Contents

Foreword xi
About the Authors xiii
Acknowledgment xv

1 Introduction 1

2 Introduction to Cryptographic Mechanisms 5
  2.1 Cryptographic Algorithms 6
    2.1.1 Symmetric Key Cryptography 6
    2.1.2 Public Key Cryptography 11
    2.1.3 Key-less Cryptographic Functions 20
  2.2 Secure Channel Establishment 21
    2.2.1 IP Layer Security 22
    2.2.2 Application Layer Security 28
  2.3 Authentication in 3GPP Networks 32
    2.3.1 AKA Authentication Vectors 35
    2.3.2 AKA Mutual Authentication 37
    2.3.3 AKA Resynchronization 37
  2.4 Security Mechanisms Threats and Vulnerabilities 38

3 Introduction to SIP 43
  3.1 What is SIP, Why Should we Bother About it and What are Competing Technologies? 44
  3.2 SIP: the Common Scenarios 46
  3.3 Introduction to SIP Operation: the SIP Trapezoid 49
  3.4 SIP Components 51
    3.4.1 User Agent 51
    3.4.2 Registrar 53
    3.4.3 Redirect Server 55
    3.4.4 Proxy 55
    3.4.5 Real-world Servers 58
  3.5 Addressing in SIP 60
3.6  SIP Message Elements 62
   3.6.1  Who are you Calling? 63
   3.6.2  Who is Calling You? 63
   3.6.3  How to Route SIP Traffic 66
   3.6.4  Even More Header-fields 67
   3.6.5  SIP Message Body 67
   3.6.6  SIP Methods 68
3.7  SIP Dialogs and Transactions 68
3.8  SIP Request Routing 73
   3.8.1  User Location Routing 74
   3.8.2  User-provisioned Routing 74
   3.8.3  ENUM: Public Phone Number Directory 75
   3.8.4  Interdomain Routing: DNS 75
   3.8.5  Routing Tables 76
3.9  Authentication, Authorization, Accounting 76
   3.9.1  User Authentication in SIP 77
   3.9.2  Authorization Policies 83
   3.9.3  Accounting 86
3.10 SIP and Middleboxes 86
3.11 Other Parts of the SIP Eco-system 89
3.12 SIP Protocol Design and Lessons Learned 89

4  Introduction to IMS 93
4.1  SIP in IMS 93
   4.1.1  Quality of Service Control 94
   4.1.2  Support for Roaming 94
   4.1.3  Security 95
   4.1.4  Efficient Resource Usage 95
4.2  General Architecture 98
   4.2.1  Subscriber and User Equipment 99
   4.2.2  Signaling Components 102
   4.2.3  Interworking Components 106
   4.2.4  QoS-related Components 109
   4.2.5  Application and Service Provisioning-related Components 111
   4.2.6  Database-related Components 111
4.3  Session Control and Establishment in IMS 112
   4.3.1  UE Registration in IMS 112
   4.3.2  Session Establishment in IMS 114

5  Secure Access and Interworking in IMS 123
5.1  Access Security in IMS 123
   5.1.1  IMS AKA Access Security 123
   5.1.2  Access-bundled Authentication 133
   5.1.3  HTTP Digest-based Access Security 136
   5.1.4  Authentication Mechanism Selection 140
5.2  Network Security in IMS 141
6 User Identity in SIP

