

Security for VoIP

Encryption, Authentication, and Firewalls

While the topic of security was of minor significance in traditional telephony, it can no longer be neglected during the integration into the IP world without becoming guilty of gross negligence. Anyone who intends to protect their VoIP installations should be familiar both with the impending threats and the countermeasures. The course systematically analyzes points of attack of VoIP and explains the available protective measures on the network and application layer. The latter are then weighted on the basis of the different VoIP architectures. The students learn how to provide adequate VoIP security in their own future projects.

Course Contents

- Principle Dangers for VoIP
- Attack on the Media Stream
- Attacks on Signaling
- Attacks on the Devices
- Security Measures in the LAN and WLAN
- Port Security and Authentication According to 802.1X
- Security Measures in the WAN
- Identity under VoIP (SIP Identity)
- Local Authentication and via Proxy Chains
- Problems with Certificates
- SIPS and S/MIME
- SRTP and SRTCP
- Key Management with SDES, ZRTP, DTLS, and MIKEY
- WebRTC
- VoIP and IPSec
- NAT Solutions: STUN, TURN, and ICE
- Firewalls and VoIP
- Session Border Controller
- SIP-Connect 2.0

E-Book You will receive the comprehensive documentation package of the ExperTeach Networking series – printed documentation, e-book, and personalized PDF! As online participant, you will receive the e-book and the personalized PDF.

Target Group

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

Prerequisites

Profound know-how of the TCP/IP protocol family and common LAN technologies is required. Students should be familiar with security concepts, such as encryption and authentication. These can be imparted, for instance, in the Security Concepts and Technologies – Encryption, Authentication and Data Integrity course. Sound basic knowledge about VoIP is another prerequisite.

This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

www.experteach-training.com/go/SEVO

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training	Prices, excl. of V.A.T.	
Classes in Germany	3 Days	€ 1,795
Online Training	3 Days	€ 1,795
Date/course venue	Course language German 	
06/03-08/03/23  Frankfurt	06/03-08/03/23	 Online

Status 11/13/2022



Table of Contents

Security for VoIP – Encryption, Authentication, and Firewalls

1 Fundamentals	2.6.4 Availability	4.2.1 Voice VLANs
1.1 Introduction	3 Securing connections	4.2.2 Port security
1.2 VoIP infrastructure	3.1 Security basics	4.2.3 Authentication with IEEE 802.1X
1.2.1 End devices	3.1.1 Encryption	4.3 Mobile employees
1.2.2 VoIP in the enterprise environment	3.1.2 Certificates	4.4 Commissioning of hardphones
1.2.3 IP Centrex	3.1.3 Integrity via hash values	5 VoIP security in the provider network
1.2.4 VoIP for residential customers	3.2 Special features of VoIP	5.1 Overview of IMS Security architecture
1.2.5 SIP Trunking	3.3 Authentication	5.1.1 Who with whom in the IMS?
1.3 VoIP over the Internet	3.3.1 Initial authentication	5.1.2 Identities in the IMS
1.4 WebRTC	3.3.2 Integrity of subsequent packets	5.1.3 Authentication and Key Agreement: First Choice in the IMS
1.5 Session Initiation Protocol (SIP)	3.3.3 Authentication with Pre-Shared Key	5.1.4 IMS AKA: The procedure
1.5.1 Addressing	3.3.4 Identity with VoIP	5.1.5 SIP Digest
1.5.2 Tasks of SIP Proxies	3.3.5 Register with authentication	5.1.6 NASS-IMS Bundled Authentication (NBA)
1.5.3 The requests from INVITE to BYE	3.3.6 SIP Identity	5.2 Generic Bootstrapping Architecture
1.5.4 A session structure in detail	3.4 Securing the media stream	5.3 RCS
1.5.5 Security relevant fields	3.4.1 SRTP and SRTCP packet formats	5.3.1 Auto Configuration
1.5.6 The Message Body	3.4.2 Encryption for SRTP	5.3.2 Registration
1.5.7 Session Description Protocol	3.4.3 Authentication for SRTP	5.4 SIP Trunking
2 Attacks on VoIP	3.4.4 Key management of SRTP	5.4.1 Registration Mode
2.1 Basic threats to VoIP	3.4.5 Key management	5.4.2 Static Mode
2.2 Attacks on confidentiality	3.4.6 Key management for signaling	5.4.3 Identity
2.2.1 Sniffing and Man in the Middle Attacks	3.4.7 Key management in Session Description Protocol	6 Integration into the security infrastructure
2.2.2 Identifying characteristics	3.4.8 MIKEY	6.1 Session Border Controller
2.3 Attacks on integrity	3.4.9 ZRTP	6.1.1 Architecture
2.3.1 Attack on the media stream	3.4.10 KMS-based key distribution	6.1.2 SBC in the IP Multimedia Subsystem (IMS)
2.3.2 Attack on the signaling	3.4.11 DTLS-based key exchange	6.1.3 Enterprise SBC
2.4 Attacks on the devices	3.4.12 T.38 and security	6.2 VoIP and firewalls
2.4.1 Denial of Service	3.4.13 MSRP and security	6.2.1 State Tables
2.4.2 Buffer overflow	3.5 Securing Signaling	6.2.2 Application Layer Gateway
2.4.3 Trojan horses etc.	3.5.1 SIP and TLS	6.3 VoIP and NAT
2.4.4 Theft of Service	3.5.2 S/MIME	6.3.1 NAT and VoIP
2.4.5 Spam for IP Telephony (SPIT)	3.5.3 SIP and IPsec	6.3.2 Hosted NAT (Latching)
2.5 Conclusion	3.6 VPN solutions	6.3.3 STUN
2.6 Objectives of security in VoIP	4 Security measures in the enterprise environment	6.3.4 TURN
2.6.1 Confidentiality	4.1 VoIP in the LAN	6.3.5 Interactive Connectivity Establishment (ICE)
2.6.2 Data integrity	4.1.1 VLANs	6.4 NAT and Early Media
2.6.3 Authenticity	4.1.2 The telephone as a switch	
	4.2 Security measures in the LAN	



ExperTech GmbH

Waldstraße 94 • 63128 Dietzenbach • Phone: +49 6074 4868-0 • Fax: +49 6074 4868-109
 info@expertech.de • www.expertech-training.com

