1. Record Nr. UNINA9910299271903321

Autore	Giustolisi Rosario
Titolo	Modelling and Verification of Secure Exams / / by Rosario Giustolisi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-67107-3
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (144 pages)
Collana	Information Security and Cryptography, , 2197-845X
Disciplina	005.8
Soggetti	Data structures (Computer science) Information theory Computer networks Machine theory Test-taking skills Information technology - Management Data Structures and Information Theory Computer Communication Networks Formal Languages and Automata Theory Revision and Exam Computer Application in Administrative Data Processing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Preliminaries and Definitions -- Security Requirements -- The Huszti-Peth Protocol -- The Remark! Internet-Based Exam -- The WATA Family -- Conclusions.
Sommario/riassunto	In this book the author introduces a novel approach to securing exam systems. He provides an in-depth understanding, useful for studying the security of exams and similar systems, such as public tenders, personnel selections, project reviews, and conference management systems. After a short chapter that explains the context and objectives of the book, in Chap. 2 the author introduces terminology for exams and the foundations required to formulate their security requirements. He describes the tasks that occur during an exam, taking account of the levels of detail and abstraction of an exam specification and the

threats that arise out of the different exam roles. He also presents a taxonomy that classifies exams by types and categories. Chapter 3 contains formal definitions of the authentication, privacy, and verifiability requirements for exams, a framework based on the applied pi-calculus for the specification of authentication and privacy, and a more abstract approach based on set-theory that enables the specification of verifiability. Chapter 4 describes the Huszti-Peth protocol in detail and proposes a security enhancement. In Chap. 5 the author details Remark!, a protocol for Internet-based exams, discussing its cryptographic building blocks and some security considerations. Chapter 6 focuses on WATA, a family of computer-assisted exams that employ computer assistance while keeping face-to-face testing. The chapter also introduces formal definitions of accountability requirements and details the analysis of a WATA protocol against such definitions. In Chaps. 4, 5, and 6 the author uses the cryptographic protocol verifier ProVerif for the formal analyses. Finally, the author outlines future work in Chap. 7. The book is valuable for researchers and graduate students in the areas of information security, in particular for people engaged with exams or protocols.