Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: International Sales international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher     Publisher
Associate Publisher     Paul Boger
Cisco Press Program Manager     Dave Dusthimer
Executive Editor     Jeff Brady
Managing Editor     Brett Bartow
Development Editor     Patrick Kanouse
Project Editor     Dan Young
Copy Editor     Seth Kerney
Technical Editors     Margaret Berson
Bob Bell
Dan Wing
Vanessa Evans
Louisa Adair
Octal Publishing, Inc.
WordWise Publishing Services LLC
Water Crest Publishing, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher     Publisher
Associate Publisher     Paul Boger
Cisco Press Program Manager     Dave Dusthimer
Executive Editor     Jeff Brady
Managing Editor     Brett Bartow
Development Editor     Patrick Kanouse
Project Editor     Dan Young
Copy Editor     Seth Kerney
Technical Editors     Margaret Berson
Bob Bell
Dan Wing
Vanessa Evans
Louisa Adair
Octal Publishing, Inc.
WordWise Publishing Services LLC
Water Crest Publishing, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher     Publisher
Associate Publisher     Paul Boger
Cisco Press Program Manager     Dave Dusthimer
Executive Editor     Jeff Brady
Managing Editor     Brett Bartow
Development Editor     Patrick Kanouse
Project Editor     Dan Young
Copy Editor     Seth Kerney
Technical Editors     Margaret Berson
Bob Bell
Dan Wing
Vanessa Evans
Louisa Adair
Octal Publishing, Inc.
WordWise Publishing Services LLC
Water Crest Publishing, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher     Publisher
Associate Publisher     Paul Boger
Cisco Press Program Manager     Dave Dusthimer
Executive Editor     Jeff Brady
Managing Editor     Brett Bartow
Development Editor     Patrick Kanouse
Project Editor     Dan Young
Copy Editor     Seth Kerney
Technical Editors     Margaret Berson
Bob Bell
Dan Wing
Vanessa Evans
Louisa Adair
Octal Publishing, Inc.
WordWise Publishing Services LLC
Water Crest Publishing, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher     Publisher
Associate Publisher     Paul Boger
Cisco Press Program Manager     Dave Dusthimer
Executive Editor     Jeff Brady
Managing Editor     Brett Bartow
Development Editor     Patrick Kanouse
Project Editor     Dan Young
Copy Editor     Seth Kerney
Technical Editors     Margaret Berson
Bob Bell
Dan Wing
Vanessa Evans
Louisa Adair
Octal Publishing, Inc.
WordWise Publishing Services LLC
Water Crest Publishing, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher     Publisher
Associate Publisher     Paul Boger
Cisco Press Program Manager     Dave Dusthimer
Executive Editor     Jeff Brady
Managing Editor     Brett Bartow
Development Editor     Patrick Kanouse
Project Editor     Dan Young
Copy Editor     Seth Kerney
Technical Editors     Margaret Berson
Bob Bell
Dan Wing
Vanessa Evans
Louisa Adair
Octal Publishing, Inc.
WordWise Publishing Services LLC
Water Crest Publishing, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.
Introduction

Voice over Internet Protocol (VoIP) has been popular in the telecommunications world since its emergence in the late 90s, as a new technology transporting multimedia over the IP network. In this book, the multimedia (or rich media) includes not only voice, but also video, instant message, presence data, and fax data over the IP network.

Today people commonly make phone calls with IP phones or client software (such as Skype or iChat) on their computer, or send instant messages to their friends. This gives them convenience and cost savings. Many telecommunications companies and other organizations have been switching their legacy phone infrastructure to a VoIP network, which reduces costs for lines, equipment, manpower, and maintenance.

However, the benefits of VoIP are not free. There are disadvantages to using VoIP. The integrated rich media makes it difficult to design the network architecture. Multiple VoIP protocols and different methods of implementation create serious interoperability issues. Integration with existing data networks creates quality of service issues. The fact that so many network elements are involved through open (or public) networks creates serious security issues, because each element and network has vulnerable factors.

The security issues especially are becoming more serious because traditional security devices (such as firewalls) and protocols (such as encryption) cannot protect VoIP services or networks from recent intelligent threats.

This book focuses on the important topic of VoIP security by analyzing current and potential threats to demonstrating the methods of prevention.

Goals and Methods

The most important goal of this book is to give you correct and practical answers for the following questions:

- What are the current and potential threats?
- What are the impacts of those threats?
- Why are current data security devices not able to protect against recent intelligent threats?
- How can you protect VoIP services and networks from those threats?
- What is lawful interception and how do you implement it?

One key methodology used in this book is to give you hands-on experience of current well-known threats by simulating them with publicly available tools. Through the simulation, you can realize the characteristics and impacts of those threats and have a better understanding of mitigation.

Another key methodology is to give you detailed examples of protection methods with protocols, products, and architecture so that you may apply them to real VoIP service environments.

This book also gives you clarification of VoIP security concepts, definitions, standards, requirements, limitations, and related terms.
Who Should Read This Book

This book is NOT designed to give you information about VoIP in general which is available almost everywhere. Instead, this book focuses on VoIP security and gives practical information to people like those in the following list:

• Managers or engineers who are planning to employ VoIP systems in their organizations
• System engineers or architects who design and implement VoIP networks
• Network administrators who administer, upgrade, or secure networks that include VoIP elements
• Security consultants who perform security assessments for VoIP environments
• Developers who implement VoIP products or solutions
• Researchers and analysts who are interested in VoIP security

This book assumes that the readers have some minimal knowledge of networking (such as TCP/IP), operating systems, and VoIP in general (such as IP phones).

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with.


Chapter 1, “Working with VoIP,” provides an overview of VoIP and its vulnerability in general. Chapters 2 through 11 are the core chapters and can be read in any order. If you do intend to read them all, the order in the book is an excellent sequence to use.

The core chapters, Chapters 2 through 11, cover the following topics:

• Chapter 2, “VoIP Threat Taxonomy”—This chapter defines VoIP threat taxonomy, based on four different categories: threats against availability, confidentiality, integrity, and social context. This chapter is not intended to provide exhaustive lists of current and potential threats, but to define the taxonomy for identifying the threat in the first place, measuring the current and potential impact, and helping implementers to develop protection methods and secure service architecture. Twenty-two typical threats are introduced with examples and features.

• Chapter 3, “Security Profiles in VoIP Protocols”—This chapter introduces the security profiles of VoIP protocols: SIP, H.323, and MGCP. The content shows how each protocol defines specific security mechanisms and recommends combined solution with other security protocols, such as IPSec, TLS, and SRTP.
• **Chapter 4, “Cryptography”**—This chapter provides a high-level understanding of cryptographic algorithms with comprehensible figures, avoiding mathematical details. Well-known cryptographic algorithms are introduced, such as DES, 3DES, AES, RAS, DSA, and hash functions (MD5, SHA, and HMAC). This chapter also covers the mechanism of key management, focusing on key distribution.

• **Chapter 5, “VoIP Network Elements”**—This chapter covers what devices are involved in the VoIP network architecture, and how they work for secure services. Session Border Controller, VoIP-aware firewalls, NAT servers, lawful interception servers, customer premise equipment, call processing servers, and media gateways are introduced.

• **Chapter 6, “Analysis and Simulation of Current Threats”**—This chapter covers two main topics: detailed analysis and hands-on simulation of most common threats, and the guidelines for mitigation. For the analysis, it examines the detailed patterns, usage examples, and impacts of the threats. For the simulation, it introduces negative testing tools that are available on the Internet so that you can have hands-on experience. The threats that this chapter covers are DoS, malformed messages, sniffing (eavesdropping), spoofing (identity theft), and VoIP spam (voice, instant message, and presence spam).

• **Chapter 7, “Protection with VoIP Protocol”**—This chapter demonstrates the details of how to make VoIP service secure with SIP and other supplementary protocols. It focuses on the methodology of protection in these five categories: authentication, encryption, transport and network layer security, threat model and prevention, and limitations.

• **Chapter 8, “Protection with Session Border Controller”**—This chapter examines security issues on the VoIP network borders, and provides the methodology of preventing the issues with an SBC. This chapter includes the details of SBC functionality (such as network topology hiding, DoS protection, overload prevention, NAT traversal, and lawful interception), as well as the method of designing service architecture with an SBC in terms of high availability, secure network connectivity, virtualization, and optimization of traffic flow.

• **Chapter 9, “Protection with Enterprise Network Devices”**—This chapter demonstrates how to protect the enterprise VoIP network with Cisco devices for practical information. Cisco firewalls, Unified Communications Manager, Unified Communications Manager Express, IP phone, and multilayer switches are used. This chapter includes security features, usage examples, and configuration guidelines for those devices.

• **Chapter 10, “Lawful Interception Fundamentals”**—This chapter covers the fundamentals of lawful interception. The topics are definition, background information, requirements from law enforcement agents, the reference model from an architectural perspective, functional specifications, request/response interface, and operational considerations.

• **Chapter 11, “Lawful Interception Implementation”**—This chapter demonstrates how to implement lawful interception into the VoIP service environment. It focuses on how the interception request and response work between functional modules, based on industry specifications.
VoIP Threat Taxonomy

The VoIP vulnerabilities that were introduced in Chapter 1, “Working with VoIP,” can be exploited to create many different kinds of threats. Attackers may disrupt media service by flooding traffic, collect privacy information by intercepting call signaling or call content, hijack calls by impersonating servers or impersonating users, make fraudulent calls by spoofing identities, and so on.

Spammers may utilize VoIP networks to deliver spam calls, instant messages, or presence information, which are more effective than email spams because it is very difficult to filter VoIP spam.

This chapter is not intended to provide exhaustive lists of current and potential threats, but to define the taxonomy for the following purposes:

• To identify the threat in the first place
• To measure the current impact and potential future impact of the threat
• To help develop the protection method and design a secure service architecture

NOTE

For an exhaustive list of all current and potential threats, go to www.voipsa.org (Voice over IP Security Alliance).

There are many possible ways to categorize the threats. This book uses the following four categories that most VoIP threats can belong to:

• Threats against availability
• Threats against confidentiality
• Threats against integrity
• Threats against social context

Each section in this chapter covers each category with typical threat examples. To give you a better understanding, each section uses figures and protocol examples with Session Initiation Protocol (SIP).
The following section introduces the most critical threats that impact service availability.

Threats Against Availability

Threats against availability are actually a group of threats against service availability that is supposed to be running 24/7 (24 hours, 7 days a week). That is, these threats aim at VoIP service interruption, typically in the form of Denial of Service (DoS).

