

# At a Glance

## Part I Casing the Establishment

1	VoIP Targets, Threats, and Components	5
2	Footprinting a UC Network	19
3	Scanning a UC Network	41
4	Enumerating a UC Network	69

## Part II Application Attacks

5	Toll Fraud and Service Abuse	111
6	Calling Number Spoofing	133
7	Harassing Calls and Telephony Denial of Service (TDoS)	149
8	Voice SPAM	189
9	Voice Social Engineering and Voice Phishing	207

## Part III Exploiting the UC Network

10	UC Network Eavesdropping	237
11	UC Interception and Modification	261
12	UC Network Infrastructure Denial of Service (DoS)	293
13	Cisco Unified Communications Manager	317

**Part IV UC Session and Application Hacking**

14	Fuzzing, Flooding, and Disruption of Service .....	361
15	Signaling Manipulation .....	407
16	Audio and Video Manipulation .....	443
17	Emerging Technologies .....	481
	Index .....	507

# Contents

Acknowledgments .....	xvii
Introduction .....	xix

## Part I Casing the Establishment

Case Study: Is There Really Any SIP in the Internet? .....	2
Scanning the Entire Internet for SIP Servers .....	2
Using the Shodan Search Engine to Locate Internet SIP Servers ...	4
<b>1</b> VoIP Targets, Threats, and Components .....	5
Campus/Internal UC .....	9
Session Initiation Protocol and SIP Trunk Threats .....	11
Increased Threats from the Public Voice Network .....	14
Hosted UC .....	15
Summary .....	16
References .....	17
<b>2</b> Footprinting a UC Network .....	19
Why Footprint First? .....	20
UC Footprinting Methodology .....	21
Scoping the Effort .....	21
Summary .....	39
References .....	39
<b>3</b> Scanning a UC Network .....	41
Our VoIP Test Bed .....	42
Network Host/Device Discovery .....	43
ICMP Ping Sweeps .....	44
Other ICMP Ping Sweeps .....	46
Port Scanning and Service Discovery .....	54
Host/Device Identification .....	59

- UC Phone Scanning and Discovery ..... 63
- Summary ..... 67
- References ..... 68
- 4 Enumerating a UC Network ..... 69**
  - SIP 101 ..... 70
    - SIP URIs ..... 71
    - SIP Architecture Elements ..... 71
    - SIP Requests ..... 72
    - SIP Responses ..... 72
    - Typical Call Flow ..... 74
    - Further Reading ..... 78
  - RTP 101 ..... 78
  - Banner Grabbing ..... 80
  - SIP User/Extension Enumeration ..... 81
  - Enumeration of Other UC Support Services ..... 97
  - UC Application-Level Enumeration ..... 102
  - Summary ..... 105
  - References ..... 106

**Part II Application Attacks**

- Case Study: A Real-world Telephony Denial of Service (TDoS) Attack .... 108
  - The Payday Loan Scam ..... 108
- 5 Toll Fraud and Service Abuse ..... 111**
  - Internal Abuse of Unmonitored Phones ..... 114
  - Full-Scale Toll Fraud ..... 119
  - Summary ..... 131
  - References ..... 131
- 6 Calling Number Spoofing ..... 133**
  - Calling Number 101 ..... 134
  - Spoofing/Masking the Calling Number with an IP PBX ..... 137
  - Anonymous Calling ..... 139
  - Network Services and Smartphone Apps ..... 145
  - Summary ..... 148
  - References ..... 148
- 7 Harassing Calls and Telephony Denial of Service (TDoS) ..... 149**
  - Harassing and Threatening Calls ..... 152
  - Social Networking TDoS ..... 158
  - Automated TDoS ..... 164
    - SIP Trunking ..... 166
    - Getting Target Numbers ..... 168

