

Course ID

**SIPSEC**

Course Duration

**2 days**

Course Title

**SIP Security: A Comprehensive Short Course**

**Related Courses**

- VoIP Security (VOIPSEC, 2 days)
- Principles of Network Security: CompTIA Security+ and US DoD Directive 8570.1 (NETSEC, 3-4 days)
- VoIP: Protocols, Design, and Implementation (VOIP, 2-3 days)
- State-of-the-art of VoIP Technology for Professionals, Managers, and Executives (VOIP-EXEC, 1 day)
- IMS: The Technology, Applications, and Challenges (IMS, 2 days)
- 3G, IMS, and the Carrier Business Economics (3G-IMS-STRAT, 2 days)
- Multimedia Applications: IMS, SIP, and VoIP (MULTIMEDIA, 2 days)
- IP-Based Systems: TCP/IP and Mobile IP (IPSYS, 2-3 days)
- Internetworking with TCP/IP Version 6 (IPV6, 2-3 days)
- MPLS: Integrated Routing with End-to-End QoS for the Next Generation Networks (MPLS, 2-3 days)
- Traffic Engineering Models for Network Design (TRAFFIC, 3 days)

**Aimed At**

Network security planning teams, network administrators, IT and telecommunications engineers, IT security management, multimedia applications/services designers and marketing/sales professionals will benefit from this course. The course will also be of interest to the homeland security, crime prevention/investigation, and law enforcement community.

**Group Size**

5-25

**Prerequisites**

- SIP Protocol, Architecture, and Design (SIP, 1 day)

Those contemplating taking this course should have completed the above course or possess equivalent knowledge and experience.

## **Course in a Nutshell**

Security is a concern for every company at every level. The introduction of media gateways to handle traditional telephony converted to SIP protocol for VoIP introduces many security management challenges on the data network. If not using media gateways, many organizations are starting to use VoIP providers who carry voice traffic on an IP network connection using the SIP protocol. The widespread adoption of SIP opens potential threats exposing the vulnerabilities of the protocol.

This course will help you understand the issues of network security as they relate to the use of the SIP protocol. We will examine the security vulnerabilities of the protocol as well as each component in a SIP design for a comprehensive review of SIP security issues. We will conclude with a discussion of the policies and procedures that enhance SIP security.

## **Customize It!**

Are you an engineer, technician, network administrator, decision maker, procurement specialist, or marketing/sales professional looking for SIP security training from your own unique perspective?

We can customize this course, usually at little to no additional cost, to a variety of audiences, orientations (business versus technical), tech level (high-level overview versus in-depth technical detail), and industries (commercial, government agencies, or military).

## **Learn How To**

- Learn how to evaluate your SIP security concerns on all levels
- Understand the key components for security planning purposes
- Discern security vulnerabilities of SIP at the protocol layer
- Design for secure network communications by understanding protocol level attack methods

## **Course Outline**

- SIP Security: An Introduction
  - SIP security challenges: An overview
  - How SIP security fits into the overall data security strategy
  - How SIP security relates to the traditional telecommunications security
  - Discussion of the SIP protocol using the OSI model
  - SIP's architectural vulnerabilities
- Physical Layer Security: Discussion of Security Factors of SIP Endpoints (Telephones)
  - Configuration files
  - Tools for loading configuration files
  - User access levels
  - Other security factors

- Data Link Layer Security
  - Firewalls and NAT's
  - SIP architecture and potential threats that are handled by the firewall
  - Denial of Service (DoS) attacks
    - DoS attacks on SIP network components
    - DoS risk mitigation
- Transport Layer Security: Digest Authentication and SIP
  - How it is implemented in the SIP protocol
  - How it is used against threats or attacks.
- Session Layer Security
  - Security vulnerabilities of the SIP protocol
    - SIP standard and attacks
    - IETF and security standards
  - Application-level security vulnerabilities
    - General
    - Vendor-specific issues for the leading vendors
  - Encryption issues for SIP
    - Encryption as it relates to SIP
    - Tradeoff between real-time processing requirements and security
- Presentation Layer Security: Rights and Access Levels
- Application Layer Security: Load Balancers, Proxy Servers, Media Servers, etc.
  - Securing SIP architecture components
  - Password issues with SIP and applications
  - User authentication
  - Remote system access issues
- Network Security Issues and SIP
  - New vulnerabilities related to SIP messages on the network
  - How SIP fits into the current network security plans and designs
- Security of Gateways, One of the Most Vulnerable Elements of SIP design
- Security Best Practices Related to the SIP Protocol
  - Security audit methods
  - Vendor management
  - Testing systems and devices: Available tools
- Wrap-up: Course Recap, Q/A, and Evaluations

**How You Will  
Learn**

- A seasoned instructor, who is also a SIP/VoIP expert, will present this course in interactive lecture format.
- Along with lecture, we will employ discussion, activities, and exercises to make the class more interesting and useful.
- If you already know something about SIP and security issues, we will build on that knowledge. If your background is less technical, we will leverage appropriate examples and analogies to convey the technical material in terms that are easier to understand.
- You will receive a printed Participant Handbook which will provide you with a record of the instructor presentation and class interaction for recall and reference back on your job.

*Revised*

*May 15f, 2007*