The typical threats against availability are as follows:

- Call flooding
- Malformed messages (protocol fuzzing)
- Spoofed messages (call teardown, toll fraud)
- Call hijacking (registration or media session hijacking)
- Server impersonating
- Quality of Service (QoS) abuse

The following subsections describe the threats with examples, which show you how they impact service availability.

Call Flooding

The typical example of DoS is intentional call flooding; an attacker floods valid or invalid heavy traffic (signals or media) to a target system (for example, VoIP server, client, and underlying infrastructure), and drops the performance significantly or breaks down the system. The typical methods of flooding are as follows:

- **Valid or invalid registration flooding**—An attacker uses this method commonly because most registration servers accept the request from any endpoints in the public Internet as an initial step of authentication. Regardless of whether the messages are valid or invalid, the large number of request messages in a short period of time (for example, 10,000 SIP REGISTER messages per second) severely impacts the performance of the server.

- **Valid or invalid call request flooding**—Most VoIP servers have a security feature that blocks flooded call requests from unregistered endpoints. So, an attacker registers first after spoofing a legitimate user, and then sends flooded call requests in a short
period of time (for example, 10,000 SIP INVITE messages per second). This impacts the performance or functionality of the server regardless of whether the request message is valid or not.

- **Call control flooding after call setup**—An attacker may flood valid or invalid call control messages (for example, SIP INFO, NOTIFY, Re-INVITE) after call setup. Most proxy servers are vulnerable because they do not have a security feature to ignore and drop those messages.

- **Ping flooding**—Like Internet Control Message Protocol (ICMP) ping, VoIP protocols use ping messages in the application layer to check out the availability of a server or keep the pinhole open in the local Network Address Translation (NAT) server, such as SIP OPTIONS message. Most IP network devices (for example, a router or firewall) in the production network do not allow ICMP pings for security reasons. However, many VoIP servers should allow the application-layer ping for proper serviceability, which could be a critical security hole.

Figure 2-1 illustrates the example of distributed flooding with zombies; an attacker compromises other computers with malware (for example, a virus) and uses them as zombies flooding registration messages. Each zombie sends 1,000 SIP REGISTER messages per second with different credentials that are randomly generated.

In Figure 2-1, the flooded messages will impact the registration server (SIP Registrar) severely as long as the server processes and replies with any error codes, such as “401 Unauthorized,” “404 Not Found,” “400 Bad Request,” and so on. The impact can be high resource consumption (for example, CPU, memory, network bandwidth), system malfunction,
or service outage. Whether the server responds or not, flooding the SIP registrar with sufficient registration messages will result in the degradation of service to the legitimate endpoints.

Not only the intentional flooding just mentioned, but also unintentional flooding exists in VoIP networks, so-called “self-attack,” because of incorrect configuration of devices, architectural service design problems, or unique circumstances. Here are some examples:

- **Regional power outage and restoration**—When the power is backed up after a regional outage, all endpoints (for example, 10,000 IP phones) will boot up and send registration messages to the server almost at the same time, which are unintentional flooded messages. Because those phones are legitimate and distributed over a wide area, it is hard to control the flooding traffic proactively.

- **Incorrect configuration of device**—The most common incorrect configuration is setting endpoint devices (for example, IP phones) to send too many unnecessary messages, such as a registration interval that is too short.

- **Misbehaving endpoints**—Problematic software (firmware) or hardware could create unexpected flooding, especially when multiple or anonymous types of endpoints are involved in the VoIP service network.

- **Legitimate call flooding**—There are unusual days or moments when many legitimate calls are made almost at the same time. One example is Mother’s Day, when a lot of calls are placed in the United States. Another example is natural disasters (for example, earthquakes), when people within the area make a lot of calls to emergency numbers (for example, 911) and their family and friends make calls to the affected area at the same time.

Those types of intentional and unintentional call flooding are common and most critical threats to VoIP service providers, who have to maintain service availability continually.

The next type is another form of threat against service availability, by means of malformed messages.

**Malformed Messages (Protocol Fuzzing)**

An attacker may create and send malformed messages to the target server or client for the purpose of service interruption. A *malformed message* is a protocol message with wrong syntax. Example 2-1 shows an example with a SIP INVITE message.
NOTE

Protocol fuzzing is another name for malformed messages. A small difference is that protocol fuzzing includes malicious messages that have correct syntax but break the sequence of messages, which may cause system error by making the state machine confused.

Example 2-1  Malformed SIP INVITE Message

Request-URI: aaaaaaaaa sip:1001@192.168.10.10 SIP/2.0
Message Header
  Via: SIP/2.0/UDP CAL-D600-5814.cc-ntd1.example.com;branch=z9hG4bK000002000005
  From: <sip:user@CAL-D600-5814.cc-ntd1.example.com>;tag=2
  To: Receiver <sip:1001@192.168.10.10>
  Call-Id: 55555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555555
  CSeq: 1 INVITE
  Contact: <sip:user@CAL-D600-5814.cc-ntd1.example.com>
  Expires: 1200
  Max-Forwards: 70
  Content-Type: application/sdp
  Content-Length: 143

Message body
Session Description Protocol
  Session Description Protocol Version (v): = = = = = = = 0
  Owner/Creator, Session Id (o): 2 2 2 IN IP4 CAL-D600-5814.cc-ntd1.example.com
  Session Name (s): Session SDP
  Connection Information (c): IN IP4 192.168.10.10
  Time Description, active time (t): 0 0
  Media Description, name and address (m): audio 9876 RTP/AVP 0
  Media Attribute (a): rtpmap:0 PCMU/8000

Note that the comments (bold letters) in Example 2-1 are not shown in the actual SIP INVITE message. You can find something wrong in the example of an INVITE message. Three SIP headers (Request-URI, From, and Call-Id) and one version in Session Description Protocol (SDP) have the wrong format.
The server receiving this kind of unexpected message could be confused (fuzzed) and react in many different ways depending on the implementation. The typical impacts are as follows:

- Infinite loop of parsing
- Buffer overflow, which may permit execution of arbitrary code
- Break state machine
- Unable to process other normal messages
- System crash

This vulnerability comes from the following sources in general:

1. Weakness of protocol specification
   Most VoIP protocols are open to the public and don’t strictly define every single line. Attackers could find where the weakness of syntax is. Additionally, there are many customizable fields or tags.

2. Ease of creating the malformed message
   Creating a message like that in Example 2-1 is easy for regular programmers. Even for nonprogrammers, many tools are available to make customized messages.

3. Lack of exception handling in the implementation
   Because of time restrictions, most implementers are apt to focus on product features and interfaces, rather than create exception handling for massive negative cases.

4. Difficulty of testing all malformed cases
   It is very difficult to test all the negative cases, even though sophisticated testing tools covering more cases are coming out these days.

The threat of malformed messages should be preventable as long as the parsing algorithm handles them properly.

The next threat is spoofed messages that are not malformed but still impact service availability.

**Spoofed Messages**

An attacker may insert fake (spoofed) messages into a certain VoIP session to interrupt the service, or insert them to steal the session. The typical examples are “call teardown” and “toll fraud.”
Call Teardown

The method of malicious call teardown is that an attacker monitors a SIP dialog and obtains session information (Call-ID, From tag, and To tag), and sends a call termination message (for example, SIP BYE) to the communication device while the users are talking. The device receiving the termination message will close the call session immediately. Figure 2-2 illustrates the example with SIP messages.

Figure 2-2  Malicious Call Teardown

Figure 2-2 assumes that the attacker already monitored call signals between User A and B, and knew the session information (SIP dialog). The attacker injects the session information to the BYE message. The IP phone of user A receives the BYE and disconnects the media channel.

Another method of attack is that an attacker sends the termination messages to random devices (especially, proxy server) without knowing session information, which may affect current call sessions.

Compared to previous threats in this section, the malicious call teardown is not a common attack because the attacker should monitor the target call session before sending a termination message (BYE).

The next type of attack, toll fraud, also requires preliminary information like credentials before making fraud calls, but it happens commonly because of monetary benefit.
Toll Fraud

A fraudulent toll call is one of the common threats these days, especially for long distance or international calls. Because most mediation devices (for example, public switched telephone network [PSTN] media gateway, proxy server) require valid credentials (for example, ID and password) before setting up the toll call, an attacker collects the credentials first in many different ways. Typically, an attacker creates spoofed messages for brute-force password assault on the server until he receives authorization. If the clients use default passwords or easy-to-guess passwords, it is much easier to find them, especially when an attacker uses a password dictionary (see Note).

NOTE

A password dictionary is a file that contains millions of frequently used passwords. Most passwords are manually created by humans (rather than by computers), so it’s highly likely that they will be simple and easy to remember. No one really wants to have to remember random passwords that are longer than 10 digits, except perhaps system administrators. For example, a user named John Kim is apt to have passwords such as “jkim,” “iamjohn,” “johnkim,” “john2kim,” “john4me,” and so on. Therefore, an attacker using a password dictionary containing millions of commonly used passwords would not need much time to crack most user-created passwords.

In some cases, the server does not require the credentials, but checks out the source IP address or subnet of the client to control the access. Especially when call trunking (for example, SIP trunking) is set up between a VoIP service provider and an enterprise customer, access control based on the source IP or subnet is commonly used. An attacker may be able to access the server by spoofing the source IP address.

Call Hijacking

Hijacking occurs when some transactions between a VoIP endpoint and the network are taken over by an attacker.

The transactions can be registration, call setup, media flow, and so on. This hijacking can make serious service interruption by disabling legitimate users to use the VoIP service. It is similar to call teardown in terms of stealing session information as a preliminary, but the actual form of attack and impact are different.

The typical cases are registration hijacking, media session hijacking, and server impersonating. The next few sections describe each of these cases.
Registration Hijacking

The registration process allows an endpoint to identify itself to the server (for example, SIP Registrar) as a device that a user is located.

An attacker monitors this transaction and sends spoofed messages to the server in order to hijack the session. When a legitimate user has been compromised, that user cannot receive inbound calls. Figure 2-3 illustrates the example with SIP messages.

In Figure 2-3, an attacker impersonates a user agent by modifying the “From” header and adding the attacker’s address to the “To” header when it sends a REGISTER message, which updates the address-of-record of the target user. All inbound calls to User A will be routed to the attacker.

This threat happens when the user agent server (Registrar) is relying on only SIP headers to identify the user agent.

