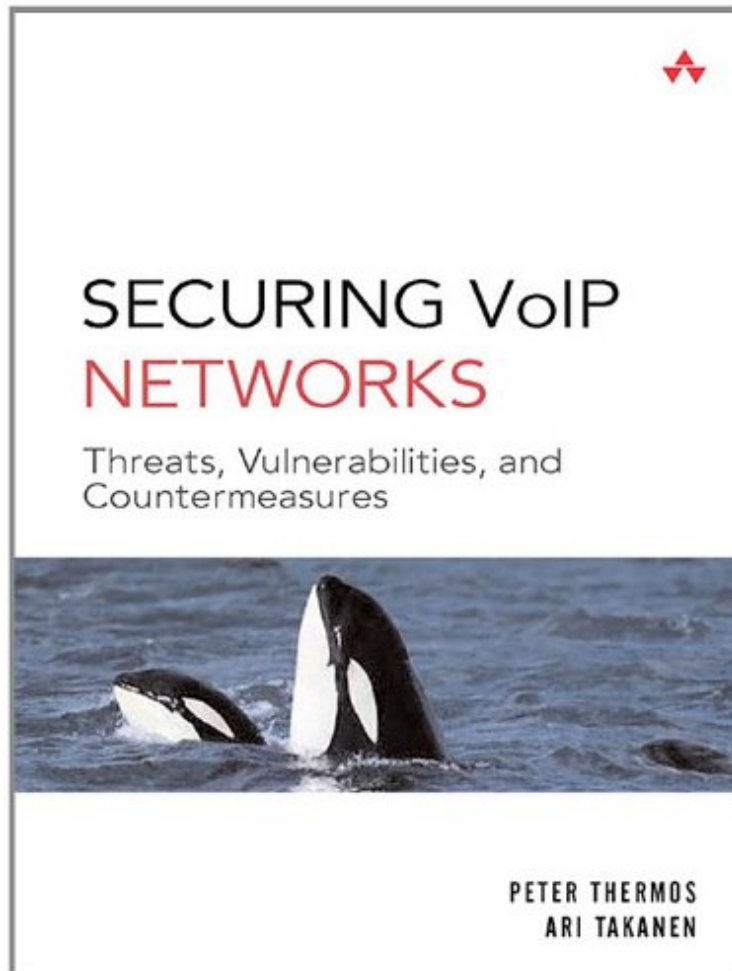


# Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures

Von Peter Thermos, Ari Takanen

*\*Download PDF | ePub | DOC | audiobook | ebooks*



 Download

 Read Online

Produktinformation -Verkaufsrang: #1746477 in eBooksVerffentlicht am: 2007-08-01Erscheinungsdatum:  
2007-08-01File Name: B0054KOKM0 | File size: 55.Mb

**Von Peter Thermos, Ari Takanen : Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures**  
before purchasing it in order to gage whether or not it would be worth my time, and all praised Securing VoIP  
Networks: Threats, Vulnerabilities, and Countermeasures:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. Securing  
VoIPVon Werner PreiningDie in diesem Buch dargestellten Grundlagen liegen bereits einige Jahre zuruck, die meisten  
haben aber auch noch heute ihre Gltigkeit. Fr jemanden der sich ernsthaft mit der Sicherheits von VoIP beschftigt, ist  
dieses Werk eine unumgngliche Grundlage. Es ist seinen Preis wert.

Kurzbeschreibung In *Securing VoIP Networks*, two leading experts systematically review the security risks and vulnerabilities associated with VoIP networks and offer proven, detailed recommendations for securing them. Drawing on case studies from their own fieldwork, the authors address VoIP security from the perspective of real-world network implementers, managers, and security specialists. The authors identify key threats to VoIP networks, including eavesdropping, unauthorized access, denial of service, masquerading, and fraud; and review vulnerabilities in protocol design, network architecture, software, and system configuration that place networks at risk. They discuss the advantages and tradeoffs associated with protection mechanisms built into SIP, SRTP, and other VoIP protocols; and review key management solutions such as MIKEY and ZRTP. Next, they present a complete security framework for enterprise VoIP networks, and provide detailed architectural guidance for both service providers and enterprise users.

- 1 Introduction
- 2 VoIP Architectures and Protocols
- 3 Threats and Attacks
- 4 VoIP Vulnerabilities
- 5 Signaling Protection Mechanisms
- 6 Media Protection Mechanisms
- 7 Key Management Mechanisms
- 8 VoIP and Network Security Controls
- 9 A Security Framework for Enterprise VoIP Networks
- 10 Provider Architectures and Security
- 11 Enterprise Architectures and Security

Kurzbeschreibung In *Securing VoIP Networks*, two leading experts systematically review the security risks and vulnerabilities associated with VoIP networks and offer proven, detailed recommendations for securing them. Drawing on case studies from their own fieldwork, the authors address VoIP security from the perspective of real-world network implementers, managers, and security specialists. The authors identify key threats to VoIP networks, including eavesdropping, unauthorized access, denial of service, masquerading, and fraud; and review vulnerabilities in protocol design, network architecture, software, and system configuration that place networks at risk. They discuss the advantages and tradeoffs associated with protection mechanisms built into SIP, SRTP, and other VoIP protocols; and review key management solutions such as MIKEY and ZRTP. Next, they present a complete security framework for enterprise VoIP networks, and provide detailed architectural guidance for both service providers and enterprise users.

- 1 Introduction
- 2 VoIP Architectures and Protocols
- 3 Threats and Attacks
- 4 VoIP Vulnerabilities
- 5 Signaling Protection Mechanisms
- 6 Media Protection Mechanisms
- 7 Key Management Mechanisms
- 8 VoIP and Network Security Controls
- 9 A Security Framework for Enterprise VoIP Networks
- 10 Provider Architectures and Security
- 11 Enterprise Architectures and Security

Synopsis In *Securing VoIP Networks*, two leading experts systematically review the security risks and vulnerabilities associated with VoIP networks and offer proven, detailed recommendations for securing them. Drawing on case studies from their own fieldwork, the authors address VoIP security from the perspective of real-world network implementers, managers, and security specialists. The authors identify key threats to VoIP networks, including eavesdropping, unauthorized access, denial of service, masquerading, and fraud; and review vulnerabilities in protocol design, network architecture, software, and system configuration that place networks at risk. They discuss the advantages and tradeoffs associated with protection mechanisms built into SIP, SRTP, and other VoIP protocols; and review key management solutions such as MIKEY and ZRTP. Next, they present a complete security framework for enterprise VoIP networks, and provide detailed architectural guidance for both service providers and enterprise users.

- 1 Introduction
- 2 VoIP Architectures and Protocols
- 3 Threats and Attacks
- 4 VoIP Vulnerabilities
- 5 Signaling Protection Mechanisms
- 6 Media Protection Mechanisms
- 7 Key Management Mechanisms
- 8 VoIP and Network Security Controls
- 9 A Security Framework for Enterprise VoIP Networks
- 10 Provider Architectures and Security
- 11 Enterprise Architectures and Security