SSL and TLS

Theory and Practice

Rolf Oppliger
Contents

Foreword xi
Preface xv
Acknowledgments xxii

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
Contents

5.7 Final Remarks 178
References 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