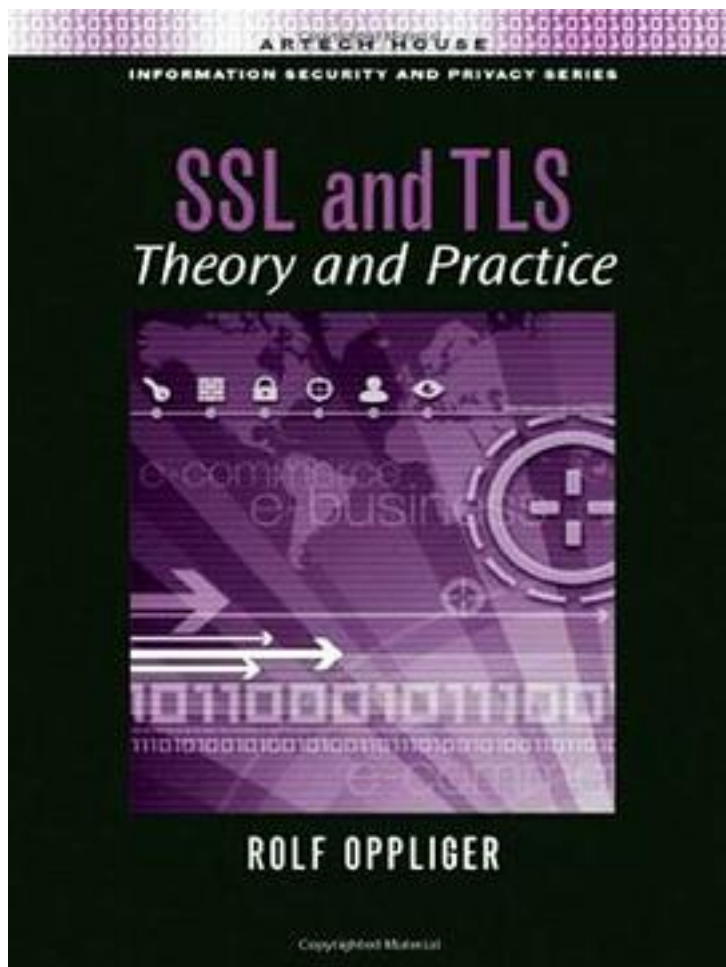


SSL and TLS : Theory and Practice



[SSL and TLS : Theory and Practice_ 下载链接1](#)

著者:Rolf Oppliger

出版者:ARTECH HOUSE

出版时间:2009

装帧:

isbn:9781596934474

SSL (secure socket layer) and TLS (Transport Layer Security) are widely deployed security protocols that are used in all kinds of web-based e-commerce and e-business

applications and are part of most contemporary security systems available today. This practical book provides a comprehensive introduction to these protocols, offering you a solid understanding of their design. Practitioners find discussions on the advantages and disadvantages of using SSL/TLS protocols compared to other Internet security protocols. This authoritative resource shows how to properly employ SSL and TLS and configure security solutions that are based on the use of the SSL/TLS protocols.

作者介绍:

目录: Foreword xi

Preface xv

Acknowledgments xxi

Chapter 1 Introduction 1

1.1 OSI Security Architecture 1

1.1.1 Security Services 4

1.1.2 Security Mechanisms 8

1.2 Security Definition 11

1.3 Final Remarks 14

References 15

Chapter 2 Cryptography Primer 17

2.1 Introduction 17

2.1.1 Preliminary Remarks 17

2.1.2 Cryptographic Systems 19

2.1.3 Classes of Cryptographic Systems 21

2.1.4 Secure Cryptosystems 22

2.1.5 Historical Background Information 24

2.1.6 Legal Situation 26

2.2 Cryptosystems Overview 28

2.2.1 Unkeyed Cryptosystems 28

2.2.2 Secret Key Cryptosystems 35

2.2.3 Public Key Cryptosystems 45

2.3 Final Remarks 59

References 60

Chapter 3 Transport Layer Security 65

3.1 Introduction 65

vii

viii

SSL and TLS: Theory and Practice

3.2

3.3

Protocol Evolution

Final Remarks

References

68

73

73

Chapter 4 SSL Protocol 75

4.1 Introduction 75

4.2 Protocols 87

4.2.1 SSL Record Protocol 87

4.2.2 SSL Handshake Protocol 94

4.2.3 SSL Change Cipher Spec Protocol 117

4.2.4 SSL Alert Protocol	118
4.2.5 SSL Application Data Protocol	120
4.3 Traffic Analysis of an SSL Session	121
4.4 Security Analysis	125
4.5 Final Remarks	129
References	130
Chapter 5 TLS Protocol	133
5.1 Introduction	133
5.1.1 TLS PRF	136
5.1.2 Generation of Keying Material	139
5.2 TLS 1.0	141
5.2.1 Cipher Suites	141
5.2.2 Certificate Management	144
5.2.3 Alert Messages	145
5.2.4 Other Differences	146
5.3 TLS 1.1	147
5.3.1 Preliminary Remarks	147
5.3.2 Cipher Suites	149
5.3.3 Certificate Management	150
5.3.4 Alert Messages	151
5.3.5 Other Differences	151
5.4 TLS 1.2	152
5.4.1 TLS Extensions	153
5.4.2 Cipher Suites	168
5.4.3 Certificate Management	173
5.4.4 Alert Messages	173
5.4.5 Other Differences	174
5.5 Traffic Analysis of a TLS Session	174
5.6 Security Analysis	178
Contents	
5.7	
Final Remarks	
References	
ix	
178	
179	
Chapter 6 DTLS Protocol	183
6.1 Introduction	183
6.2 DTLS 1.0	186
6.2.1 Record Protocol	187
6.2.2 Handshake Protocol	190
6.3 DTLS 1.2	194
6.4 Security Analysis	195
6.5 Final Remarks	195
References	196
Chapter 7 Firewall Traversal	199
7.1 Introduction	199
7.2 SSL/TLS Tunneling	202
7.3 SSL/TLS Proxying	205
7.4 Final Remarks	206
References	207
Chapter 8 Public Key Certificates and PKIs	209
8.1 Introduction	209
8.1.1 PGP Certificates	213

8.1.2 X.509 Certificates 215
8.2 Server Certificates 218
8.2.1 Wildcard Certificates 220
8.2.2 International Step-Up and SGC Certificates 220
8.2.3 Extended Validation Certificates 221
8.3 Client Certificates 222
8.4 Final Remarks 223
References 224
Chapter 9 Conclusions and Outlook 227
9.1 Deployment 227
9.2 Research Challenges 230
9.2.1 Performance Optimization 230
9.2.2 Protection Against MITM Attacks 232
9.2.3 Trust Management 235
9.3 Future Developments 235
References 236
SSL and TLS: Theory and Practice
Appendix Standardized TLS Cipher Suites 239
Abbreviations and Acronyms 243
About the Author 249
Index 251
• • • • • (收起)

[SSL and TLS : Theory and Practice 下载链接1](#)

标签

网络

安全

协议

[Security]

TLS

评论

[SSL and TLS : Theory and Practice_ 下载链接1](#)

书评

[SSL and TLS : Theory and Practice_ 下载链接1](#)