

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
- Lokale Authentisierung und über Proxy-Ketten
- Probleme mit Zertifikaten
- SIPS und S/MIME
- SRTP und SRTCP
- Schlüsselmanagement mit SDES und MIKEY
- VoIP und IPSec
- NAT-Probleme: STUN, TURN und ICE
- Firewalls und VoIP
- Session Border Controller

Jeder Teilnehmer erhält ausführliche Kursunterlagen aus der Reihe ExperTeach Networking in deutscher Sprache.

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.

Vormerkung und Buchung

Gerne merken wir für Sie für die Dauer von zwei Wochen kostenfrei und unverbindlich einen Kursplatz vor. Auf www.experteach.de können Sie unter *Anmeldung* bequem Vormerkung, Buchung und Hotelreservierung vornehmen. Oder rufen Sie uns einfach an unter 06074-4868-0.

Für geschlossene Teilnehmergruppen modifizieren wir diesen Kursinhalt gerne entsprechend Ihren Anforderungen. Bitte sprechen Sie uns an!



Auf Wunsch senden wir Ihnen gerne unseren kompletten Katalog zu, der Sie über alle Trainings und andere Dienstleistungen informiert.

3 Tage € 1.545,00 • CHF 2.395,00 • zzgl. MwSt.

Termin/Kursort

| | | | |
|-----------------|------------|-----------------|---------|
| 13.06.-15.06.12 | Hamburg | 22.10.-24.10.12 | Wien |
| 13.08.-15.08.12 | Frankfurt | 22.10.-24.10.12 | München |
| 19.09.-21.09.12 | Düsseldorf | 10.12.-12.12.12 | Hamburg |

Aktuelle Informationen finden Sie auf www.experteach.de SEVO





Security für VoIP – Verschlüsselung, Authentisierung und Firewalls

1 Grundlagen

- 1.1 Einleitung
- 1.2 Die VoIP-Infrastruktur
 - 1.2.1 Endgeräte
 - 1.2.2 VoIP im Enterprise
 - 1.2.3 VoIP im Provider Backbone
 - 1.2.4 VoIP für Privatkunden
 - 1.2.5 Das IP Multimedia Subsystem
- 1.3 Session Initiation Protocol (SIP)
 - 1.3.1 Adressierung
 - 1.3.2 Aufgaben von SIP Proxys
 - 1.3.3 Der Protokoll-Aufbau
 - 1.3.4 Die Requests von INVITE bis BYE
 - 1.3.5 Ein Session-Aufbau im Detail
 - 1.3.6 Session Description Protocol
 - 1.3.7 H.323
 - 1.3.8 H.248/MEGACO
- 1.4 Ziele von Security bei VoIP
 - 1.4.1 Vertraulichkeit
 - 1.4.2 Datenintegrität
 - 1.4.3 Authentizität
 - 1.4.4 Nachweisbarkeit
 - 1.4.5 Verfügbarkeit

2 Angriffe auf VoIP

- 2.1 Prinzipielle Gefahren für VoIP
- 2.2 Angriff auf die Vertraulichkeit
 - 2.2.1 Sniffing und Man in the Middle Attacks
 - 2.2.2 Ermittlung von Kenngrößen
- 2.3 Angriffe auf die Integrität
 - 2.3.1 Angriff auf den Medienstrom
 - 2.3.2 Angriff auf die Signalisierung
- 2.4 Angriffe auf die Geräte
 - 2.4.1 Denial of Service
 - 2.4.2 Buffer Overflow
 - 2.4.3 Trojanische Pferde etc.
 - 2.4.4 Theft of Service
- 2.5 Spam for IP Telephony (SPIT)
- 2.6 Fazit

3 Netzsicherheit

- 3.1 VoIP im LAN
 - 3.1.1 VLANs
 - 3.1.2 Der Anschluss von IP-Telefonen
 - 3.1.3 Das Telefon als Switch
- 3.2 Gefahren im LAN
 - 3.2.1 ARP Cache Poisoning
 - 3.2.2 Fluten der Switching Table
 - 3.2.3 VLAN Hopping
 - 3.2.4 Mirror Ports
 - 3.2.5 Rogue DHCP Server
 - 3.2.6 Spanning-Tree-Angriffe

- 3.3 Security-Maßnahmen im LAN
 - 3.3.1 Voice VLANs
 - 3.3.2 Port Security
 - 3.3.3 Authentisierung mit IEEE 802.1X
- 3.4 WLAN-Aspekte
 - 3.4.1 Sicherheit mit WPA / IEEE 802.11i
 - 3.4.2 Authentifizierung nach IEEE 802.1X
- 3.5 DSL
- 3.6 Mobilfunk
- 3.7 MPLS-Backbone
- 3.8 Das Internet

4 Absichern der Verbindungen

- 4.1 Security-Grundlagen
 - 4.1.1 Verschlüsselung
 - 4.1.2 Integrität über Hash-Werte
 - 4.1.3 Authentisierung
- 4.2 Besonderheiten bei VoIP
- 4.3 Identität bei VoIP
 - 4.3.1 Lokale Authentisierung
 - 4.3.2 Authentisierung über Proxy-Ketten
 - 4.3.3 Authentisierung mittels P-Asserted-Identity
- 4.4 Absichern der Signalisierung
 - 4.4.1 SIPS
 - 4.4.2 S/MIME
- 4.5 Absichern des Medienstroms
 - 4.5.1 SRTP und SRTCP – Paketformate
 - 4.5.2 Verschlüsselung bei SRTP
 - 4.5.3 Authentisierung bei SRTP
- 4.6 Key Management
 - 4.6.1 Schlüsselmanagement für die Signalisierung
 - 4.6.2 Schlüsselmanagement im Session Description Protocol
 - 4.6.3 MIKEY
 - 4.6.4 ZRTP
- 4.7 VPN-Lösungen
 - 4.7.1 SSL VPNs
 - 4.7.2 IPsec VPNs

5 Integration in die Security-Infrastruktur

- 5.1 NAT und VoIP
 - 5.1.1 STUN
 - 5.1.2 TURN
 - 5.1.3 Interactive Connectivity Establishment (ICE)
- 5.2 VoIP und Firewalls
 - 5.2.1 State Tables
 - 5.2.2 Application Layer Gateway
 - 5.2.3 MIDCOM
- 5.3 Session Border Controller
 - 5.3.1 Lösen des NAT-Problems
 - 5.3.2 Accounting

- 5.3.3 Architektur
- 5.3.4 SBC im Provider-Umfeld
- 5.3.5 SBC im IP Multimedia Subsystem (IMS)
- 5.3.6 SBC im Enterprise



ExperTeach Gesellschaft für Netzwerkkompetenz mbH

Waldstr. 94 • D-63128 Dietzenbach
 Telefon +49 6074 4868-0 • Telefax +49 6074 4868-109
 info@experteach.de • www.experteach.de

© ExperTeach GmbH, alle Angaben ohne Gewähr

Stand 08.05.2012