

# Security for VoIP

## Encryption, Authentication, and Firewalls

The hackers do not lack any fantasy—they develop and utilize new types of attacks on IP end devices and applications every day. In this context, VoIP opens completely new options for attackers. Comprehensive know-how is required by those aiming to adequately protect their own VoIP installation.

### Course Contents

- Security Problems in the LAN: Sniffing and Man-in-the-Middle Attacks
- ARP Cache Poisoning
- Switching Table Corruption and Flooding
- VLAN Hopping
- Port Security and Authentication According to IEEE 802.1X
- Denial of Service (DOS)
- VoIP and WLAN
- SRTP and SRTCP
- Key Management with MIKEY
- VoIP and IPSec
- Attacks on Signaling
- Firewalls and VoIP
- Dynamic Ports and State Tables
- NAT Problems: STUN and TURN
- Application Level Gateways and Session Border Controller

In this course of the ExperTeach Networking series, each student will receive the comprehensive ExperTeach course documentation.

### Target Group

This course addresses designers and technicians responsible for the design and implementation of VoIP installations.

### Knowledge Prerequisites

Profound know-how of the IP protocol family and common LAN technologies is required. Sound basic knowledge about VoIP is another prerequisite.

### Course Objectives

The course systematically analyzes points of attack of VoIP and discusses various protection measures. The students learn how to provide adequate VoIP security in their own future projects.



### Reservation and Registration

We will be glad to make a free and non-binding course reservation for you for the duration of two weeks. On [www.experteach-training.com](http://www.experteach-training.com) under *Registration*, you can conveniently make course reservations, registrations, and hotel reservations. Alternatively, call us under +49 6074 4868-0.

For closed groups of participants, we can modify the course contents according to your requirements. Do not hesitate to contact us!



2 days €1,195 exclusive of V.A.T.

### Course date (mm/dd/yy)/Location

02/06-02/08/12	Frankfurt	08/13-08/15/12	Frankfurt
03/21-03/23/12	Düsseldorf	09/19-09/21/12	Düsseldorf
05/02-05/04/12	München	10/22-10/24/12	München
05/02-05/04/12	Wien	10/22-10/24/12	Wien
06/13-06/15/12	Hamburg	12/10-12/12/12	Hamburg

Up-to-date information: [www.experteach-training.com](http://www.experteach-training.com) SEVO



EXPERTeach





## Security for VoIP – Encryption, Authentication, and Firewalls

- 1 Threats for VoIP**
  - 1.1 The VoIP Infrastructure
    - 1.1.1 SIP
    - 1.1.2 H.323
  - 1.2 Objectives of VoIP Security
    - 1.2.1 Confidentiality
    - 1.2.2 Integrity and Authenticity
    - 1.2.3 Traceability
    - 1.2.4 Availability
  - 1.3 Attacks on Signaling
  - 1.4 Attacks on Payload
    - 1.4.1 Eavesdropping
    - 1.4.2 Forging
  - 1.5 Attacks on the Devices
    - 1.5.1 Denial of Service
    - 1.5.2 Theft of Service
    - 1.5.3 Spam for IP Telephony (SPIT)
    - 1.5.4 Trojan Horses, etc.
- 2 VoIP Security in the LAN**
  - 2.1 VoIP in the LAN
    - 2.1.1 Redundancy and Spanning Tree
    - 2.1.2 IEEE 802.1Q and 802.1p
    - 2.1.3 Connection of IP Phones
    - 2.1.4 The Phone as a Switch
  - 2.2 Sniffing and Man-in-the-Middle Attacks
    - 2.2.1 ARP Cache Poisoning
    - 2.2.2 ICMP Redirect and Router Advertisement
    - 2.2.3 Flooding the Switching Table
    - 2.2.4 Rogue DHCP Server
    - 2.2.5 VLAN Hopping
    - 2.2.6 Spanning Tree Attacks
    - 2.2.7 Mirror Ports
  - 2.3 Security Measures in the LAN
    - 2.3.1 Voice VLANs
    - 2.3.2 Port Security
    - 2.3.3 Authentication with IEEE 802.1X
  - 2.4 WLAN Aspects
    - 2.4.1 Problems with WEP
    - 2.4.2 Security with WPA / IEEE 802.11i
- 3 Security with SRTP**
  - 3.1 SRTP and SRTCP
  - 3.2 Symmetrical Encryption
  - 3.3 Encryption with SRTP
    - 3.3.1 AES Counter Mode
    - 3.3.2 Key Management
  - 3.4 Authentication
    - 3.4.1 Hash Values
    - 3.4.2 Keyed Hash
  - 3.5 Authentication with SRTP
  - 3.6 Lifetime and Distribution of the Master Keys

- 3.6.1 MIKEY
- 3.6.2 MIKEY with Pre-Shared Key
- 3.6.3 MIKEY with Public Key
- 3.6.4 MIKEY with Diffie-Hellman
- 3.7 Overhead and Efficiency
- 4 VoIP with IPSec and Secure Signaling**
  - 4.1 IPSec
    - 4.1.1 Tunnel Mode and Transport Mode
    - 4.1.2 Encapsulating Security Payload (ESP)
    - 4.1.3 IPSec and VoIP
    - 4.1.4 Overhead and Efficiency
  - 4.2 Security and SIP
    - 4.2.1 SIPS
    - 4.2.2 S/MIME
  - 4.3 H.235
    - 4.3.1 Secure Signaling
    - 4.3.2 Secure Media Streams
- 5 VoIP and Firewalls**
  - 5.1 NAT and VoIP
    - 5.1.1 STUN
    - 5.1.2 TURN
    - 5.1.3 Additional Problems with IPSec
  - 5.2 VoIP and Firewalls
    - 5.2.1 State Tables
    - 5.2.2 Application Layer Gateway
    - 5.2.3 MIDCOM
    - 5.2.4 Session Border Controller
- A List of Abbreviations**



**ExperTeach Gesellschaft für Netzwerkkompetenz mbH**

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

© ExperTeach GmbH, all specifications made are exempted from liability.

Status 12/21/2011