CHAPTER

30

Security Issues in VoIP Telecommunication Networks

Xiaohui Yang, Ram Dantu, Duminda Wijesekera

30.1. INTRODUCTION

The Session Initialization Protocol (SIP) working group is dedicated to the development of SIP, specified as a standard under RFC 3261 and its extensions [1]. SIP communication was developed as an application layer protocol like HTTP to create, modify, and terminate multimedia sessions among endpoints. SIP was originally designed to signal IP-based voice communication (VoIP) but has expanded into the areas of video, file transfer, and instant messaging. SIP protocol provides only the signaling for connections but does not transmit data, in contrast to the Real-time Transport Protocol (RTP) [2], which transmits real-time data between peers. As SIP gains prevalence, it is important to study potential security threats and analyze possible solutions. Several SIP security issues are examined in this chapter, and in addition several solutions and best practices are presented. The chapter also presents a number of vulnerabilities that are not uncommon even in large enterprises. SIP is increasingly being adapted by home users and businesses and with the increase in use comes the increase of the risk of vulnerabilities.

The fundamental issues in VoIP security are unauthorized use and the compromise of the communication medium. The integrity information is compromised if any unauthorized user can view it. There are many possibilities of making the data compromise harmful for users, such as an intruding user can record conversations, modify calls, and steal personal information. This is because of the basic implementation flaws in VoIP networks. Servers, clients, and protocols have weak spots that allow for vulnerabilities. There are several vulnerabilities in VoIP and it is particularly vulnerable to Man-in-the-Middle (MITM) attacks, in which the attacker intercepts call-signaling SIP message traffic and masquerades as the calling party to the called party and/or vice versa. Once the attacker has gained this position, he/she can hijack calls via a redirection server. While the MITM attack hijacks calls between users, Pharming attacks lure the user into giving personal information like passwords and credit card numbers over the phone call. Phishing and Pharming over VoIP are becoming increasingly rampant as VoIP seems to have an architecture conducive to attacks.

In this chapter, we will describe some of the components and functions of a non-peer to peer (P2P)-based VoIP network and the issues involved in providing all the functionality provided by the Public Switched Telephone Network (PSTN) and VoIP phones. We will then discuss

Das Ch30-9780124158153 2011/11/18 10:14 Page 764 #2

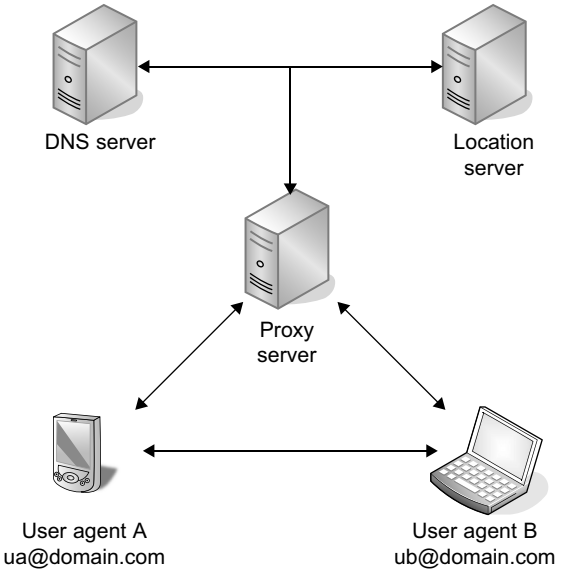


FIGURE 30-1 Main SIP components.

some of the security issues and how these issues are exploited even in commercial VoIP providers with some suggestions for improvement in security. In the later sections, we will illustrate the organization of the small World VoIP (SW-VoIP) with details on the P2PSIP operations, functions, and its improvement in performance over the currently deployed OpenVoIP. Finally, we will summarize the different categories of security issues that are present in VoIP systems and provide an overview of the solutions detailed in the preceding sections.

30.2. CONNECTION ESTABLISHMENT AND CALL ROUTING

This section describes the main components of a SIP network, which work cohesively to form the communication bridge between the end terminals.

30.2.1. SIP Networking Components

A network consists of different logical components that communicate with each other in a predefined way. The major components of the SIP networks demonstrated in Figure 30-1 are as follows:

- **User agents (UAs):** The User agent represents the endpoints of a communication (*i.e.,* SIP Phone). The User agents are logically divided into UA server and UA client, depending on the terminal initiating and responding to the request.
- **Proxy servers:** A Proxy server is present in every SIP Domain. It acts as an intermediate server, receiving connection requests from UAs, or other Proxy servers. The Proxy server communicates with the location server and the redirect server. AQ:11
- **Redirect servers:** A redirect server processes all proxy server requests and performs call rerouting for User agents.
- **Registrar servers:** A registrar server is responsible for registering User agents. It sends the logged information about the UA to the location server for administrative purposes and future requests.
- **Location servers:** A location server maintains the binding of logical addresses to the physical address of the hardware inside a SIP domain.

In most of the currently deployed systems, the registrar servers and the proxy servers are distinguished logically and may reside on the same physical box. SIP authentication is similar to a digest-based HTTP authentication. Whenever SIP requests like REGISTER, INVITE, and BYE are received from a User agent, the SIP server challenges the User agent with an Unauthorized (401) or Proxy-authorization required (407) message. On the arrival of the message, the User agent applies an MD5 hashing algorithm to the SIP message fields (*request-URI*, username, shared *password, SIP server*, realm, and *nonce*) to compute the hash value. The digest value is sent along with the SIP request again to the server to authenticate the requester. Once the requester has been authenticated, a SIP connection is established between the users. Users can now use this communication mechanism to exchange voice data. There are several different call routing scenarios that exist today. Two of the most common cases are discussed below.

Das Ch30-9780124158153 2011/11/18 10:14 Page 765 #3

Connection Between Two Clients Within the Same SIP Domain. Figure 30-2 shows the connection establishment between User agent A and User agent B placed within the same SIP domain. So both ~~the~~ User agents share the same proxy/registrar server.

1. User agent A initiates the connection to the destination B. The connection request reaches the ~~P~~proxy server from A, which contains the logical SIP address to the destination.
2. The proxy server requests the information from the location server for the physical address of the destination.
3. The proxy server resolves the subsequent address into an IP address from the DNS server.
4. The proxy sends a connection request to User agent B using the destination IP address.
5. User agent B responds to the proxy server with a response indicating whether the connection is accepted.
6. User agent A establishes a direct RTP connection with User agent B.

Connection Establishment Between User Agents of Different Domains. Figure 30-3 shows that User agent A initiates a connection to User agent B. The connection request of A reaches the ~~P~~proxy server of its own domain, containing the destination SIP address of User agent B. The proxy server of UA-A identifies the destination address from the domain name contained in the request. When the destination address does not belong to its own domain, ~~P~~proxy server of A queries the DNS server to resolve the IP address of the destination B's proxy server. The sequence of events that occur during the connection establishment are as follows:

1. A's ~~P~~proxy server creates a connection request to B's proxy server.

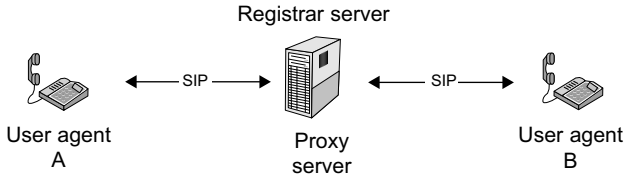


FIGURE 30-2 Connectivity between SIP User agents.

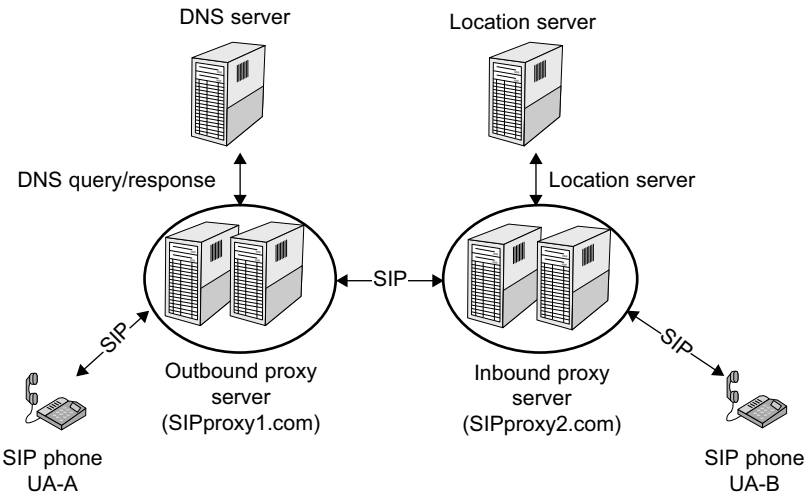


FIGURE 30-3 Details of connection establishment.

Das Ch30-9780124158153 2011/11/18 10:14 Page 766 #4

2. B's Proxy server requests the location server for the SIP address from the connection request.
3. Contacted DNS server resolves the physical address from the location server into IP address.
4. B's proxy server creates a connection with the destination B.
5. User agent B responds to the proxy server, indicating the connection acceptance/rejection, and if accepted, B's Proxy server accepts the connection from User agent A.
6. The connection between the User agent A and its proxy server is accepted.
7. User agent A establishes a direct RTP connection with User agent B.

The SIP specification recommends using TLS and IPSec for authentication, but most deployed systems use only SIP authentication for peer, resulting in many vulnerabilities in the system that make attacks such as eavesdropping, scanning, Denial of Service (DoS), hijacking, man-in-the-middle, session tear down, redirect attacks, RTP attacks, and spam over Internet telephony (SPIT) possible. We will discuss a few important vulnerabilities with examples of real world exploitation in ATT and Vonage SIP phones. The next section describes the Man-in-the-Middle attacks and how they can impact the communication.

30.3. MAN-IN-THE-MIDDLE ATTACKS

VoIP relies on a number of application protocols on the Internet for communication. The openness of the technology over the Internet, and the public's inability to freely connect to the SS & network, makes VoIP open to more attacks than the PSTN. In addition, most currently deployed VoIP systems depend on the DNS to work properly. Therefore, any vulnerability in SIP, RTP, and DNS can compromise the security in communication. In a *Man-in-the-Middle (MITM)* attack, the attacker tampers with SIP signaling, diverts calls, wiretaps the communication path, and even hijacks calls by tempering with the VoIP signaling and/or media traffic, which makes it one of the most serious threats to the security and trust of existing VoIP protocols and systems. This is illustrated in the Figure 30-4.

Vonage VoIP is a prominent U.S. residential VoIP service provider with millions of customers. Zhang et al. [3] launched a MITM attack on their own test-bed to show the exploitations over the current Vonage VoIP system. They produced the MITM attack by launching a DNS spoof attack.

Two different network setups were used to illustrate the exploit. The first setup, illustrated in Figure 30-5, is the SIP phone directly connected to the Internet, with the attacker machine

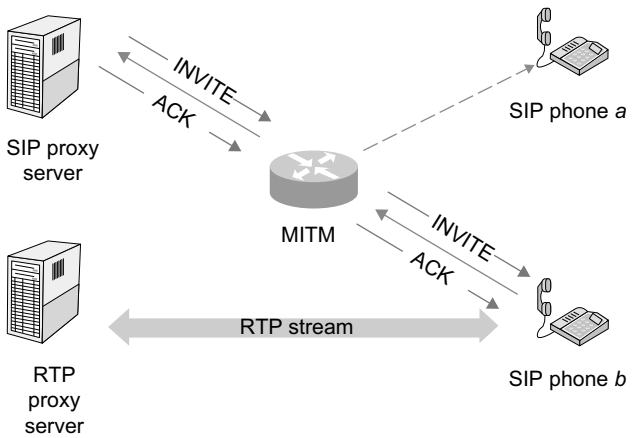


FIGURE 30-4 The first VoIP attack setup [2].

