

1. Record Nr.	UNINA9910822478603321
Autore	Hardjono Thomas
Titolo	Security in wireless LANs and MANs // Thomas Hardjono, Lakshminath R. Dondeti
Pubbl/distr/stampa	Boston, : Artech House, 2005
ISBN	1-58053-756-1
Edizione	[1st ed.]
Descrizione fisica	xviii, 243 p. : ill
Collana	Artech House computer security series
Altri autori (Persone)	DondetiLakshminath R
Disciplina	005.8
Soggetti	Metropolitan area networks (Computer networks) - Security measures Wireless communication systems - Security measures Wireless LANs - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Title from title screen.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Security in Wireless LANs and MANs -- Contents vii -- Preface xv -- Acknowledgments xvii -- Chapter 1 Introduction 1 -- Part I Authentication and Authorization in WLANs -- Chapter 2 Authentication in WLANs: An Overview 9 -- 2.1 INTRODUCTION 9 -- 2.2 BASIC ENTITIES AND REQUIREMENTS IN WLANS 10 -- 2.3 AUTHENTICATION MODELS FOR WLANS 14 -- 2.4 THE UNIVERSAL ACCESS METHOD 16 -- 2.5 THE 802.1X AUTHENTICATION FRAMEWORK 18 -- 2.6 THE RADIUS PROTOCOL 23 -- 2.7 DEVICE AUTHENTICATION FOR NETWORK ELEMENTS 27 -- 2.8 SUMMARY 35 -- References 35 -- Chapter 3 EAP, TLS, and Certificates 37 -- 3.1 INTRODUCTION 37 -- 3.2 THE EXTENSIBLE AUTHENTICATION PROTOCOL 38 -- 3.3 OVERVIEW OF TLS 43 -- 3.4 AN OVERVIEW OF CERTIFICATES AND PKI 49 -- 3.5 SUMMARY 54 -- References 55 -- Chapter 4 EAP Methods 57 -- 4.1 INTRODUCTION 57 -- 4.2 THE EAP-TLS METHOD 57 -- 4.3 PEAP: EAP-OVER-TLS-OVER-EAP 62 -- 4.4 TUNNELED TLS (EAP-TTLS) 70 -- 4.5 EAP-SIM 76 -- 4.6 EAP-AKA 82 -- 4.7 EAP-FAST 84 -- 4.8 RADIUS SUPPORT FOR EAP 86 -- 4.9 SUMMARY 87 -- References 88 -- Part II Data Protection in Wireless LANs -- Chapter 5 WEP 93 -- 5.1 INTRODUCTION 93 -- 5.2 THREAT MODEL 94 -- 5.3 ENTITY AUTHENTICATION 95 -- 5.4 WEP ENCAPSULATION AND DECAPSULATION 98 -- 5.5 DESIGN FLAWS IN WEP 103 -- 5.6 SUMMARY 106 -- References 106 -- Chapter 6 802.11i Security: RSNA 109 -- 6.1

INTRODUCTION 109 -- 6.2 802.11I SECURITY GOALS 110 -- 6.3 COMPONENTS OF AN RSN 113 -- 6.4 STEPS IN ESTABLISHING AN RSN ASSOCIATION 115 -- 6.5 MUTUAL AUTHENTICATION IN RSNAS 117 -- 6.6 SA AND KEY MANAGEMENT IN RSNS 119 -- 6.7 KEY DOWNLOAD PROTOCOLS IN 802.11I 128 -- References 130 -- Chapter 7 CCMP 131 -- 7.1 INTRODUCTION 131 -- 7.2 AES CCM MODE 132 -- 7.3 SECURITY ANALYSIS OF THE CCM MODE 135 -- 7.4 802.11I CCMP 137 -- 7.5 SUMMARY 141 -- References 141 -- Chapter 8 TKIP 143 -- 8.1 INTRODUCTION 143 -- 8.2 TKIP DESIGN 144. 8.3 MESSAGE INTEGRITY PROTECTION USING MICHAEL 147 -- 8.4 CONFIDENTIALITY 148 -- 8.5 REPLAY PROTECTION 150 -- 8.6 TKIP ENCAPSULATION AND DECAPSULATION 151 -- 8.7 SUMMARY 154 -- References 154 -- Part III Wireless Roaming Security -- Chapter 9 Security inWiFi Roaming 157 -- 9.1 INTRODUCTION 157 -- 9.2 ROAMING IN DIAL-UP IP SERVICES: BACKGROUND 158 -- 9.3 WIFI ROAMING: ENTITIES AND MODELS 162 -- 9.4 WISPR: THE WIRELESS ISP ROAMING ARCHITECTURE 167 -- 9.5 SUMMARY 171 -- References 172 -- Chapter 10 3G-WLAN Roaming 173 -- 10.1 INTRODUCTION 173 -- 10.2 A BRIEF HISTORY OF GSM AND 3G 173 -- 10.3 3G-WLAN INTERWORKING: THE 3GPP PERSPECTIVE 174 -- 10.4 THE 3GPP-WLAN INTERWORKING ARCHITECTURE 177 -- 10.5 SUMMARY 185 -- References 185 -- Part IV WMAN Security -- Chapter 11 An Overview of 802.16 WMANs 189 -- 11.1 INTRODUCTION 189 -- 11.2 BACKGROUND ON 802.16 WMANS 190 -- 11.3 NETWORK ENTRY AND INITIALIZATION 194 -- 11.4 THE PRIVACY KEY MANAGEMENT (PKM) PROTOCOL 197 -- 11.5 CERTIFICATES IN 802.16 204 -- 11.6 SUMMARY 209 -- References 209 -- Chapter 12 Wireless MAN Security 211 -- 12.1 INTRODUCTION 211 -- 12.2 WMAN THREAT MODEL AND SECURITY REQUIREMENTS 212 -- 12.3 PKMV2 214 -- 12.4 AUTHENTICATION AND ACCESS CONTROL IN PKMV2 216 -- 12.5 CCM ENCAPSULATION OF 802.16 MPDUS 224 -- 12.6 SECURE ENCAPSULATION OF MULTICAST AND BROADCAST MPDUS 227 -- 12.8 SUMMARY 229 -- References 229 -- Chapter 13 Conclusion and Outlook 231 -- About the Authors 235 -- Index 237.

Sommario/riassunto

With the popularity of the Wireless Local Area Network (WLAN) standard 802.11 WiFi® and the growing interest in the next generation Wireless Metropolitan Area Network (WMAN) standard 802.16 WiMax®, the need for effective solutions to the inherent security weaknesses of these networking technologies has become of critical importance. Thoroughly explaining the risks associated with deploying WLAN and WMAN networks, this groundbreaking book offers you practical insight into identifying and overcoming these security issues.
