1. Record Nr. UNISA996465920903316

Titolo	Security Protocols [[electronic resource]] : 11th International Workshop, Cambridge, UK, April 2-4, 2003, Revised Selected Papers / / edited by Bruce Christianson, Bruno Crispo, James A. Malcolm, Michael Roe
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (X, 354 p.)
Collana	Security and Cryptology ; ; 3364
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Algorithms Management information systems Computer science Computers and civilization Operating systems (Computers) Cryptology Computer Communication Networks Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Computers and Society Operating Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"11th in our series of International Workshops on Security Protocols"--Pref.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Where Have All the Protocols Gone? -- A Protocol’s Life After Attacks... -- A Protocol’s Life After Attacks... -- Towards Flexible Credential Negotiation Protocols -- Towards Flexible Credential Negotiation Protocols -- Man-in-the-Middle in Tunnelled Authentication Protocols -- Man-in-the-Middle in Tunnelled Authentication Protocols -- Towards a Framework for Autonomic Security Protocols -- Towards a Framework for Autonomic Security Protocols -- Client v. Server Side

Protocols, Interfaces and Storage -- Client v. Server Side Protocols, Interfaces and Storage -- Guaranteeing Access in Spite of Distributed Service-Flooding Attacks -- Guaranteeing Access in Spite of Distributed Service-Flooding Attacks -- Protocol Codesign -- Protocol Codesign -- Enforcing Security Policies for Distributed Objects Applications -- Enforcing Security Policies for Distributed Objects Applications -- Regular SPKI -- Regular SPKI -- Federated Identity-Management Protocols -- Federated Identity-Management Protocols -- Enforcing the Unenforceable -- Is the Verification Problem for Cryptographic Protocols Solved? -- Secure Sessions from Weak Secrets -- Secure Sessions from Weak Secrets -- Panel Session: Is Protocol Modelling Finished? -- WAR: Wireless Anonymous Routing -- WAR: Wireless Anonymous Routing -- Limitations of IPsec Policy Mechanisms -- Limitations of IPsec Policy Mechanisms -- Deniable Authenticated Key Establishment for Internet Protocols -- Deniable Authenticated Key Establishment for Internet Protocols -- Protocols for Supporting a Public Key Infrastructure in Ad Hoc Networks -- Protocols for Supporting a Public Key Infrastructure in Ad Hoc Networks -- What We Can Learn from API Security -- Addressing New Challenges by Building Security Protocols Around Graphs -- From Security Protocols to Systems Security -- From Security Protocols to Systems Security -- Biometrics to Enhance Smartcard Security -- Biometrics to Enhance Smartcard Security -- Blind Publication: A Copyright Library without Publication or Trust -- Blind Publication: A Copyright Library Without Publication or Trust.

Sommario/riassunto

Greetings. These are the proceedings of the 11th in our series of International Workshops on Security Protocols. Our theme this time was “Where have all the Protocols gone?” Once upon a time security protocols lived mainly in the network and transport layers. Now they increasingly hide in applications, or in specialised hardware. Does this trend lead to better security architectures, or is it an indication that we are addressing the wrong problems? The intention of the workshops is to provide a forum where incompletely workedoutideascanstimulatediscussion,openupnewlinesofinvestigation, and suggestmoreproblems. The positionpaperspublished herehavebeen revisedby the authors in the light of their participation in the workshop. In addition, we publish edited transcripts of some of the discussions, to give our readers access to some of the roads ahead not (yet) taken. We hope that these revised position papers and edited transcripts will give you at least one interesting idea of your own to explore. Please do write and tell us what it was. Our purpose in publishing these proceedings is to produce a conceptual map which will be of enduring interest, rather than to be merely topical. This is perhaps just as well, given the delay in production. This year we moved to new computer-based recording technology, and of course it failed completely.