1. Record Nr. UNISA996202527503316

Titolo	Communications and Multimedia Security [[electronic resource]] : 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014, Proceedings / / edited by Bart De Decker, André Zúquete
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2014
ISBN	3-662-44885-8
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (XII, 157 p. 37 illus.)
Collana	Security and Cryptology ; ; 8735
Disciplina	005.8
Soggetti	Computer security Biometrics (Biology) Computer communication systems E-commerce Data encryption (Computer science) Management information systems Computer science Systems and Data Security Biometrics Computer Communication Networks e-Commerce/e-business Cryptology Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Preface -- Organization -- Table of Contents -- Part I: Research Papers -- Malicious MPLS Policy Engine Reconnaissance -- 1 Introduction -- 2 Related Work -- 3 MPLS Policy Engine -- 4 Policy Engine State Analysis Design -- 4.1 Network Model -- 4.2 Adversary Model -- 4.3 Probe Elements -- 4.4 Simulation Scenarios -- 5 Analysis Results -- 5.1 Probing Process Validation -- 5.2 Policy Reveal -- 6 MPLS Policy States Probability -- 7 Conclusions -- References -- USB

Connection Vulnerabilities on Android Smartphones: Default and Vendors' Customizations -- 1 Introduction -- 2 Attack Scenario -- 3 Vulnerabilities -- 3.1 AT COMMANDS -- 3.2 Vulnerabilities Disc covered and AT Samsung Proprietary Commands -- 3.3 ADB Enabled -- 4 Anatomy of the Attack (Script) -- 4.1 Architecture -- 4.2 Using the Vulnerabilities Found -- 5 Conclusion -- References -- Free Typed Text Using Keystroke Dynamics for Continuous Authentication -- 1 Introduction -- 2 Biometrics and Keystroke Dynamics -- 3 State of the Art -- 4 Software Design and Algorithm -- 4.1 Architecture -- 4.2 Absolute Scores -- 4.3 Relative Scores -- 4.4 Decision Criterion -- 4.5 Parameter Space -- 5 Validation -- 5.1 Tool Description for Artificial Attacks -- 5.2 Acceptance Neighbourhoods Study -- 5.3 Transients Study for Sample Reduction -- 5.4 Weights Study -- 5.5 ROC Curve -- 5.6 Evaluations Scheme -- 6 Conclusions -- References -- Secure Storage on Android with Context-Aware Access Control -- 1 Introduction -- 2 Related Work -- 3 General Approach -- 3.1 Security Requirements -- 3.2 Usability Requirements -- 3.3 Interoperability Requirements -- 3.4 Assumptions -- 3.5 Architecture -- 4 Secure Asset Storage -- 4.1 Protocols -- 5 Context-Aware Asset Management -- 6 Prototype: Context-Aware File Management -- 6.1 File Server -- 6.2 Administration Component -- 6.3 Mobile Component -- 7 Evaluation.
8 Conclusions and Future Work -- References -- Part II: Work in Progress -- A Study on Advanced Persistent Threats -- 1 Introduction -- 2 Definition: What Is APT? -- 3 Attack Model: How Does APT Work? -- 3.1 Phases of an APT Attack -- 3.2 Case Study of APT Attacks -- 3.3 Countermeasures -- 4 Related Work -- 5 Conclusion -- References -- Dynamic Parameter Reconnaissance for Stealthy DoS Attack within Cloud Systems -- 1 Introduction -- 2 Attack Mechanism Outline -- 3 Threat Model -- 4 Literature Review -- 5 Estimating Cloud Migration Parameters -- 6 Analysis and Discussion -- 7 Conclusions and Future Work -- References -- Touchpad Input for Continuous Biometric Authentication -- 1 Introduction -- 2 Related Work -- 3 Data Collection -- 4 Results -- 5 Discussions and Conclusions -- References -- A Federated Cloud Identity Broker-Model for Enhanced Privacy via Proxy Re-Encryption -- 1 Introduction -- 2 Federated Cloud Identity Broker-Model -- 2.1 Cryptographic Preliminaries -- 2.2 Model Architecture -- 2.3 Requirements -- 3 Concrete Model and Proof of Concept -- 3.1 Components -- 3.2 Communication Interfaces -- 3.3 Process Flows -- 4 Evaluation and Discussion -- 5 Conclusions and Future Work -- References -- D-Shuffle for Pret ˆ`a Voter -- 1 Introduction -- 1.1 Pret ˆa `Voter Overview -- 1.2 Motivation and Contribution -- 2 The Design of the Verifiable D-Shuffle -- 2.1 Intuition Behind the Design -- 2.2 The Construction of the D-Shuffle -- 2.3 Security of the D-Shuffle -- 2.4 On Instantiations of the D-Shuffle -- 2.5 On the Efficiency of D-Shuffle -- 3 The D-Shuffle Used for Pret ˆa `Voter -- 4 Conclusion -- References -- A Secrecy of the D-Shuffle -- B Non-interactive Zero knowledge proofs -- An Approach to Information Security Policy Modeling for Enterprise Networks -- 1 Introduction -- 2 Related Work -- 3 A Policy Model -- 4 A Policy Algebra.
5 Conclusion -- References -- Part III: Extended Abstracts -- Introduction to Attribute Based Searchable Encryption -- 1 Introduction -- 2 Formal Definition of ABSE -- 3 Conclusion -- References -- Risk Analysis of Physically Unclonable Functions -- 1 Introduction -- 2 Physically Unclonable Functions -- 3 Risk Analysis -- 4 Conclusion and Outlook -- References -- Decentralized Bootstrap for Social Overlay Networks -- 1 Introduction -- 1.1 Problem -- 1.2 Contribution -- 2

Decentralized Bootstrap for Our Social Overlay Network -- 3 Conclusions and Future Work -- References -- Part IV: Keynotes -- Enhancing Privacy with Quantum Networks -- 1 Introduction -- 2 Preliminaries -- 3 Oblivious Transfer -- 4 Conclusions -- References -- The Fundamental Principle of Breach Prevention -- 1 Introduction -- 2 What Is a Malicious Insider? -- 3 Data-Centric Security -- 4 Information Security "Rules of Thumb" -- Author Index.

Sommario/riassunto

This book constitutes the refereed proceedings of the 15th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security, CMS 2014, held in Aveiro, Portugal, in September 2014. The 4 revised full papers presented together with 6 short papers, 3 extended abstracts describing the posters that were discussed at the conference, and 2 keynote talks were carefully reviewed and selected from 22 submissions. The papers are organized in topical sections on vulnerabilities and threats, identification and authentification, applied security.