Media Session Hijacking

When a media session is being negotiated between VoIP endpoints, an attacker may send spoofed messages to either one of them to redirect the media to another endpoint such as the attacker’s phone or voicemail box. The victim will only be able to talk with the attacker’s endpoint. Figure 2-4 illustrates the example with SIP messages.
In Figure 2-4, User A tries to make a call to User B and the IP phone of User B is ringing. Having monitored call requests to User B, an attacker detects the call and sends 200 OK messages to User A with the IP/port address of the attacker’s voicemail server. User A leaves a voice message for User B in the attacker’s voicemail box. This hijacking happens before the media session is established between User A and (the intended) user B.

Even after the media session is established between A and B, an attacker can still hijack an active session by sending a Re-Invite message to User A.

Server Impersonating

A VoIP client sends a request message to a server in the target domain for registration, call setup or routing, and so on. It is possible for an attacker to impersonate the server, receive the request message, and then manipulate it for malicious purposes.

The typical method of impersonating a server is attacking the local TFTP server or Domain Name Service (DNS) server as the initial step. An attacker may intrude into the TFTP server and replace the configuration file for IP phones with his file having an IP address of a malicious server (for example, SIP Registrar).

The IP phones downloading the malicious file will send a request message to the wrong server.
An attacker may also compromise the DNS server and replace the entry of current VoIP server with an IP address of a malicious server. The IP phones looking up the server IP will receive a wrong one. Figure 2-5 illustrates an example based on SIP transactions with a Redirect server.

**Figure 2-5  Server Impersonating**

In Figure 2-5, the attacker compromised the local DNS server first by replacing the IP address (10.1.1.10) of original.redirect.com with 10.10.10.10, which is the attacker’s redirect server.

When User A tries to make a call to User B, the IP phone looks up the IP address of the redirect server (original.redirect.com) and receives the IP (10.10.10.10) of the impersonated server. The INVITE message is sent to the impersonated server, and it replies “302 Moved Temporarily” with wrong contact information that could be a dummy address or attacker’s proxy server for further threat. The original redirect server (10.1.1.10) cannot receive any call request in this situation.

**QoS Abuse**

The elements of a media session are negotiated between VoIP endpoints during call setup time, such as media type, coder-decoder (codec) bit rate, and payload type. For example, it may be necessary or desirable to use G.729 when leaving a network (to conserve bandwidth)
but to use G.711 when calls are staying inside a network (to keep call quality higher). An attacker may intervene in this negotiation and abuse the Quality of Service (QoS), by replacing, deleting, or modifying codecs or payload type.

Another method of QoS abuse is exhausting the limited bandwidth with a malicious tool so that legitimate users cannot use bandwidth for their service. Some VoIP service providers or hosting companies limit the bandwidth for certain groups of hosts to protect the network. An attacker may know the rate limit and generate excessive media traffic through the channel, so voice quality between users may be degraded.

In this section so far, you have learned about threats against availability, such as call flooding, malformed messages, spoofed messages (call teardown, toll fraud), call hijacking (registration and media session hijacking, server impersonating), and QoS abuse. The next section covers another type of threat: attacks against call data and media confidentiality.

**Threats Against Confidentiality**

Another category of VoIP threat is the threat against confidentiality.

Unlike the service interruptions in the previous section, threats against confidentiality do not impact current communications generally, but provide an unauthorized means of capturing media, identities, patterns, and credentials that are used for subsequent unauthorized connections or other deceptive practices.

VoIP transactions are mostly exposed to the confidentiality threat because most VoIP service does not provide full confidentiality (both signal and media) end-to-end. In fact, full encryption of message headers is not possible because intermediary servers (for example, SIP proxy server) have to look at the headers to route the call. In some cases, the servers have to insert some information into the header (for example, Via header in SIP) as the protocol is designed.

This section introduces the most popular types of confidentiality threats: eavesdropping media, call pattern tracking, data mining, and reconstruction.

**Eavesdropping Media**

Eavesdropping on someone’s conversation has been a popular threat since telecommunication service started a long time ago, even though the methods of eavesdropping are different between legacy phone systems and VoIP systems.

In VoIP, an attacker uses two methods typically. One is sniffing media packets in the same broadcasting domain as a target user’s, or on the same path as the media. The other is compromising an access device (for example, Layer 2 switch) and forwarding (duplicating) the target media to an attacker’s device.
The media can be voice-only or integrated with video, text, fax, or image. Figure 2-6 illustrates these cases.

**Figure 2-6  Eavesdropping Media**

In Figure 2-6, the attacker’s device that is in the same broadcasting domain as the IP phone of User A can capture all signals and media through the hub. This figure also shows the possibility that the attacker intrudes in a switch or router, and configures a monitoring port for voice VLAN, and forwards (duplicates) the media to the attacker’s capturing device.

Another possible way of eavesdropping media is that an attacker taps the same path as the media itself, which is similar to legacy tapping technique on PSTN. For example, the attacker has access to the T1 itself and physically splits the T1 into two signals.

Although this technique is targeting media, the next method (call pattern tracking) is targeting signal information.
Call Pattern Tracking

*Call pattern tracking* is the unauthorized analysis of VoIP traffic from or to any specific nodes or network so that an attacker may find a potential target device, access information (IP/port), protocol, or vulnerability of network. It could also be useful for traffic analysis—knowing who called who, and when. For example, knowing that a company’s CEO and CFO have been calling the CEO and CFO of another company could indicate that an acquisition is under way. For another example, knowing that a CEO called her stockbroker immediately after meeting with someone with insider stock knowledge is useful. That is, this is useful for learning about people and information.

To show an example of unauthorized analysis, sample messages that an attacker may capture in the middle of a network are illustrated in Example 2-2. It shows simple SIP request (INVITE) and response (200 OK) messages, but an attacker can extract a great deal of information from them by analyzing the protocol (key fields are highlighted).

**Example 2-2 Exposed Information from SIP Messages**

```
INVITE sip:9252226543@192.168.10.10:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.10.10:5060;branch=z9hG4bK00002000005
From: Alice <sip:4085251111@10.10.10.10:5060>;tag=2345
To: Bob <sip:9252226543@192.168.10.10>
Call-Id: 9252226543-0001
CSeq: 1 INVITE
Contact: <sip:4085251111@10.10.10.10>
Expires: 1200
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 143

Session Description Protocol Version (v): = 0
Owner/Creator, Session Id (o): 2 2 2 IN IP4 10.10.10.10
Session Name (s): Session SDP
Connection Information (c): IN IP4 10.10.10.10
Media Description, name and address (m): audio 9876 RTP/AVP 0 8 18
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): rtpmap:18 G729a/8000

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.10.10.10:5060;branch=z9hG4bK00002000005
From: Alice <sip:4085251111@10.10.10.10:5060>;tag=2345
To: Bob <sip:9252226543@192.168.10.10>;tag=4567
Call-Id: 9252226543-0001
CSeq: 1 INVITE
Contact: <sip:9252226543@172.26.10.10>
Content-Type: application/sdp
Content-Length: 131
```
The following list shows sample information that the attacker may extract from Example 2-2:

- The IP address of the SIP proxy server is 192.168.10.10, and the listening port is 5060.
- They use User Datagram Protocol (UDP) packets for signaling without any encryption, such as Transport Layer Security (TLS) or Secure Multipurpose Internet Mail Extension (S/MIME).
- The proxy server does not require authentication for a call request.
- The caller (Alice), who has a phone number 4085251111, makes a call to Bob at 9252226543.
- The IP address of Alice’s phone is 10.10.10.10 and a media gateway is 172.26.10.10 (supposing that the call goes to PSTN).
- The media gateway opens a UDP port, 20000, to receive Real-time Transport Protocol (RTP) stream from Alice’s phone.
- The media gateway accepts only G.729a codec (Alice’s phone offered G.711a, G.711u, and G.729a initially).

The information just presented can be used for future attacks, such as DoS attack on the proxy server or the media gateway.

### Data Mining

Like email spammers who collect email addresses from various sources like web pages or address books, VoIP spammers also collect user information like phone numbers from intercepted messages, which is one example of data mining.

The general meaning of data mining in VoIP is the unauthorized collection of identifiers that could be user name, phone number, password, URL, email address, strings or any other identifiers that represent phones, server nodes, parties, or organizations on the network. In Example 2-2, you can see that kind of information from the messages.

An attacker utilizes the information for subsequent unauthorized connections such as:

- Toll fraud calls
- Spam calls (for example, voice, Instant Messaging (IM), presence spam)
• Service interruptions (for example, call flooding, call hijacking, and call teardown)
• Phishing (identity fraud; see the section “Threats Against Social Context” for more information)

With valid identities, attackers could have a better chance to interrupt service by sending many different types of malicious messages. Many servers reject all messages, except registration, unless the endpoint is registered.

Reconstruction

Reconstruction means any unauthorized reconstruction of voice, video, fax, text, or presence information after capturing the signals or media between parties. The reconstruction includes monitoring, recording, interpretation, recognition, and extraction of any type of communications without the consent of all parties. A few examples are as follows:

• Decode credentials encrypted by a particular protocol.
• Extract dual-tone multifrequency (DTMF) tones from recorded conversations.
• Extract fax images from converged communications (voice and fax).
• Interpret the mechanism of assigning session keys between parties.

These reconstructions do not affect current communications, but they are utilized for future attacks or other deceptive practices.

In this section so far, you have learned about threats against confidentiality such as eavesdropping media, call pattern tracking, data mining, and reconstruction. The next section covers another type of threats: breaking message and media integrity.

Threats Against Integrity

Another category of VoIP threat is the threat against integrity, which impacts current service severely in most cases.

The basic method of the integrity threat is altering messages (signals) or media after intercepting them in the middle of the network. That is, an attacker can see the entire signaling and media stream between endpoints as an intermediary. The alteration can consist of deleting, injecting, or replacing certain information in the VoIP message or media.

This section is divided into two types of threat at a high level:

• Threats against message integrity (message alteration)
• Threats against media integrity (media alteration)

The next section describes and gives examples of each type of threat.
Message Alteration

Message alteration is the threat that an attacker intercepts messages in the middle of communication entities and alters certain information to reroute the call, change information, interrupt the service, and so on. The typical examples are call rerouting and black holing.

Call Rerouting

Call rerouting is any unauthorized change of call direction by altering the routing information in the protocol message. The result of call rerouting is either to exclude legitimate entities or to include illegitimate entities in the path of call signal or media.

Figure 2-7 illustrates the example of including a malicious entity during call setup.

