INFORMATION SECURITY SERIES

Jianfeng Ma
Zhuo Ma
Changguang Wang
et al.

Security Access in Wireless Local Area Networks

From Architecture and Protocols to Realization

无线局域网安全接入
——体系结构与协议

高等教育出版社
HIGHER EDUCATION PRESS

Jianfeng Ma
Zhuo Ma
Changguang Wang
et al.

INFORMATION SECURITY SERIES

Security Access in Wireless Local Area Networks

From Architecture and Protocols to Realization

无线局域网安全接入

——体系结构与协议

With 209 figures

高等教育出版社
HIGHER EDUCATION PRESS

AUTHORS:

Prof. Jianfeng Ma
Key Laboratory of Computer Networks and Information Security (Ministry of Education)
Xidian University
Xi'an 710071, China
E-mail:
jfma@mail.xidian.edu.cn

Dr. Zhuo Ma
School of Computer Science
Xidian University
Xi'an 710071, China
E-mail:
mazhuo@mail.xidian.edu.cn

Dr. Changguang Wang
School of Computer Science
Xidian UniversityXi'an 710071, China
E-mail:
wangchangguang@sohu.com

图书在版编目（CIP）数据

无线局域网安全接入 = Security Access in Wireless Local Area Networks：英文 / 马建峰等著. —北京：高等教育出版社，2009.4
（信息安全系列丛书）
ISBN 978-7-04-026210-0

Ⅰ. 无… Ⅱ. 马… Ⅲ. 无线电通信－局部网络－安全技术－英文 Ⅳ. TN925

中国版本图书馆CIP数据核字（2009）第033616号

策划编辑 陈红英 **责任编辑** 陈红英 **封面设计** 张 楠
责任印制 陈伟光

出版发行	高等教育出版社	购书热线	010-58581118
社 址	北京市西城区德外大街 4 号	免费咨询	800-810-0598
邮政编码	100120	网 址	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	涿州市星河印刷有限公司	畅想教育	http://www.widedu.com
开 本	787 × 1092 1/16	版 次	2009 年 4 月第 1 版
印 张	28.25	印 次	2009 年 4 月第 1 次印刷
字 数	680 000	定 价	58.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号 26210-00

Sales only inside the mainland of China
仅限中国大陆地区销售

Preface

Networks have entered a wireless era. As a wireless communication technology, Wireless Local Area Network (WLAN) has been widely adopted in our daily life. Mobility and easy-deployment make WLAN devices commonplace in educational institutions, hospitals, manufacturing, inventory control, and the military, etc.

In this context, we have witnessed an evolution of our society towards mobile e-commerce, e-business and e-government and towards an increasing dependence on wireless communication systems. Unfortunately, such a evolution brings new vulnerabilities and risks, especially in WLAN. It is now clear that the security access is essential to protect the networks. Therefore, effective solutions for the security access in WLAN should be studied from the architecture and protocols to realization.

Recently, a substantial body of work on security access in WLAN has appeared in the literature of security. This has provided impetus for the deployment of WLAN. As the investigators of many scientific research projects of the WLAN security, the authors realize that it is a difficult job to design and analyze security access protocols or systems in WLAN. This book is born under such a background. The aim of this book is to deal with the various aspects of the security access in WLAN, among which, the security access architecture, security protocols, security management and evaluation, etc., are studied in detail.

The book is organized into the following 11 chapters.

Chapter 1 starts with an overview of the architecture and transmission technology of WLAN. Discussion of the IEEE 802.11 series standards, and the application and development trends of WLAN follow. The key issues of the WLAN security are analyzed and summarized next. Finally, to solve these problems, three kinds of architectures which we designed and implemented in the following chapters are overviewed.

Chapter 2 is concerned with the security attacks and requirements in WLAN. Based on this, a management-based WLAN security architecture is introduced. The last section contains an integrated security authentication architecture for mobile terminals. Its feasibility is verified through realizing a prototype of the software system.

Chapter 3 is devoted to analyze and improve the security of WAPI, provides a scheme which is compatible with WAPI and IEEE 802.11i, and gives a

self-verified public key based authentication and key agreement protocol in WAPI.

