Security Access in Wireless Local Area Networks

From Architecture and Protocols to Realization
Jianfeng Ma
Zhuo Ma
Changguang Wang
et al.

Security Access in Wireless Local Area Networks

From Architecture and Protocols to Realization

With 209 figures
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 an 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.  
Xi’an, 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, People’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 .............................................................................................................. 1
  1.1 Overview ........................................................................................................... 2
    1.1.1 Architecture of WLAN ............................................................................. 2
    1.1.2 Transmission Technologies and Specifications ......................................... 5
    1.1.3 Series Specifications of IEEE 802.11 ...................................................... 9
    1.1.4 Applications ........................................................................................... 15
    1.1.5 Development Trends ............................................................................. 17
  1.2 Key Issues of WLAN Security ........................................................................... 20
    1.2.1 Security Access ...................................................................................... 20
    1.2.2 Fast roaming and handoff ....................................................................... 22
    1.2.3 Secure Integration of Heterogeneous Wireless Networks ........................ 22
    1.2.4 Privacy Protection ................................................................................. 23
    1.2.5 WLAN Security Management ............................................................... 24
    1.2.6 TPM-based Security Access .................................................................... 24
  1.3 Realization ......................................................................................................... 25
Questions and discussion .......................................................................................... 26
References .................................................................................................................. 27

2 Security Architecture Framework ............................................................................ 29
  2.1 Security Attacks and Requirements ................................................................... 29
    2.1.1 Logical Attacks ....................................................................................... 31
    2.1.2 Physical Attacks ..................................................................................... 34
    2.1.3 Security Requirements .......................................................................... 36
  2.2 Management-Based WLAN Security Architecture .......................................... 38
    2.2.1 The Design Methods of Security Architecture ........................................ 38
    2.2.2 Framework ............................................................................................ 39
    2.2.3 Logical Realization of Key Components ................................................. 43
2.2.4 Analysis.......................................................................................... 47
2.3 Evolution of Security Architecture for WLAN Access..................... 48
  2.3.1 WEP.......................................................................................... 50
  2.3.2 IEEE 802.1X............................................................................ 53
  2.3.3 WPA ....................................................................................... 55
  2.3.4 IEEE 802.11i Security Framework ..................................... 58
  2.3.5 WAPI ....................................................................................... 60
  2.3.6 Others....................................................................................... 62
2.4 The Integrated Security Access Authentication Architecture for
  WLAN Terminals ................................................................................ 62
  2.4.1 Design Concepts........................................................................ 63
  2.4.2 The Architecture Scheme .................................................. 64
  2.4.3 Flow of Integrated Authentication Operations ..................... 69
  2.4.4 Prototype Implementation.................................................. 73
Questions and Discussions ..................................................................... 83
References .............................................................................................. 84

3 Security Access Protocol........................................................................ 87
  3.1 Security Analysis of WAPI .......................................................... 87
    3.1.1 WAPI Specification .......................................................... 87
    3.1.2 WAPI Implementation Plan ............................................... 89
    3.1.3 Security Analysis of WAI in WAPI Implementation Plan..... 91
    3.1.4 Implementation Plan Overcomes the Weaknesses of the
          Original WAPI ........................................................................... 94
  3.2 Analysis and Improvement of WAPI............................................. 96
    3.2.1 Universally Composable Security ...................................... 96
    3.2.2 Improvement of WAPI...................................................... 97
    3.2.3 Analysis of Improved Protocol ........................................... 102
  3.3 Authentication Scheme that Compatible with 802.11i and WAPI...... 104
    3.3.1 Compatible Scheme .......................................................... 104
    3.3.2 Security Analysis of Compatible Scheme.......................... 107
    3.3.3 Compatibility Analysis of New Scheme................................ 109
  3.4 WAPI-XG1 Access Authentication and Fast Handoff Protocol.......... 110
    3.4.1 Overview............................................................................ 111
    3.4.2 Authentication Protocol .................................................... 112
    3.4.3 Unicast Key Agreement Protocol........................................ 114
3.4.4 Group key notification protocol .............................................. 115
3.4.5 Security Analysis ..................................................................... 115
3.4.6 Improved Authentication and Fast Handoff Protocols
   Based on WAPI-XG1 ................................................................. 117
3.5 Self-Certified Public Key based WAPI Authentication and Key
   Agreement Protocol................................................................. 125
   3.5.1 Authentication and Key Agreement Protocol ..................... 126
   3.5.2 Authentication of Self-Certified Certificate and Key
       Agreement at STA .............................................................. 127
   3.5.3 Security Analysis ............................................................ 129
   3.5.4 Protocol Features and Performance Analysis ..................... 130
Questions and discussion .................................................................... 132
References .................................................................................... 133