Das Ch30-9780124158153 2011/11/18 10:14 Page 767 #5

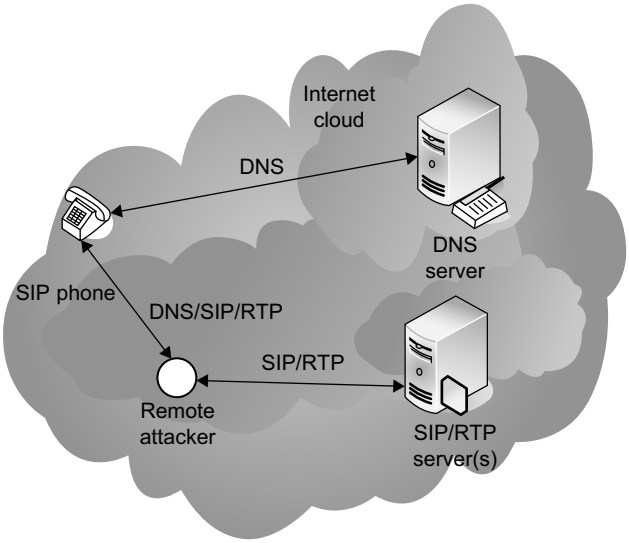


FIGURE 30-5 Attack step 1.

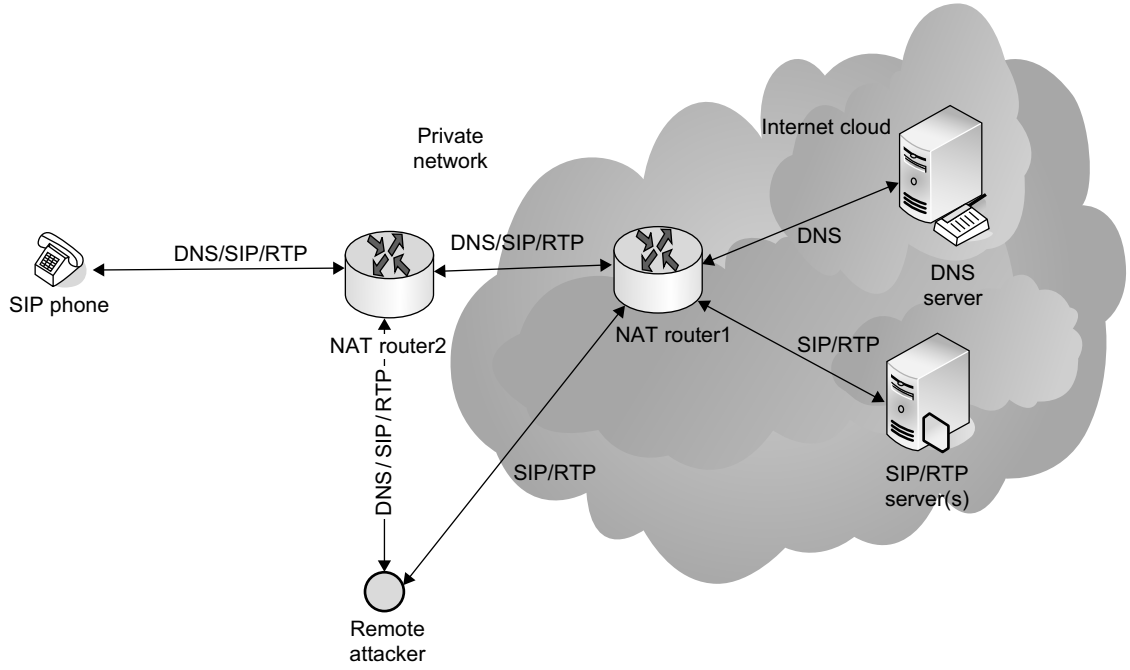


FIGURE 30-6 Attack step 2.

anywhere inside the network. In this network, the attacker uses a wiretap device to capture live traffic to/from the SIP phone. In the second network setup, demonstrated in Figure 30-6, the SIP phone is behind two NAT routers, whereas in most popular existing networks, the SIP phone

Das Ch30-9780124158153 2011/11/18 10:14 Page 768 #6

is behind only one NAT router. The Vonage SIP phone sends "destination unreachable" ICMP packets to the Vonage DNS server when receiving spoofed DNS responses with unmatched port numbers from the attackers. ~~Zhang et al.~~ [3] use the NAT router2 to block this ICMP traffic from reaching the actual Vonage DNS server.

30.3.1. DNS Spoofing on Vonage

Figure 30-7 shows the flow of messages involved in the DNS spoof attack in a Vonage system.

1. Initially, a misinformed INVITE message is sent to the SIP phone by the remote attacker.
2. The phone crashes and reboots on sending a trying message to the actual SIP server.
3. After some time, SIP sends a DNS query to the Vonage DNS server for the SIP server's address.
4. If the remote attacker sends a spoofed DNS response to the Vonage phone, it will receive the spoofed DNS response before the real DNS response from the legitimate Vonage DNS.
5. The attacker doesn't have the actual DNS message from the phone, so he/she has to try 1100 possible port numbers in the spoofed DNS response, before the legitimate response arrives.
6. If the spoofed DNS port number is wrong, the SIP phone will send a port unreachable ICMP packet to the attacker.
7. If the attacker finds the match with the actual DNS port number, the Vonage phone accepts the spoofed DNS response and sends a REGISTER message to the attacker machine perceiving it as the actual Vonage server.
8. If the remote attacker does not receive the REGISTER message from the target within the predefined time period, the Vonage phone accepts the authentic DNS response from the actual Vonage server.

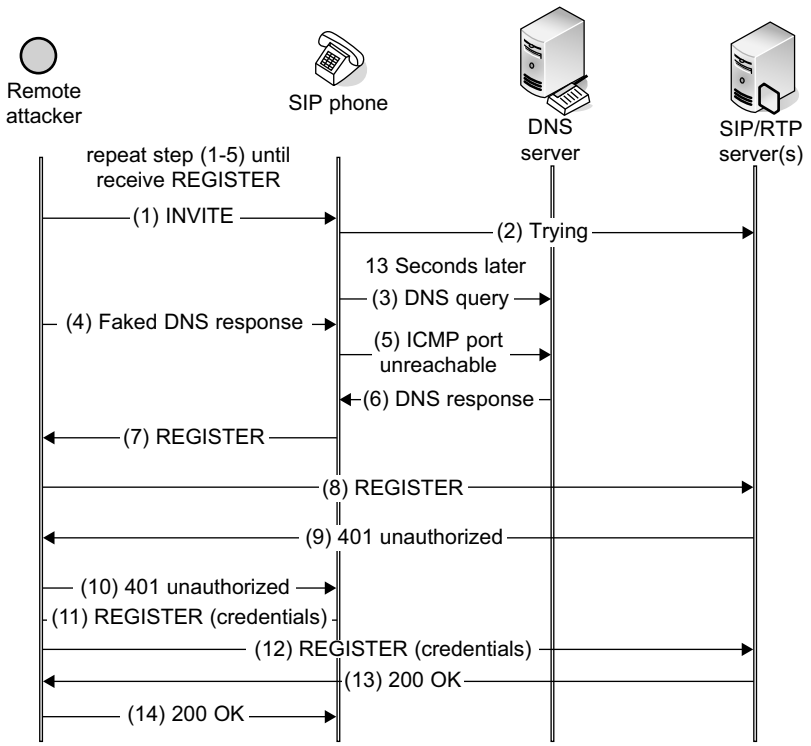


FIGURE 30-7 Message flow in DNS spoofing.

Das Ch30-9780124158153 2011/11/18 10:14 Page 769 #7

9. The process continues again, from sending the misinformed INVITE message, until the phone registers with the attacker machine.
10. Meanwhile, the remote attacker forwards messages to the Vonage server from the SIP phone acting as the man-in-the-middle.

30.3.2. Exploiting Vulnerabilities

By exploiting the SIP vulnerability, a remote man-in-the-middle can do the following:

- Divert calls to any place on the Internet allowing attackers to wiretap calls.
- Redirect a VoIP call to a third party without authorization.
- Launch billing attacks on VoIP users.
- Interrupt calls by sending BUSY and BYE.

30.3.3. Wiretapping Incoming Calls

As illustrated in Figure 30-8, the remote attacker changes the IP address and port number of the incoming RTP stream, when the SIP server sends an INVITE message. The remote attacker sends a modified INVITE message with the attacker's IP address and port number to the SIP phone and forwards the RINGING and TRYING message from the SIP phone to the SIP server. When the three-way handshake is complete, the remote attacker will be able to wiretap RTP streams between the SIP phone and the RTP server as MITM.

30.3.4. Wiretapping Outgoing Calls

As Figure 30-9 shows, when a remote attacker receives the SIP INVITE message, he/she modifies the IP address and port number for the upcoming RTP stream and forwards to the SIP server. The attacker then forwards INVITE messages and authentication messages with modified destination addresses. Once a TRYING message is forwarded from the server to the SIP phone, the remote attacker modifies the OK message by changing the RTP termination information and sends it back to the SIP phone and modifies the response ACK from the SIP phone which is sent back to the SIP server. Thus, the remote attacker wiretaps RTP streams between the SIP phone and the RTP server.

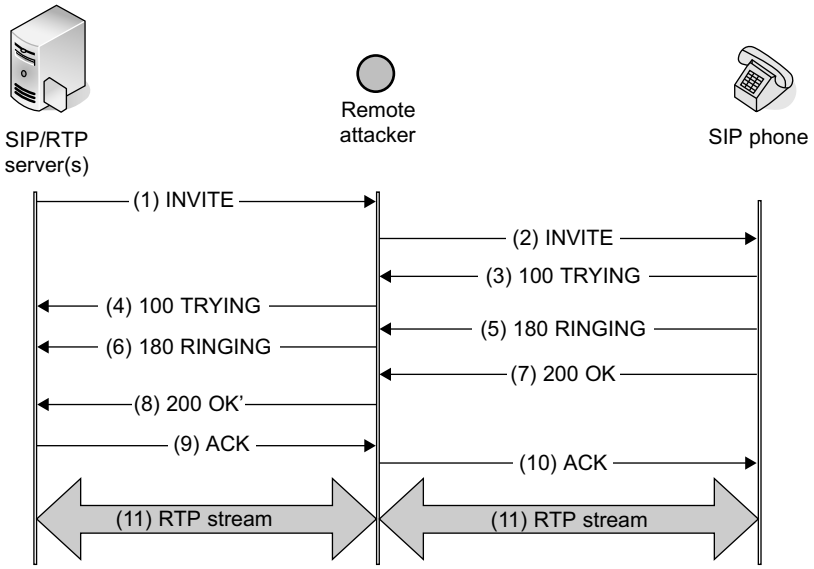
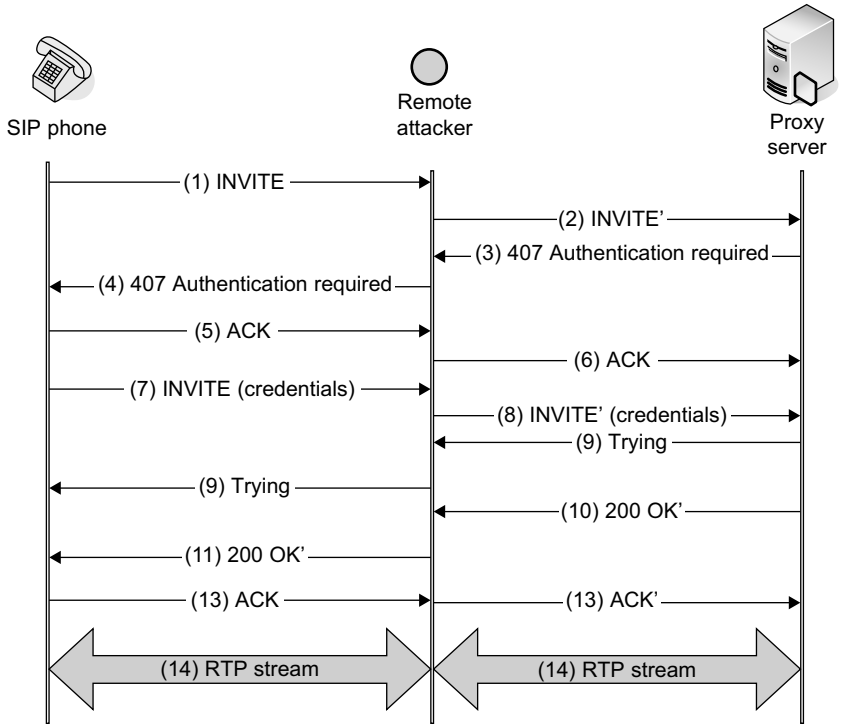


FIGURE 30-8 Wiretapping.

