1. Record Nr. UNINA9910144210003321

Titolo	Security Protocols : 10th International Workshop, Cambridge, UK, April 17-19, 2002, Revised Papers / / edited by Bruce Christianson, Bruno Crispo, James A. Malcolm, Michael Roe
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	3-540-39871-6
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (VIII, 248 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2845
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer networks Operating systems (Computers) Algorithms Computers and civilization Management information systems Computer science Cryptology Computer Communication Networks Operating Systems Algorithm Analysis and Problem Complexity Computers and Society Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	(Transcript) -- Keynote Address -- Weak Authentication: How to Authenticate Unknown Principals without Trusted Parties -- Is Entity Authentication Necessary? -- A Structured Operational Modelling of the Dolev-Yao Threat Model -- On Trust Establishment in Mobile Ad-Hoc Networks -- Legally Authorized and Unauthorized Digital Evidence -- Shrink-Wrapped Optimism: The DODA Approach to Distributed Document Processing -- Contractual Access Control -- Confidentiality Levels and Deliberate/Indeliberate Protocol Attacks -- Analyzing

Delegation Properties -- Combinatorial Optimization of Countermeasures against Illegal Copying -- Protocols with Certified-Transfer Servers -- An Architecture for an Adaptive Intrusion-Tolerant Server -- Supporting Imprecise Delegation in KeyNote -- Modeling Protocols for Secure Group Communications in Ad Hoc Networks -- Delegation of Signalling Rights -- Mobile IPv6 Security -- Concluding Discussion: Accounting for Resources -- Back to the Beginning.

Sommario/riassunto

Once again we bring you the proceedings of the International Workshop on Security Protocols. It seems hard to believe that we have reached the tenth event in this annual series. This year our theme was “Discerning the Protocol Participants.” Security protocols are usually described in terms of the active participants – Alice c- putes foo and sends it to Bob. However most security protocols also include o?-line participants, which are not synchronously involved in the exchange of messages: a bank may participate on behalf of a customer, and an arbiter may subsequently be asked to interpret the meaning of a run. These silent partners to the protocol have their own security policies, and assumptionsaboutidentity,authorizationandcapabilityneedtobere-examined when the agenda of a hidden participant may change. We hope that the position papers published here, which have been rewritten and rethought in the light of the discussions at the workshop, will be of interest, not just for the speci?c contributions they make but also for the deeper issues which they expose. In order to identify these issues more clearly, we include transcripts for some of the discussions which took place in Cambridge during the workshop. What would you have liked to add? Do let us know.