4 Security Protocols for Fast BSS Transition ..................................... 135
   4.1 IEEE 802.11r ....................................................................... 135
      4.1.1 Introduction .................................................................. 136
      4.1.2 Fast BSS Transition Protocol ...................................... 137
      4.1.3 Fast BSS Transition Flow .......................................... 140
      4.1.4 Security Consideration .............................................. 142
   4.2 Security Solution for IEEE 802.11r Drafts .............................. 144
      4.2.1 MIC Authentication Based Solutions ............................. 144
      4.2.2 Hash Chain Based FT Mechanism ............................... 148
      4.2.3 Mechanism Analysis .................................................. 154
   4.3 FT Security Solution Based on Location ................................ 155
      4.3.1 Proactive Neighbor Caching Mechanism Based on Moving
           Direction and QoS Guarantee .......................................... 156
      4.3.2 Active Probing Algorithm Assisted by Location ............. 161
      4.3.3 Secure FT Solution Based on Location ......................... 169
Questions and discussion .................................................................. 171
References .................................................................................... 172

5 Security Protocols in WLAN Mesh ............................................. 175
   5.1 Overview of WLAN Mesh .................................................. 175
      5.1.1 SnowMesh ................................................................. 177
      5.1.2 SEE-Mesh ................................................................. 180
5.1.3 IEEE 802.11s Draft ........................................................... 183
5.1.4 Classification of Wireless Mesh Networks ....................... 184
5.1.5 Security Requirements of WLAN Mesh ......................... 186
5.2 WLAN Mesh Authentication Schemes .................................. 187
  5.2.1 Centralized Authentication ........................................... 187
  5.2.2 Distributed Authentication ......................................... 188
  5.2.3 Pre-Shared Key Authentication .................................... 189
  5.2.4 MSA ........................................................................ 190
  5.2.5 4-way Mesh Handshake .............................................. 191
  5.2.6 Identity-based Mesh Authentication Protocol .................. 196
5.3 Protocols for Access Authentication, Secure Fast Handoff and Roaming.......................................................... 202
  5.3.1 Access Authentication Protocol .................................... 202
  5.3.2 Security Analysis ..................................................... 211
  5.3.3 Performance Analysis ................................................ 215
5.4 Design and Implementation of Mesh Access Authentication System ........................................... 218
  5.4.1 Technological Foundations ......................................... 219
  5.4.2 Design and Implementation ......................................... 223
Questions and discussion .................................................. 229
References ............................................................................. 230