Figure 2-7  Call Rerouting

In Figure 2-7, an attacker keeps monitoring the call request message (for example, SIP INVITE) from User A to a redirect server. When User A initiates a call, the IP phone sends an INVITE message to the redirect server, as shown in Example 2-3.
Chapter 2: VoIP Threat Taxonomy

Example 2-3  *IP Phone Sends an INVITE Message to the Redirect Server*

| INVITE sip:Bob@192.168.10.10:5060 SIP/2.0 |
|-----------------|---------------------------------|
| Via: SIP/2.0/UDP 10.10.10.10:5060;branch=z9hG4bK00002000005 |
| From: UserA <sip:UserA@10.10.10.10:5060>;tag=2345 |
| To: Bob <sip:Bob@192.168.10.10> |
| Call-Id: 9252226543-0001 |
| CSeq: 1 INVITE |
| Contact: <sip:UserA@10.10.10.10> |
| Max-Forwards: 70 |
| Content-Length: 0 |

The attacker detects the INVITE and intercepts the response message (that is, “302 Moved Temporarily”) from the redirect server, as shown in the continuation of Example 2-3.

SIP/2.0 302 Moved Temporarily
From: UserA <sip:UserA@10.10.10.10:5060>;tag=2345
To: Bob <sip:Bob@192.168.10.10>;tag=6789
Call-Id: 9252226543-0001
CSeq: 1 INVITE
Contact: <sip:Bob@10.1.1.10>
Content-Length: 0

The attacker replaces the IP address of the proxy server (10.1.1.10) in the Contact header with his proxy server (172.26.1.10), and sends to the IP phone, as shown in the continuation of Example 2-3.

SIP/2.0 302 Moved Temporarily
From: UserA <sip:UserA@10.10.10.10:5060>;tag=2345
To: Bob <sip:Bob@192.168.10.10>;tag=6789
Call-Id: 9252226543-0001
CSeq: 1 INVITE
Contact: <sip:Bob@172.26.1.10>
Content-Length: 0

The IP phone sends a new INVITE to attacker’s proxy server rather than the legitimate server, and his server relays the message as shown in the picture. From now on, the attacker in the middle can see all signals between the endpoints and modify for any malicious purpose.

**Call Black Holing**

*Call black holing* is any unauthorized method of deleting or refusing to pass any essential elements of protocol messages, in the middle of communication entities. The consequence of call black holing is to delay call setup, refuse subsequent messages, make errors on applications, drop call connections, and so on. Here are a few examples with SIP:

1. An attacker as an intermediary drops only ACK messages between call entities so that the SIP dialog cannot be completed, even though there could be early media between them.
2. An attacker as an intermediary deletes media session information (SDP) in the INVITE message, which could result in one-way audio or call disconnection.

3. An attacker as an intermediary refuses to pass all messages to a specific user (victim) so that the user cannot receive any inbound calls.

The call rerouting and black holing belong to message alteration as previously described. The next section covers media alteration as part of the threat against integrity.

**Media Alteration**

*Media alteration* is the threat that an attacker intercepts media in the middle of communication entities and alters media information to inject unauthorized media, degrade the QoS, delete certain information, and so on. The media can be voice-only or integrated with video, text, fax, or image. The typical examples are media injection and degrading.

**Media Injection**

*Media injection* is an unauthorized method in which an attacker injects new media into an active media channel or replaces media in an active media channel. The consequence of media injection is that the end user (victim) may hear advertisement, noise, or silence in the middle of conversation. Figure 2-8 illustrates the example with voice stream.

**Figure 2-8  Media Injection**

In Figure 2-8, User A with an IP phone makes a call to User B who has a PSTN phone through a media gateway. After the call setup, the IP phone sends voice (RTP) packets to the media gateway. An attacker in the middle monitors the RTP sequence number of the voice packets, and adjusts the sequence number of illegitimate packets (for example, advertisements), and injects them into the voice channel so that they will arrive before the legitimate packets. User B in PSTN hears the injected voice.
Media Degrading

Media degrading is an unauthorized method in which an attacker manipulates media or media control (for example, Real-Time Control Protocol [RTCP]) packets and reduces the QoS of any communication. Here are a couple of examples:

1. An attacker intercepts RTCP packets in the middle, and changes (or erases) the statistic values of media traffic (packet loss, delay, and jitter) so that the endpoint devices may not control the media properly.

2. An attacker intercepts RTCP packets in the middle, and changes the sequence number of the packets so that the endpoint device may play the media with wrong sequence, which degrades the quality.

In this section so far, you have learned about VoIP threats against integrity such as message alteration (call rerouting, call black holing) and media alteration (media injection, media degrading). The next section covers another type of threats: social threats.

Threats Against Social Context

A threat against social context (as known as “social threat”) is somewhat different from other technical threats against availability, confidentiality, or integrity, as previously discussed, in terms of the intention and methodology. It focuses on how to manipulate the social context between communication parties so that an attacker can misrepresent himself as a trusted entity and convey false information to the target user (victim).

The typical threats against social context are as follows:

- Misrepresentation of identity, authority, rights, and content
- Spam of call (voice), IM, and presence
- Phishing

**NOTE**

A call with misrepresentation is initiated by an attacker who is a communication entity, which is different from the threats in the “Threats Against Integrity” section, which are based on interception and then modification.

The general meaning of spam is unsolicited bulk email that you may see every day. It wastes network bandwidth and system resources, as well as annoying email users. The spam exists in VoIP space as well, so-called VoIP spam, in the form of voice, IM, and presence spam. This section looks into each type of VoIP spam with SIP protocol. The content refers to RFC 5039.1
Phishing is becoming popular in the VoIP world these days as a method of getting somebody’s personal information by deceiving the identity of an attacker.

The following sections give more details about these social threats.

**NOTE**
These same types of attacks are equally available in today’s PSTN environment.

### Misrepresentation

*Misrepresentation* is the intentional presentation of a false identity, authority, rights, or content as if it were true so that the target user (victim) or system may be deceived by the false information. These misrepresentations are common elements of a multistage attack, such as phishing.

Identity misrepresentation is the typical threat that an attacker presents his identity with false information, such as false caller name, number, domain, organization, email address, or presence information.

Authority or rights misrepresentation is the method of presenting false information to an authentication system to obtain the access permit, or bypassing an authentication system by inserting the appearance of authentication when there was none. It includes presentation of password, key, certificate, and so on. The consequence of this threat could be improper access to toll calls, toll calling features, call logs, configuration files, presence information of others, and so on.

Content misrepresentation is the method of presenting false content as if it came from a trusted source of origin. It includes false impersonation of voice, video, text, or image of a caller.

### Call Spam (SPIT)

*Call (or voice) spam* is defined as a bulk unsolicited set of session initiation attempts (for example, INVITE requests), attempting to establish a voice or video communications session. If the user should answer, the spammer proceeds to relay their message over real-time media. This is the classic telemarketer spam, applied to VoIP, such as SIP. This is often called SPam over IP Telephony, or SPIT.

The main reason SPIT is becoming popular is that it is cost-effective for spammers. As you know, legacy PSTN-call spam already exists in the form of telemarketer calls. Although these calls are annoying, they do not arrive in the same kind of volume as email spam. The difference is cost; it costs more for the spammer to make a phone call than it does to send email. This cost manifests itself in terms of the cost for systems that can perform telemarketer calls, and in cost per call. However, the cost is dramatically dropped when switching to
SPIT for many reasons: low hardware cost, low line cost, ease of writing a spam application, no boundary for international calls, and so on. Additionally, in some countries, such telemarketing calls over the PSTN are regulated.

In some cases, spammers utilize computational and bandwidth resources provided by others, by infecting their machines with viruses that turn them into “zombies” that can be used to generate call spam.

Another reason SPIT is getting popular is its effectiveness, compared to email spams. For email spams, you may already realize that there is a big difference between turning on and off a spam filter for your email account. In fact, most spam filters for email today work very well (filter more than 90 percent of spams) because of the nature of email; store and forward. All emails can be stored and examined in one place before forwarding to users. Even though users may still receive a small percentage of email spams, they usually look at profiles (for example, sender name and subject) and delete most of them without seeing the contents. However, the method of filtering emails does not work for SPIT because voice is real-time media. Only after listening to some information initially can users recognize whether it is a spam or not. So, spammers try to put main information in the initial announcement so that users may listen to it before hanging up the phone. There is a way to block those call attempts based on a blacklist (spammers’ IP address or caller ID), but it is useless if spammers spoof the source information.

You can find more information on SPIT and mitigation methods in Chapter 6, “Analysis and Simulation of Current Threats.”

The next topic is a different type of VoIP spam, IM spam.

**IM Spam (SPIM)**

IM spam is similar to email. It is defined as a bulk unsolicited set of instant messages, whose content contains the message that the spammer is seeking to convey. This is often called Spam over Instant Messaging, or SPIM.

SPIM is usually sent in the form of request messages that cause content to automatically appear on the user’s display. The typical request messages in SIP are as follows:

- **SIP MESSAGE request** (most common)
- **INVITE request** with large Subject headers (since the Subject is sometimes rendered to the user)
- **INVITE request** with text or HTML bodies
Example 2-4 shows examples with SIP INVITE and MESSAGE.

Example 2-4  IM Spam

```
INVITE sip:Bob1@192.168.10.10:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.10.10:5060;branch=z9hG4bK00002000005
From: Spammer <sip:spammer1@10.10.10.10>;tag=2345
To: Bob <sip:Bob1@192.168.10.10>
Call-Id: 9252226543-0001
CSeq: 1 INVITE
Subject: Hi there, buy a cool stuff in our website www.spam-example.com
Contact: <sip:spammer1@10.10.10.10>
Expires: 1200
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 143

MESSAGE sip:Bob1@192.168.10.10:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.10.10:5060;branch=z9hG4bK00002000005
From: Spammer <sip:spammer1@10.10.10.10>;tag=2345
To: Bob <sip:Bob1@192.168.10.10>
Call-Id: 9252226543-0001
CSeq: 1 MESSAGE
Max-Forwards: 70
Content-Type: test/plain
Content-Length: 25

Hi there, buy a cool stuff in our website www.spam-example.com
```

SPIM is very much like email, but much more intrusive than email. In today’s systems, IMs automatically pop up and present themselves to the user. Email, of course, must be deliberately selected and displayed.

Presence Spam (SPPP)

Presence spam is similar to SPIM. It is defined as a bulk unsolicited set of presence requests (for example, SIP SUBSCRIBE requests) in an attempt to get on the “buddy list” or “white list” of a user to subsequently send them IM or INVITEs. This is occasionally called SPam over Presence Protocol, or SPPP.

