1.	Record Nr.	UNISA996465521003316
	Titolo	Security Protocols [[electronic resource]] : 9th International Workshop, Cambridge, UK, April 25-27, 2001 Revised Papers / / edited by Bruce Christianson, Bruno Crispo, James A. Malcolm, Michael Roe
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2002
	ISBN	3-540-45807-7
	Edizione	[1st ed. 2002.]
	Descrizione fisica	1 online resource (X, 246 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2467
	Disciplina	005.8
	Soggetti	Data encryption (Computer science) Algorithms Computer communication systems Management information systems Computer science Computers and civilization Operating systems (Computers) Cryptology Algorithm Analysis and Problem Complexity Computer Communication Networks 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 at the end of each chapters and index.
	Nota di contenuto	Keynote Address: Mobile Computing versus Immobile Security -- Experiences of Mobile IP Security -- Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World -- Denial of sService, Address Ownership, and Early Authentication in the IPv6 World -- Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols -- Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols -- Thwarting Timing Attacks Using ATM Networks -- Thwarting Timing

Attacks Using ATM Networks -- Towards a Survivable Security Architecture for Ad-Hoc Networks -- Towards a Survivable Security Architecture for Ad-Hoc Networks -- PIM Security -- PIM Security -- Merkle Puzzles Revisited — Finding Matching Elements between Lists -- Merkle Puzzles Revisited -- Encapsulating Rules of Prudent Security Engineering -- Encapsulating Rules of Prudent Security Engineering -- A Multi-OS Approach to Trusted Computer Systems -- A Multi-OS Approach to Trusted Computer Systems -- A Proof of Non-repudiation -- A Proof of Non-repudiation -- Using Authority Certificates to Create Management Structures -- Using Attribute Certificates for Creating Management Structures -- Trust Management and Whether to Delegate -- Trust Management and Whether to Delegate -- You Can’t Take It with You -- Protocols Using Keys from Faulty Data -- Protocols Using Keys from Faulty Data -- On the Negotiation of Access Control Policies -- Negotiation of Access Control Policies -- Intrusion-Tolerant Group Management in Enclaves -- Lightweight Authentication in a Mobile Network -- Bluetooth Security — Fact or Fiction? -- Concluding Discussion When Does Confidentiality Harm Security? -- The Last Word.

Sommario/riassunto

Hello and welcome. These are the proceedings of the 9th International Workshop on Security Protocols, the ?rst to be held in the new millennium. This year our theme was “mobile computing versus immobile security”. As usual, the insights and challenges which emerged during the workshop are re?ected in the position papers, which appear here in rewritten form. Transcripts are also included of the discussions which took place in C- bridge as the initial versions were presented. These transcripts are intended to provide a perspective on lines of argument which are worth pursuing further. Our desire is that you will join with us in this activity, and that as a result you will, like many of our participants, feel moved to propound something quite di?erent from what you originally planned. Our thanks as always to Prof. Roger Needham, FRS and to Microsoft - search Ltd. (Cambridge) for the use of the meeting room and co?ee machine. Thanks also to Lori Klimaszewska of the University of Cambridge Computing Service for transcribing the audio tapes (and for revealing in “Audrey James” a previously unsuspected double life of a well-known double agent), and to Dr. Mary Buchanan for her assistance in editing the transcripts into a Thucydidean mould. Actually, we are often asked how we go about producing the transcripts, especially upon those occasions when, for various reasons, no audio recording was made. This year we bow to pressure and reveal the details of our methodology in the Afterword.