6 Authenticated Key Exchange Protocol .................................... 231
  6.1 IKEv2 ........................................................................... 231
     6.1.1 Introduction ............................................................ 232
     6.1.2 The Initial Exchanges ............................................ 234
     6.1.3 The CREATE_CHILD_SA Exchange ......................... 235
     6.1.4 The INFORMATIONAL Exchange ............................ 236
     6.1.5 Authentication of the IKE_SA ................................. 237
     6.1.6 Extensible Authentication Protocol Methods .............. 237
     6.1.7 Generating Keying Material ................................... 238
     6.1.8 Analysis of IKEv2 ................................................. 240
  6.2 Key Exchange Protocol in WLAN .................................. 241
     6.2.1 Protocol Design Requirement .................................. 241
     6.2.2 Wireless Key Exchange Protocol ............................. 242
     6.2.3 Protocol Analysis .................................................. 244
  6.3 Extension of Provably Secure Model for Key Exchange Protocol ........................................ 246
<table>
<thead>
<tr>
<th>Section</th>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.1</td>
<td>Canetti-Krawczyk Model</td>
<td>246</td>
</tr>
<tr>
<td>6.3.2</td>
<td>Analysis and Extension for Canetti-Krawczyk Model</td>
<td>256</td>
</tr>
<tr>
<td></td>
<td>Questions and discussion</td>
<td>262</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>263</td>
</tr>
<tr>
<td>7</td>
<td>Privacy Protection for WLAN</td>
<td>265</td>
</tr>
<tr>
<td>7.1</td>
<td>Mobile Anonymity</td>
<td>265</td>
</tr>
<tr>
<td>7.2</td>
<td>IPSec-based Anonymity Connection Protocols in WLAN</td>
<td>267</td>
</tr>
<tr>
<td>7.2.1</td>
<td>Anonymity Architecture Model</td>
<td>268</td>
</tr>
<tr>
<td>7.2.2</td>
<td>Anonymity Connection Protocols</td>
<td>269</td>
</tr>
<tr>
<td>7.2.3</td>
<td>Implementation of protocols</td>
<td>274</td>
</tr>
<tr>
<td>7.2.4</td>
<td>Protocol Analysis</td>
<td>276</td>
</tr>
<tr>
<td>7.3</td>
<td>Universally Composable Anonymous Authentication Protocol</td>
<td>277</td>
</tr>
<tr>
<td></td>
<td>Questions and Discussion</td>
<td>292</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>293</td>
</tr>
<tr>
<td>8</td>
<td>Adaptive Security Policy</td>
<td>295</td>
</tr>
<tr>
<td>8.1</td>
<td>Overview</td>
<td>295</td>
</tr>
<tr>
<td>8.1.1</td>
<td>Adaptive Security</td>
<td>297</td>
</tr>
<tr>
<td>8.1.2</td>
<td>Evolution of Adaptive Security Architecture</td>
<td>298</td>
</tr>
<tr>
<td>8.1.3</td>
<td>Dynamic Security Policy Framework</td>
<td>301</td>
</tr>
<tr>
<td>8.2</td>
<td>Framework of WLAN Adaptive Security Policy</td>
<td>307</td>
</tr>
<tr>
<td>8.2.1</td>
<td>Requirement Analysis</td>
<td>307</td>
</tr>
<tr>
<td>8.2.2</td>
<td>Framework of Adaptive Security</td>
<td>308</td>
</tr>
<tr>
<td>8.2.3</td>
<td>Policy-Based Security Management Framework</td>
<td>309</td>
</tr>
<tr>
<td>8.3</td>
<td>Adaptive Security Communication Model for WLAN</td>
<td>314</td>
</tr>
<tr>
<td>8.3.1</td>
<td>System Model</td>
<td>314</td>
</tr>
<tr>
<td>8.3.2</td>
<td>Evidence Theory Based Security Inference Method</td>
<td>317</td>
</tr>
<tr>
<td>8.3.3</td>
<td>Analytical Hierarchy Process Based Adaptive Security Policy Decision-Making</td>
<td>321</td>
</tr>
<tr>
<td></td>
<td>Questions and Discussion</td>
<td>328</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>328</td>
</tr>
<tr>
<td>9</td>
<td>Evaluation Method of Security Performance</td>
<td>331</td>
</tr>
<tr>
<td>9.1</td>
<td>View Model of Security Service</td>
<td>331</td>
</tr>
<tr>
<td>9.1.1</td>
<td>Service Classification</td>
<td>333</td>
</tr>
</tbody>
</table>
9.1.2 QoSS Security Services View ........................................... 334
9.1.3 Description of Security Service View .............................. 347
9.2 Entropy Weight Coefficient Based WLAN Security Threat
Quantification Model .............................................................. 354
9.2.1 Risk Parameters Description ......................................... 355
9.2.2 Security Risk Evaluation Model ..................................... 358
9.2.3 Model Analysis ............................................................ 362
Questions and Discussion ....................................................... 365
References ............................................................................. 365

10 Architecture of Trusted Terminal ........................................... 367
10.1 Trusted Computing Technology ........................................ 367
10.1.1 TCG’s Definition of Trust ........................................... 369
10.1.2 Applications of Trusted Computing .............................. 371
10.1.3 Overview of TCG Architecture Specification ................. 374
10.1.4 TMP Hardware Architecture ....................................... 380
10.1.5 TMP Software Architecture ....................................... 383
10.1.6 Relationships between TPM and TMP ......................... 384
10.2 TC-based Security Architecture for Terminals .................. 385
10.2.1 Security Kernel-Based Architecture ............................. 385
10.2.2 Micro Kernel-based Architecture ................................. 390
10.2.3 VMM-Based Architecture ......................................... 392
10.2.4 LSM Mechanism-based Architecture .......................... 394
Questions and Discussion ....................................................... 398
References ............................................................................. 398

11 Architecture of Trusted Network Connect ............................ 401
11.1 From Trusted Platform to Trusted Network ...................... 401
11.1.1 Trusted Transmission ................................................ 401
11.1.2 Platform Authentication ............................................ 402
11.1.3 Trusted Network Connect ......................................... 404
11.2 TPM-Based Trusted Architecture .................................... 412
11.2.1 Trusted Computing Model ....................................... 412
11.2.2 Trusted Architecture of Mobile Terminal ..................... 413
11.2.3 Trusted Network Architecture ................................... 414
11.3 Architecture of Mobile Device Accessing Trusted Network ..... 416
11.3.1 Premise and Assumption................................................ 416
11.3.2 Access Entities.............................................................. 416
11.3.3 Architecture of Accessing Trusted Network..................... 418
11.3.4 Analysis ................................................................. 422

Questions and Discussion.......................................................... 422
References ................................................................................. 422

Index .......................................................................................... 425