The cost of SPPP is within a small constant factor of IM spam, so the same cost estimates can be used here. What would be the effect of such spam? Most presence systems provide some kind of consent framework. A watcher that has not been granted permission to see the user’s presence will not gain access to their presence. However, the presence request is usually noted and conveyed to the user, allowing them to approve or deny the request. This request itself can be spam, as shown in Example 2-5.
In SIP, this is done using the watcherinfo event package. This package allows a user to learn the identity of the watcher, in order to make an authorization decision. This could provide a vehicle for conveying information to a user; Example 2-5 shows the example with SIP SUBSCRIBE.

**Example 2-5  Presence Spam**

```plaintext
SUBSCRIBE sip: bob@example.com SIP/2.0
Event: presence
To: sip: bob@example.com
From: sip: buy-cool-dvds-and-games@spam-example.com
Contact: sip: buy-cool-dvds-and-games@spam-example.com
Call-ID: knsd08alas9dy@3.4.5.6
CSeq: 1 SUBSCRIBE
Expires: 3600
Content-Length: 0
```

A spammer in Example 2-5 generates the SUBSCRIBE request from the identity (sip:buy-cool-dvds-and-games@spam-example.com), and this brief message can be conveyed to the user, even though the spammer does not have permission to access presence. As such, presence spam can be viewed as a form of IM spam, where the amount of content to be conveyed is limited. The limit is equal to the amount of information generated by the watcher that gets conveyed to the user through the permission system.

**Phishing**

The general meaning of *phishing* is an illegal attempt to obtain somebody’s personal information (for example, ID, password, bank account number, credit card information) by posing as a trust entity in the communication. In VoIP, phishing is typically happening through voice or IM communication, and voice phishing is sometimes called “vishing.”

The typical sequence is that a phisher picks target users and creates request messages (for example, SIP INVITE) with spoofed identities, pretending to be a trusted party. When the target user accepts the call request, either voice or IM, the phisher provides fake information (for example, bank policy announcement) and asks for personal information. Some information like user name and password may not be directly valuable to the phisher, but it may be used to access more information useful in identity theft.

Here are a couple of phishing examples:

1. A phisher makes a call to a target user and leaves a voice message like: “This is an important message from ABC Bank. Because our system has changed, you need to change your password. Please call back at this number: 1-800-123-4567.” When the target user calls the number back, the phisher’s Interactive Voice Response (IVR) system picks up the call and acquires the user’s password by asking “Please enter your current password for validation purposes . . ..”
A phisher sends an instant text message to a smart phone (for example, PDA phone) or softphone (for example, Skype client) users, saying “This message is from ABC Bank. Your credit card rate has been increased. Please check it out on our website: http://www.abcbank.example.com.” When the users click the URL, it goes to a phisher’s website (example.com) that appears to have exactly the same web page that ABC Bank has. The fake website collects IDs and passwords that the users type in.

In this section, you have learned about VoIP threats in a social context, such as misrepresentation, call spamming, IM spamming, presence spamming and phishing. For more detailed information about VoIP spamming, refer to Chapter 6, “Analysis and Simulation of Current Threats.”

Summary

VoIP vulnerabilities can be exploited to create many different kinds of threats. The threats can be categorized as four different types: threats against availability, confidentiality, integrity, and social context.

A threat against availability is a threat against service availability that is supposed to be running 24/7. That is, the threat is aiming at VoIP service interruption, typically, in the form of DoS. The examples are call flooding, malformed messages (protocol fuzzing), spoofed messages (call teardown, toll fraud), call hijacking (registration or media session hijacking), server impersonating, and QoS abuse.

A threat against confidentiality does not impact current communications generally, but provides an unauthorized means of capturing conversations, identities, patterns, and credentials that are used for the subsequent unauthorized connections or other deceptive practices. VoIP transactions are mostly exposed to the confidentiality threat because most VoIP service does not provide full confidentiality (both signal and media) end-to-end. The threat examples are eavesdropping media, call pattern tracking, data mining, and reconstruction.

A threat against integrity is altering messages (signals) or media after intercepting them in the middle of the network. That is, an attacker can see the entire signaling and media stream between endpoints as an intermediary. The alteration can consist of deleting, injecting, or replacing certain information in the VoIP message or media. The typical examples are call rerouting, call black holing, media injection, and media degrading.

A threat against social context focuses on how to manipulate the social context between communication parties so that an attacker can misrepresent himself as a trusted entity and convey false information to the target user. The typical examples are misrepresentation (identity, authority, rights, and content), voice spam, instant message spam, presence spam, and phishing.
End Notes


References


Numerics

3DES (Triple Data Encryption Standard), 87

A

c: access
control, Unified CME, 259–261
devices, 13, 277
deployment, 284–286
IP phones, 278
Switch, 278–282
VLAN ACLs, 282–284
policies, 213
ports, preventing, 279
SBCs, 208
Access Control Engines. See ACEs
Access Control Lists. See ACLs
Access Function (AF), 116, 295
access gateways, 74
ACEs (Access Control Engines), 216
ACF (admission confirm), 50
ACLs (Access Control Lists), 108, 215
DoS protection, 216
VLANs, 282–284
Active-Active mode, 231
Active-Standby mode, 230–231, 250
Address Resolution Protocol. See ARP
addresses
alias address modification, 50
call content interception, 301–302
limited-use, 171
NAT, 21, 109–113
obfuscation, 170
translation, 49
traversal, 222–224
address-of-record (AoR), 69
AddRoundKey() function, 92
admission confirm (ACF), 50
admissions, control, 49
AES (Advanced DES), 89–92
AF (Access Function), 116, 295
aggregation routers, 327–328
ALG (Application Layer Gateway), 253

algorithms
DES, 87. See also DES
DSA, 95–96
hashing, 96
MAC, 99–100
MD5, 97–98
SHA, 98–99
RSA, 95
SHA, 84
alias address modification, 50
Alliance for Telecommunications Industry
Solutions (ATIS), 292
alteration
media, 37–38
messages, 35–37
amplification, DoS and, 197
Analog Telephone Adapter (ATA), 117
analysis, 160
flooding attacks, 135–137
malformed messages, 150–153
service policies, 234–237
sniffing/eavesdropping, 158–161
spoofing, 164–165
unintentional flooding, 139
anchoring media, 240
ANMPv3 (Simple Network Management
Protocol version 3), 316
Annex D (H.235) baseline security, 54
Annex E (H.235) signature security, 55–56
Annex F (H.235) hybrid security, 56–57
Answer messages, 334
AoR (address-of-record), 69
Application Layer Gateway (ALG), 253
applications
 pkcs7-mime types, 183
VoIP, 12
architecture
Cisco SII architecture, 313, 329
connectivity, 232–234
hardware, DoS protection, 215–216
LI, 294–297
networks, 8
SBC locations, 224
services, 5
  Active-Active, 231
  Active-Standby, 230–231
  high availability, 229–230
  network connectivity, 232–234
  policy analysis, 234–237
  SBCs, 228–229
  traffic flow optimization, 239–244
  virtualization, 237–238

area codes, 8

ARP (Address Resolution Protocol)
  firewalls, 252
  misbehaving endpoints, 140–141
  responses, limiting, 282

ASA firewalls, 251–256

asymmetric (public) key cryptography, 92–93
  DSA, 95–96
  RSA, 93–95

ATA (Analog Telephone Adapter), 117

ATIS (Alliance for Telecommunications Industry Solutions), 292

attacks
  DoS, 128
    intentional flooding, 129–138
    unintentional flooding, 138–143
  MITM, 198
  replay, 326
  TCP SYN, 128

attributes, service policies, 234

audio, saving, 161

AuditConnection (AUCX), 75

AUEP (AuditEndpoint), 75

authentication, 14, 175
  CHAP, 119
  devices, 270
  digest, 68–69, 198, 271–272
  files, 270
  identity, 69–70
  images, 270
  integrity, 53
  MAC, 99–100
  PAP, 119
  signaling, 271
  Unified CM, 269–273
  user-to-proxy, 176–179
  user-to-user, 179–182
  white lists, 214

authentication-only security services, 53

authority, 39

authorization, 272
  calls, 49
  white lists, 214

availability, threats against, 20–30

B

B2BUA (Back-to-Back User Agent), 59, 118

bandwidth
  control, 49, 109
  management, 49
  transcoding, 226–227

baseline security (H.235), 54

benefits of VoIP, 6–8

binding information, 282

black holing, calls, 36

black traffic, 213

black/white lists, consent-based, 171

blind transfers, 336

blocking after-hours calls, 266–267

bodies, formatting S/MIME, 186–188

borders
  SBCs
    between access and core networks, 206–207
    between core and peer networks, 207
    troubleshooting, 204–206
  sessions, 203

