1. Record Nr. UNISA996465349503316

Autore	Boyd Colin
Titolo	Protocols for Authentication and Key Establishment [[electronic resource] /] / by Colin Boyd, Anish Mathuria, Douglas Stebila
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2020
ISBN	3-662-58146-9
Edizione	[2nd ed. 2020.]
Descrizione fisica	1 online resource (XXVIII, 521 p. 17 illus.)
Collana	Information Security and Cryptography, , 1619-7100
Disciplina	005.73
Soggetti	Data structures (Computer science) Computer communication systems Data protection Computer security Data Structures and Information Theory Computer Communication Networks Security Systems and Data Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction to Authentication and Key Establishment -- Computational Security Models -- Protocols Using Shared Key Cryptography -- Authentication and Key Transport Using Public Key Cryptography -- Key Agreement Protocols -- Transport Layer Security Protocol -- Identity-Based Key Agreement -- Password-Based Protocols -- Group Key Establishment -- App. A, Standards for Authentication and Key Establishment -- App. B, Tutorial: Building a Key Establishment Protocol -- App. C, Summary of Notation.
Sommario/riassunto	This book is the most comprehensive and integrated treatment of the protocols required for authentication and key establishment. In a clear, uniform presentation the authors classify most protocols in terms of their properties and resource requirements, and describe all the main attack types, so the reader can quickly evaluate protocols for particular applications. In this edition the authors introduced new chapters and updated the text throughout in response to new developments and

updated standards. The first chapter, an introduction to authentication and key establishment, provides the necessary background on cryptography, attack scenarios, and protocol goals. A new chapter, computational security models, describes computational models for key exchange and authentication and will help readers understand what a computational proof provides and how to compare the different computational models in use. In the subsequent chapters the authors explain protocols that use shared key cryptography, authentication and key transport using public key cryptography, key agreement protocols, the Transport Layer Security protocol, identity-based key agreement, password-based protocols, and group key establishment. The book is a suitable graduate-level introduction, and a reference and overview for researchers and practitioners with 225 concrete protocols described. In the appendices the authors list and summarize the relevant standards, linking them to the main book text when appropriate, and they offer a short tutorial on how to build a key establishment protocol. The book also includes a list of protocols, a list of attacks, a summary of the notation used in the book, general and protocol indexes, and an extensive bibliography.