

Sicherheitsmechanismen für Voice over IP

von

Dr. Behrooz Moayeri

Inhaltsverzeichnis

<u>INHALTSVERZEICHNIS</u>		<u>I</u>
<u>1</u>	<u>VORWORT</u>	<u>1-1</u>
<u>2</u>	<u>MOTIVATION</u>	<u>2-3</u>
2.1	Sicherheitsrelevante Unterschiede zwischen TDM und VoIP	2-4
2.2	Exemplarische Angriffsszenarien	2-9
<u>3</u>	<u>STANDARDS FÜR VOIP-SICHERHEIT</u>	<u>3-17</u>
3.1	Bestandteile von VoIP-Sicherheit	3-17
3.2	Transport Layer Security (TLS)	3-18
3.3	Sicherheit beim Real-Time Transport Protocol (RTP)	3-20
3.4	Sicherheit beim Session Initiation Protocol (SIP)	3-26
3.5	Sicherheit bei H.323	3-35
3.6	Standards für die Sicherheit von VoWLAN	3-42
<u>4</u>	<u>VOIP-VERSCHLÜSSELUNG</u>	<u>4-44</u>
4.1	Motivation für VoIP-Verschlüsselung	4-44
4.2	Akzeptanz der Verschlüsselungstechnik	4-45
4.3	Grundlagen der VoIP-Verschlüsselung	4-48
4.4	VoIP-Verschlüsselung bei einigen führenden Herstellern	4-51
4.4.1	Alcatel-Lucent	4-51
4.4.2	Avaya	4-54
4.4.3	Cisco Systems	4-56
4.4.4	Nortel	4-62
4.4.5	Siemens	4-63
4.4.6	Snom	4-65
4.5	Planung der VoIP-Verschlüsselung	4-66
4.6	Nutzung von IP-VPNs	4-69
4.7	Verschlüsselung und QoS	4-78
4.8	VoIP-Verschlüsselung über Unternehmensgrenzen hinaus	4-81
4.8.1	Zukunft der externen Telefonie	4-81

4.8.2	Schlüsselmanagement	4-82
4.9	Weitere Anforderungen an VoIP-Verschlüsselung	4-90
4.10	Rolle von Open-Source	4-91
4.11	VoIP-Verschlüsselung und gesetzliche Vorschriften	4-92
4.12	Fazit zu VoIP-Verschlüsselung	4-94

5 HOCHVERFÜGBARKEITSDSIGN FÜR VOIP 5-96

5.1	Motivation für Redundanz	5-96
5.2	Redundanter Anschluss zentraler Komponenten	5-100
5.3	Motivation für die redundante Auslegung von Telefonieservern	5-102
5.4	Unterschiedliche Clustermodelle	5-104
5.5	Redundante Auslegung von Gateways	5-106
5.6	Wartungsleistungen	5-108
5.7	Redundanztests	5-109
5.8	Survival Gateways	5-110
5.9	Optimaler Einsatzzeitpunkt von Releases	5-112
5.10	Hochverfügbare Umgebung am Beispiel von Herstellerlösungen	5-115
5.10.1	Avaya	5-115
5.10.2	Cisco	5-116
5.10.3	Siemens	5-117

6 SICHERHEITSMCHANISMEN IM IP-NETZ 6-120

6.1	IP-Telefonie und IEEE 802.1X	6-120
6.1.1	Grundlagen der portbasierenden Authentifizierung	6-120
6.1.2	Umgang mit IP-Telefonen ohne 1X-Unterstützung	6-127
6.1.3	Umgang mit 1X-fähigen IP-Telefonen	6-129
6.2	Schutz für Quality of Service (QoS)	6-138
6.2.1	QoS als Sicherheits- und Vertrauensfrage	6-138
6.2.2	Denkbare Vertrauensgrenzen	6-139
6.2.3	Denkbare QoS-Architektur	6-141
6.2.4	Call Admission Control (CAC)	6-142
6.3	VoIP und Intrusion Detection / Intrusion Prevention	6-145
6.4	Netztrennung als Sicherheitsmechanismus für VoIP	6-147

6.4.1	Motivation für Netztrennung	6-147
6.4.2	Trennung auf der Ebene der passiven Infrastruktur	6-147
6.4.3	Trennung aller aktiven Bestandteile	6-148
6.4.4	Trennung eines Teils der aktiven Netzkomponenten	6-150
6.4.5	Gemeinsame Nutzung der aktiven Komponenten	6-152
6.4.6	Varianten des VLAN-Designs	6-155
6.4.7	Anschlussmodelle	6-161
6.4.8	Trennung der Subnetzebene für Sprache und Daten	6-163
6.4.9	Telefone und PC in denselben IP-Subnetzen	6-164
6.4.10	Authentifizierung bei unterschiedlichen VLAN-Konzepten	6-166
6.4.11	Kopplung der verschiedenen Vertrauensbereiche	6-168
6.4.12	Virtual Routing and Forwarding (VRF)	6-176
6.4.13	Kombination von Trennungs- und Kopplungsansätzen	6-179
6.4.14	Netztrennung im WLAN	6-181
6.5	Maßnahmen auf Switchs	6-183
7	<u>VOIP ÜBER VERTRAUENSGRENZEN HINWEG</u>	7-185
7.1	VoIP-Kommunikationsprofil	7-185
7.2	Problematik NAT	7-187
7.3	Firewalling bei H.323	7-189
7.4	Firewalling bei SIP	7-194
7.5	Problematik proprietärer Signalisierung	7-203
7.6	Bewertung von Firewall-Architekturen	7-205
7.7	VoIP über Provider-Umgebungen	7-206
8	<u>GESETZLICHE ASPEKTE</u>	8-209
8.1	Maßgebliche Gesetze und Regelungen	8-209
8.2	Notruftelefonie	8-210
8.3	Aufbewahrungspflicht für Verbindungsdaten	8-218
9	<u>MAßNAHMENKATALOG VOIP-SICHERHEIT</u>	9-219
9.1	Kombination von Maßnahmen auf verschiedenen Ebenen	9-219
9.2	Maßnahmen bezogen auf VoIP-Komponenten	9-220
9.2.1	Telefonieserver	9-221

9.2.2	IP-Telefone	9-228
9.2.3	Gateways	9-231
9.2.4	Applikationsserver	9-232
9.2.5	VoIP-Management	9-233
9.3	Maßnahmen auf der Netzebene	9-235
9.3.1	Verschlüsselung	9-235
9.3.2	Netztrennung	9-235
9.3.3	Firewalling	9-236
9.3.4	Authentifizierung	9-236
9.3.5	Weitere Maßnahmen auf der Netzebene	9-237
9.4	Physikalische Sicherheit	9-238
9.5	Sichere Stromversorgung	9-239
9.6	Besondere Sicherheitsmechanismen bei Filialen	9-239
9.7	Sicherheitsstufenmodell	9-240
9.7.1	Empfohlene Vorgehensweise	9-240
9.7.2	Basissicherheit	9-244
9.7.3	Mittlere Sicherheit	9-245
9.7.4	Hohe Sicherheit	9-245

ABBILDUNGSVERZEICHNIS **247**

TABELLENVERZEICHNIS **252**