BTS (Cisco Broadband Telephony Softswitch), 302

C

CA (Certificate Authority), 95

CALEA (Communications Assistance for Law Enforcement Act), 292

call content (CC), 292

call content channel (CCC), 296

call content connection identifier (CCCID), 316

call data (CD), 292

call data channel (CDC), 296

calls
  after-hours call blocking, 266–267
  authorization, 49
black holing, 36
content
collection interfaces, 329–339
interception, 301–302
control
flooding, 21, 129
signaling, 49
flow, 20–22
digest authentication, 176
H.323, 50–52
through SBCs, 210
SIP, 60–61
forwarding, 303
hijacking, 26
pattern tracking, 32–33
processing
servers, 117–120
units, 216
requests, flooding, 129
rerouting, 35
spam, 39
tear down, 25
toll fraud, 26
transfers, 336
CAM (content-addressable memory), 278–279
capacity, LI, 304
CAPF certificates, 268
CC (call content), 292
CCC (call content channel), 296
CCChange message, 334
CCCID (call content connection identifier), 316
CCClose message, 334
CCOpen message, 334
CD (call data), 292
CDC (call data channel), 296
Certificate Authority (CA), 95
certificates, 269–277
S/MIME, 184
Unified CM, 267–269
CFs (Collection Functions), 116, 296, 315
CHAP (Challenge Handshake Authentication Protocol), 119
Cisco Broadband Telephony Softswitch (BTS) 10200, 328
Cisco Lawful Intercept Control MIB (CISCO-TAP-MIB), 327
Cisco PSTN Gateway 2200 (PGW 2200), 328
Cisco Unified Communications Manager Express. See Unified CME
Cisco Unified Communications Manager. See Unified CM
Cisco Unity SCCP device certificates, 269
Cisco Unity server certificates, 269
Class of Restriction (COR), 264–266
click-to-call feature, 8
clients
UAC, 58, 175
web, 13
CMS (cryptographic message syntax), 183
Collection Functions (CFs), 116, 296, 315
commands
enable password, 259
enable secret, 259
ip http access-class, 263
ip http authentication, 264
ip http secure-server, 263
make, 162
make no-open-ssld, 162
rtpw, 192
SIPcrack, 162
communications, real-time, 11
components
H.323, 49–50
SIP, 58–59
vulnerabilities, 12–13
ConferecePartyChange message, 334
certainty
breaches, 326
threats against, 30–34
configuration
access devices, 284–286
firewalls
ASA and PIX, 254–256
FWSM, 257–258
LI, 325–327
SBCs
Active-Active, 231
Active-Standby, 230–231
high availability, 229–230
network connectivity, 232–234
service architecture design, 228–229
service policy analysis, 234–237
traffic flow optimization, 239–244
virtualization, 237–238
security
VoIP-aware firewalls, 108–109
SIP sessions, 61–67
troubleshooting, 22
Unified CM, 275–277
wrong configuration of devices, 139
consent-based black/white lists, 171
consultative transfers, 336
content
connection interfaces, 329–339
encryption, LI, 302
filtering, 168
misrepresentation, 39
control
access, Unified CME, 259–261
admissions, 49
bandwidth, 49, 109
media, 240
MGCP, 74–75
phone registrations, Unified CME, 261–262
ping, 220
planes, 314
registration timers, 217–220
security profiles, 75–77
transcoding, 226–227
conversion, protocols, 226
COR (Class of Restriction), 264–266
cost savings, 6–7
CPE (Customer Premise Equipment), 116–117
SBCs, 209
cracking passwords, 163
CRCX (CreateConnection), 75
CreateConnection (CRCX), 75
cryptanalysis, 83
cryptographic message syntax (CMS), 183
cryptography, 83
asymmetric (public) key, 92–93
DSA, 95–96
RSA, 93–95
symmetric (private) key, 84–85
3DES, 87
AES, 89–92
DES, 85–87
Customer Premise Equipment (CPE), 116–117

D
DAI (Dynamic ARP Inspection), 282
Data Encryption Standard. See DES
data integration, 12
data mining, 33–34
data security infrastructure, 15
DDoS (Distributed Denial-of-Service), 197
deployment
access devices, 284–286
firewalls, 250
location, 239–240
derivation, keys, 188–190
DES (Data Encryption Standard), 54, 85–87
design
configuration. See configuration
service architecture, 228–229
Active-Active, 231
Active-Standby, 230–231
high availability, 229–230
network connectivity, 232–234
service policy analysis, 234–237
traffic flow optimization, 239–244
virtualization, 237–238
detection
by target subscribers, LI, 300–301
unauthorized creation of intercepts, 303
devices
access, 13, 277
deployment, 284–286
IP phones, 278
Switch, 278–282
VLAN ACLs, 282–284
authentication, 270
cost savings, 6–7
configuration, 22
cracking passwords, 163
cryptanalysis, 83
cryptographic message syntax (CMS), 183
cryptography, 83
design
configuration. See configuration
data integration, 12
data mining, 33–34
data security infrastructure, 15
data integration, 12
data mining, 33–34
data security infrastructure, 15
devices
lack of, 11
MD, 298, 339–341
security, 108

LI, 114–116
NAT, 109–113
SBC, 113–114
VoIP-aware firewalls, 108–109
services, 116
call processing servers, 117–120
CPE, 116–117
wrong configuration of, 139
DF (Delivery Function), 116, 295–296
DHCP (Dynamic Host Configuration Protocol)
DoS attacks, mitigating, 281
Servers, preventing fraudulent, 280
dialed digital translation, 50
DialedDigitExtraction message, 334
dictionaries, passwords, 26
Differentiated Services Code Point (DSCP), 228
Diffie-Hellman key-exchange procedures, 54
digest authentication, 68–69, 271–272
limitations of, 198
Digital Signature Algorithm. See DSA
digital signatures, 95
disadvantages of VoIP, 8–10
Distributed Denial-of-Service (DDoS), 197
distribution, keys, 101–103
DLCX (DeleteConnection), 75
DNS (Domain Name Service), 316
domains, 113
SBCs, 203
DoS (Denial-of-Service) attacks, 128
and amplification, 197
DHCP, mitigating, 281
flooding, 114
intentional flooding, 129–138
protection, 109
SBCs, 206, 213–216
unintentional flooding, 138–143
DSA (Digital Signature Algorithm), 95–96
DSCP (Differentiated Services Code Point), 228
DTMF (dual-tone multifrequency), 34, 273
Dynamic ARP Inspection (DAI), 282
Dynamic Host Configuration Protocol. See DHCP
dynamic triggering, 308

eavesdropping, 154
analysis, 158–161
media, 30–31
mitigation, 161
simulation, 154–158
Edge Services Router (ESR), 327
EIGRP (Enhanced Interior Gateway Routing), 252
e-mail, spam, 165
mitigation, 168–172
SPPP, 167–168
voice, 165–166
emergency calls, 9
Enable Application Level Authorization check box, 273, 277
Enable Digest Authentication check box, 276
enable password command, 259
enable secret command, 259
encryption, 14, 182
content, LI, 302
media, 188–193, 274
S/MIME, 183–188
signaling, 273
Unified CM, 273–275
encryption key (KE), 53
EndpointConfiguration (EPCF), 75
endpoints
devices, 140
misbehaving, 140–141
troubleshooting, 22
Enhanced Interior Gateway Routing (EIGRP), 252
EOFB (Enhanced OFB), 53
EPCF (EndpointConfiguration), 75
ESR (Edge Services Router), 327
ETSI (European Telecommunications Standards Institute), 292
European Council Resolution, 292
exchanges, keys, 185–186
expiration time, registration timer control, 217–220
exposed interfaces, 11
extensions, preventing network, 280
fake (spoofed) messages, 24–30
features, rich, 8
file authentication, 270
filtering
  content, 168
  SIP messages, 158
Find-Me-Follow-Me (FMFM), 8
firewalls, 249–251
  ASA and PIX, 251–256
  deployment, 250
  FWSM, 256–258
  limitations, 258–259
  SBCs, 207
  VoIP-aware, 108–109
First Available, 221
flooding
  calls, 20–22
  control, 129
  request, 129
DoS attacks, 114, 128
  intentional, 129–138
  unintentional, 138–143
MAC CAM, mitigating, 278–279
messages, 132, 137
ping, 129
registration, 129
SBCs, 206, 213–216
traffic, 132
flow
  calls
    digest authentication, 176
    through SBCs, 210
    SIP, 60–61
  process. See process flow
traffic, 239–244. See also traffic
FMFM (Find-Me-Follow-Me), 8
formatting S/MIME bodies, 186–188
forwarding calls, 303
FQDN (fully qualified domain name), 316
fraud
  COR, 264–266
  DHCP servers, preventing, 280
toll, 26
full cone NAT, 109
fully qualified domain name (FQDN), 316
functionality, SBCs, 208, 226–228
  DoS protection, 213–216
  LI, 224–225
  NAT traversal, 222–224
  network topology hiding, 208–212
  overload protection, 216–222
functions. See also commands
  AddRoundKey(), 92
  hash, 97–98
  MixColumns(), 91
  ShiftRows(), 90
  SubBytes(), 89
fuzzing, protocol, 22–24
FWSM firewalls, 256–258
G
gatekeepers, 50
gateways, 50
  ALG, 253
  EIGRP, 252
  media, 119
  MGCP, 74–77
  trunking, 328
Unified CM, 267
  authentication, 269–273
  configuration, 275–277
  encryption, 273–275
  integrity, 269–273
  security, 267–269
Unified CME, 259
  access control, 259–261
  after-hours call blocking, 266–267
  COR, 264–266
  phone registration control, 261–262
  secure GUI management, 263–264
geographical limitations, 7
Gigabit Switch Router (GSR), 327
global power outages, 139
government law, LI. See LI
gray traffic, 214
GSR (Gigabit Switch Router), 327
H.225 (Q.931), 48
H.235, 48
  Annex D (baseline security), 54
  Annex E (signature security), 55–56
  Annex F (hybrid security), 56–57
H.245, 48
H.323, 48
  call flow, 50–52
  components, 49–50
  overview of, 48–52
  security profiles, 52–57
hacking, 83. See also cryptography
hairpinning, 328
handshakes, TLS, 71–73
hardware, DoS protection, 215–216
Hash-based Message Authentication Code (HMAC), 303
hashing algorithms, 96
  MAC, 99–100
  MD5, 97–98
  SHS, 98–99
headers
  Cisco SII architecture, 313–329
  SIP P-DCS, 309–313
heavy traffic, comparing to malicious flooding, 136
hiding topologies, 208–212
high availability, 229–230
  network connectivity with, 233
hijacking
  calls, 26
  media sessions, 27
  registration, SIP, 195
HMAC (Hash-based Message Authentication Code), 303
HTTPS certificates, 268
hybrid security (H.235), 56–57

IAD (integrated access device), 117, 139
IAP (intercept access point), 295, 308
identity
  authentication, 69–70

theft, 162
  analysis, 164–165
  mitigation, 165
  simulation, 162–164
IETF (Internet Engineering Task Force), 183
IM (Instant Messaging), 5
  spam, 167
  SPIM, 40–41
images, authentication, 270
impersonation, 326
  servers, 28–29, 196
implementation of LI intercept request interfaces, 308–329
inbound calls, 112. See also calls
infrastructure
  data security, 15
  IP, 10
  sources of vulnerability, 10–13
injection, media, 37
inspection, protocol messages, 108
Instant Messaging. See IM
integrated access device (IAD), 117, 139
integration
  data, 12
  voice, 12
integrity
  authentication, 53
  threats against, 34–38
  Unified CM, 269–273
intentional flooding, 129–138
  SBCs, 206
Interactive Voice Response (IVR), 42
intercept access point (IAP), 295, 308
intercept request interfaces, 308
  Cisco SII, 313–329
  SIP P-DCS headers, 309–313
interception
  call content, 301–302
  capacity, 304
  unauthorized creation and detection of intercepts, 303
interfaces
  content connection, 329–339
  devices, Cisco SII, 314
  exposed, 11
intercept request, 308
Cisco SII, 313–329
SIP P-DCS headers, 309–313
link-layer, 340
management, 12
Unified CME, 263–264
network layer, 340
physical, 340
request/response, LI, 297–300
user control, 7

