1. Record Nr. UNINA9910708392603321

Titolo	Prisoner release in the District of Columbia : the role of halfway houses and community supervision in prisoner rehabilitation : hearing before the Subcommittee on the District of Columbia of the Committee on Government Reform, House of Representatives, One Hundred Seventh Congress, first session, July 20, 2001
Pubbl/distr/stampa	Washington : , : U.S. Government Printing Office, , 2001
Descrizione fisica	1 online resource (iii, 160 pages)
Soggetti	Prisoners - Washington (D.C.) Halfway houses - Washington (D.C.) Community-based corrections - Washington (D.C.) Legislative hearings.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Distributed to some depository libraries in microfiche. "Serial no. 107-23."
Nota di bibliografia	Includes bibliographical references.

2. Record Nr. UNINA9910574046903321

Titolo	ICT Systems Security and Privacy Protection : 37th IFIP TC 11 International Conference, SEC 2022, Copenhagen, Denmark, June 13–15, 2022, Proceedings / / edited by Weizhi Meng, Simone Fischer-Hübner, Christian D. Jensen
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-031-06975-7
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (522 pages)
Collana	IFIP Advances in Information and Communication Technology, , 1868-422X ; ; 648
Disciplina	005.8
Soggetti	Data protection Computer engineering Computer networks Computers Cryptography Data encryption (Computer science) Data and Information Security Computer Engineering and Networks Computing Milieux Computer Communication Networks Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Privacy Models and Preferences: -- A Privacy Calculus Model for Contact Tracing Apps: Analyzing the German Corona-Warn-App -- Deriving and Using Synthetic Consequences for Privacy Risk Modeling -- Stuart Shapiro Enhanced Privacy in Smart Workplaces: Employees' Preferences for Transparency Indicators and Control Interactions in the Case of Data Collection with Smart Watches -- Network Security and IDS -- DAEMON: Dynamic Auto-Encoders for contextualised anomaly detection applied to security MONitoring -- FOCUS: Frequency based detection of Covert Ultrasonic Signals -- Passive, Transparent, and

Selective TLS Decryption for Network Security Monitoring -- Network Security and Privacy -- A study on the use of 3rd party DNS resolvers for malware filtering or censorship circumvention -- RAAM: A Restricted Adversarial Attack Model with Adding Perturbations to Traffic Features -- Evaluation of Circuit Lifetimes in Tor -- Forensics -- D-Cloud-Collector: Admissible Forensic Evidence from Mobile Cloud Storage -- Robust PDF Files Forensics Using Coding Style -- Light-Weight File Fragments Classification using Depthwise Separable Convolution -- Trust and PETs -- Novel Approaches for the Development of Trusted IoT Entities -- Requirements and Secure Serialization for Selective Disclosure Verifiable Credentials -- Crypto-based solutions -- UP-MLE: Effcient and Practical Updatable Block-Level MessageLocked Encryption Scheme Based on Update Properties -- CryptKSP: A Kernel Stack Protection Model based on AES-NI Hardware Feature -- Usable Security -- Usability Insights from Establishing TLS Connections -- Usability of Antivirus Tools in a Threat Detection Scenario -- Data Minimisation Potential for Timestamps in Git: An Empirical Analysis of User Configurations -- Blockchain -- Greedy Networking in Cryptocurrency Blockchain -- Towards Supporting Attribute-Based Access Control in Hyperledger Fabric Blockchain -- Mobile Security and Privacy -- AndroClonium: Bytecode-Level Code Clone Detection for Obfuscated Android Apps -- One Light, One App: Tackling A Common Misperception Causing Breach of User Privacy -- Double-X: Towards Double-Cross-based Unlock Mechanism on Smartphones -- PETs and Crypto -- Post-Quantum Cheating Detectable Private Information Retrieval -- Anonymous Trusted Data Relocation for TEEs -- Efficient Volume-Hiding Encrypted Multi-Maps with Support for Conjunctive Queries -- Vulnerabilities -- Upside Down: Exploring the Ecosystem of Dark Web Data Markets -- An Effcient Use-after-Free Mitigation Approach via Static Dangling Pointer Nullification.

Sommario/riassunto

This book constitutes the refereed proceedings of the 37th IFIP TC 11 International Conference on Information Security and Privacy Protection, SEC 2022, held in Copenhagen, Denmark, in June 2022. The 29 full papers presented were carefully reviewed and selected from 127 submissions. The papers present novel research on theoretical and practical aspects of security and privacy protection in information processing systems. They are organized in topical sections on privacy models and preferences; network security and IDS; network security and privacy; forensics; trust and PETs; crypto-based solutions; usable security; blockchain; mobile security and privacy; PETs and crypto; and vulnerabilities.