Das Ch30-9780124158153 2011/11/18 10:14 Page 770 #8



AQ:9 **FIGURE 30-9**

30.3.5. Recommendations

- The SIP messages and RTP streams can be protected by the use of SSL/TLS and SRTP.
- VoIP phones must undergo in-depth Fuzz testing in order to resist some of the attacks and vulnerabilities.
- There is a need for the development of a lightweight VoIP intrusion detection system, which can be deployed on the phone.

In the context of MITM, the attacker can hijack calls and transparently listen to conversations between the terminals. This attack is potentially dangerous, since it leads to unlawful interception of calls between parties which may involve confidential information exchange between the parties. Voice pharming is another attack like web phishing, where the attacker impersonates the legitimate caller and retrieves useful information. In the next section, we will discuss how voice calls are lured to give away vital information.

30.4. VOICE PHARMING

VoIP carries voice calls over the public Internet rather than PSTN. One of the requirements of this VoIP protocol is that it must be trustworthy and reliable. However, some experiments show that it is vulnerable to various attacks like phishing, pharming, etc. Voice phishing lures people into dialing malicious phone numbers (given by a malicious e-mail or phone call) and tries to make users reveal sensitive information. Pharming is similar to phishing in which hackers reroute browsers to an identical malicious site to steal the identity and commit fraud. It directs victims to malicious representatives even when they have dialed correct phone numbers. Hence, to minimize such threats to current VoIP users, all segments along the VoIP path need to be protected. We will discuss the vulnerability of voice pharming present in the commercial VoIP service providers like AT&T and Vonage.

Das Ch30-9780124158153 2011/11/18 10:14 Page 771 #9

30.4.1. VoIP Call Detour

A call detour is the process of transparently diverting RTP voice streams of any call to a remote machine (attacker) on the Internet [3], as shown in Figure 30-10. A VoIP call detour is considered in four scenarios: (1) a PSTN phone calls an AT&T SIP phone; (2) an AT&T SIP phone calls a PSTN phone; (3) a PSTN phone calls a Vonage SIP phone; and (4) a Vonage SIP phone calls a PSTN phone. It is assumed that there is a MITM between the SIP phone and the SIP server who is also connected with a remote server.

The detour attack is performed between an AT&T SIP phone and a PSTN phone to demonstrate the vulnerability of VoIP calling.

1. The MITM attacker intercepts the INVITE message from either the SIP phone or the SIP server and sends a copy to the remote device with the stolen IP address and port number.
2. The MITM attacker modifies the SDP part of the INVITE message with the IP address and port number of a remote device. Then, he/she sends this modified message to the original destination.

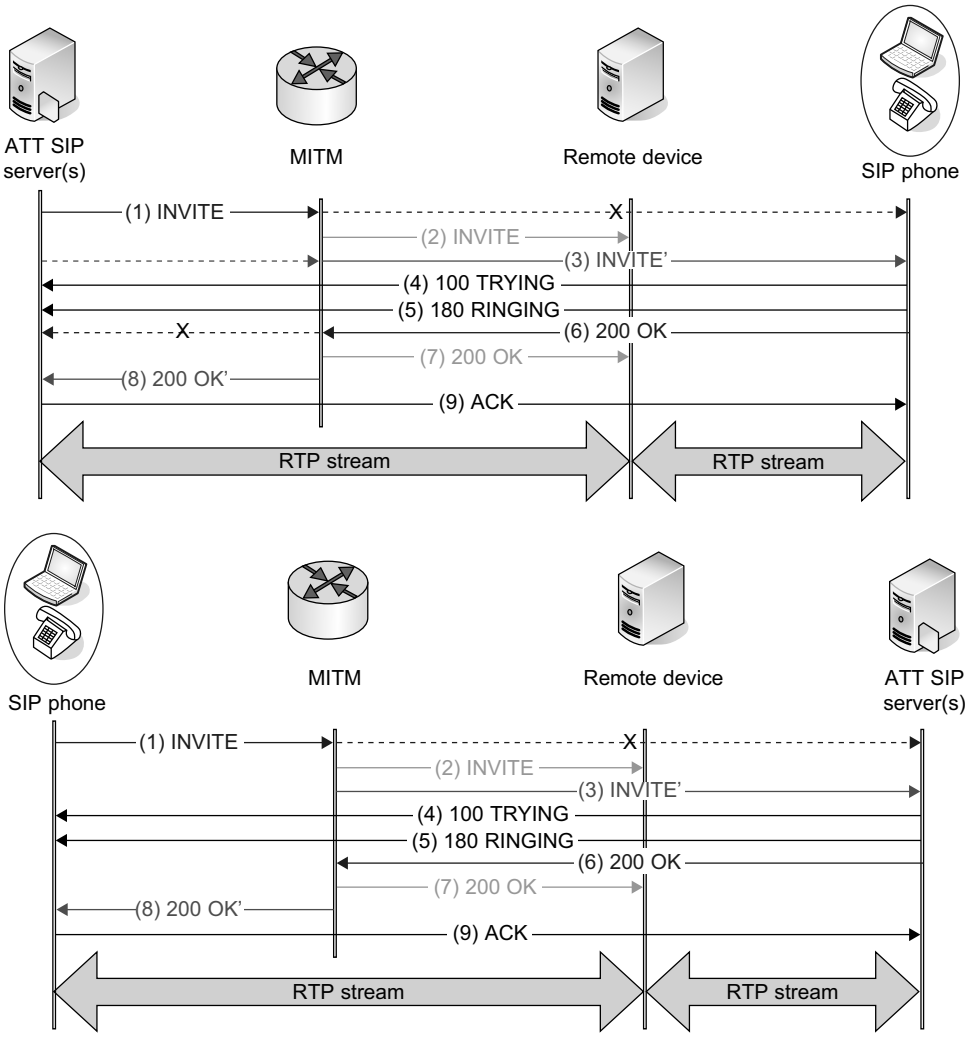


FIGURE 30-10 Voice pharming.

Das Ch30-9780124158153 2011/11/18 10:14 Page 772 #10

3. The MITM attacker will not intercept any 100 TRYING or 180 RINGING message.
4. When the callee accepts the call and the MITM intercepts it, a copy is sent to the remote device to inform it about the IP address and port number of the upcoming RTP stream.
5. The MITM attacker changes the IP address and port number in the SDP and sends the modified 200 OK message to the original destination.
6. This makes both caller and callee to send their information to the remote server.

This attack does not work inside the Vonage SIP phone network. The Vonage server checks the RTP stream's IP address in the received INVITE or 200 OK messages and will not send any RTP stream if it is different from the registered IP address of the SIP phone. Hence, Vonage's SIP-based VoIP is robust against detour attacks.

A slight modification is made to the detour attack where the MITM attacker does not modify the message; instead, the remote device modifies the RTP port number. This causes the Vonage SIP server to send its RTP stream to the remote device and, hence, is vulnerable to detour attacks.

30.4.2. Redirection of VoIP calls

The caller who is identified by request URI sends an INVITE message to the callee to initiate a call. These INVITE messages from the SIP proxy to the SIP phone are not authenticated. Hence, MITM can change the request URI-field and redirect the call.

30.4.3. Hijacking a Call Forwarding Setup

Call forwarding is a feature that allows the telephone subscribers to forward an incoming call. The caller will input the phone number to which the incoming calls have to be forwarded. The input number is transferred via RTP event packets to the Vonage RTP server which acknowledges the call forwarding number.

Assume the MITM attacker is in between the SIP phone and Vonage RTP server, as illustrated in Figure 30-11. The attacker can now modify the call forwarding number. Once the caller inputs the call forwarding number, the SIP phone will send the number to the Vonage RTP server. The MITM attacker can intercept the RTP packets and send the modified number to the RTP server.

30.4.4. Voice Pharming Attacks

To analyze the mode of execution of a VoIP voice pharming attack, we will discuss with a small example considering Citibank as demonstrated in Figure 30-12 [3]. Citibank provides a phone banking service, which allows its customers to have checks issued and paid to anyone by calling Citibank. The customers will be asked to enter their SSN or personal taxpayer identification number and telephone access code to provide service options. The caller will be authenticated by being asked questions and once they are authenticated they can issue checks. To launch a voice pharming attack, the attacker needs to (1) set up a bogus Interactive Voice Response (IVR) that sounds like the authentic IVR system, (2) redirect the calls toward Citibank phone banking to the malicious IVR, and/or a phone the attacker uses. Assume the MITM is in a place (e.g., gateway, wireless router, and firewall) and checks if there are any calls to financial institutions. By using a call redirection attack, the attacker can divert the call to his malicious IVR. Then, it starts asking questions which the caller will answer since they have dialed the correct phone number. Thus, the attacker will get the all the necessary information he/she wants.

30.4.5. Strategies to Avoid Voice Pharming Attacks

The cause for all these attacks is the lack of security of SIP messages and RTP traffic between VoIP servers and SIP phones. However, security can be achieved by encrypting and authenticating the fields of SIP messages and RTP traffic. Protecting the integrity and authenticity is not

Das Ch30-9780124158153 2011/11/18 10:14 Page 773 #11

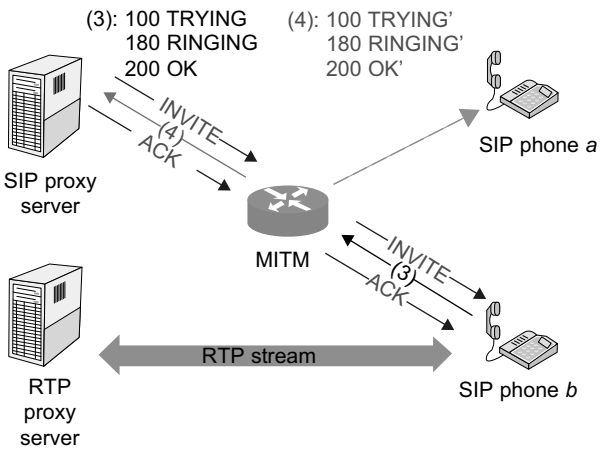


FIGURE 30-11 Call redirection.