	Audio Content .....	169
	Call Generation .....	170
	Attack Timing .....	171
	TDoS Attack Demonstration .....	171
	Using Virtual Queues .....	179
	Using Automated DoS to Cover Fraud .....	181
	Call Pumping .....	182
	DTMF DoS and Fuzzing .....	185
	Summary .....	186
	References .....	187
<b>8</b>	Voice SPAM .....	189
	Understanding Voice SPAM .....	190
	The FTC Robocall Challenge .....	195
	Other Types of UC SPAM .....	195
	Summary .....	205
	References .....	205
<b>9</b>	Voice Social Engineering and Voice Phishing .....	207
	Voice Social Engineering .....	209
	Voice Phishing .....	219
	Anatomy of a Traditional Email-based Phishing Attack .....	220
	Summary .....	230
	References .....	230

## Part III Exploiting the UC Network

	Case Study: The Angry Ex-Employee .....	234
<b>10</b>	UC Network Eavesdropping .....	237
	UC Privacy: What's at Risk .....	238
	TFTP Configuration File Sniffing .....	239
	Number Harvesting .....	239
	Call Pattern Tracking .....	239
	Conversation Eavesdropping and Analysis .....	239
	First, Gain Access to the UC Traffic .....	240
	Compromising a Network Node .....	243
	Now That We Have Access, Let's Sniff! .....	249
	Summary .....	259
	References .....	259
<b>11</b>	UC Interception and Modification .....	261
	ARP Poisoning .....	263
	ARP Poisoning Attack Scenario .....	264

Application-Level Interception Techniques .....	280
How to Insert Rogue Applications .....	281
SIP Rogue Application .....	282
Summary .....	291
References .....	292
<b>12 UC Network Infrastructure Denial of Service (DoS) .....</b>	<b>293</b>
Call and Session Quality .....	294
Measuring UC Call Quality .....	294
Network Latency .....	295
Jitter .....	295
Packet Loss .....	296
UC Call Quality Tools .....	296
What Are DoS and DDoS Attacks? .....	301
Flooding Attacks .....	301
Network Availability Attacks .....	307
Supporting Infrastructure Attacks .....	311
Summary .....	316
References .....	316
<b>13 Cisco Unified Communications Manager .....</b>	<b>317</b>
Introduction to the Basic Cisco UC Components .....	318
IP PBX and Proxy .....	318
Hard Phones .....	319
Softphones .....	322
Voicemail .....	323
Switches and Routing .....	323
Communication Between Cisco Phones and CUCM with SCCP .....	324
Basic Deployment Scenarios .....	329
Network Reconnaissance .....	331
Sniffing .....	332
Scanning and Enumeration .....	334
Exploiting the Network .....	347
Summary .....	355
References .....	355

## Part IV UC Session and Application Hacking

Case Study: An Attack Against Central SIP .....	358
<b>14 Fuzzing, Flooding, and Disruption of Service .....</b>	<b>361</b>
Access to SIP and RTP .....	362
What Is Fuzzing? .....	363
Vulnerabilities 101 .....	364
Who's Fuzzing? .....	365
Flooding .....	376

Summary .....	404
References .....	405
<b>15 Signaling Manipulation .....</b>	<b>407</b>
Registration Manipulation .....	408
Registration Removal .....	409
Registration Addition .....	414
Registration Hijacking .....	417
Redirection Attacks .....	432
Session Teardown .....	434
SIP Phone Reboot .....	438
Other Signaling Manipulation Tools .....	440
Summary .....	441
References .....	441
<b>16 Audio and Video Manipulation .....</b>	<b>443</b>
Media Manipulation .....	445
Audio Insertion and Mixing .....	446
Video Dropping, Injection, and DoS with VideoJak and VideoSnarf .....	468
Media “Steganophony” .....	470
Summary .....	479
References .....	479
<b>17 Emerging Technologies .....</b>	<b>481</b>
Other Enterprise UC Systems .....	483
Microsoft Lync .....	484
Over-the-Top (OTT)/Internet Softphone Applications .....	488
Skype .....	489
Mobility and Smartphones .....	490
Security .....	491
Other Forms of Communications .....	493
Video .....	493
Text Messaging .....	493
Messaging .....	495
Enterprise Messaging .....	497
Social Networking .....	498
Bring Your Own Device (BYOD) .....	500
Security .....	500
The Cloud .....	500
Hosted UC .....	501
Security .....	501
WebRTC .....	502
Security .....	503
Summary .....	503
References .....	503
Index .....	507