1. Record Nr. UNINA9910483382603321

Titolo	Technology and Practice of Passwords : 9th International Conference, PASSWORDS 2015, Cambridge, UK, December 7-9, 2015, Proceedings / / edited by Frank Stajano, Stig F. Mjølsnes, Graeme Jenkinson, Per Thorsheim
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-29938-7
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XV, 151 p. 19 illus. in color.)
Collana	Security and Cryptology ; ; 9551
Disciplina	005.82
Soggetti	Computer security Computer communication systems Data encryption (Computer science) Management information systems Computer science Algorithms Computers and civilization Systems and Data Security Computer Communication Networks Cryptology Management of Computing and Information Systems Algorithm Analysis and Problem Complexity 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	Intro -- Preface -- Organization -- Non-refereed Presentations -- Contents -- Human Factors -- Expert Password Management -- 1 Introduction -- 2 Background -- 2.1 Coping Strategies -- 2.2 Security Practices of Experts and Non-Experts -- 3 Study -- 4 Results Overview -- 5 Thematic Analysis -- 5.1 Expert Awareness -- 5.2 Combining Strategies to Remember Passwords -- 5.3 A Personal Assessment of Risk -- 5.4 Usability Problems -- 6 Discussion -- 6.1 What Do Experts

Do Right? -- 6.2 What Do Experts Do Wrong? -- 7 Conclusion -- References -- Assessing the User Experience of Password Reset Policies in a University -- 1 Introduction -- 2 Related Work -- 3 Methodology -- 3.1 Systems Under Analysis -- 3.2 Helpdesk Log Analysis -- 3.3 User Interviews -- 3.4 NASA Raw Task Load Index (NASA-RTLX) -- 4 Results: Helpdesk Log Analysis -- 4.1 Results -- 5 Results: User Interviews and NASA-RTLX -- 5.1 Results -- 5.2 RTLX Data Analysis -- 6 Discussion -- 6.1 Recommendations for Practitioners -- 7 Conclusions -- References -- Analyzing 4 Million Real-World Personal Knowledge Questions (Short Paper) -- 1 Introduction -- 1.1 Related Work -- 2 Methodology -- 3 Strength Evaluation -- 4 Conclusion -- References -- ITSME: Multi-modal and Unobtrusive Behavioural User Authentication for Smartphones -- 1 Introduction -- 2 Related Work -- 2.1 Unimodal Systems -- 2.2 Multimodal Systems -- 3 Background -- 3.1 Considered Sensors -- 3.2 Considered Classifiers -- 3.3 Performance Metric -- 4 Our Solution -- 4.1 Setup -- 4.2 Data Collection -- 4.3 Feature Extraction -- 4.4 Data Fusion -- 4.5 Decision Making -- 5 Parameters -- 5.1 Parameters -- 6 Results -- 6.1 Unimodal Systems -- 6.2 Multimodal Systems -- 7 Discussion -- 8 Conclusion and Future Work -- References -- Attacks -- Verification Code Forwarding Attack (Short Paper) -- 1 Introduction.
2 SMS-Based Verification and Its Security -- 3 Study Procedures -- 3.1 Experiment -- 3.2 Semi-structured Interview -- 3.3 Survey -- 4 Conclusion -- References -- What Lies Beneath? Analyzing Automated SSH Bruteforce Attacks -- 1 Introduction -- 2 Related Work -- 3 Data Collection Methodology -- 4 Characteristics of Attacking Systems -- 4.1 Number of IPs per /24 -- 4.2 Countries with the Most Aggressive Sources -- 4.3 IP Addresses as a Ratio of the Total Allocation per Country -- 5 Password Analysis -- 5.1 Password Length -- 5.2 Password Composition Compared to Known Dictionaries -- 5.3 Dictionary Sharing and Splitting Among Sources -- 5.4 Reattempting Username-Password Combination -- 6 Username Analysis -- 7 Timing Analysis -- 8 Recommendations -- 9 Conclusion -- References -- Cryptography -- Catena Variants -- 1 Introduction -- 2 Preliminaries -- 2.1 Notational Conventions -- 2.2 Catena -- 3 Hash-Function Instantiations -- 4 Using Different Graphs -- 4.1 (g,)-Bit-Reversal Graph -- 4.2 Shifted (g,)-Bit-Reversal Graph -- 4.3 (g,,)-Gray-Reverse Graph -- 4.4 Tradeoff Resistance -- 5 Extensions -- 6 Discussion and Recommendations -- 7 Conclusion -- A Memory-Hardness and Garbage-Collector Attacks -- A.1 Memory-Hardness -- A.2 (Weak) Garbage-Collector Attacks -- B Hash-Function Instantiations -- B.1 Compression Function of Argon2 -- B.2 BlaMka -- B.3 Galois-Field Multiplication -- B.4 MultHash -- C Extensions of Catena -- C.1 Password-Independent Random Layer -- C.2 Password-Dependent Random Layer -- D Penalties Caused by Shifting Sampling Points -- References -- On Password-Authenticated Key Exchange Security Modeling -- 1 Introduction -- 2 Different BPR-style Models -- 2.1 The Models' Main Foundations -- 2.2 Differences in Accepting, Terminating, and Partnering -- 2.3 A Bug in the RoR Model -- 3 A Well-Motivated Definition -- 3.1 The Definition Itself.
3.2 Examples of How It Functions -- 4 The Quality of Partner Uniqueness -- 4.1 An Obstacle Caused by the test query -- 4.2 A ``secure'' PAKE Protocol Where Non-negligible Multiple Partnering May Occur -- 4.3 Lessons Learned on Requirements -- 5 Conclusion and Future Work -- A BPR-style Models Revisited -- References -- Strengthening Public Key Authentication Against Key Theft (Short Paper) -- 1 Introduction -- 1.1 Threat Model -- 2 Revocable Public Key Authentication -- 2.1 Basic RSA Authentication -- 2.2 The Mediator

	Service -- 3 Rate Limiting Password Guesses -- 3.1 Key Fragment Encryption -- 3.2 Authenticating Requests to the Mediator -- 4 Conclusion -- References -- Author Index.
Sommario/riassunto	This book constitutes the thoroughly refereed post-conference proceedings of the 9th International Conference on Passwords, PASSWORDS 2015, held in Cambridge, UK, in December 2015. The 6 revised full papers presented together with 3 revised short papers were carefully reviewed and selected from 32 initial submissions. The papers are organized in topical sections on human factors, attacks, and cryptography.