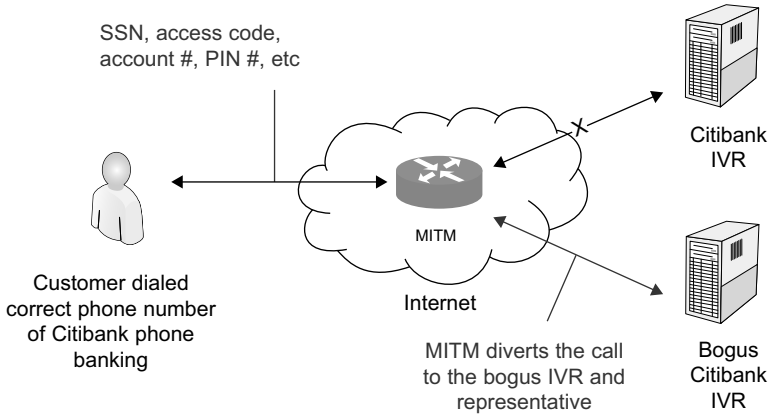


FIGURE 30-12 Voice pharming.

trivial because during the routing process, fields such as request-URI etc. need to be known at all intermediate SIP proxies. The proxy may even need to change the URI. Hence, end-to-end protection of a SIP message is not possible. Therefore, the integrity and authenticity of SIP messages have to be protected hop-by-hop (SSL or TLS) by providing hop-by-hop encryption between the VoIP phones and next hop VoIP servers. Unless both the communication parties are authenticated, the hop-by-hop encryption or authentication may still be vulnerable to the MITM attack. Public key infrastructure (PKI) can be used to provide such authentications.

Attackers stealing information such as credit card and social security number details with malicious information over the telephone calls will degrade the trust placed in a VoIP communication system. People are using VoIP service for daily phone use; the presence of these vulnerabilities will make the user reluctant to give information over the phone. User billing is an important service in a VoIP communication; the services offered need to be charged for their usage. VoIP opens doors for a special type of attack which could increase the telephone bill for the user. These are the billing attacks which are discussed in the next section.

Das Ch30-9780124158153 2011/11/18 10:14 Page 774 #12

30.5. BILLING ATTACKS

Billing is one of the important services in telecommunication and has direct relevance to almost every user. In VoIP, the two most important requirements are reliability and trustworthiness. The present VoIP billing services are based on VoIP signaling; hence, any attack on the VoIP is a potential threat to the billing service. Our experiments show the vulnerabilities between AT&T and Vonage SIP phones [4].

30.5.1. Billing Attacks on SIP

Existing commercial VoIP services have either a limited or an unlimited call time. Call rates depend on the country to which they are made and most plans include free calls within a geographic area. In these cases, the remote attacker can prolong the calls or create unauthorized sessions so that the VoIP subscriber will be paying more for the service when it is not required. The Man-in-the-Middle (MITM) attack plays an important role in the billing attacks. There are four kinds of billing attacks that can be performed on a VoIP subscriber between AT&T and Vonage SIP.

30.5.2. Invite Replay Billing Attack

An invite replay attack results in unauthorized calls by replaying INVITE messages to a different destination. This vulnerability is an effect of the SIP implementation error of anti-replay functionality. This exploitation cannot be stopped even with the SIP authentication of INVITE messages.

In Figure 30-13, the MITM in-between the AT&T SIP UA and AT&T SIP server can intercept all the messages going between them. The remote attacker can send the INVITE message to the proxy server, who can make unauthorized calls with a modified INVITE message from the AT&T phone.

1. The attacker intercepts all the communication between the AT&T SIP phone and AT&T server.
2. The AT&T phone sends INVITE messages to the AT&T server with all the subscriber credentials.
3. The server requests for authentication in the response message.
4. The phone authenticates the INVITE message to the proxy on request.
5. The remote attacker intercepts this INVITE message with the authentication credentials.
6. The remote attacker can modify the Session Description (SDP) and is able to establish a session between the remote attacker and the SIP server.
7. Now the MITM can speak to anyone and listen to voice messages of the legitimate subscriber.

The experiment illustrated in Figure 30-14 shows that the intercepted INVITE messages can be replayed successfully after 1 week of the INVITE message being intercepted. Thus, this attack can be launched on the subscriber anytime. Also, the results show that the Vonage SIP is immune to such kinds of replay attacks and the Vonage SIP server has implemented anti-replay correctly.

The steps below show the general message flow between the clients with remote attackers in the network setup for demonstration of fake busy, bye delay, and bye drop billing attacks as illustrated in Figures 30-15 to 30-18. The call is made from the Vonage SIP phone to the AT&T SIP phone. These steps demonstrate the message flow during Fake Busy Billing attacks, Bye Delay Billing attacks, and Bye Drop Billing attacks.

1. The Vonage SIP phone sends an INVITE message to the Vonage SIP server and authenticates the INVITE message.
2. The MITM1 intercepts the INVITE message from the Vonage SIP phone and modifies its SDP to the attacker's IP address and port number.
3. The MITM1 sends the modified SIP INVITE message to the Vonage server. The Vonage server informs the AT&T server the Vonage phone is trying to connect to the AT&T SIP phone.

Das Ch30-9780124158153 2011/11/18 10:14 Page 775 #13

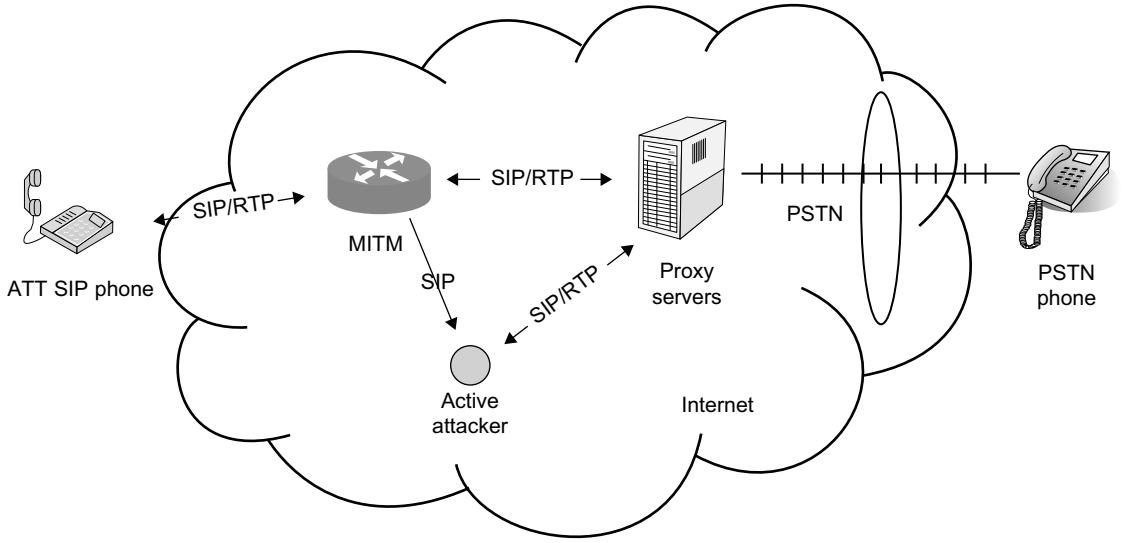


FIGURE 30-13 Invite replay billing attacks.

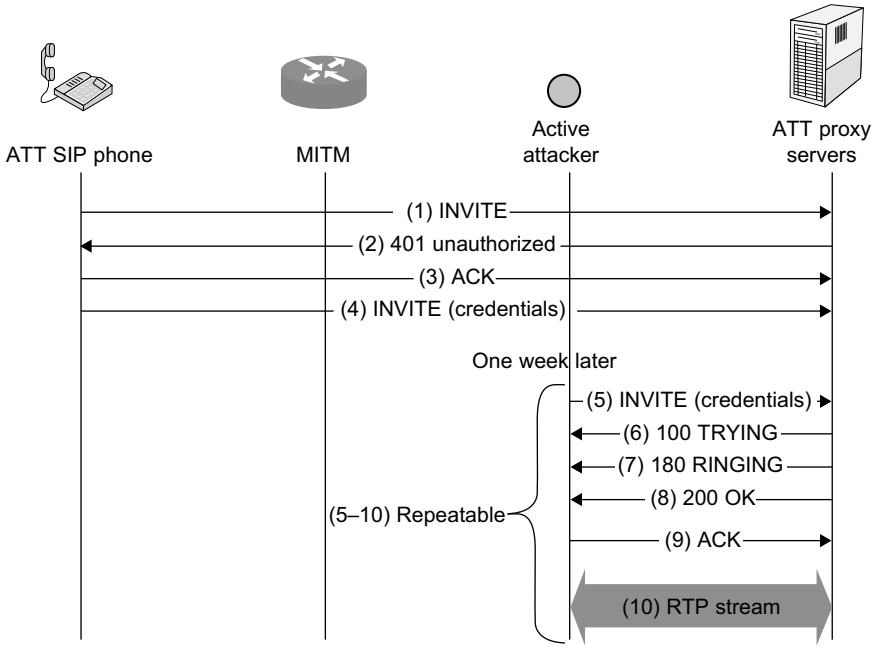


FIGURE 30-14 Details of a billing attack.

Das Ch30-9780124158153 2011/11/18 10:14 Page 776 #14

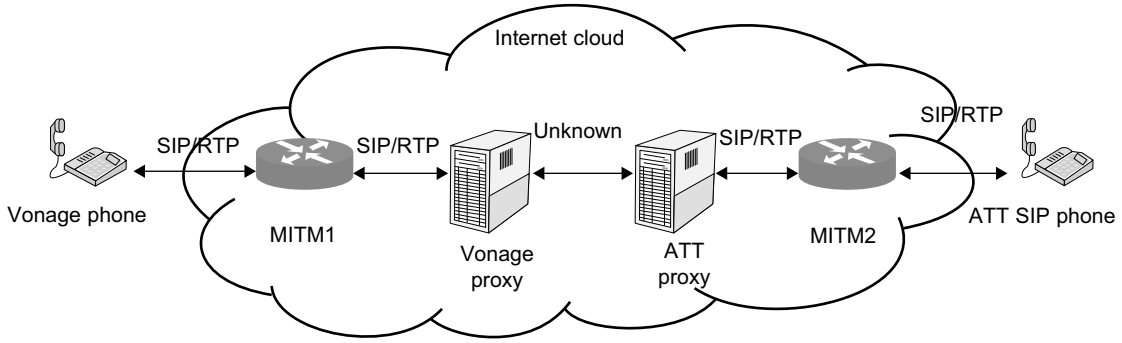


FIGURE 30-15 A billing attack.

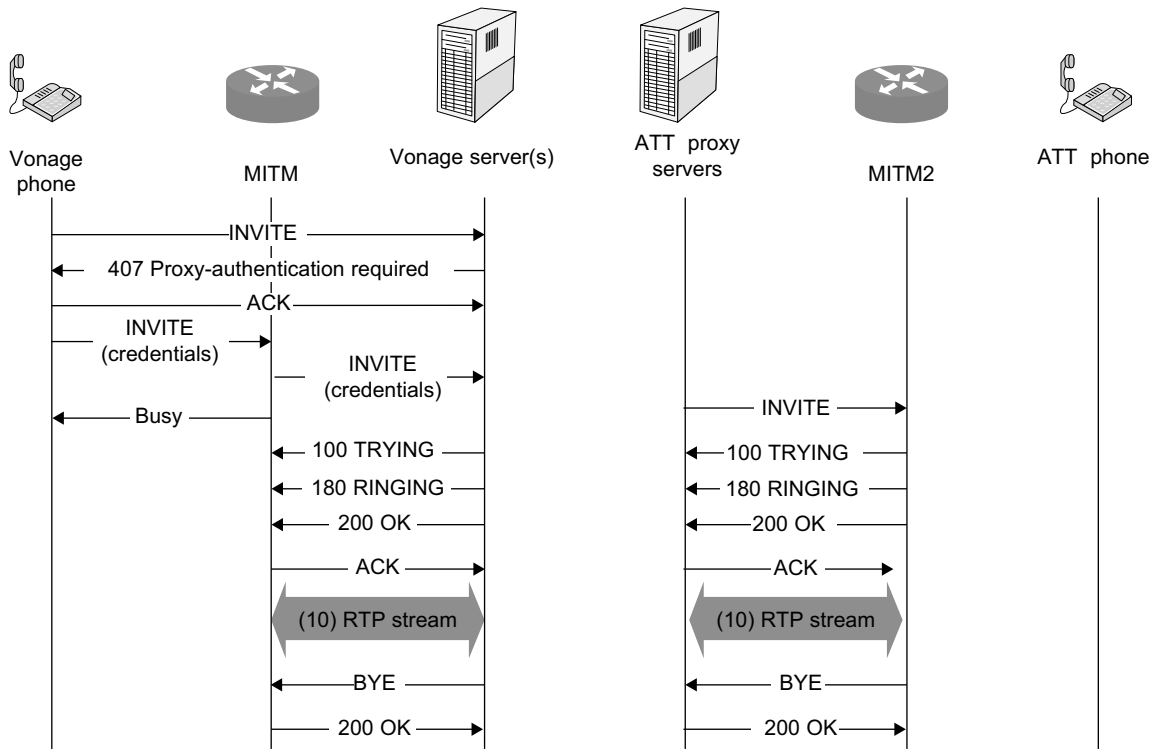


FIGURE 30-16 Fake busy billing attack.

