

SIP SECURITY

Dorgham Sisalem

John Floroiu

Jiri Kuthan

Ulrich Abend

Henning Schulzrinne

 **WILEY**

A John Wiley and Sons, Ltd., Publication

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 <i>Symmetric Key Cryptography</i> | 6 |
| 2.1.2 <i>Public Key Cryptography</i> | 11 |
| 2.1.3 <i>Key-less Cryptographic Functions</i> | 20 |
| 2.2 Secure Channel Establishment | 21 |
| 2.2.1 <i>IP Layer Security</i> | 22 |
| 2.2.2 <i>Application Layer Security</i> | 28 |
| 2.3 Authentication in 3GPP Networks | 32 |
| 2.3.1 <i>AKA Authentication Vectors</i> | 35 |
| 2.3.2 <i>AKA Mutual Authentication</i> | 37 |
| 2.3.3 <i>AKA Resynchronization</i> | 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 <i>User Agent</i> | 51 |
| 3.4.2 <i>Registrar</i> | 53 |
| 3.4.3 <i>Redirect Server</i> | 55 |
| 3.4.4 <i>Proxy</i> | 55 |
| 3.4.5 <i>Real-world Servers</i> | 58 |
| 3.5 Addressing in SIP | 60 |

| | | |
|----------|--|------------|
| 3.6 | SIP Message Elements | 62 |
| 3.6.1 | <i>Who are you Calling?</i> | 63 |
| 3.6.2 | <i>Who is Calling You?</i> | 63 |
| 3.6.3 | <i>How to Route SIP Traffic</i> | 66 |
| 3.6.4 | <i>Even More Header-fields</i> | 67 |
| 3.6.5 | <i>SIP Message Body</i> | 67 |
| 3.6.6 | <i>SIP Methods</i> | 68 |
| 3.7 | SIP Dialogs and Transactions | 68 |
| 3.8 | SIP Request Routing | 73 |
| 3.8.1 | <i>User Location Routing</i> | 74 |
| 3.8.2 | <i>User-provisioned Routing</i> | 74 |
| 3.8.3 | <i>ENUM: Public Phone Number Directory</i> | 75 |
| 3.8.4 | <i>Interdomain Routing: DNS</i> | 75 |
| 3.8.5 | <i>Routing Tables</i> | 76 |
| 3.9 | Authentication, Authorization, Accounting | 76 |
| 3.9.1 | <i>User Authentication in SIP</i> | 77 |
| 3.9.2 | <i>Authorization Policies</i> | 83 |
| 3.9.3 | <i>Accounting</i> | 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 | <i>Quality of Service Control</i> | 94 |
| 4.1.2 | <i>Support for Roaming</i> | 94 |
| 4.1.3 | <i>Security</i> | 95 |
| 4.1.4 | <i>Efficient Resource Usage</i> | 95 |
| 4.2 | General Architecture | 98 |
| 4.2.1 | <i>Subscriber and User Equipment</i> | 99 |
| 4.2.2 | <i>Signaling Components</i> | 102 |
| 4.2.3 | <i>Interworking Components</i> | 106 |
| 4.2.4 | <i>QoS-related Components</i> | 109 |
| 4.2.5 | <i>Application and Service Provisioning-related Components</i> | 111 |
| 4.2.6 | <i>Database-related Components</i> | 111 |
| 4.3 | Session Control and Establishment in IMS | 112 |
| 4.3.1 | <i>UE Registration in IMS</i> | 112 |
| 4.3.2 | <i>Session Establishment in IMS</i> | 114 |
| 5 | Secure Access and Interworking in IMS | 123 |
| 5.1 | Access Security in IMS | 123 |
| 5.1.1 | <i>IMS AKA Access Security</i> | 123 |
| 5.1.2 | <i>Access-bundled Authentication</i> | 133 |
| 5.1.3 | <i>HTTP Digest-based Access Security</i> | 136 |
| 5.1.4 | <i>Authentication Mechanism Selection</i> | 140 |
| 5.2 | Network Security in IMS | 141 |

