

1. Record Nr.	UNINA9910143903903321
Titolo	Infrastructure Security : International Conference, InfraSec 2002 Bristol, UK, October 1-3, 2002 Proceedings // edited by George Davida, Yair Frankel, Owen Rees
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2002
ISBN	3-540-45831-X
Edizione	[1st ed. 2002.]
Descrizione fisica	1 online resource (XII, 340 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2437
Disciplina	005.8
Soggetti	Seguridad informática Computer Communication Networks Operating Systems Management of Computing and Information Systems Cryptology Database Management Computers and Society
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	Biometrics -- Biometric Authentication in Infrastructure Security -- Denial of Access in Biometrics-Based Authentication Systems -- Identification, Authentication, and Process -- A Novel Approach to Proactive Password Checking -- Single Sign-On Architectures -- Active Digital Credentials: Dynamic Provision of Up-to-Date Identity Information -- Analysis Process -- How to Buy Better Testing Using Competition to Get the Most Security and Robustness for Your Dollar -- Structured Risk Analysis -- A Model Enabling Law Compliant Privacy Protection through the Selection and Evaluation of Appropriate Security Controls -- Mobile Networks -- Authentication and Authorization of Mobile Clients in Public Data Networks -- A Contemporary Foreword on GSM Security -- Vulnerability Assessment and Logs -- Vulnerability Assessment Simulation for Information Infrastructure Protection -- Pseudonymizing Unix Log Files -- System Design -- DPS: An Architectural Style for Development of Secure Software -- A New

Infrastructure for User Tracking Prevention and Privacy Protection in Internet Shopping -- Different Smartcard-Based Approaches to Physical Access Control -- Formal Methods -- Authenticity and Provability — A Formal Framework -- Protocol Engineering Applied to Formal Analysis of Security Systems -- Cryptographic Techniques -- Applications of Multiple Trust Authorities in Pairing Based Cryptosystems -- Plausible Deniability Using Automated Linguistic Stegonagraphy -- Virtual Software Tokens - A Practical Way to Secure PKI Roaming -- Bit-Serial AOP Arithmetic Architectures over  $GF(2^m)$  -- Networks -- A Practical Distributed Authorization System for GARA -- Design of a VPN Software Solution Integrating TCP and UDP Services.

---

## Sommario/riassunto

Infrastructure Security Conference 2002 (InfraSec 2002) was created to promote security research and the development of practical solutions in the security of infrastructures – both government and commercial – such as the effective prevention of, detection of, reporting of, response to and recovery from security incidents. The conference, sponsored by the Datacard Group and Hewlett-Packard Laboratories, was held on October 1–3, 2002. Organizational support was provided by the Center for Cryptography, Computer and Network Security Center at the University of Wisconsin- Milwaukee. Organizing a conference is a major undertaking requiring the efforts of many individuals. The Conference President, Graham Higgins (Datacard Group), oversaw all arrangements for the conference, and the General Chair, Susan Thompson (Datacard Group), oversaw the local organization and registration. Local arrangements were directed by Jan Ward (Hewlett-Packard Laboratories) and Jamie Wilson (Datacard Group). Financial arrangements were managed by Natalie Churchill (Hewlett-Packard Laboratories). We wish to thank the organizers, without whose support this conference would not have been possible. This conference program included two keynote speakers: Bob Evans (Office of the e-Envoy) and Vic Maconachy (Department of Defense). The program committee considered 44 submissions of which 23 papers were accepted. Each submitted paper was reviewed by a minimum of three referees. These proceedings contain revised versions of the accepted papers. Revisions were not checked and the authors bear full responsibility for the content of their papers.

---