4. Meanwhile, the MITM1 sends BUSY message to the Vonage SIP phone.
5. The AT&T server sends an INVITE message to the AT&T SIP phone.
6. MITM2 intercepts the INVITE message and sends TRYING, RINGING messages to the AT&T server.
7. MITM2 modifies the SDP in the INVITE message to its own IP address and port in the Acknowledgment message (OK).
8. The Vonage SIP server sends TRYING, RINGING, and OK messages to the MITM1.
9. Now the SIP servers send ACK to their respective MITMs.

Das Ch30-9780124158153 2011/11/18 10:14 Page 777 #15

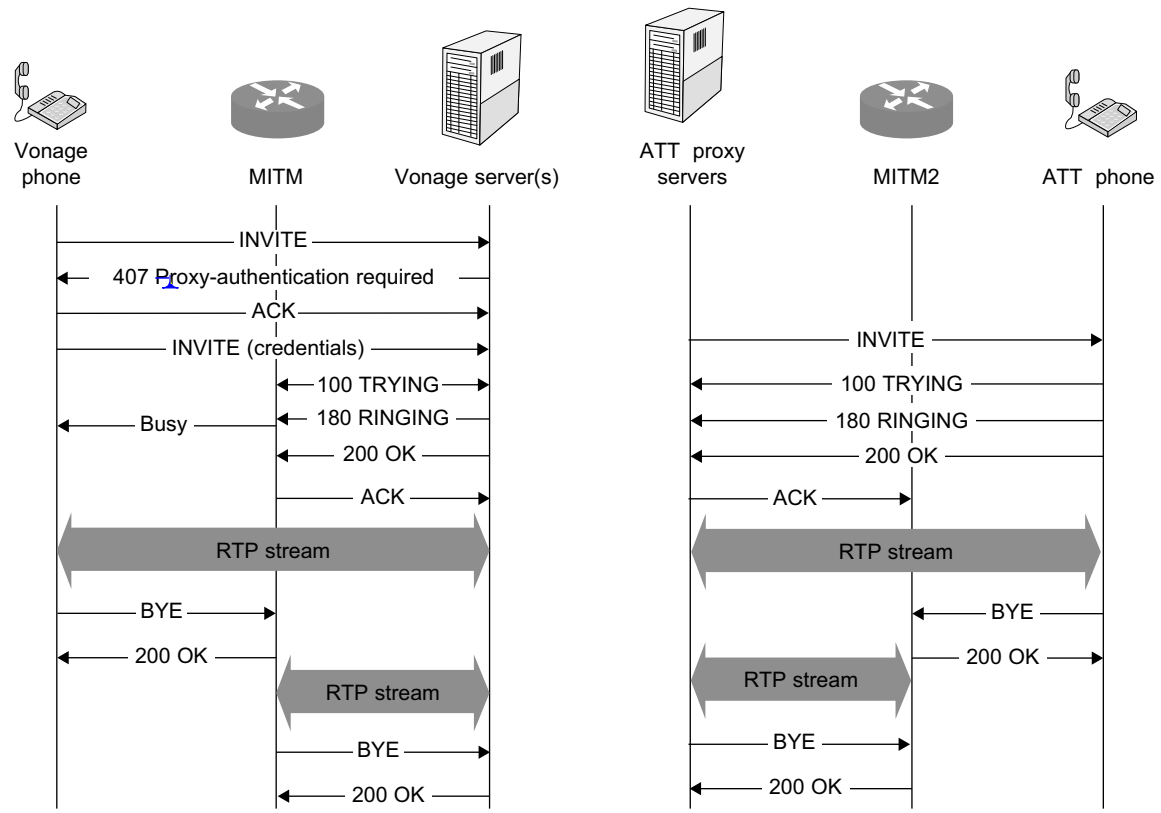


FIGURE 30-17 Bye delay billing attack.

30.5.3. Fake Busy Billing Attack

The fake busy billing attack potentially exploits the VoIP calls and controls the call duration resulting in call termination for which the subscriber has to pay.

Figure 30-16 below shows that the network consists of two MITMs; one MITM is placed between the Vonage SIP phone and the Vonage SIP server, and the other MITM is placed between the AT&T SIP phone and the AT&T server at the other end. The experiment described in Ref. [4] established a session between MITM1 and MITM2 for 34 min before letting the conversation end. The Vonage phone's call activity showed a 34-min call being made to the AT&T phone, while the caller thinks that the attempted call failed and the callee doesn't even know he/she was called.

30.5.4. Bye Delay Billing Attack

The bye delay billing attack deliberately extends the call duration by delaying the BYE messages. In this attack, when the caller or callee hangs up by sending a BYE message, the MITM intercepts the BYE message and sends back a 200 OK message. This gives the caller or callee the impression that the call has been terminated. The MITM1 and MITM2 generate a bogus call between them generating a bogus RTP stream and maintaining the connection alive.

The experiment in Ref. [4] created a hypothetical call for 19 min between the MITMs and the call activity in the Vonage SIP showed prolonged call time; thus, this attack can increase the charges for calls made by VoIP subscribers.

Das Ch30-9780124158153 2011/11/18 10:14 Page 778 #16

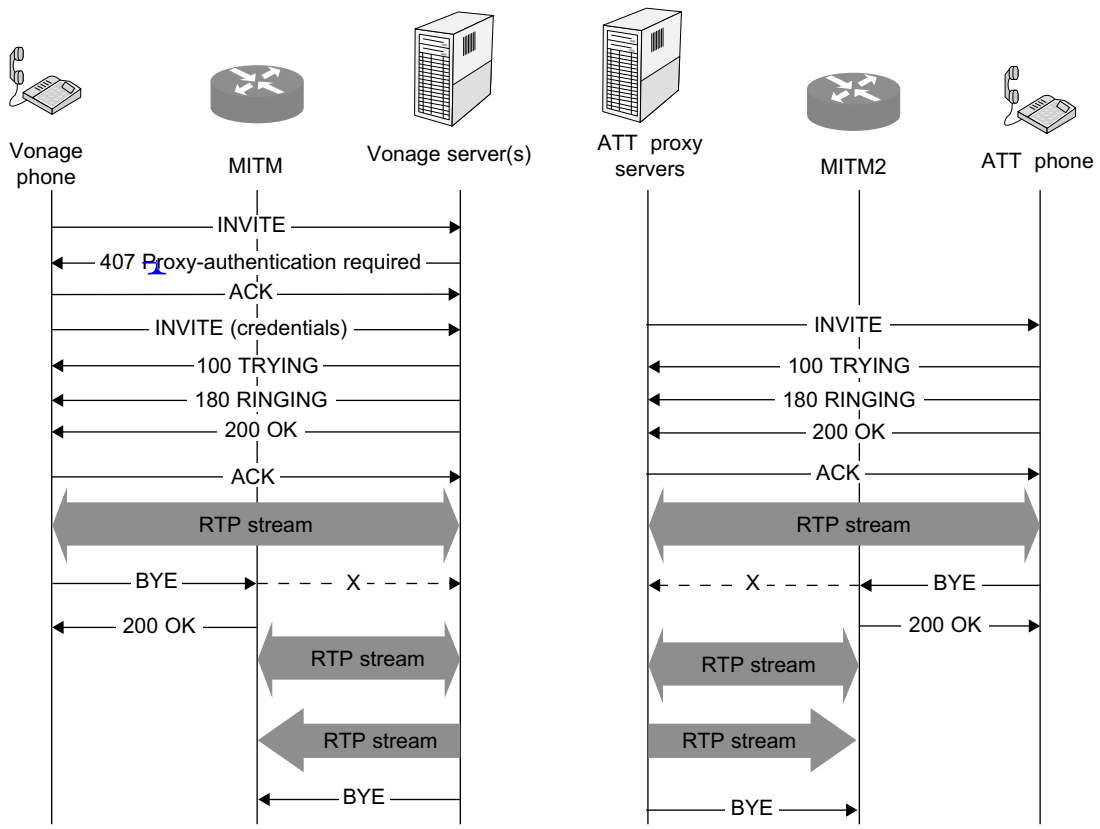


FIGURE 30-18 Bye drop billing attack.

30.5.5. Bye Drop Billing Attack

BYE drop billing attacks prolong calls by simply dropping the BYE message from the caller or callee. In the experiment, the call lasted for 2 min and the MITMs intercepted the BYE messages from the SIP phone and replied with a 200 OK message, creating a bogus RTP stream between the MITMs. With the attack, the call lasted about 218 min before the servers sent a BYE message to terminate the call. The call activity in the Vonage SIP showed 240 min of billable call time though the actual call lasted for merely 2 min.

With the billing attacks on the mobile phone helping the service provider to gain money for unused calls, it also presents inconvenience to the user with call teardowns during a conversation. These vulnerabilities in the system make it unreliable and insecure. P2PSIP is an alternative to the traditional server-based system and expected to avoid these vulnerabilities from the server-based service. Eventually, P2PSIP is still vulnerable to the common attacks because of the underlying SIP signaling. In the next section, we will go through some of the potential vulnerabilities in the P2PSIP telecommunication and the recommendation/solutions to control the exploits during communication.

30.6. SECURITY REQUIREMENTS OF A P2P TELECOMMUNICATION NETWORK

There are a number of commercial P2P-based VoIP systems that have been developed. Among

Das Ch30-9780124158153 2011/11/18 10:14 Page 779 #17

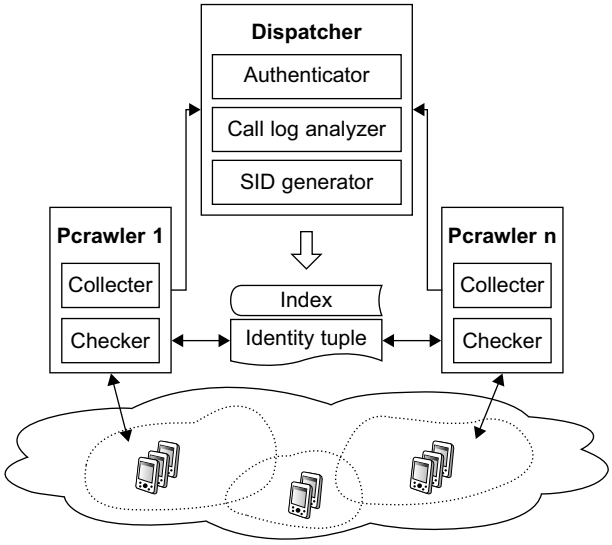


FIGURE 30-19 The PCrawler in action.

them, the most popular P2P-based VoIP application, Skype, [35] uses proprietary protocols to communicate between super nodes and ordinary nodes [3]. Super nodes form the P2P network. Ordinary nodes will be promoted to super node status when they have sufficient bandwidth and a host of other factors. But the P2PSIP protocol used by Skype is proprietary and the new feature is hard to add on. Also, the existence of a central server violates the intention of the P2P network. Hence, an open SIP-based P2P VoIP network is needed.