Chapter 4 deals with protocols regarding the efficiency of handoff. IEEE 802.11r standard is studied and two new secure fast handoff schemes, which are MIC based and Hash-chain-based respectively, are proposed. At last, we present the secure and fast handoff solution based on location. This solution is characterized by the following functions, QoS guaranteeing, location probing and location-based fast switching.

Chapter 5 focuses on security access techniques in mesh networks. Based on the analysis of mesh authentication protocols, an identity-based authentication protocol is proposed. Furthermore, a comprehensive solution for the WLAN mesh network secure access, taking the fast handoff and roaming of mesh devices into consideration, is given. There is also a simple mesh authentication system, which is designed and implemented for the purpose of verification and realization of authentication schemes in a wireless mesh network.

Chapter 6 introduces a new WLAN key exchange protocol called WIKE, which is based on IKEv2. The analysis of provably secure model Canetti-Krawczyk model follows. Then the relationship between the security definitions of the CK model and the security properties of the key exchange protocol is discussed. At last, the CK model under an identity-based system which lacks the forward secrecy is extended.

Chapter 7 is a further study on the WLAN anonymity from the aspects of anonymous connection method, and a universally composable secure anonymous model is introduced.

Chapter 8 deals with the security adaptivity on the architecture level. In this chapter, a framework of the adaptive security architecture of WLAN, a policy-based security management framework of WLAN and its implementation process, and a decision-making process to achieve the WLAN adaptive security policy are presented.

Chapter 9 is devoted to a fuzzy assessment method based on entropy-weight coefficient, aiming at the randomness and fuzziness of WLAN attacks.

Chapter 10 is concerned with the trusted computing technology, trusted computing framework, trusted platform module, and trusted mobile platform. In particular, the trusted computing based client security architecture is discussed. The last section gives a comparison among secure kernel based, micro kernel based and virtual machine based terminal architectures.

Chapter 11 proposes a Trusted Mobile IP platform (TMIP) framework based on the TNC architecture and combined with the trusted mobile platform architecture. Meanwhile, the architecture of a TPM-based mobile device accessing trusted network is put forward.

Each chapter of the book is organized in the order of technology introduction, analysis or proof of system schemes, model realization and problem discussion. Such organization can help the readers thoroughly understand not only the latest research on the WLAN security architecture, but also the trends of related technologies. Then readers can clearly comprehend the relationship

between the related technologies and the contents in each chapter by the problem discussion. This organization is helpful for readers to macroscopically grasp the concepts of the related technologies. Besides, it is beneficial for the graduate students to select research topics and take on research works. In this book, a lot of latest international research results and security proof models are adopted for those scheme proofs, which facilitates graduate students to master the international prevalent research methods and tools.

We expect that this book will prove useful for those who are researchers and engineers in wireless communications, electrical and computer engineering, or be used as a reference for graduate students in relevant majors.

Jianfeng Ma
Zhuo Ma
Changguang Wang
et al.
Xian, March 2009

Contributors

Zhenqiang Wu, Ph.D
School of Computer, Xidian University, China

Junzhi Yan, Ph.D
School of Computer, Xidian University, China

Xiang Lu, Ph.D
School of Computer, Xidian University, China

Qi Jiang, Ph.D
School of Computer, Xidian University, China

Kai Yang, Ph.D
School of Computer, Xidian University, China

Acknowledgements

Over the past several years, many people have given their help and suggestions to us to produce this book. We would like to thank the students and former students in the Key Laboratory of Computer Networks and Information Security (Ministry of Education, Pepole's Republic of China), Xidian University. In particular, many thanks to Xinghua Li, Fan Zhang, Chunjie Cao, for their research in formal analysis of security protocols; Weidong Yang, for his research in fast handoff in WLAN; Qingqi Pei, Yulong Shen, Chao Wang, Yong Zeng, Chao Yang, Li Yang, Zhihong Liu, Hongbin Zhang, Kun Zhao, Hongyue Liu, Haizheng Yu, Junwei Zhang, Liqiang Mao, Ayong Ye, Xindong Duan, for their invaluable comments, criticisms and suggestions which make the book better. Sincere thanks also to Hongying Chen, our editor at Higher Education Press, for her support and help.

