Course ID
VOIPSEC

Course Title
VoIP Security

Course Duration
2 day

Related Courses

- IP-Based Systems: TCP/IP and Mobile IP (IPSYS, 2-3 days)
- Multimedia Applications: IMS, SIP, and VoIP (2 day(s), MULTIMEDIA)

Aimed At

Network security planning teams, network administrators, IT and telecom engineers, and IT security management. This course is also beneficial for the homeland security community and crime prevention/investigation officers.

Group Size

5-25

Prerequisites

- 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)

Before taking this course, you should have completed either of the two courses listed above or possess equivalent experience.

Course in a Nutshell

Security is a concern for every company at every level. The wide adoption of VoIP and new protocol standards has introduced many new issues. For most enterprises, the adoption of VoIP is a migration path – a fact that contributes to increased complexity for the IT security personal and network administrators. VoIP introduces new systems, vendors, applications, servers, operating systems, and the like. The introduction of media gateways to handle traditional telephony converted to VoIP on the data network introduces security management challenges on the network. If not using media gateways, organizations are adopting VoIP providers that carry traffic on an IP network connection.

This course will help you understand the issues of VoIP security on all levels of the network. We will follow the OSI model to ensure that all levels are covered. We will begin by learning the technical concepts related to network security. We will then study the protocols such as SIP and H.323 on the IP network. We will conclude with a discussion of the policies and procedures that enhance VoIP security.

Customize It!

- Are you involved with commercial or military deployment planning for VoIP? Depending on your background and job, we can tailor the course to focus on the technical or managerial issues.
- Are you a network engineer or administrator who would like to “fill in the holes” and catch up with the state-of-the-art of security planning? Let us know so we can focus on the areas that interest you the most.
- Are you a VoIP network or application installer who would like to learn the security concepts and theory that underlie your craft? We can focus on the tools and techniques that will help you become more “tech savvy” on VoIP

security issues.

- Are you a manager, executive, or sales person whose work involves VoIP security systems? If so, we can emphasize those parts of the course that deal with policy management, vendor audits, and procedural security issues.

Learn How To

- Learn how to evaluate your VoIP security concerns on all levels
- Understand the key components of the OSI model as they relate to VoIP security planning
- Discern security vulnerabilities of SIP and other popular VoIP protocols
- Design for secured network communications by understanding protocol level attack methods
- Formulate global policies for managing VoIP security

Course Outline

- VoIP Security: An Introduction
  - Overview of VoIP security challenges
  - How VoIP relates to overall data security strategy
  - How VoIP relates to traditional telecom security
  - Introduction to the OSI model
  - Learning VoIP security using the OSI model: An introduction
  - VoIP architectural vulnerabilities
- Physical Layer Security
  - Cabling and devices
  - Data center and server access, etc.
  - Endpoints
- Data Link Layer Security
  - Firewalls and NAT's
  - DoS Attacks
- Transport Layer Security
  - Digest authentication
- Session Layer Security
  - Protocols
    - SIP standard and attacks
    - H.323
    - IETF RFC VoIP standards
  - Application-level security vulnerabilities
    - Vendor-specific issues
  - Encryption
- Presentation Layer Security
  - Rights and access levels
- Application Layer Security
  - Password issues with VoIP and applications
  - User authentication

- Remote system access issues
- Network Security Issues and VoIP
- Gateway Security
  - MGCP
  - Megaco/H.248
- Network Policies and Security Management
- Security Best Practices
  - Security audit methods
  - Vendor management
  - Testing systems and devices: Available tools
- Wrap-up: Summary, Q/A, and Evaluations

How You Will Learn

- A seasoned instructor will present this course in interactive lecture format
- Along with lecture, we use exercises, puzzles, case studies, and interesting group activities to enrich the instruction and drive home the essential points.
- If you already know something about the technology, we will build on that. We'll compare and contrast what's familiar with what's new, making new ideas easier to learn as well as more relevant.
- If your background is less technical, we will use meaningful and ingenious examples and analogies to simplify the complex subject matter.
- You will receive a printed Participant Handbook which will help you remember and retain what you learned in class and apply it on your job.

Revised *Sept. 3, 2006*