

# Security für VoIP

## Verschlüsselung, Authentisierung und Firewalls

Während bei der traditionellen Telefonie das Thema Sicherheit eine eher untergeordnete Bedeutung spielte, kann man sich diesem bei der Integration in die IP-Welt nicht mehr entziehen, ohne grob fahrlässig zu handeln. Wer seine VoIP-Installation adäquat schützen will, sollte sowohl mit den drohenden Gefahren als auch den Gegenmaßnahmen vertraut sein. Der Kurs analysiert systematisch Angriffspunkte von VoIP und stellt die zur Verfügung stehenden Schutzmaßnahmen auf Netzwerk- und Applikationsebene dar. Letztere werden dann auf der Basis der unterschiedlichen VoIP-Architekturen gegeneinander abgewogen. Die Teilnehmer lernen, wie sie in späteren eigenen Projekten für eine angemessene Sicherheit von VoIP sorgen können.

### Kursinhalt

- Prinzipielle Gefahren für VoIP
- Angriffe auf den Medienstrom
- Angriffe auf die Signalisierung
- Angriffe auf die Geräte
- Security-Maßnahmen im LAN und WLAN
- Port Security und Authentisierung nach 802.1X
- Security-Maßnahmen im WAN
- Identität bei VoIP (SIP-Identity)
- Lokale Authentisierung und über Proxy-Ketten
- Probleme mit Zertifikaten
- SIPS und S/MIME
- SRTP und SRTCP
- Schlüsselmanagement mit SDES, ZRTP, DTLS und MIKEY
- WebRTC
- VoIP und IPsec
- NAT-Lösungen: STUN, TURN und ICE
- Firewalls und VoIP
- Session Border Controller
- SIP-Connect 2.0

**E-Book** Sie erhalten das ausführliche deutschsprachige Unterlagenpaket aus der Reihe ExperTeach Networking – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

### Zielgruppe

Der Kurs wendet sich an Planer und Techniker, die für die Konzeption und Realisierung von VoIP-Installationen zuständig sind.

### Voraussetzungen

Gute Kenntnisse der TCP/IP-Protokollfamilie und gängiger LAN-Technologien sind erforderlich. Die Teilnehmer müssen mit Security-Konzepten wie Verschlüsselung und Authentisierung vertraut sein. Diese können z.B. im Kurs Security in IP-Netzen – Sicherheitslücken erkennen und schließen erlernt werden. Zusätzlich wird ein solides Grundwissen zu VoIP vorausgesetzt.

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.at/go/SEVO](http://www.experteach.at/go/SEVO)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.	
<b>Termine in Deutschland</b>	<b>3 Tage</b>	<b>€ 1.995,-</b>
<b>Termine in Österreich</b>	<b>3 Tage</b>	<b>€ 1.995,-</b>
<b>Online Training</b>	<b>3 Tage</b>	<b>€ 1.995,-</b>
<b>Termin/Kursort</b>	Kurssprache Deutsch	
04.10.-06.10.23	☐ Online	22.07.-24.07.24  München
13.12.-15.12.23	Düsseldorf	22.07.-24.07.24  Online
13.12.-15.12.23	Online	30.09.-02.10.24  Online
18.03.-20.03.24	Frankfurt	30.09.-02.10.24  Wien
18.03.-20.03.24	Online	18.11.-20.11.24  Frankfurt
22.05.-24.05.24	Hamburg	18.11.-20.11.24  Online
22.05.-24.05.24	Online	