In a P2PSIP system, [24] distributed hash tables (DHTs) are used to identify peers and store resources preferred for the P2PSIP overlay design. It uses DHT routing algorithms such as CAN [5] and Chord [6]. P2P-over-SIP proposes to use SIP as a transport layer protocol with all P2P messages tunneled over SIP messages in creating the P2PSIP architecture [22]. To enhance the interoperability between P2PSIP and non-P2PSIP networks, DHT and SIP functionality are separated in other applications [23]. The Resource Location and Discovery (RELOAD) base protocol provides clients an abstract storage and messaging service between a set of cooperating peers in the overlay network. It supports P2PSIP networking and functions and also provides lightweight load on participating peers which ensures high performance in system routing.

30.6.1. Security

Security solutions in server-based VoIP systems are hard to be made due to P2P's distributed admission and call control. Peer admission control, call flow, and resources storage may provide unauthorized users or nodes to launch attacks by initiating, modifying, terminating, or eavesdropping on calls. To counter these threats, Skype has its own security mechanism that deploys a central server for the user authentication and encrypts the media stream. But due to the proprietary protocol and the possible poor implementation, [21] it may also be possible for a hacker to fake a valid authentication, using buffer overflow to crash the system. Also, the speech over Skype system may also be dropped or garbled [36].

Seedorf [7] proposed mitigating solutions of these threats in which use of only IP addresses for node-ID generation, iterative routing, and self-certifying SIP-URIs are recommended for the secure node-ID assignment, secure routing table maintenance, and secure message forwarding.

Das Ch30-9780124158153 2011/11/18 10:14 Page 780 #18

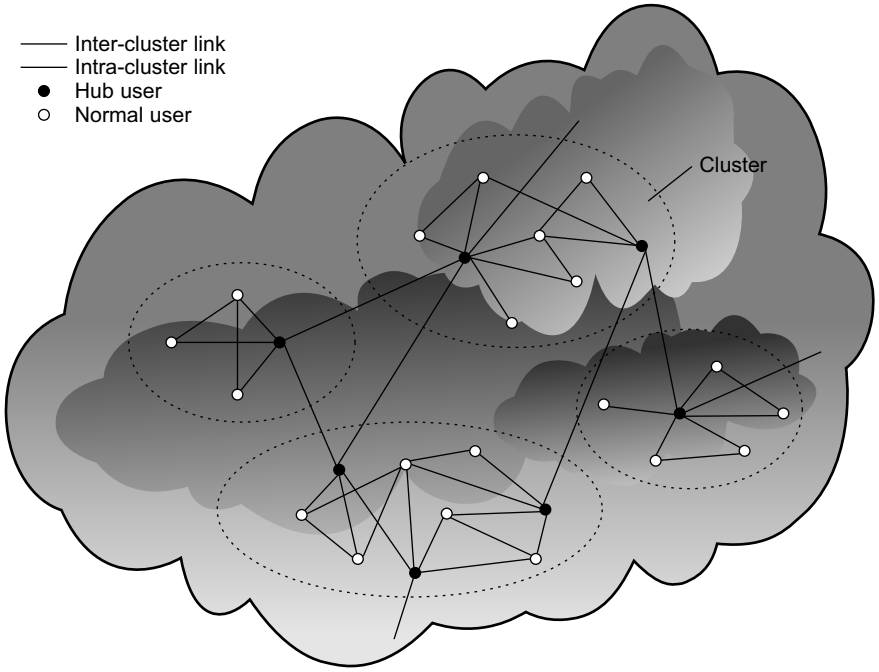


FIGURE 30-20 Routing in a small world VoIP system.

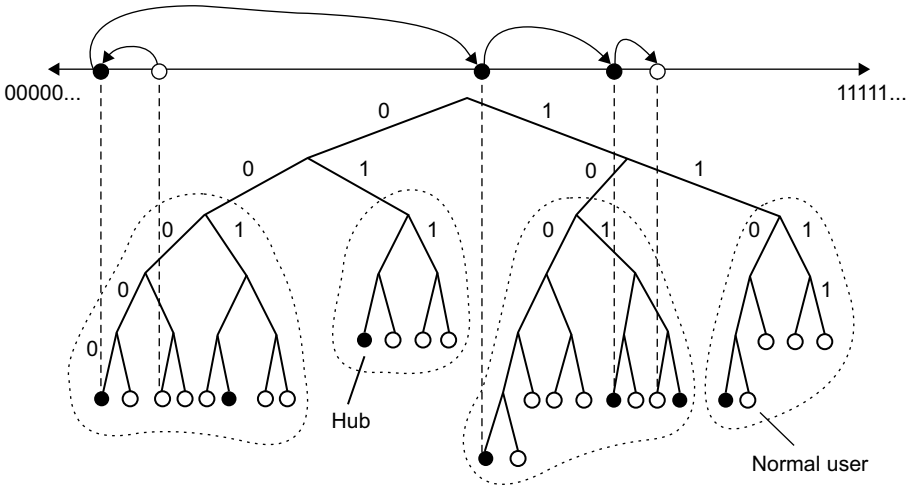


FIGURE 30-21 Closeness-based routing.

Bryan et al. [8] proposed using TLS and public key certificates to ensure secure routing and NAT traversal in a P2PSIP network. They proposed a centralized certificate server for the initial enrollment only and iterative routing to reduce DoS attacks. Reload [8] defines a security model based on a certificate enrollment service in which each node on P2PSIP has one or more public key certificates. These certificates allow peers to verify the origin and correctness of a message.

Das Ch30-9780124158153 2011/11/18 10:14 Page 781 #19

Algorithm 2: Join and Leave

```
1  OnJoin()
2  Join exiting P2P VoIP network;
3  if (Num_of_Recommenders ≥ n_r) then
4      Acquire small world identity SID and CID;
5      for (i = 1; i ≤ Number_of_Friends; i++) do
6          Retrieve SID_i and CID_i from u_i;
7          Calculate popularity p_i of u_i;
8          Elect a hub user h with highest p;
9      end
10     S Flag = 1;
11 else
12     S Flag = 0;
13 end
14 OnLeave()
15 if (SFlag = 1) then
16     if (u_a.hub = 1) then
17         for (i = 1; i ≤ Number_of_Friends; i ++)
           do
18             Inform u_i its leave;
19             Ask u_i to cache its information and elect
               a new hub with the next highest p;
20             Set Timer(t_i) to u_i;
21             Close connection
22         end
23     else
24         Inform all the connected friends its leave
           and close connection;
25     end
26 else
27     Leave existing P2P VoIP network;
28 end
```

FIGURE 30-22 Joining and leaving algorithms.

Song et al. [9] provided a summary of security threats like replay attacks, message manipulation, cryptographic attacks, man-in-the-middle attack, inappropriate usage, Denial of Service, etc. The authors also analyzed the security risks in each layer of P2PSIP architecture, and the security relationship among these layers. Birkos et al. [10] proposed a mechanism that uses symmetric/asymmetric cryptography and a key refresh mechanism to protect the signaling exchange in P2PSIP overlays.

30.6.2. Vulnerabilities in Application Services

Some security vulnerabilities of applications include social misuses (e.g., Spam over Internet Telephony, a.k.a. SPIT), social services (e.g., emergency service and lawful interception), phone services (e.g., billing and voicemail), real-time, and media communication. SPIT is defined as a set of bulk unsolicited voice calls sent to multiple

Das Ch30-9780124158153 2011/11/18 10:14 Page 782 #20

Algorithm 3: Congestion avoidance

```
1  OnReceive()
2  if (n_c < NC_max) then
3  |   FConn = 0;
4  |   Enqueue the task of TCP connection;
5  |   n_c ++;
6  else
7  |   FConn = 1;
8  end
9  OnSend()
10 if (FConn = 0) then
11 |  Generate TCP connection request;
12 else
13 |  for (i = 1; i ≤ Numb_of_friends; i++) do
14 |  |  Find the next hub h with highest popularity
   |  |  p;
14 |  end
16 |  Repeat OnSend to h;
17 end
```

FIGURE 30-23 Congestion avoidance algorithm.

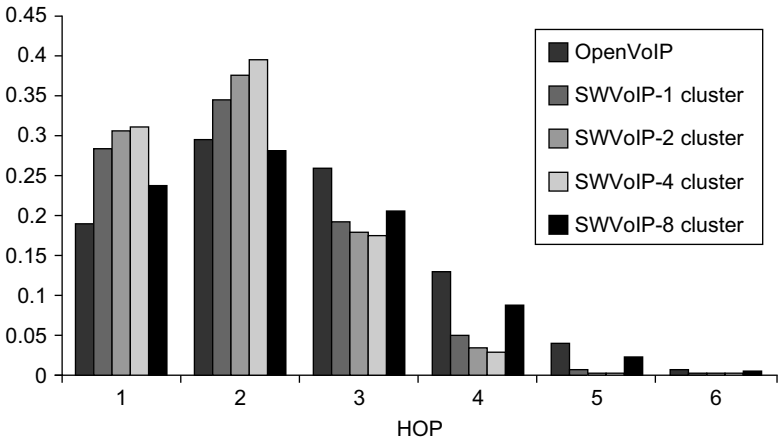


FIGURE 30-24

receivers. Some anti-solutions proposed for centralized server-based VoIP networks include list-based filtering (black and white list), rule-based filtering (score and reputation rating), source authentication (challenge-response), user feedback, Bayesian distribution filtering, etc. But due to the distributed nature of P2PSIP systems, they suffer from lack of trust, identity theft, and privacy violations [11–14].

Providing a secure emergency service on a P2PSIP-based VoIP network is even harder. Due to the distributed nature of the P2P, prioritizing emergency signaling in P2PSIP overlays and finding users' physical location are the major

Das Ch30-9780124158153 2011/11/18 10:14 Page 783 #21

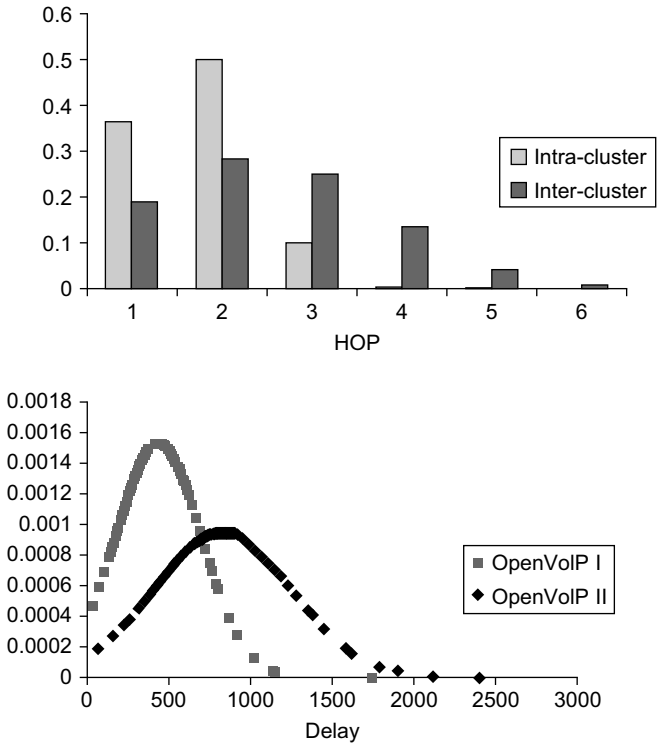


FIGURE 30-25

difficulties. Schulzrinne et al. [15, 41] present a framework that uses the LoST protocol to locate the caller's physical location and route the call to the appropriate Public Safety Answering Point (PSAP) [25]. Due to the distributed nature of P2PSIP, location-to-URI mappings should be stored in a distributed database which leads to attacks like placing bogus emergency calls or arbitrarily adding, removing, and updating entries in the mapping database.