| | | |
|----------|---|------------|
| 6 | User Identity in SIP | 145 |
| 6.1 | Identity Theft | 145 |
| 6.2 | Identity Authentication using S/MIME | 147 |
| | 6.2.1 <i>Providing Encryption with S/MIME</i> | 148 |
| | 6.2.2 <i>Providing Integrity and Authentication with S/MIME</i> | 150 |
| 6.3 | Identity Authentication in Trusted Environments | 150 |
| 6.4 | Strong Authenticated Identity | 153 |
| 6.5 | Identity Theft Despite Strong Identity | 158 |
| 6.6 | User Privacy and Anonymity | 161 |
| | 6.6.1 <i>User-provided Privacy</i> | 162 |
| | 6.6.2 <i>Network-provided Privacy</i> | 163 |
| 6.7 | Subscription Theft | 165 |
| 6.8 | Fraud and SIP | 168 |
| | 6.8.1 <i>Theft of SIP Services</i> | 169 |
| | | |
| 7 | Media Security | 173 |
| 7.1 | The Real-time Transport Protocol | 174 |
| 7.2 | Secure RTP | 175 |
| | 7.2.1 <i>The SRTP Cryptographic Context</i> | 177 |
| | 7.2.2 <i>The SRTP Payload Structure</i> | 179 |
| | 7.2.3 <i>Sequence Numbering</i> | 181 |
| | 7.2.4 <i>The Key Derivation Procedure</i> | 181 |
| | 7.2.5 <i>The SRTP Interaction with Forward Error Correction</i> | 183 |
| 7.3 | Key Exchange | 184 |
| | 7.3.1 <i>SDP Security Descriptions for Media Streams</i> | 187 |
| | 7.3.2 <i>Multimedia Internet Keying</i> | 191 |
| | 7.3.3 <i>ZRTP</i> | 202 |
| | 7.3.4 <i>DTLS-SRTP</i> | 214 |
| | 7.3.5 <i>The Capability Negotiation Framework</i> | 219 |
| | 7.3.6 <i>Summary</i> | 221 |
| | | |
| 8 | Denial-of-service Attacks on VoIP and IMS Services | 225 |
| 8.1 | Introduction | 225 |
| 8.2 | General Classification of Denial-of-service Attacks | 229 |
| 8.3 | Bandwidth Consumption and Denial-of-service Attacks on SIP Services | 230 |
| 8.4 | Bandwidth Depletion Attacks | 233 |
| 8.5 | Memory Depletion Attacks | 234 |
| | 8.5.1 <i>General Memory Depletion Attacks</i> | 234 |
| | 8.5.2 <i>Memory Depletion Attacks on SIP Services</i> | 235 |
| 8.6 | CPU Depletion Attacks | 243 |
| | 8.6.1 <i>Message parsing</i> | 244 |
| | 8.6.2 <i>Security checks</i> | 245 |
| | 8.6.3 <i>Application execution</i> | 245 |
| 8.7 | Misuse Attacks | 246 |
| | 8.7.1 <i>TCP/IP Protocol Deviation Attacks</i> | 246 |
| | 8.7.2 <i>Buffer Overflow Attacks</i> | 247 |

