Título:

Autor:

Editorial:

Tema:

Sinopsis

Precio: $995.00

Año: 2008

Edición: 1ª

ISBN: 9781587054693

VoIP security issues are becoming increasingly serious because voice networks and services cannot be protected from recent intelligent attacks and fraud by traditional systems such as firewalls and NAT alone. After analyzing threats and recent patterns of attacks and fraud, consideration needs to be given to the redesign of secure VoIP architectures with advanced protocols and intelligent products, such as Session Border Controller (SBC). Another type of security issue is how to implement lawful interception within complicated service architectures according to government requirements.

Voice over IP Security focuses on the analysis of current and future threats, the evaluation of security products, the methodologies of protection, and best practices for architecture design and service deployment. This book not only covers technology concepts and issues, but also provides detailed design solutions featuring current products and protocols so that you can deploy a secure VoIP service in the real world with confidence.

Voice over IP Security gives you everything you need to understand the latest security threats and design solutions to protect your VoIP network from fraud and security incidents.

Patrick Park has been working on product design, network architecture design, testing, and consulting for more than 10 years. Currently Patrick works for Cisco® as a VoIP test engineer focusing on security and interoperability testing of rich media collaboration gateways. Before Patrick joined Cisco, he worked for Covad Communications as a VoIP security engineer focusing on the design and deployment of secure network architectures and lawful interception (CALEA). Patrick graduated from the Pusan National University in South Korea, where he majored in computer engineering.

Understand the current and emerging threats to VoIP networks

Learn about the security profiles of VoIP protocols, including SIP, H.323, and MGCP

Evaluate well-known cryptographic algorithms such as DES, 3DES, AES, RAS, digital signature (DSA), and hash function (MD5, SHA, HMAC)

Analyze and simulate threats with negative testing tools

Secure VoIP services with SIP and other supplementary protocols

Eliminate security issues on the VoIP network border by deploying an SBC

Configure enterprise devices, including firewalls, Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, IP phones, and multilayer switches to secure VoIP network traffic

Implement lawful interception into VoIP service environments