

# 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.expertech.at](http://www.expertech.at) 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 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.expertech.at](http://www.expertech.at) SEVO





|   |  |   |
|---|--|---|
| <b>1 Grundlagen</b>                                 | <b>3.3</b> Security-Maßnahmen im LAN                             | <b>5.3.3</b> Architektur                          |
| <b>1.1</b> Einleitung                               | <b>3.3.1</b> Voice VLANs   | <b>5.3.4</b> SBC im Provider-Umfeld               |
| <b>1.2</b> Die VoIP-Infrastruktur                   | <b>3.3.2</b> Port Security                                       | <b>5.3.5</b> SBC im IP Multimedia Subsystem (IMS) |
| <b>1.2.1</b> Endgeräte                              | <b>3.3.3</b> Authentisierung mit IEEE 802.1X                     | <b>5.3.6</b> SBC im Enterprise                    |
| <b>1.2.2</b> VoIP im Enterprise                     | <b>3.4</b> WLAN-Aspekte  |   |
| <b>1.2.3</b> VoIP im Provider Backbone              | <b>3.4.1</b> Sicherheit mit WPA / IEEE 802.11i                   |   |
| <b>1.2.4</b> VoIP für Privatkunden                  | <b>3.4.2</b> Authentifizierung nach IEEE 802.1X                  |   |
| <b>1.2.5</b> Das IP Multimedia Subsystem            | <b>3.5</b> DSL   |   |
| <b>1.3</b> Session Initiation Protocol (SIP)        | <b>3.6</b> Mobilfunk   |   |
| <b>1.3.1</b> Adressierung                           | <b>3.7</b> MPLS-Backbone   |   |
| <b>1.3.2</b> Aufgaben von SIP Proxys                | <b>3.8</b> Das Internet  |   |
| <b>1.3.3</b> Der Protokoll-Aufbau                   |  |   |
| <b>1.3.4</b> Die Requests von INVITE bis BYE        | <b>4 Absichern der Verbindungen</b>                              |   |
| <b>1.3.5</b> Ein Session-Aufbau im Detail           | <b>4.1</b> Security-Grundlagen                                   |   |
| <b>1.3.6</b> Session Description Protocol           | <b>4.1.1</b> Verschlüsselung                                     |   |
| <b>1.3.7</b> H.323                                  | <b>4.1.2</b> Integrität über Hash-Werte                          |   |
| <b>1.3.8</b> H.248/MEGACO                           | <b>4.1.3</b> Authentisierung                                     |   |
| <b>1.4</b> Ziele von Security bei VoIP              | <b>4.2</b> Besonderheiten bei VoIP                               |   |
| <b>1.4.1</b> Vertraulichkeit                        | <b>4.3</b> Identität bei VoIP                                    |   |
| <b>1.4.2</b> Datenintegrität                        | <b>4.3.1</b> Lokale Authentisierung                              |   |
| <b>1.4.3</b> Authentizität                          | <b>4.3.2</b> Authentisierung über Proxy-Ketten                   |   |
| <b>1.4.4</b> Nachweisbarkeit                        | <b>4.3.3</b> Authentisierung mittels P-Asserted-Identity         |   |
| <b>1.4.5</b> Verfügbarkeit                          | <b>4.4</b> Absichern der Signalisierung                          |   |
| <b>2 Angriffe auf VoIP</b>                          | <b>4.4.1</b> SIPS  |   |
| <b>2.1</b> Prinzipielle Gefahren für VoIP           | <b>4.4.2</b> S/MIME  |   |
| <b>2.2</b> Angriff auf die Vertraulichkeit          | <b>4.5</b> Absichern des Medienstroms                            |   |
| <b>2.2.1</b> Sniffing und Man in the Middle Attacks | <b>4.5.1</b> SRTP und SRTCP – Paketformate                       |   |
| <b>2.2.2</b> Ermittlung von Kenngrößen              | <b>4.5.2</b> Verschlüsselung bei SRTP                            |   |
| <b>2.3</b> Angriffe auf die Integrität              | <b>4.5.3</b> Authentisierung bei SRTP                            |   |
| <b>2.3.1</b> Angriff auf den Medienstrom            | <b>4.5.4</b> Key Management von SRTCP                            |   |
| <b>2.3.2</b> Angriff auf die Signalisierung         | <b>4.6</b> Key Management  |   |
| <b>2.4</b> Angriffe auf die Geräte                  | <b>4.6.1</b> Schlüsselmanagement für die Signalisierung          |   |
| <b>2.4.1</b> Denial of Service                      | <b>4.6.2</b> Schlüsselmanagement im Session Description Protocol |   |
| <b>2.4.2</b> Buffer Overflow                        | <b>4.6.3</b> MIKEY   |   |
| <b>2.4.3</b> Trojanische Pferde etc.                | <b>4.6.4</b> ZRTP  |   |
| <b>2.4.4</b> Theft of Service                       | <b>4.7</b> VPN-Lösungen  |   |
| <b>2.5</b> Spam for IP Telephony (SPIT)             | <b>4.7.1</b> SSL VPNs  |   |
| <b>2.6</b> Fazit                                    | <b>4.7.2</b> IPsec VPNs  |   |
| <b>3 Netzsicherheit</b>                             | <b>5 Integration in die Security-Infrastruktur</b>               |   |
| <b>3.1</b> VoIP im LAN                              | <b>5.1</b> NAT und VoIP  |   |
| <b>3.1.1</b> VLANs                                  | <b>5.1.1</b> STUN  |   |
| <b>3.1.2</b> Der Anschluss von IP-Telefonen         | <b>5.1.2</b> TURN  |   |
| <b>3.1.3</b> Das Telefon als Switch                 | <b>5.1.3</b> Interactive Connectivity Establishment (ICE)        |   |
| <b>3.2</b> Gefahren im LAN                          | <b>5.2</b> VoIP und Firewalls                                    |   |
| <b>3.2.1</b> ARP Cache Poisoning                    | <b>5.2.1</b> State Tables  |   |
| <b>3.2.2</b> Fluten der Switching Table             | <b>5.2.2</b> Application Layer Gateway                           |   |
| <b>3.2.3</b> VLAN Hopping                           | <b>5.2.3</b> MIDCOM  |   |
| <b>3.2.4</b> Mirror Ports                           | <b>5.3</b> Session Border Controller                             |   |
| <b>3.2.5</b> Rogue DHCP Server                      | <b>5.3.1</b> Lösen des NAT-Problems                              |   |
| <b>3.2.6</b> Spanning-Tree-Angriffe                 | <b>5.3.2</b> Accounting  |   |



**ExperTeach GmbH Training Center Wien**

Millennium Tower, 24. Etage  
Handelskai 94-96 • A-1200 Wien  
Telefon +43 66 43 45 39 64  
info@experteach.at • www.experteach.at

© ExperTeach GmbH, alle Angaben ohne Gewähr

Stand 08.05.2012