Lawful interception (LI) service is used to record telephone calls by a legal body such as a court of law [16]. It involves finding the right intercepting point for the target and collecting signaling information and/or media traffic. The major problem is the lack of a fixed call path and the separation of signaling and voice messages. It becomes more difficult due to the absence of a centralized server.

Billing is a fundamental service available in commercial telephone systems and in Internet telephony, which is expected to provide reliability, trustworthiness, integrity, and non-repudiation. But the distribution of billing records and the lack of coordination in a distributed environment may cause free riding [34] results in attacks like DDOS and other inherent storage treats [38].

Voicemail systems are used to record calls and store voice messages when the incoming call is not answered. Main security vulnerabilities identified are privacy and integrity protection, [27] eavesdropping and interception during transmission, and unwanted information revelation during storage. Authentication, encryption, and approaches like SRTP [2] are used to provide security but storage is still vulnerable due to the distributed nature.

Das Ch30-9780124158153 2011/11/18 10:14 Page 784 #22

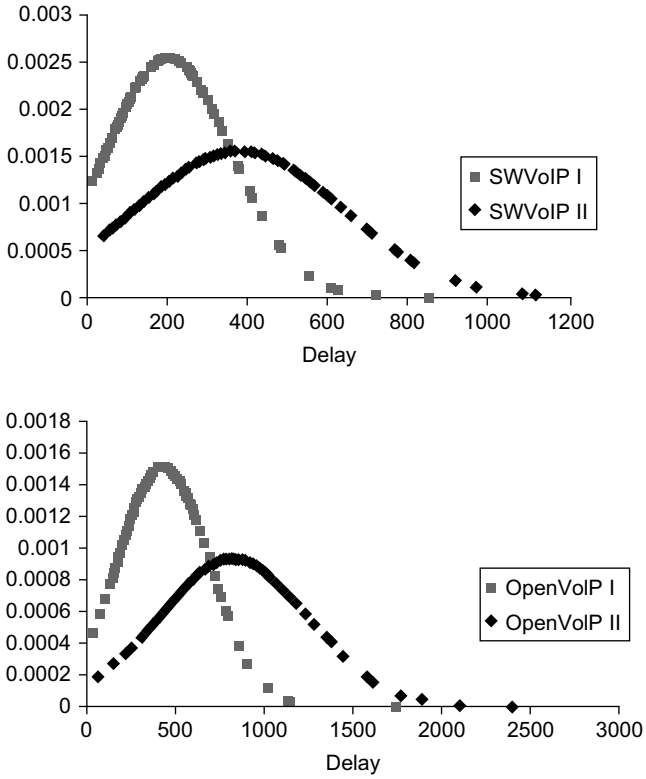


FIGURE 30-26

RTP and the Real-time Transport Control Protocol (RTCP) [2] are used in P2PSIP for end-to-end media communication in which the RTP data stream is vulnerable to attacks like eavesdropping, replay, etc.

30.6.3. Mitigate Vulnerabilities

Edge Resident Solutions. Edge resident solutions provide vulnerability-mitigating techniques at the edge of the network. Spam can be controlled by associating some level of trust with every P2PSIP entity that can be achieved by using one-way hash functions for the public key generation. In case of an emergency call, every entity in a P2PSIP network should be able to prioritize emergency signals and find the corresponding PSAP URIs [17]. All the protocols should support the distributed database. In lawful interception, each P2P-based end device should be allowed to intercept all outgoing and incoming traffic. Security for timely communications [28–32] can be provided by inserting a code that provides security for the edge device.

Limited Core-Based Solutions. In this solution, due to the difficulty of providing fully distributed security services in a P2P network, it provides a few key security mechanisms in the core.

Spam can be controlled by using the certificate-based security mechanism as in Reload [8]. Voicemail security can be achieved by encrypting the voicemail in which the key exchange is handled using a group of central authentication servers [26]. Seedorf proposes a design for legal interception by placing an intercepting point chosen based on the target identity's node-ID and key-ID on the signaling path under the control of a Law Enforcement Agency (LEA) [16].

Das Ch30-9780124158153 2011/11/18 10:14 Page 785 #23

IP-Layer-Based Solutions. To prevent SPIT attacks, a legitimate IP address and port authentication is provided by a central controller. To provide a solution for lawful interception, LEA can authorize the network operator to authenticate the target's identity and intercept messages at the IP-layer.

Recommendations. End-to-end security is important for multi-modal streams consisting of audio, video, and text messages. Such media communication is secured by using TLS, SRTP, and SDES. Most security services are provided on the terminal devices, and hence, new codes or new applications can be easily added in such a way that is backward compatible with existing P2PSIP. Mobility support is also an important feature of VoIP systems, which is recommended to support distributed mobility by the mapping and membership management in P2PSIP systems. Other important requirements are privacy and trust, which can be obtained by encryption, authentication, customer feedback, etc. Another issue for the P2PSIP security services is NAT traversal [18]. Using Reload is recommended. It provides functions for NAT traversal which use ICE [33] to establish new Reload or application protocol connections. Small world VoIP (SWVoIP) [37, 39, 40] is a social trust-based peer-to-peer communication, which reduces the threats posed on a normal VoIP system.

30.7. SMALL WORLD VoIP-P2PSIP-BASED ON TRUST

Normally, in P2P VoIP, the VoIP service (voice, SMS, etc.) is launched only after the address of the receiver is queried through P2P routing, which introduces much maintenance cost and communication degradation and is more susceptible to security attacks. These demerits of P2P VoIP have made it less effective when compared with normal VoIP networks. Small World-VoIP (SW-VoIP) is a novel work in improving P2P VoIP by analyzing the user behavior [19]. As the title suggests we are creating a small world by forming a cluster of users who communicate frequently. This is more a telephone or mobile centric approach since the analysis of the user behavior is done using his/her call log. The authors have also thrown light into algorithms improving routing [6, 20]. The important part of this work lies in how the behavior analysis is used in optimizing the network.

The four main design goals which the author has set are coping with changing IP addresses, having a centralized control, handling complexities caused by customized services, and delay protection. The first goal, i.e., the changing IP problem caused by mobile users who dynamically change their IP, needs dynamically binding the IP address to the fixed phone number of the user. Next, to ensure that there is a centralized control for enabling services like E-911, CALLEA, etc., the services are distributed to some users who have high credibility and more contacts. Thus, these users become engaged in transferring control messages for the above discussed services. To ensure delay protection, the users are grouped based on the social relationships and these users can find the user who called them by looking up popularly accessed nodes. Second best routes are also provided to avoid traffic on a particular line.

30.7.1. Small World VoIP Construction

For constructing the call graph, the first step is to set up a method to track call logs of a user to find his/her calling patterns. Distributed Peer Crawler is used to collect call log information from the users in the network. The distributed peer crawler crawls the peer-to-peer network to get the call logs of all the users, which can be downloaded later since getting the call logs directly of all users at a time leads to more delay due to processing. The PCrawler (as shown in Figure 30-19) constructs a small world overlay once a user is active in the network. It has two components: the call log collector and a consistency checker. There is a dispatcher, which disseminates PCrawler to all the clusters depending on the size of the network. These dispatchers are instrumental in authenticating the PCrawlers before they start a session with the clusters and collect the call logs of the users. The reason for

Das Ch30-9780124158153 2011/11/18 10:14 Page 786 #24

the authentication is to make sure that these crawlers are not used for malicious attacks on the networks. Apart from collecting call logs from the usage, these crawlers also check the status, i.e., if the user had a new SID or a new IP, of the user using a breadth-first search algorithm.

30.7.2. Closeness-Based Routing

The Figure 30-20 depicts the general routing in a cluster system. Clustering uses three algorithms. The first looks up the user in the cluster. It is done by closeness-based routing (illustrated in Figure 30-21). In case of a caller agent calling a callee, the caller needs to know the address information of the callee. The DHT uses a tuple consisting of key and value but this algorithm differs in a way where it uses a hash value of IP and port as the key and uses the same method to find the user object and to find the closest user for that key. It also shows how hubs act as supervisors of clusters. Hubs with higher popularity make them more trusted by users. So, each user can choose its hub based on a credibility value given to it and from the list of hubs his/her friends have.

30.7.3. Join and Leave

The second algorithm, described in Figure 30-22, defines the things to do by the user to join or leave a cluster. To make sure malicious elements do not join the network, it has been communicated and recommended to a certain number of members who are already on the SW-VoIP network. After this step, the user joins the network by setting up his status flag to 1 and then can actively participate in the network. For a normal user to leave the process is simple. It just informs its friends and passes its stored keys to a close friend and leaves. But when it comes to a user who was a hub, the next hub needs to be calculated before the current hub user leaves. This is done by calculating the next popular user in the cluster and the users elect the next hub.

30.7.4. Congestion Avoidance

The third algorithm is the congestion avoidance algorithm (as described in Figure 30-23). Because the hub nodes are needed to transfer control messages, the hub nodes have a high likelihood of being congested, because all TCP connection requests cause the majority of the delay. Here, the proposed algorithm uses a formula to calculate the next best node for routing which is used in case a node is found to be affected by congestion. The users inside find it by checking the flag FConn which is set to one if it is found to be affected by congestion. So, the users will calculate the next best node for routing its service requests.

30.7.5. Experimental Evaluation

All algorithms were implemented and evaluated. Simulations were conducted by using real-life call logs of 97 users using mobile phones for 9 months at MIT by the Reality Mining project group. The mobile phones used were Nokia 6600s loaded with software needed for the research. The deployed test bed had around 1000+ nodes and 300+ PlanetLab machines using OpenVoIP developed by a research group at Columbia University. Setting up to six different time periods like weekday, weekend, school open winter break, daytime, and nighttime as parameters they have generated traffic on the network. The evaluation of the test bed showed some important things. It was found that 10% of the users were always active. The SW-VoIP shows a higher percentage of 1 or 2 hops and a lesser percentage of multi-hops than OpenVoIP. It also showed if the number of clusters was 2–4, SW-VoIP showed better results, thereby indicating that the more closed the group is, the better the performance is. Further results of the evaluation are discussed.

We observed that there are a larger number of intra-cluster calls than inter-cluster calls. We generate these two kinds of user lookup traffic on four clusters of the SW-VoIP system, respectively, and illustrate the system performance in the following figures. For intra-cluster calls, most of the routings are processed in 1∼3 hops with the delay of 0–400 ms, whereas inter-cluster routings have the scattered test results ranging from 1 to 6 hops with 0–1000 ms delays.

Das Ch30-9780124158153 2011/11/18 10:14 Page 787 #25

We further explored user lookup performance under heavy network traffic. We attempted to build as many connections as possible by simultaneously launching user lookup traffic on 97 nodes in OpenVoIP and SW-VoIP, respectively, based on real-life call logs. The traffic generated include messages issued not only from those 97 users but also from an additional 52 users in the P2P VoIP network, as shown in the figure of user call degree distribution. We assume that these 97 users in SW-VoIP are divided into four clusters as in earlier described experiments, and a congestion avoidance mechanism has little effect on the average link traversal of our SW-VoIP communications. We compared two systems by evaluating user lookup delay under up to 10,000 simultaneous messages. It is observed in the following figure that not only does SW-VoIP have less of an average delay than OpenVoIP but the delays in SW-VoIP also increase much less than those in OpenVoIP. This shows that SW-VoIP has a better congestion avoidance capability than OpenVoIP.

Thus, SW-VoIP proves to be better in performance when compared with OpenVoIP. SW-VoIP is expected to work well with a number of users also because it is using real-life call logs. The implementation of the algorithm is simple with methods that can be easily scalable to existing VoIP networks and services. So, the proposed small world VoIP system is effective and has achieved the goals of effective P2P VoIP for mobile users.