6.1 Identity Theft

6.2 Identity Authentication using S/MIME

6.2.1 Providing Encryption with S/MIME

6.2.2 Providing Integrity and Authentication with S/MIME

6.3 Identity Authentication in Trusted Environments

6.4 Strong Authenticated Identity

6.5 Identity Theft Despite Strong Identity

6.6 User Privacy and Anonymity

6.6.1 User-provided Privacy

6.6.2 Network-provided Privacy

6.7 Subscription Theft

6.8 Fraud and SIP

6.8.1 Theft of SIP Services

7 Media Security

7.1 The Real-time Transport Protocol

7.2 Secure RTP

7.2.1 The SRTP Cryptographic Context

7.2.2 The SRTP Payload Structure

7.2.3 Sequence Numbering

7.2.4 The Key Derivation Procedure

7.2.5 The SRTP Interaction with Forward Error Correction

7.3 Key Exchange

7.3.1 SDP Security Descriptions for Media Streams

7.3.2 Multimedia Internet Keying

7.3.3 ZRTP

7.3.4 DTLS-SRTP

7.3.5 The Capability Negotiation Framework

7.3.6 Summary

8 Denial-of-service Attacks on VoIP and IMS Services

8.1 Introduction

8.2 General Classification of Denial-of-service Attacks

8.3 Bandwidth Consumption and Denial-of-service Attacks on SIP Services

8.4 Bandwidth Depletion Attacks

8.5 Memory Depletion Attacks

8.5.1 General Memory Depletion Attacks

8.5.2 Memory Depletion Attacks on SIP Services

8.6 CPU Depletion Attacks

8.6.1 Message parsing

8.6.2 Security checks

8.6.3 Application execution

8.7 Misuse Attacks

8.7.1 TCP/IP Protocol Deviation Attacks

8.7.2 Buffer Overflow Attacks
8.7.3 SIP Protocol Misuse Attacks

8.8 Distributed Denial-of-service Attacks
8.8.1 DDoS Attacks with Botnets
8.8.2 IP-based Amplification Attacks
8.8.3 DNS-based Amplification Attacks
8.8.4 Loop-based Amplification Attacks on SIP Services
8.8.5 Forking-based Amplification Attacks on SIP Services
8.8.6 Reflection-based Amplification Attacks on SIP Services

8.9 Unintentional Attacks
8.9.1 Flash Crowds
8.9.2 Implementation and Configuration Mistakes

8.10 Address Resolution-related Attacks
8.10.1 DNS Servers Security Threats
8.10.2 Effects of DNS Attacks
8.10.3 Countermeasures and General Protection Mechanisms for DNS Services
8.10.4 DNS-related Attacks on SIP Services
8.10.5 Protecting SIP Proxies from DNS-based Attacks

8.11 Attacking the VoIP Subscriber Database
8.11.1 Web-based Attacks on the Subscriber Database
8.11.2 SIP-based Attacks on the Subscriber Database

8.12 Denial-of-service Attacks in IMS Networks
8.12.1 Bandwidth Depletion Attacks
8.12.2 Memory Depletion Attacks
8.12.3 CPU Depletion Attacks
8.12.4 Protocol Misuse Attacks
8.12.5 Web-based Attacks

8.13 DoS Detection and Protection Mechanisms
8.14 Detection of DoS Attacks
8.14.1 Signature-based DoS Detection
8.14.2 Anomaly-based DDoS Detection

8.15 Reacting to DoS Attacks
8.15.1 Dynamic Filtering
8.15.2 Rate Limiting
8.15.3 IP Traceback

8.16 Preventing DoS Attacks
8.16.1 Access Control
8.16.2 Memory Protection
8.16.3 Architectural Consideration

8.17 DDoS Signature Specification
8.17.1 Fuzzing
8.17.2 Honeypots

9 SPAM over IP Telephony
9.1 Introduction
9.2 Spam Over SIP: Types and Applicability
9.2.1 General Types of Spam 293

9.3 Why is SIP Good for Spam? 294

9.4 Legal Side of Unsolicited Communication 296
  9.4.1 Protection of Personal Privacy 296
  9.4.2 Protection of Property 297
  9.4.3 Legal Aspects of Prohibition of Unsolicited Communication by Service Providers 298
  9.4.4 Effectiveness of Legal Action 299

9.5 Fighting Unsolicited Communication 299
  9.5.1 Antispam Measures Based on Identity 300
  9.5.2 Content Analysis 306
  9.5.3 Collaborative Filtering 307
  9.5.4 Interactive Antispam Solutions 307
  9.5.5 Preventive Antispam Methods 312

9.6 General Antispam Framework 314

Bibliography 317

Index 331