International Telecommunication Union. See ITU
Internet Engineering Task Force (IETF), 183
Internet service providers (ISPs), 204
interoperability, 8
interruption threats
against availability, 20–30
against confidentiality, 30–34
against integrity, 34–38
against social context, 38–43
spoofed messages, 24–30
invalid call request flooding, 129
invalid registration flooding, 129
INVITE message, 112
IP (Internet Protocol) network infrastructure, 10
ip http access-class command, 263
ip http authentication command, 264
ip http secure-server command, 263
IP phones, 117, 278
IP-based PBX, 118
IPSec, 73, 195, 268
ISPs (Internet service providers), 204
ITU (International Telecommunication Union), 48
IVR (Interactive Voice Response), 42

K
KE (encryption key), 53
keys
asymmetric (public) cryptography, 92–93

DSA, 95–96
RSA, 93–95
distribution, 101–103
exchanges, S/MIME, 185–186
management, 100–101
SRTP, 188–190

symmetric (private) cryptography, 84–85

3DES, 87
AES, 89–92
DES, 85–87
KS (salting key), 53

L
LAES (Lawfully Authorized Electronic Surveillance), 309
Law Enforcement Administration Function (LEAF), 116, 297
law enforcement agencies. See LEAs
lawful interception. See LI
Lawfully Authorized Electronic Surveillance (LAES), 309
layers, security, 193–195
LEAF (Law Enforcement Administration Function), 116, 297
LEAs (law enforcement agencies), 292
impersonation, 326
MDs, 339–341
requirements for, 293–294
Least Busy, 222
legacy system security, 14
legal issues, 9
legitimate call flooding, 22
LI (lawful interception), 9, 114–116
Cisco SII, 313–329
configuration, 327
content connection interfaces, 329–339
intercept request interfaces, 308
MDs, 339–341
operational issues, 300–304
overview of, 292–293
reference models, 294–297
request/response interfaces, 297–300
requirements for LEAs, 293–294
SBCs, 207, 224–225
SIP P-DCS headers, 309–313
libSRTP tool, 191–193
limitations
ARP responses, 282
digest authentication, 198
firewalls, 258–259
geographical, 7
S/MIME, 198
SIP, 198–199
TLS, 199
limited-use addresses, 171
link-layer interfaces, 340
Linux resource monitoring, 134
load balancing, 220–222
local hairpinning, 328
locations, deployment, 240

M
MAC (Media Access Control), 278–279
MAC (Message Authentication Code), 99–100
make command, 162
make no-openssl command, 162
malformed messages, 22–24, 143–144
analysis, 150–153
mitigation, 154
simulation, 144–150
malicious call teardown, 25
malicious flooding, comparing to heavy traffic, 136
management
bandwidth, 49
firewalls, 252
interfaces, 12
Unified CME, 263–264
keys, 100–103
zones, 49
man-in-the-middle (MITM) attack, 198
marking QoS, 228
master keys, 188–190
MC (Multipoint Controller), 50
MCU (Multipoint Control Unit), 50
MD (mediation device), 308
MD5 (Message Digest 5), 97–98, 303
MDCX (ModifyConnection), 75
mdpasswd, 328
MDs (Mediation Devices), 339–341
mduserid, 328
media
alteration, 37–38
anchoring, 240
control, 240
degrading, 38
eavesdropping, 30–31
encryption, 188–193, 274
gateways, 74, 119
injection, 37
rich servers, 119
rich service, 7
traversal, 241
Media Access Control. See MAC
Media Gateway Control Protocol. See MGCP
media session hijacking, 27
MediaReport message, 334
mediation device (MD), 298, 308, 339-341
Message Authentication Code (MAC), 99–100
Message Digest 5 (MD5), 97–98, 303
messages
alteration, 35–37
CDC, 333–334
cryptographic, S/MIME, 183–188
cryptographic, S/MIME, 183–188
cryptographic, S/MIME, 183–188
cryptographic, S/MIME, 183–188
cryptographic, S/MIME, 183–188
cryptographic, S/MIME, 183–188
flooding, 132, 137
forgery, 326
INVITE, 112
malformed, 22–24, 143–144
analysis, 150–153
mitigation, 154
simulation, 144–150
ping, control, 220
privacy, 94
protocol inspection, 108
SIP
filtering, 158
INVITE, 23
NAT, 111
spoofed, 24–30
MGCP (Media Gateway Control Protocol), 74–75
security profiles, 75–77
mining data, 33–34
misbehaving endpoints, 140–141
misrepresentation, 39
mitigation
DHCP DoS attacks, 281
flooding attacks, 137–138
MAC CAM flooding, 278–279
malformed messages, 154
sniffing/eavesdropping, 161
spam, 168-172
spoofing, 165
unintentional flooding, 141, 143
MITM (man-in-the-middle) attack, 198
MixColumns() function, 91
mobility, 11
services, 7
models
reference, LI, 294–297
threats, 195–198
modes
Active-Standby, 250
packets, 296
routed
ASA and PIX firewalls, 251–252
FWSM firewalls, 256
SIP, 130
transparent
ASA and PIX firewalls, 252
FWSM firewalls, 256
ModifyConnection (MDCX), 75
monitoring resources, 134
multihoming, 301
multimedia, SIP, 57–58
overview of, 58–67
security profiles, 67–73
multipart/signed content type, 183
Multipoint Control Unit (MCU), 50
Multipoint Controller (MC), 50
myths versus reality, 14–15

N
NAPT (Network Address and Port Translation), 110
NAT (Network Address Translation), 21, 109–113
SBCs, 207
traversal, 222–224
National Institute of Standards and Technology (NIST), 5
negative testing tools, 129
Network Address and Port Translation. See NAPT
Network Address Translation. See NAT
network interface card (NIC), 140, 216
network layer
interfaces, 340
security, 193–195
networks
architecture, 8
borders
between access and core networks, 206–207
between core and peer networks, 207
troubleshooting, 204–206
connectivity, 232–234
extensions, preventing, 280
IP, 10
PSTN, 5
topologies, hiding, 208–212
vulnerabilities, 13
NetworkSignal message, 334
NIC (network interface card), 140, 216
NIST (National Institute of Standards and Technology), 5
nonrepudiation, 55
NotificationRequest (RQNT), 75
NTFY (Notify), 75
numbers, translation, 227–228

O
obfuscation, addresses, 170
OFB (Output Feedback Mode), 53
open networks, 11
Open Shortest Path First (OSPF), 251
open VoIP protocols, 11
operating systems, 12
Origination message, 334
OSPF (Open Shortest Path First), 251
Output Feedback Mode (OFB), 53
overload protection, 216–222

P
PacketCable, 292, 316, 328
packets
modes, 296
RTCP, 38
SRTP, processing, 190–191
PAP (Password Authentication Protocol), 119
passwords
cracking, 163
dictionaries, 26
patterns, tracking, 32–33
payload of CCC diagrams, 331
peer SBCs, 207–208
performance, call flooding, 20–22
personalized ring tones, 8
PGW 2200 (Cisco PSTN Gateway 2200), 328
phishing, 42–43
phone portability, 7
phone registration control, Unified CME, 261–262
physical interfaces, 340
ping
control, 220
flooding, 21, 129
PIX firewalls, 251–256
policies
access, 213
services, 234–237
Policy Engine, DoS protection, 216
port restricted cone NAT, 109
portability of phones, 7
port access, preventing, 279
power outages, 9
global, 139
regional, 22
predesign considerations for LI, 325
pre-provisioning, 308
presence spam (SPPM), 41–42, 167–168
prespoofing scans, 162
prevention
fraudulent DHCP servers, 280
network extensions, 280
port access, 279
threats, 195–198
privacy
breaches, 326
messages, 94
private (symmetric) key cryptography, 84–85
3DES, 87
AES, 89–92
DES, 85–87
process flow
for conference calls, 322–324
for forwarding calls, 319–321
for inbound calls, 311
for outbound calls, 310
for standard calls, 316–319
processing packets, SRTP, 190–191
profiles, security, 52–57
MGCP, 75–77
SIP, 67–73
properties, SHA, 99
Proportional Distribution, 222
protocols, 38
ARP
firewalls, 252
limiting responses, 282
CHAP, 119
conversion, 226
fuzzing, 22–24
H.323
overview of, 48–52
security profiles, 52–57
IPSec, 73
messages
inspection, 108
malformed, 22–24
MGCP, 74–75
security profiles, 75–77
open VoIP, 11
PAP, 119
proxy servers, 118
RIP, 251
RTCP, 48
RTP, 48
intercepted information, 332
SRTP, 188–193
SCCP, 253
SDP, 58, 226
SIP, 7, 57–58
call flow, 60–61
components, 58–59
encryption, 182
filtering, 158
limitations of, 198–199
malformed messages, 144
modes, 130
overview of, 58–67
registration hijacking, 195
S/MIME, 183–188
security profiles, 67–73
SRTP, 267
stacks, 13
UDP, 33, 274
PROTOS SIP version, 144
provisioning, 315
proxy servers, 59
user-to-proxy authentication, 176–179
PSTNs (public switched telephone networks), 5 LI, 292
public (asymmetric) key cryptography, 92–93
DSA, 95–96
RSA, 93–95
public access networks, SBCs, 206–207
public networks, 11
public service telephone networks. See PSTNs