30.8. CONCLUSION

To conclude the chapter, we summarize the sections discussed above. While discussing the setup and the networking components involved in a VoIP communication using SIP, we have empirically investigated the trust issues of the currently deployed VoIP systems and their implications to the VoIP users. Our experiments show that leading deployed VoIP services (e.g., Vonage, AT&T, and Gizmo) are vulnerable to exploitations like unauthorized call diversion, eavesdropping, wire-tapping, etc., which essentially violates the VoIP users' basic trust that their VoIP calls will reach the intended callee only. We further show that such unauthorized call diversion could lead to a brand new attack on VoIP users. For example, the voice pharming attack, which could trick the most cautious VoIP callers into giving out sensitive information (SSN, credit card number) to the adversary. Also, our experimental results show that millions of subscribers to leading commercial VoIP service providers such as Vonage and AT&T are vulnerable to various billing attacks, and the billing of existing SIP-based VoIP services is not trustworthy. The results show that existing VoIP users are susceptible to identity theft and financial loss due to the lack of the trust in currently deployed VoIP systems.

Considering the rapid development of P2P-based telecom networks, many open issues remain to be solved. To date, P2PSIP is still in the formative stage and no formal protocols have been defined. Security problems and corresponding solutions may vary according to these choices as well. The design of a SW-VoIP system aims to provide distributed control, epidemic updating, and adaptive trust computing to P2P VoIP users, which are important for the deployment of telecommunication services. Based on previous research on P2PSIP security, we have discussed foreseeable abuses and possible countermeasures to application services of standard telephony. Described security services consist of social attacks (e.g., spam), social services (e.g., emergency service and lawful interception), phone services (billing and voicemail), and real-time communications. Furthermore, security and performance trade-offs are described for the feasibility of solutions, and a set of best practices are recommended for the security services deployment.

ACKNOWLEDGEMENTS

We would like to thank Kalyan Pathapati Subbu, Vikram Chandrasekaran, Srikanth Jonnada and Chaitra Urs for all the editing support and help provided.

Das Ch30-9780124158153 2011/11/18 10:14 Page 788 #26

EXERCISES

(Note: there is no single answer for the following questions; however, you can find several tips by looking at the RFCs and some of the cited references.)

1. Examine the SIP protocol and list the possible DoS attacks with respect to the client and the server.
2. List possible ways of blocking spam in a VoIP network and describe how this is different from e-mail spam.
3. Compare SIP and P2PSIP protocols with respect to security, privacy, and performance.
4. Examine the P2PSIP protocol and explore the possible MITM and redirection attacks.
5. List the performance issues for implementing lawful interception for signaling and media in P2PSIP protocol and recommend ways for avoiding the attacks.
6. What are the issues in offering billing services in a P2PSIP network. Discuss how this service can be supported by telecommunication providers across the globe.
7. Describe the ways to improve the performance of a P2PSIP (in particular time for hashing) network using social networks.

REFERENCES

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A.R. Johnston, J. Peterson, R. Sparks, et al., SIP: session initiation protocol, RFC 3261, Internet Engineering Task Force, June 2002.

[2] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, RTP: a transport protocol for real-time applications, RFC 3550, July 2003.

AQ:1 [3] X. Wang, R. Zhang, X. Yang, X. Jiang, D. Wijesekera, Voice Pharming Attack and the Trust of VoIP, SecureComm, September 2008.

[4] R. Zhang, X. Wang, X. Yang, X. Jiang, Billing attacks on SIP-based VoIP Systems, WOOT, August 2007.

AQ:2 [5] S. Ratnasamy, P. Francis, M. Handley, R. Karp, S. Shenker, A scalable content-addressable network, in: Proceedings of ACM SIGCOMM, 2001.

AQ:3 [6] I. Stoica, R. Morris, D. Karger, F. Kaashoek, H. Balakrishnan, Chord: a scalable peer-to-peer lookup service for internet applications, in: SIGCOMM, San Diego, CA, August 2001.

[7] J. Seedorf, Security challenges for Peer-to-Peer SIP, IEEE Netw. 20 (5) (2006) 38–45. AQ:4

[8] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset, H. Schulzrinne, Resource Location and Discovery (RELOAD) Base Protocol, July 12, 2010, draft-ietf-P2PSIP-base-09.

[9] H. Song, M. Matuszewski, D. York, P2PSIP Security Overview and Risk Analysis, September 28, 2009, draft-matuszewski-P2PSIP-security-requirements-06.

[10] K. Birkos, C. Pageorgiou, P. Galiotos, T. Dagiuklas, C. Tselios, S. Kotsopoulos, Security Mechanisms and Key Refresh for P2PSIP Overlays, March 1, 2010, draft-birkos-p2psip-security-key-refresh-00.

[11] D. Bryan, B. Lowekamp, M. Zangrilli, The design of a versatile, secure P2PSIP communications architecture for the public internet, in: Proceedings of the Fifth International Workshop on Hot Topics in Peer-to-Peer Systems, Hot-P2P '08, workshop @ IPDPS 2008, April 2008.

[12] B. Nilanjan, S. Samir, S. Subir, Anti-vamming trust enforcement in peer-to-peer VoIP networks, in: International Conference on Communications and Mobile Computing, 2006.

[13] F. Cao, D.A. Bryan, B.B. Lowekamp, Providing secure services in Peer-to-Peer communications networks with central security servers, in: Proceedings of ICIW 2006.

[14] L. Jean Camp, A. Friedman, Peer to Peer Security Telecommunications Policy Research Conference, Washington DC, September 2003.

[15] B. Rosen, H. Schulzrinne, J. Polk, A. Newton, Framework for Emergency Calling Using Internet Multimedia, draft-ietf-ecrit-framework-10, July 27, 2009.

[16] J. Seedorf, Lawful Interception in P2P-based VoIP Systems, IPTCOMM, 2008.

[17] H. Schulzrinne, R. Marshall, Requirements for emergency context resolution with internet technologies, January 2008, RFC 5012.

[18] J. Rosenberg, Interactive connectivity establishment (ICE): a protocol for network address translator (NAT) traversal for offer/answer protocols, RFC 5245, April 2010.

[19] X. Yang, A. Stavrou, R. Dantu, D. Wijesekera, Small World VoIP, MobiCase, 2010.

[20] A.J. Ganesh, A.-M. Kermarrec, L. Massoulie, Peer-to-Peer membership management for gossip-based protocols, IEEE Trans. Comput. 52 (2) (2003). AQ:5

[21] K. Singh, H Schulzrinne, Peer-to-peer Internet telephony using SIP, NOSSDAV, June 2005. AQ:6

[22] D.A. Bryan, B.B. Lowekamp, C. Jennings, SOSIMPLE: a serverless, standards-based, P2P SIP communication system, IEEE, AAA-IDEA, 2005.

[23] K. Singh, H. Schulzrinne, Using an External DHT as a SIP Location Service, Columbia University

Das Ch30-9780124158153 2011/11/18 10:14 Page 789 #27

Technical Report CUCS-007-06, New York, February 2006.

[24] D. Bryan, P. Matthews, E. Shim, D. Willis, S. Dawkins, Concepts and Terminology for Peer to Peer SIP, July 7, 2008, draft-ietf-p2psip-concepts-02.

AQ:7 [25] H. Schulzrinne, H. Tschofenig, A. Newton, T. Hardie, LoST: a protocol for mapping geographic locations to public safety answering points, in: Performance, Computing, and Communications Conference, IEEE International, IPCCC 2007.

[26] D.A. Bryan, P2PSIP: On the Road to a World without Servers, Business Communications Review, v37 n3, April 2007.

[27] H. Li, M. Singhal, Trust management in distributed systems, IEEE Comput. 40 (2007).

[28] ITU-T, P.800 – Methods for Subjective Determination of Transmission Quality. http://www.itu.int/rec/T-REC-P.800/en, August 1996, (accessed 26.01.08).

[29] ITU-T, G.109 – Definition of Categories of Speech Transmission Quality. http://www.itu.int/rec/T-REC-G.109-199909-I/en, September 1999, (accessed 26.01.08).

[30] ITU-T, Y.1530 – Call Processing Performance for Voice Service in Hybrid IP Networks Pre-Published. http://www.itu.int/rec/T-REC-Y.1530/en, November 2007, (accessed 26.01.08).

[31] Telecommunications Industry Association (TIA). March 2006. Technical Service Bulletin (TSB)-116A – Telecommunications – IP Telephony Equipment – Voice Quality Recommendations for IP Telephony.

[32] ITU-T, G.109 – Definition of Categories of Speech Transmission Quality. http://www.itu.int/rec/T-REC-G.109-199909-I/en, September 1999, (accessed 26.01.08).

[33] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, STUN-Simple traversal of user datagram protocol (UDP) trough network address translators (NATs), RFC 3489.

[34] E. Adar, B.A. Huberman, Free riding on Gnutella, First Monday 5 (10) (2000).

[35] www.skype.com AQ:10

[36] S.L. Garfinkel, VoIP and Skype Security, Skype Security Overview, rev 1.6, January 2005.

[37] X. Yang, D. Wijesekera, R. Dantu, Achieving Peer-to-Peer Telecommunication Services through Social Hashing, CCNC 2008.

[38] R. Zhang, X. Wang, R. Farley, X. Yang, X. Jiang, On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers, ASIACCS, March 2009.

[39] X. Yang, D. Wijesekera, R. Dantu, A society-integrated test-bed architecture for peer-to-peer telecommunications, in: Proceedings of Fifth International Conference on Test-bed and Research Infrastructures for the Development of Network & Communities and Workshops, 2009, pp. 50–56.

[40] V. Chandrasekaran, R. Dantu, N.K Gupta, X. Yang, D. Wijesekera, Efficiency of Social Connection-based Routing in P2P VoIP Networks, IAMCOM 2010.

[41] B. Rosen, Framework for Emergency Calling Using Internet Multimedia, draft-ietf-ecrit-framework-05, August 2008.

[42] B. Rosen, H. Schulzrinne, J. Polk, A. Newton, Framework for Emergency Calling Using Internet Multimedia, draft-ietf-ecrit-framework-11, IETF, September 8, 2011.

Author Queries

AQ:1 Please provide more details for the references [3,4,14,16,37–40].
AQ:2 Please provide publisher name and location, if any for the references [5,11,12,13].
AQ:3 Please provide the Publisher name and location for the reference [6].
AQ:4 Please check the edit made to the reference [7,28,30,32,34].
AQ:5 Please provide the page range, if any, for the references [20, 27].
AQ:6 Please note that references have been renumbered to arrange them sequentially, and also note that the References [21-41] (new No.) are not cited anywhere in the text, please cite them in the text accordingly.
AQ:7 Please check the edit made to the reference [15] and also provide the publisher name and location, if any.
AQ:8 Please provide citation for Figures 30.24–30.26 in the text.
AQ:9 Please provide caption for Figures 30.9, 30.24–30.26.
AQ:10 Please provide complete details for the reference [35].
AQ:11 Please fix the word "Proxy server" (Caps or lowercase)? Inconsistent throughout the chapter.

Non-Print Items

Abstract

As VoIP telecommunication networks are becoming popular, more and more VoIP calls are being made to accomplish security critical activities, e.g., E911 services, phone banking. However, the security ramifications of using VoIP have not been fully recognized, and there exists a substantial gap in the understanding of the potential impact of VoIP exploits on the VoIP users. In this chapter, we describe the components and functionalities of non-P2P and P2P VoIP networks and discuss the potential attacks to them such as MITM, spoofing, wiretapping, pharming, etc. We also illustrate a mechanism of using small world network to improve call performance of a P2P VoIP system and evaluate it over the currently deployed OpenVoIP system.

Keywords: voice over IP, telecommunications, session initiation protocol, security, P2P, small world networks