1. Record Nr. UNISA996465633403316

Autore	Chen Qingfeng
Titolo	Secure transaction protocol analysis : models and applications / / Qingfeng Chen, Chengqi Zhang, Shichao Zhang
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer, , [2008] ©2008
ISBN	3-540-85074-0
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XI, 234 p.)
Collana	Lecture Notes in Computer Science ; ; 5111
Disciplina	005.8
Soggetti	Computer networks - Security measures Electronic commerce - Security measures Computer network protocols
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	Overview of Security Protocol Analysis -- Formal Analysis of Secure Transaction Protocols -- Model Checking in Security Protocol Analysis -- Uncertainty Issues in Secure Messages -- Applications of Data Mining in Protocol Analysis -- Detection Models of Collusion Attacks -- Conclusion and Future Works.
Sommario/riassunto	The present volume arose from the need for a comprehensive coverage of the state of the art in security protocol analysis. It aims to serve as an overall course-aid and to provide self-study material for researchers and students in formal methods theory and applications in e-commerce, data analysis and data mining. The volume will also be useful to anyone interested in secure e-commerce. The book is organized in eight chapters covering the main approaches and tools in formal methods for security protocol analysis. It starts with an introductory chapter presenting the fundamentals and background knowledge with respect to formal methods and security protocol analysis. Chapter 2 provides an overview of related work in this area, including basic concepts and terminology. Chapters 3 and 4 show a logical framework and a model checker for analyzing secure transaction protocols. Chapter 5 explains how to deal with uncertainty issues in secure messages, including inconsistent messages and conflicting

beliefs in messages. Chapter 6 integrates data mining with security protocol analysis, and Chapter 7 develops a new technique for detecting collusion attack in security protocols. Chapter 8 gives a summary of the chapters and presents a brief discussion of some emerging issues in the field.