

# CONTENTS IN DETAIL

<b>ACKNOWLEDGMENTS</b>	<b>xiii</b>
------------------------	-------------

<b>INTRODUCTION</b>	<b>1</b>
---------------------	----------

Book Overview .....	1
Lab Setup .....	3
SIP/IAX/H.323 Server .....	4
SIP Setup .....	5
H.323 Setup (Ekiga) .....	5
IAX Setup .....	5

<b>1</b>	
<b>AN INTRODUCTION TO VOIP SECURITY</b>	<b>7</b>

Why VoIP .....	8
VoIP Basics .....	9
How It Works .....	9
Protocols .....	9
Deployments .....	11
VoIP Security Basics .....	13
Authentication .....	13
Authorization .....	14
Availability .....	14
Encryption .....	15
Attack Vectors .....	15
Summary .....	16

## **PART I**

### **VOIP PROTOCOLS**

<b>2</b>	
<b>SIGNALING: SIP SECURITY</b>	<b>19</b>

SIP Basics .....	20
SIP Messages .....	21
Making a VoIP Call with SIP Methods .....	22
Registration .....	22
The INVITE Request .....	23
Enumeration and Registration .....	25
Enumerating SIP Devices on a Network .....	25
Registering with Identified SIP Devices .....	26
Authentication .....	27
Encryption .....	29
SIP Security Attacks .....	31
Username Enumeration .....	31
SIP Password Retrieval .....	33

Man-in-the-Middle Attack .....	38
Registration Hijacking .....	38
Spoofing SIP Proxy Servers and Registrars .....	41
Denial of Service via BYE Message .....	42
Denial of Service via REGISTER .....	44
Denial of Service via Un-register .....	44
Fuzzing SIP .....	45
Summary .....	47

### **3 SIGNALING: H.323 SECURITY 49**

H.323 Security Basics .....	50
Enumeration .....	50
Authentication .....	52
Authorization .....	54
H.323 Security Attacks .....	55
Username Enumeration (H.323 ID) .....	56
H.323 Password Retrieval .....	58
H.323 Replay Attack .....	60
H.323 Endpoint Spoofing (E.164 Alias) .....	63
E.164 Alias Enumeration .....	65
E.164 Hopping Attacks .....	66
Denial of Service via NTP .....	67
Denial of Service via UDP (H.225 Registration Reject) .....	68
Denial of Service via Host Unreachable Packets .....	70
Denial of Service via H.225 nonStandardMessage .....	71
Summary .....	72

### **4 MEDIA: RTP SECURITY 73**

RTP Basics .....	74
RTP Security Attacks .....	75
Passive Eavesdropping .....	76
Active Eavesdropping .....	82
Denial of Service .....	88
Summary .....	91

### **5 SIGNALING AND MEDIA: IAX SECURITY 93**

IAX Authentication .....	94
IAX Security Attacks .....	96
Username Enumeration .....	96
Offline Dictionary Attack .....	97
Active Dictionary Attack .....	100
IAX Man-in-the-Middle Attack .....	102
MD5-to-Plaintext Downgrade Attack .....	103
Denial of Service Attacks .....	106
Summary .....	110

## **PART II VOIP SECURITY THREATS**

### **6 ATTACKING VOIP INFRASTRUCTURE 113**

Vendor-Specific VoIP Sniffing .....	114
Hard Phones .....	115
Compromising the Phone's Configuration File .....	116
Uploading a Malicious Configuration File .....	117
Exploiting Weaknesses of SNMP .....	119
Cisco CallManager and Avaya Call Center .....	120
Using Nmap to Scan VoIP Devices .....	121
Scanning Web Management Interfaces with Nikto .....	122
Discovering Vulnerable Services with Nessus .....	123
Modular Messaging Voicemail System .....	123
Infrastructure Server Impersonation .....	126
Spoofing SIP Proxies and Registrars .....	126
Redirecting H.323 Gatekeepers .....	127
Summary .....	128

### **7 UNCONVENTIONAL VOIP SECURITY THREATS 131**

VoIP Phishing .....	133
Spreading the Message .....	133
Receiving the Calls .....	136
Making Free Calls .....	138
Caller ID Spoofing .....	139
Example 1 .....	140
Example 2 .....	142
Example 3 .....	143
Example 4 .....	144
Anonymous Eavesdropping and Call Redirection .....	146
Spam Over Internet Telephony .....	147
SPIT and the City .....	148
Lightweight SPIT with Skype/Google Talk .....	150
Summary .....	152

### **8 HOME VOIP SOLUTIONS 153**

Commercial VoIP Solutions .....	154
Vonage .....	155
Voice Injection (RTP) .....	162
Username/Password Retrieval (SIP) .....	166
PC-Based VoIP Solutions .....	167
Yahoo! Messenger .....	168
Google Talk .....	170
Microsoft Live Messenger .....	172
Skype .....	173

SOHO Phone Solutions .....	173
Summary .....	175

## **PART III ASSESS AND SECURE VOIP**

<b>9</b>		
<b>SECURING VOIP</b>		<b>179</b>
SIP over SSL/TLS .....	180	
Secure RTP .....	181	
SRTP and Media Protection with AES Cipher .....	182	
SRTP and Authentication and Integrity Protection with HMAC-SHA1 .....	182	
SRTP Key Distribution Method .....	183	
ZRTP and Zfone .....	183	
Firewalls and Session Border Controllers .....	186	
The VoIP and Firewall Problem .....	186	
The Solution .....	187	
Summary .....	187	
<b>10</b>		
<b>AUDITING VOIP FOR SECURITY BEST PRACTICES</b>		<b>189</b>
VoIP Security Audit Program .....	190	
Summary .....	197	
<b>INDEX</b>		<b>199</b>