1. **Record Nr.** UNISA996465951903316

Titolo Financial cryptography and data security : 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12-16, 2007 : revised selected papers / / Sven Dietrich, Rachna Dhamija (eds.)

Pubbl/distr/stampa Berlin ; ; Heidelberg : , : Springer, , [2007]
Â©2007

ISBN 3-540-77366-5

Edizione [1st ed. 2007.]

Descrizione fisica 1 online resource (XII, 392 p.)

Collana Lecture Notes in Computer Science ; ; 4886

Disciplina 005.8

Soggetti Computer security

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 Keynote Address -- Leaving Room for the Bad Guys -- Payment Systems -- Vulnerabilities in First-Generation RFID-enabled Credit Cards -- Conditional E-Cash -- A Privacy-Protecting Multi-Coupon Scheme with Stronger Protection Against Splitting -- Panel -- Panel: RFID Security and Privacy -- Position Statement in RFID S&P Panel: RFID and the Middleman -- Position Statement in RFID S&P Panel: Contactless Smart Cards -- Position Statement in RFID S&P Panel: From Relative Security to Perceived Secure -- Anonymity -- A Model of Onion Routing with Provable Anonymity -- K-Anonymous Multi-party Secret Handshakes -- Authentication -- Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer -- Scalable Authenticated Tree Based Group Key Exchange for Ad-Hoc Groups -- On Authentication with HMAC and Non-random Properties -- Anonymity and Privacy -- Hidden Identity-Based Signatures -- Space-Efficient Private Search with Applications to Rateless Codes -- Cryptography and Commercial Transactions -- Cryptographic Securities Exchanges -- Improved Multi-party Contract Signing -- Informant: Detecting Sybils Using Incentives -- Financial Transactions and Web Services -- Dynamic Virtual Credit Card Numbers -- The Unbearable Lightness of PIN Cracking -- Panel -- Virtual Economies: Threats and

Risks -- Invited Talk -- Usable SPACE: Security, Privacy, and Context for the Mobile User -- System Presentation -- Personal Digital Rights Management for Mobile Cellular Devices -- Cryptography -- Certificate Revocation Using Fine Grained Certificate Space Partitioning -- An Efficient Aggregate Shuffle Argument Scheme -- Usable Security Workshop -- Preface -- Full Papers -- An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks -- WSKE: Web Server Key Enabled Cookies -- Usability Analysis of Secure Pairing Methods -- Low-Cost Manufacturing, Usability, and Security: An Analysis of Bluetooth Simple Pairing and Wi-Fi Protected Setup -- Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers -- Short Papers -- What Instills Trust? A Qualitative Study of Phishing -- Phishing IQ Tests Measure Fear, Not Ability -- Mental Models of Security Risks -- Improving Usability by Adding Security to Video Conferencing Systems -- A Sense of Security in Pervasive Computing— Is the Light on When the Refrigerator Door Is Closed?.

| Sommario/riassunto | The 11th International Conference on Financial Cryptography and Data Security (FC 2007, http://fc07. ifca. ai), organized by the International Financial Crypt- raphy Association (IFCA, http://www. ifca. ai/), was held in Tobago, February 12–15, 2007. The conference is a well-established and premier international - rum for research, advanced development, education, exploration, and debate - garding security in the context of ?nance and commerce. We continue to cover all aspects of securing transactions and systems, which this year included a range of technical areas such as cryptography, payment systems, anonymity, privacy, - thentication, and commercial and ?nancial transactions. For the ?rst time, there was an adjacent workshop on Usable Security, held after FC 2007 in the same - cation. The papers are included in the last part of this volume. The conference goal was to bring together top cryptographers, data-security specialists, and c- puter scientists with economists, bankers, implementers, and policy makers. The goal was met this year: there were 85 submissions, out of which 17 research papers and 1 system presentation paper were accepted. In addition, the conference featured two distinguished speakers, Mike Bond and Dawn Jutla, and two panel sessions, one on RFID and one on virtual economies. As always, there was the rump session on Tuesday evening, colorful as usual. |