

1. Record Nr.	UNINA9910143692503321
Autore	Nakhjiri Madjid
Titolo	AAA and network security for mobile access [[electronic resource] ] : radius, diameter, EAP, PKI and IP mobility // Madjid Nakhjiri and Mahsa Nakhjiri
Pubbl/distr/stampa	Chichester, England ; ; Hoboken, NJ, : John Wiley & Sons, c2005
ISBN	1-280-24272-8 9786610242726 0-470-01746-5 0-470-01745-7
Edizione	[1st edition]
Descrizione fisica	1 online resource (319 p.)
Classificazione	54.32 53.72
Altri autori (Persone)	NakhjiriMahsa
Disciplina	004.62 005.8
Soggetti	Wireless Internet - Security measures Mobile computing - Security measures Electronic books.
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	AAA AND NETWORK SECURITY FOR MOBILE ACCESS; Contents; Foreword; Preface; About the Author; Chapter 1 The 3 "A"s: Authentication, Authorization, Accounting; 1.1 Authentication Concepts; 1.1.1 Client Authentication; 1.1.2 Message Authentication; 1.1.3 Mutual Authentication; 1.1.4 Models for Authentication Messaging; 1.1.4.1 Two-Party Authentication Model; 1.1.4.2 Three-Party Authentication Model; 1.1.5 AAA Protocols for Authentication Messaging; 1.1.5.1 User-AAA Server; 1.1.5.2 NAS-AAA Server Communications; 1.1.5.3 Supplicant (User)-NAS Communications; 1.2 Authorization 1.2.1 How is it Different from Authentication? 1.2.2 Administration Domain and Relationships with the User; 1.2.3 Standardization of Authorization Procedures; 1.2.3.1 Authorization Messaging; 1.2.3.2 Policy Framework and Authorization; 1.3 Accounting; 1.3.1 Accounting Management Architecture; 1.3.1.1 Accounting Across Administrative

Domains; 1.3.2 Models for Collection of Accounting Data; 1.3.2.1 Polling Models for Accounting; 1.3.2.2 Event-Driven Models for Accounting; 1.3.3 Accounting Security; 1.3.4 Accounting Reliability; 1.3.4.1 Interim Accounting; 1.3.4.2 Transport Protocols 1.3.4.3 Fail-Over Mechanisms 1.3.5 Prepaid Service: Authorization and Accounting in Harmony; 1.4 Generic AAA Architecture; 1.4.1 Requirements on AAA Protocols Running on NAS; 1.5 Conclusions and Further Resources; 1.6 References; Chapter 2 Authentication; 2.1 Examples of Authentication Mechanisms; 2.1.1 User Authentication Mechanisms; 2.1.1.1 Basic PPP User Authentication Mechanisms; 2.1.1.2 Shortcoming of PPP Authentication Methods; 2.1.1.3 Extensible Authentication Protocol (EAP) as Extension to PPP; 2.1.1.4 SIM-Based Authentication; 2.1.2 Example of Device Authentication Mechanisms 2.1.2.1 Public Key Certificate-Based Authentication 2.1.2.2 Basics of Certificate-Based Authentication; 2.1.3 Examples of Message Authentication Mechanisms; 2.1.3.1 HMAC-MD5; 2.2 Classes of Authentication Mechanisms; 2.2.1 Generic Authentication Mechanisms; 2.2.1.1 Extensible Authentication Protocol (EAP); 2.2.1.2 EAP Messaging; 2.3 Further Resources; 2.4 References; Chapter 3 Key Management Methods; 3.1 Key Management Taxonomy; 3.1.1 Key Management Terminology; 3.1.2 Types of Cryptographic Algorithms; 3.1.3 Key Management Functions; 3.1.4 Key Establishment Methods; 3.1.4.1 Key Transport 3.1.4.2 Key Agreement 3.1.4.3 Manual Key Establishment; 3.2 Management of Symmetric Keys; 3.2.1 EAP Key Management Methods; 3.2.2 Diffie-Hellman Key Agreement for Symmetric Key Generation; 3.2.2.1 Problems with Diffie-Hellman; 3.2.3 Internet Key Exchange for Symmetric Key Agreement; 3.2.4 Kerberos and Single Sign On; 3.2.4.1 Kerberos Issues; 3.2.5 Kerberized Internet Negotiation of Keys (KINK); 3.3 Management of Public Keys and PKIs; 3.4 Further Resources; 3.5 References; Chapter 4 Internet Security and Key Exchange Basics; 4.1 Introduction: Issues with Link Layer-Only Security 4.2 Internet Protocol Security

---

## Sommario/riassunto

AAA (Authentication, Authorization, Accounting) describes a framework for intelligently controlling access to network resources, enforcing policies, and providing the information necessary to bill for services. AAA and Network Security for Mobile Access is an invaluable guide to the AAA concepts and framework, including its protocols Diameter and Radius. The authors give an overview of established and emerging standards for the provision of secure network access for mobile users while providing the basic design concepts and motivations. AAA and Network Security for Mobile Ac

---