| | | |
|----------|---|------------|
| 8.7.3 | <i>SIP Protocol Misuse Attacks</i> | 247 |
| 8.8 | Distributed Denial-of-service Attacks | 250 |
| 8.8.1 | <i>DDoS Attacks with Botnets</i> | 251 |
| 8.8.2 | <i>IP-based Amplification Attacks</i> | 253 |
| 8.8.3 | <i>DNS-based Amplification Attacks</i> | 254 |
| 8.8.4 | <i>Loop-based Amplification Attacks on SIP Services</i> | 255 |
| 8.8.5 | <i>Forking-based Amplification Attacks on SIP Services</i> | 257 |
| 8.8.6 | <i>Reflection-based Amplification Attacks on SIP Services</i> | 257 |
| 8.9 | Unintentional Attacks | 258 |
| 8.9.1 | <i>Flash Crowds</i> | 258 |
| 8.9.2 | <i>Implementation and Configuration Mistakes</i> | 259 |
| 8.10 | Address Resolution-related Attacks | 259 |
| 8.10.1 | <i>DNS Servers Security Threats</i> | 261 |
| 8.10.2 | <i>Effects of DNS Attacks</i> | 262 |
| 8.10.3 | <i>Countermeasures and General Protection Mechanisms for DNS Services</i> | 262 |
| 8.10.4 | <i>DNS-related Attacks on SIP Services</i> | 263 |
| 8.10.5 | <i>Protecting SIP Proxies from DNS-based Attacks</i> | 265 |
| 8.11 | Attacking the VoIP Subscriber Database | 265 |
| 8.11.1 | <i>Web-based Attacks on the Subscriber Database</i> | 266 |
| 8.11.2 | <i>SIP-based Attacks on the Subscriber Database</i> | 269 |
| 8.12 | Denial-of-service Attacks in IMS Networks | 270 |
| 8.12.1 | <i>Bandwidth Depletion Attacks</i> | 271 |
| 8.12.2 | <i>Memory Depletion Attacks</i> | 271 |
| 8.12.3 | <i>CPU Depletion Attacks</i> | 273 |
| 8.12.4 | <i>Protocol Misuse Attacks</i> | 274 |
| 8.12.5 | <i>Web-based Attacks</i> | 274 |
| 8.13 | DoS Detection and Protection Mechanisms | 274 |
| 8.14 | Detection of DoS Attacks | 274 |
| 8.14.1 | <i>Signature-based DoS Detection</i> | 275 |
| 8.14.2 | <i>Anomaly-based DDoS Detection</i> | 275 |
| 8.15 | Reacting to DoS Attacks | 278 |
| 8.15.1 | <i>Dynamic Filtering</i> | 278 |
| 8.15.2 | <i>Rate Limiting</i> | 278 |
| 8.15.3 | <i>IP Traceback</i> | 279 |
| 8.16 | Preventing DoS Attacks | 280 |
| 8.16.1 | <i>Access Control</i> | 280 |
| 8.16.2 | <i>Memory Protection</i> | 283 |
| 8.16.3 | <i>Architectural Consideration</i> | 285 |
| 8.17 | DDoS Signature Specification | 289 |
| 8.17.1 | <i>Fuzzing</i> | 289 |
| 8.17.2 | <i>Honeypots</i> | 290 |
| 9 | SPAM over IP Telephony | 291 |
| 9.1 | Introduction | 291 |
| 9.2 | Spam Over SIP: Types and Applicability | 292 |

| | | |
|-------|---|------------|
| 9.2.1 | <i>General Types of Spam</i> | 293 |
| 9.3 | Why is SIP Good for Spam? | 294 |
| 9.4 | Legal Side of Unsolicited Communication | 296 |
| 9.4.1 | <i>Protection of Personal Privacy</i> | 296 |
| 9.4.2 | <i>Protection of Property</i> | 297 |
| 9.4.3 | <i>Legal Aspects of Prohibition of Unsolicited Communication by Service Providers</i> | 298 |
| 9.4.4 | <i>Effectiveness of Legal Action</i> | 299 |
| 9.5 | Fighting Unsolicited Communication | 299 |
| 9.5.1 | <i>Antispam Measures Based on Identity</i> | 300 |
| 9.5.2 | <i>Content Analysis</i> | 306 |
| 9.5.3 | <i>Collaborative Filtering</i> | 307 |
| 9.5.4 | <i>Interactive Antispam Solutions</i> | 307 |
| 9.5.5 | <i>Preventive Antispam Methods</i> | 312 |
| 9.6 | General Antispam Framework | 314 |
| | Bibliography | 317 |
| | Index | 331 |