

1. Record Nr.	UNINA9910484673403321
Titolo	Security Protocols : 12th International Workshop, Cambridge, UK, April 26-28, 2004. Revised Selected Papers // edited by Bruce Christianson, Bruno Crispo, James A. Malcolm, Michael Roe
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-40926-2
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (X, 390 p.)
Collana	Security and Cryptology ; ; 3957
Disciplina	005.8
Soggetti	Computer communication systems Data encryption (Computer science) Algorithms Management information systems Computer science Computers and civilization Operating systems (Computers) Computer Communication Networks Cryptology 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	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Introduction: Authentic Privacy -- Limits to Anonymity When Using Credentials -- Limits to Anonymity When Using Credentials (Transcript of Discussion) -- A Cryptographic Framework for the Controlled Release of Certified Data -- A Cryptographic Framework for the Controlled Release of Certified Data (Transcript of Discussion) -- One User, Many Hats; and, Sometimes, No Hat: Towards a Secure Yet Usable PDA -- One User, Many Hats; and Sometimes, No Hat (Transcript of Discussion) -- Authentication Components: Engineering Experiences

and Guidelines -- Authentication Components: Engineering Experiences and Guidelines (Transcript of Discussion) -- Accountable Privacy -- Accountable Privacy (Transcript of Discussion) -- Toward a Broader View of Security Protocols -- Toward a Broader View of Security Protocols (Transcript of Discussion) -- Privacy, Control and Internet Mobility -- Privacy, Control and Internet Mobility (Transcript of Discussion) -- Controlling Who Tracks Me -- Controlling Who Tracks Me (Transcript of Discussion) -- BLIND: A Complete Identity Protection Framework for End-Points -- BLIND: A Complete Identity Protection Framework for End-Points (Transcript of Discussion) -- Privacy Is Linking Permission to Purpose -- Privacy is Linking Permission to Purpose (Transcript of Discussion) -- Establishing Trust with Privacy -- Establishing Trust with Privacy (Transcript of Discussion) -- Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System -- Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System (Transcript of Discussion) -- The Dancing Bear: A New Way of Composing Ciphers -- The Dancing Bear: A New Way of Composing Ciphers (Transcript of Discussion) -- Identity and Location -- Identity and Location (Transcript of Discussion) -- Security of Emergent Properties in Ad-Hoc Networks (Transcript of Discussion) -- Pseudonymity in the Light of Evidence-Based Trust -- Pseudonymity in the Light of Evidence-Based Trust (Transcript of Discussion) -- Secure Processor Consistent with Both Foreign Software Protection and User Privacy Protection -- Secure Processor Consistent with Both Foreign Software Protection and User Privacy Protection (Transcript of Discussion) -- Why Are We Authenticating (Transcript of Discussion) -- Anonymous Authentication -- Anonymous Authentication (Transcript of Discussion) -- Towards a Mechanism for Discretionary Overriding of Access Control -- Towards a Mechanism for Discretionary Overriding of Access Control (Transcript of Discussion) -- Last Orders.

Sommario/riassunto

Here are the proceedings of the 12th International Workshop on Security Protocols. We hope that you will enjoy them, and that they will cause you to think at least one heretical thought. Please write or e-mail and share it with us. Our theme this workshop was "Authentic Privacy." Traditionally we have based authentication upon a rather strong notion of identity, and have then built other security services on top of authentication. Perhaps if we want a more nuanced notion of privacy, then we need to re-examine some of our assumptions, particularly when attackers and defenders share the same resources and infrastructure. The position papers published here have been revised by the participants in the workshop, and are followed by edited (heavily in some cases) transcripts of parts of the discussions which they led. Our thanks to Sidney Sussex College Cambridge for the use of their facilities, to Johanna Hunt at the University of Hertfordshire for organizing the logistics of the workshop and orchestrating the production of these proceedings, to Lori Klimaszewska of the University of Cambridge Computing Service for transcribing the audio tapes (in which "viruses without halos" could have caused havoc but didn't), and to Donald Hunt for impeccable copy editing. Finally, it is both a sadness and a pleasure to pay our tribute to David Wheeler, one of the original forty-niners at the Cambridge Computer Laboratory and author of the initial orders for EDSAC. The second version of initial orders is the Platonic bootstrap.
