man-in-the-Middle in Tunnelled Authentication Protocols	
<i>N. Asokan*, Valtteri Niemi, Kaisa Nyberg</i>	28
Discussion	42
Towards a Framework for Autonomic Security Protocols	
<i>Simon N. Foley*, Hongbin Zhou</i>	49
Discussion	55
Client v. Server Side Protocols, Interfaces and Storage	
<i>Geraint Price</i>	63
Discussion	74
Guaranteeing Access in Spite of Distributed Service-Flooding Attacks	
<i>Virgil D. Gligor</i>	80
Discussion	97
Protocol Codesign	
<i>Hassen Saidi, Victoria Stavridou*, Bruno Duterte</i>	106
Discussion	114
Enforcing Security Policies for Distributed Objects Applications	
<i>Bogdan C. Popescu*, Bruno Crispo, Andrew S. Tanenbaum, Maas Zeeman</i>	119
Discussion	131

Regular SPKI

<i>Mads Dam</i>	134
Discussion	151

Federated Identity-Management Protocols

<i>Birgit Pfitzmann*, Michael Waidner</i>	153
Discussion	175

Enforcing the Unenforceable

<i>Peter Y.A. Ryan</i>	178
------------------------------	-----

Is the Verification Problem for Cryptographic Protocols Solved?

<i>Giampaolo Bella, Cristiano Longo, Lawrence Paulson*</i>	183
--	-----

Secure Sessions from Weak Secrets

<i>Bruce Christianson*, Michael Roe, David Wheeler</i>	190
Discussion	206

Panel Session: Is Protocol Modelling Finished?

<i>Mike Roe</i>	213
-----------------------	-----

WAR: Wireless Anonymous Routing

<i>Matt Blaze*, John Ioannidis, Angelos D. Keromytis, Tal Malkin,</i> <i>Avi Rubin</i>	218
Discussion	233

Limitations of IPsec Policy Mechanisms

<i>Jari Arkko*, Pekka Nikander</i>	241
Discussion	252

Deniable Authenticated Key Establishment for Internet Protocols

<i>Colin Boyd, Wenbo Mao*, Kenneth G. Paterson</i>	255
Discussion	272

Protocols for Supporting a Public Key Infrastructure in Ad Hoc Networks

<i>Mike Burmester, Alec Yasinsac*</i>	274
Discussion	283

What We Can Learn from API Security

<i>Ross Anderson</i>	288
----------------------------	-----

Addressing New Challenges by Building Security Protocols Around Graphs	
<i>Kamil Kulesza*, Zbigniew Kotulski</i>	301
From Security Protocols to System Security	
<i>Brian Monahan</i>	307
Discussion	323
Biometrics to Enhance Smartcard Security	
<i>Giampaolo Bella, Stefano Bistarelli, Fabio Martinelli*</i>	324
Discussion	333
Blind Publication: A Copyright Library without Publication or Trust	
<i>James A. Malcolm</i>	336
Discussion	341
And Finally	350
Author Index	351