This book is supported in part by the National High Technology Research and Development Program of China (2007AA01Z429), and the Key Program of National Natural Science Foundation of China (60633020), National Natural Science Foundation of China (60872041).

Since the WLAN security involves a large amount of new technologies, some of which are still even in evolution, the shortcomings are inevitable in this book. Criticism and constructive feedback from specialists and readers are warmly expected.

Contents

1 Introduction

Abstract The combination of computing and mobile communication technologies makes mobility ubiquitous. Whenever and wherever, it is becoming possible for anyone to communicate with anyone else in whatever modes with the development of mobile computing technologies. Now the Short Message Service (SMS) has become popular, in which the Multimedia Message Service (MMS), Mobile Multimedia Mail Service (MMMS), Mobile Instant Message (MIM) and Location-based Service (LBS) have been greatly recommended as the value-added services by the mobile operation business. It can be predicted that the value-added service of wireless networks, such as future mobile offices, mobile banks, and mobile e-commerce, will be a new fashion and bring operation business more profits and a vaster development space.

With a series of specifications for the mobile e-commerce and mobile TV being published, the mobile e-commerce will be widely used within a few years and a new highlight of the enterprise information. In order to realize the personalized wireless service, the wireless market controlled by the mobile operation business will be split. The future structure of wireless networks will include the Wireless Local Area Networks (WLANs), Wireless Metropolitan Area Networks (WMANs), and Wireless Wide Area Networks (WWANs). Especially, the IEEE 802.11 series standards specify the access technologies. In this chapter, the architecture and transmission technologies of WLAN are introduced firstly. Then, the IEEE 802.11 series standards are described, and applications and development trends of WLAN are discussed. The key issues of the WLAN security are analyzed and summarized next. Finally, to solve these problems, three kinds of architectures which we designed and implemented in the following chapters are given.

1.1 Overview

With the rapid development of information network technologies, the information access methods have been changed greatly. People have not been satisfied with the fixed terminals. Therefore, a new type of local area network, which is called WLAN [1], is becoming widely accepted. WLAN is a flexible data communication system where a user connects to a Local Area Network (LAN) using the radio frequency (RF) technology. It provides all the features and benefits of traditional LAN technologies such as Ethernet and Token Ring without the limitations of wires or cables. To a certain extent, WLAN is implemented as an extension or an alternative for a wired LAN, so as to minimize the wired connections. It provides the connectivity of the final few meters between a backbone network and the mobile users.

IEEE 802.11 series specifications [2] are the most attractive and fast growing connection options for WLAN. Because of its easy and fast deployment and installation, more and more users are considering using this type of network connection technology.

1.1.1 Architecture of WLAN

An IEEE 802.11 WLAN is a group of mobile terminals which are located within a limited physical area. The architecture of IEEE 802.11 WLAN consists of several components and two types of topologies [1] which are different from the wired LANs. The general architecture is presented in Fig.1.1.

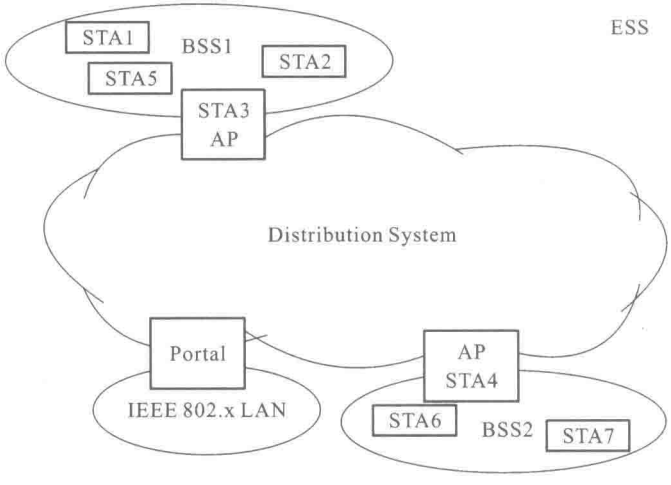

Fig. 1.1. General architecture of WALN