1. Record Nr. UNINA9910830826703321

Autore	Niemi Valtteri
Titolo	UMTS security [[electronic resource] /] / by Valterri Niemi and Kaisa Nyberg
Pubbl/distr/stampa	Chichester, England, : John Wiley & Sons, 2003
ISBN	1-280-26914-6 9786610269143 0-470-09158-4 0-470-09156-8
Descrizione fisica	1 online resource (287 p.)
Altri autori (Persone)	NybergKaisa <1948->
Disciplina	005.8 621.38456
Soggetti	Computer security Computer networks - Security measures Mobile communication systems - Security measures Wireless communication systems - Security measures Global system for mobile communications - Security measures
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 (p. [257]-265) and index.
Nota di contenuto	Universal Mobile Telecommunications System Security; Contents; Preface; PART I: SECURITY ARCHITECTURE FOR UMTS; 1 Introduction to Security and to UMTS; 1.1 Security in Telecommunications; 1.1.1 General security principles; 1.1.2 GSM security; 1.2 The Background to 3G; 1.3 The 3G Partnership Project (3GPP); 1.4 3GPP Network Architecture; 1.4.1 Elements in the architecture; 1.4.2 Protocols in the 3GPP system; 1.5 WCDMA Radio Technology; 1.5.1 CDMA: an example; 1.5.2 Basic facts of WCDMA; 1.5.3 Handovers; 1.5.4 Power control; 2 UMTS Security Features in Release 1999; 2.1 Access Security to UMTS 2.1.1 Mutual authentication2.1.2 Temporary identities; 2.1.3 UTRAN encryption; 2.1.4 Integrity protection of RRC signalling; 2.1.5 Set-up of UTRAN security mechanisms; 2.1.6 Summary of access security in the CS and PS domains; 2.2 Interworking with GSM; 2.2.1 Interworking scenarios; 2.2.2 Cases with SIM; 2.2.3 Cases with USIM; 2.2.4 Handovers from one system to another; 2.3 Additional Security

Features in Release 1999; 2.3.1 Ciphering indicator; 2.3.2 Identification of the UE; 2.3.3 Security for Location Services (LCs); 2.3.4 User-to-USIM authentication
2.3.5 Security in the USIM application toolkit2.3.6 Mobile Execution Environment (MExE); 2.3.7 Lawful interception; 3 Security Features in Releases 4 and 5; 3.1 Network Domain Security; 3.1.1 MAPsec; 3.1.2 IPsec; 3.1.3 IPsec-based mechanisms in UMTS; 3.1.4 Role of firewalls; 3.2 IMS Security; 3.2.1 Basics of SIP; 3.2.2 IMS architecture; 3.2.3 Architecture for securing access to the IMS; 3.2.4 Principles for IMS access security; 3.2.5 Use of HTTP Digest AKA; 3.2.6 Security mode set-up; 3.2.7 Integrity protection with ESP; 3.2.8 Error case handling; 3.3 Other Security Systems
3.3.1 Higher layer security systems3.3.2 Link layer security systems; PART II: CRYPTOGRAPHIC ALGORITHMS; 4 Introduction to Cryptography; 4.1 The Science of Cryptology; 4.1.1 Cryptographic systems; 4.1.2 Security and vulnerability; 4.1.3 Developing cryptology into a publicly available science; 4.1.4 Public cryptographic development efforts; 4.2 Requirements and Analysis of Cryptographic Algorithms; 4.2.1 Block ciphers; 4.2.2 Stream ciphers; 4.2.3 Message authentication codes; 5 3GPP Algorithm Specification Principles; 6 Confidentiality and Integrity Algorithms
6.1 Requirements for the Confidentiality Algorithm6.1.1 Functional requirements; 6.1.2 Algorithm operation; 6.1.3 Interfaces to the algorithm; 6.2 Requirements for the Integrity Algorithm; 6.2.1 Overview; 6.2.2 Interface; 6.3 Design Task Force; 6.4 Getting Started; 6.4.1 SAGE contribution to SA3; 6.4.2 Modes around MISTY1; 6.4.3 Particular security criteria; 6.5 Design Process; 6.5.1 The teams; 6.5.2 Design documentation; 6.5.3 Conclusion of evaluation; 6.6 Confidentiality Algorithm; 6.6.1 The f8 stream cipher mode; 6.6.2 Description of f8; 6.6.3 Security
6.7 Extension of the UMTS Confidentiality Algorithm

Sommario/riassunto

Can you afford not to read this book?..... The Universal Mobile Telecommunication System (UMTS) offers a consistent set of services to mobile computer and phone users and numerous different radio access technologies will co-exist within the UMTS system's core network - security is, therefore, of the utmost importance. UMTS Security focuses on the standardized security features of UMTS and brings together material previously only available in specifications, design documents and presentations in one concise form. In addition, this unique volume also covers non-standard i