Stand 28.09.2023



**EXPERTeach**



# Inhaltsverzeichnis

## Security für VoIP – Verschlüsselung, Authentisierung und Firewalls

<b>1 Grundlagen</b>	<b>3.3 Authentisierung</b>	<b>5.1.5 SIP Digest</b>
<b>1.1 Einleitung</b>	<b>3.3.1 Initiale Authentisierung</b>	<b>5.1.6 NASS-IMS-Bundled Authentication (NBA)</b>
<b>1.2 VoIP-Infrastruktur</b>	<b>3.3.2 Integrität der Folgepakete</b>	<b>5.2 Generic Bootstrapping Architecture</b>
<b>1.2.1 Endgeräte</b>	<b>3.3.3 Authentisieren mit Pre-Shared Key</b>	<b>5.3 RCS</b>
<b>1.2.2 VoIP im Enterprise-Umfeld</b>	<b>3.3.4 Identität bei VoIP</b>	<b>5.3.1 Auto-Konfiguration</b>
<b>1.2.3 IP Centrex</b>	<b>3.3.5 Register mit Authentisierung</b>	<b>5.3.2 Registrierung</b>
<b>1.2.4 VoIP für Privatkunden</b>	<b>3.3.6 SIP Identity</b>	<b>5.4 SIP-Trunking</b>
<b>1.2.5 SIP Trunking</b>	<b>3.4 Absichern des Medienstroms</b>	<b>5.4.1 Registration Mode</b>
<b>1.3 VoIP über das Internet</b>	<b>3.4.1 SRTP und SRTCP – Paketformate</b>	<b>5.4.2 Static Mode</b>
<b>1.4 WebRTC</b>	<b>3.4.2 Verschlüsselung bei SRTP</b>	<b>5.4.3 Identität</b>
<b>1.5 Session Initiation Protocol (SIP)</b>	<b>3.4.3 Authentisierung bei SRTP</b>	
<b>1.5.1 Adressierung</b>	<b>3.4.4 Key Management von SRTP</b>	<b>6 Integration in die Security-Infrastruktur</b>
<b>1.5.2 Aufgaben von SIP Proxys</b>	<b>3.4.5 Key Management</b>	<b>6.1 Session Border Controller</b>
<b>1.5.3 Die Requests von INVITE bis BYE</b>	<b>3.4.6 Schlüsselmanagement für die Signalisierung</b>	<b>6.1.1 Architektur</b>
<b>1.5.4 Ein Session-Aufbau im Detail</b>	<b>3.4.7 Schlüsselmanagement im Session Description Protocol</b>	<b>6.1.2 SBC im IP Multimedia Subsystem (IMS)</b>
<b>1.5.5 Sicherheitsrelevante Felder</b>	<b>3.4.8 MIKEY</b>	<b>6.1.3 Enterprise-SBC</b>
<b>1.5.6 Der Message Body</b>	<b>3.4.9 ZRTP</b>	<b>6.2 VoIP und Firewalls</b>
<b>1.5.7 Session Description Protocol</b>	<b>3.4.10 KMS-basierte Schlüsselverteilung</b>	<b>6.2.1 State Tables</b>
<b>2 Angriffe auf VoIP</b>	<b>3.4.11 DTLS-basierter Schlüsselaustausch</b>	<b>6.2.2 Application Layer Gateway</b>
<b>2.1 Prinzipielle Gefahren für VoIP</b>	<b>3.4.12 T.38 und Security</b>	<b>6.3 VoIP und NAT</b>
<b>2.2 Angriff auf die Vertraulichkeit</b>	<b>3.4.13 MSRP und Security</b>	<b>6.3.1 NAT und VoIP</b>
<b>2.2.1 Sniffing und Man in the Middle Attacks</b>	<b>3.5 Absichern der Signalisierung</b>	<b>6.3.2 Hosted NAT (Latching)</b>
<b>2.2.2 Ermittlung von Kenngrößen</b>	<b>3.5.1 SIP und TLS</b>	<b>6.3.3 STUN</b>
<b>2.3 Angriffe auf die Integrität</b>	<b>3.5.2 S/MIME</b>	<b>6.3.4 TURN</b>
<b>2.3.1 Angriff auf den Medienstrom</b>	<b>3.5.3 SIP und IPsec</b>	<b>6.3.5 Interactive Connectivity Establishment (ICE)</b>
<b>2.3.2 Angriff auf die Signalisierung</b>	<b>3.6 VPN-Lösungen</b>	<b>6.4 NAT und Early Media</b>
<b>2.4 Angriffe auf die Geräte</b>		
<b>2.4.1 Denial of Service</b>	<b>4 Sicherheitsmaßnahmen im Enterprise-Umfeld</b>	
<b>2.4.2 Buffer Overflow</b>	<b>4.1 VoIP im LAN</b>	
<b>2.4.3 Trojanische Pferde etc.</b>	<b>4.1.1 VLANs</b>	
<b>2.4.4 Theft of Service</b>	<b>4.1.2 Das Telefon als Switch</b>	
<b>2.4.5 Spam for IP Telephony (SPIT)</b>	<b>4.2 Security-Maßnahmen im LAN</b>	
<b>2.5 Fazit</b>	<b>4.2.1 Voice VLANs</b>	
<b>2.6 Ziele von Security bei VoIP</b>	<b>4.2.2 Port Security</b>	
<b>2.6.1 Vertraulichkeit</b>	<b>4.2.3 Authentisierung mit IEEE 802.1X</b>	
<b>2.6.2 Datenintegrität</b>	<b>4.3 Mobile Mitarbeiter</b>	
<b>2.6.3 Authentizität</b>	<b>4.4 Inbetriebnahme von Hardphones</b>	
<b>2.6.4 Verfügbarkeit</b>		
<b>3 Absichern der Verbindungen</b>	<b>5 VoIP-Security im Providernetz</b>	
<b>3.1 Security-Grundlagen</b>	<b>5.1 Architektur der IMS Security im Überblick</b>	
<b>3.1.1 Verschlüsselung</b>	<b>5.1.1 Wer mit wem im IMS?</b>	
<b>3.1.2 Zertifikate</b>	<b>5.1.2 Identitäten im IMS</b>	
<b>3.1.3 Integrität über Hash-Werte</b>	<b>5.1.3 Authentication and Key Agreement: Erste Wahl im IMS</b>	
<b>3.2 Besonderheiten bei VoIP</b>	<b>5.1.4 IMS AKA: Der Ablauf</b>	