Q
QoS (quality of service), 8
abuse, 29–30
firewalls, 250
marking, 228
SBCs, 207

R
RADIUS (Remote Authentication Dial-In User Service), 120, 264
Random Select, 222
realms, 113
SBCs, 203
real-time communications, 11
Real-Time Control Protocol (RTCP), 38
reconstruction, 34
redirect servers, 59
redirection, 336
Redirection message, 334
reference models, LI, 294–297
regional power outages, 22
REGISTER requests, 59
registration
flooding, 20, 129
hijacking, 27
SIP, 195
phone control, 261–262
SIP with Digest Authentication, 177
timer control, 217–220
regulatory mandates, SBCs, 207
Release message, 334
Remote Authentication Dial-In User Service (RADIUS), 120, 264
replay attacks, 326
reputation systems, 169
requests
calls, flooding, 20, 129
interfaces, LI, 297–300
REGISTER, 59
requirements for LEAs, 293–294
rerouting calls, 35
residential gateways, 74
resources, monitoring, 134
responses
ARP, limiting, 282
interfaces, LI, 297–300
RestartInProgress (RSIP), 75
restricted cone NAT, 109
restrictions
access ports, 280
after-hours call blocking, 266–267
COR, 264–266
rich media, 8
servers, 119
services, 7
rights misrepresentation, 39
ring tones, 8
RIP (Routing Information Protocol), 251
Rivest, Shamir, and Adleman. See RSA
Round Robin, 221
routed mode
ASA and PIX firewalls, 251–252
FWSM firewalls, 256
routers, 13
aggregation, 327–328
routings, EIGRP, 252
RQNT (NotificationRequest), 75
RSA (Rivest, Shamir, and Adleman), 93–95
key distribution, 102
RSIP (RestartInProgress), 75
RTCP (Real-Time Transport Control Protocol), 48
RTP (Real-Time Transport Protocol), 48
intercepted information, 332
SRTP, 71, 188–193
rtpw command, 192
data security infrastructure, 15
devices, 108
  lack of, 11
  LI, 114–116
  NAT, 113
  SBC, 113–114
  VoIP-aware firewalls, 109
DoS attacks, 128
  intentional flooding, 129–138
  unintentional flooding, 138–143
encryption, 182
  media, 188–193
  S/MIME, 183–188
firewalls, 249–251
  ASA and PIX, 251–256
  FWSM, 256–258
  limitations, 258–259
GUI management, Unified CME, 263–264
IPSec, 73, 195
legacy systems, 14
LI, 326–327
malformed messages, 143–144
  analysis, 150–153
  mitigation, 154
  simulation, 144–150
network layer, 193–195
profiles, 52–57
  MGCP, 75–77
  SIP, 67–73
sniffing/eavesdropping, 154
  analysis, 158–161
  mitigation, 161
  simulation, 154–158
sources of vulnerability, 10–12
  components, 12–13
spam, 165
  IM, 167
  mitigation, 168–172
  SPPP, 167–168
  voice, 165–166
spoofing, 162
  analysis, 164–165
  mitigation, 165
  simulation, 162–164
TLS, 253
transport layer, 193–195
Unified CM, 267–269
servers  
call processing, 117–120  
DHCP, preventing fraudulent, 280  
impersonating, 196  
imersonation, 28–29  
LI, 114–116  
NAT traversal, 222–224  
proxy, 59  
   user-to-proxy authentication, 176–179  
redirect, 59  
rich media, 119  
TFTP, 12  
UAS, 58, 175  
web, 13  
proxy  
Service Independent Interception (SII), 292, 308  
Service Level Agreement (SLA), 229  
Service Provider Administration Function (SPAF), 116, 297  
ServiceInstance message, 334  
services  
ar chitecture, 5  
   Active-Active, 231  
   Active-Standby, 230–231  
   high availability, 229–230  
   SBCs, 228–229  
devices, 116  
   call processing servers, 117–120  
   CPE, 116–117  
 mobility, 7  
 rich media, 7  
 security profiles, 52–57  
 spoofed messages, 24–30  
 threats  
   against availability, 20–30  
   against confidentiality, 30–34  
   against integrity, 34–38  
   against social context, 38–43  
Session Border Controllers. See SBCs  
Session Description Protocol. See SDP  
Session Initiation Protocol. See SIP  
sessions  
 borders, 203  
 keys, 188–190  
 media hijacking, 27  
 SIP configuration, 61–67  
 tearing down, 196  
SHA (Secure Hash Algorithm), 84  
ShiftRows() function, 90  
SHS (Secure Hash Standard), 98–99  
signaling  
   authentication, 271  
   encryption, 273  
   H.235, 54  
signatures  
   digital, 95  
   security (H.235), 55–56  
SII (Service Independent Interception), 292, 308  
Simple Network Management Protocol version 3 (SNMPv3), 316  
simulation  
   flooding attacks, 129–135  
   malformed messages, 144–150  
   sniffing/eavesdropping, 154–158  
   spoofing, 162–164  
simultaneous rings on multiple phones, 8  
SIP (Session Initiation Protocol), 7, 57–58  
   call flow, 60–61  
   components, 58–59  
   encryption, 182–193  
   limitations of, 198–199  
   messages  
      filtering, 158  
      malformed, 144  
   modes, 130  
   NAT, 111  
   overview of, 58–67  
   P-DCS headers, 309–313  
   registration  
      with Digest Authentication, 177  
      hijacking, 195  
   security profiles, 67–73  
   session configuration, 61–67  
   URIs, 184  
SIP INVITE message, 23  
SIP OPTION, 220  
SIP Proxy server certificates, 269  
SIP Swiss Army Knife (SIPSAK), 129  
SIPcrack command, 162  
SIPSAK (SIP Swiss Army Knife), 129  
Skinny Call Control Protocol (SCCP), 253  
SLA (Service Level Agreement), 229
sniffing, 154
   analysis, 158–161
   mitigation, 161
   simulation, 154–158
social context, threats against, 38–43
softphones, 117
Softswitch, 118
SPAF (Service Provider Administration Function), 116, 297
spam, 165
   calls, 39
   IM, 167
   mitigation, 168–172
   presence, 41–42
   SPPP, 167–168
   voice, 165–166
Spam over Instant Messaging (SPIM), 40–41
SPam over IP Telephony (SPIT), 39
spoofing, 162
   analysis, 164–165
   messages, 24–30
   mitigation, 165
   simulation, 162–164
SPPP (presence spam), 41–42, 167–168
SRST-enabled gateway certificates, 268
SRTP (Secure RTP), 71, 188–193, 267
   packet processing, 190–191
   testing, 191–193
SSH (Secure Shell), 316
SSI (Service Independent Interception), 292
stacks, protocols, 13
static load balancing, 220
stream analysis, 160
SubBytes() function, 89
SubjectSignal message, 334
superusers, 264
Switch, 278–282
switches, 13
symmetric (private) key cryptography, 84–85
   3DES, 87
   AES, 89–92
   DES, 85–87
symmetric NAT, 110

T
TACACS+, 120
TCP (Transmission Control Protocol), SYN
   attacks, 128
tear down calls, 25
tearing down sessions, 196
telecommunication service providers (TSPs), 292
Telecommunications Industry Associations (TIA), 292
TerminationAttempt message, 334
testing
   malformed messages, 144–150
      analysis, 150–153
      mitigation, 154
   negative testing tools, 129
   sniffing/eavesdropping, 154–158
      analysis, 158–161
      mitigation, 161
   SRTP, 191–193
   Turing tests, 168
TFTP servers, 12
threats
   against availability, 20–30
   against confidentiality, 30–34
   DoS attacks, 128
      intentional flooding, 129–138
      unintentional flooding, 138–143
   against integrity, 34–38
   malformed messages, 143–144
      analysis, 150–153
      mitigation, 154
      simulation, 144–150
   models, 195–198
   sniffing/eavesdropping, 154
      analysis, 158–161
      mitigation, 161
      simulation, 154–158
   against social context, 38–43
   spam, 165
      IM, 167
      mitigation, 168–172
      SPPP, 167–168
      voice, 165–166
spoofing, 162
  analysis, 164–165
  mitigation, 165
  simulation, 162–164
TIA (Telecommunications Industry
  Associations), 292
timers, registration control, 217–220
TLS (Transport Layer Security), 33, 71–73, 253
  limitations, 199
toll fraud, 26
tools
  libSRTP, 191–193
  malformed messages, 144–150
    analysis, 150–153
    mitigation, 154
  negative testing, 129
  SIPSAX, 129
  Wireshark, 156
topologies
  hiding, 208–212
  ToS (type of service), 228
tracking call patterns, 32–33
traffic
  black, 213
  call flooding, 20–22
  firewalls, 249–251
    ASA and PIX, 251–256
    FWSM, 256–258
    limitations, 258–259
  flooding, 132
  flow optimization, 239–244
  gray, 214
  white, 213
transactions
  call hijacking, 26
  MGCP, 74
transcoding, 226–227, 333
transferring calls, 303
transfers, 336
translation
  addresses, 49
  dialed digital, 50
  NAT, 21, 109–113
  numbers, 227–228
transparent mode
  ASA and PIX firewalls, 252
  FWSM firewalls, 256
Transport Layer Security. See TLS
traversal
  media, 241
  NAT, 222–224
Triple DES (3DES), 87
troubleshooting
  borders, 204–206
    between access and core networks, 206–207
    between core and peer networks, 207
  device configuration, 22
  endpoints, 22
  static load balancing, 220
trunking gateways, 74, 328
TSPs (telecommunication service providers), 292
tunneling, 195
Turing tests, 168
type of service (ToS), 228
types
  of firewalls, 249–251
    ASA and PIX, 251–256
    FWSM, 256–258
    limitations, 258–259
  of keys, 189
  of NAT, 110
U
UAC (User Agent Client), 58, 175
UAS (User Agent Server), 58, 175
uBR (Universal Broadband Router), 327
UDP (User Datagram Protocol), 33, 272
unauthorized creation and detection of
  intercepts, 303
Unified CM (Cisco Unified Communications
  Manager), 267
    authentication, 269–273
    configuration, 275–277
    encryption, 273–275
    integrity, 269–273
    node certificates, 268
    security, 267–269
Unified CME (Cisco Unified Communications
  Manager Express), 259
    access control, 259–261
    after-hours call blocking, 266–267
    COR, 264–266
phone registration control, 261–262
secure GUI management, 263–264
Uniform Resource Indicators. See URIs
unintentional flooding, 138–143
SBCs, 206
Universal Broadband Router (uBR), 327
UNIX, resource monitoring, 134
URIs (Uniform Resource Indicators), 184
limitations of, 199
User Agent Client (UAC), 58
User Agent Server (UAS), 58
user control interfaces, 7
User Datagram Protocol (UDP), 33, 274
User-Based Security Model (USM), 326
user-to-proxy authentication, 176–179
user-to-user authentication, 179–182
USM (User-Based Security Model), 326

V

VACM (View-based Access Control Model), 326
valid call request flooding, 129
valid registration flooding, 129
View-based Access Control Model (VACM), 326
virtual LANs. See VLANs
Virtual SBC (VSBC), 237
virtualization, 237–238
VLANs (virtual LANs), 282–284
voice
integration, 12
spam, 39, 165–166

VoIP (Voice over IP)
applications, 12
benefits of, 6–8
disadvantages of, 8–10
firewalls, 108–109
protocol stacks, 13
VSBC (Virtual SBC), 237
vulnerability
components, 12–13
sources of, 10–12

W

web clients/servers, 13
white traffic, 213
Windows, resource monitoring, 135
Wireshark, 156
wiretapping, 14, 114–116
operational issues, 300–304
overview of, 292–293
reference models, 294–297
request/response interfaces, 297–300
requirements for LEAs, 293–294
wrong configuration of devices, 139

Z

zone management, 49