Voice Pharming Attack and the Trust of VoIP

Xinyuan Wang†, Ruishan Zhang†, Xiaohui Yang†, Xuxian Jiang‡, Duminda Wijesekera†

†Department of Computer Science
George Mason University
Fairfax, VA 22030, USA
{xwangc, rzhang3, xyang3, dwijesek}@gmu.edu

‡Department of Computer Science
N.C. State University
Raleigh, NC 27606, USA
jiang@cs.ncsu.edu

ABSTRACT

Voice communication is fundamental to the normal operation of our society. The general public have put a lot of trust in voice communication and they have been relying on it for many critical and sensitive information exchange (e.g., emergency 911 calls, calls to customer service of financial institutions). Now more and more voice calls are carried, at least partially, over the public Internet rather than traditional Public Switched Telephone Network (PSTN). The security ramifications of using VoIP, however, have not been fully recognized. It is not clear how secure and trustworthy the currently deployed VoIP systems are, and there exists a substantial gap in the understanding of the potential impact of VoIP exploits on the VoIP users. In this paper, we seek to fill this gap by investigating the trust issues of currently deployed VoIP systems and their implications to the VoIP users.

Our experiments with leading deployed VoIP services (e.g, Vonage, AT&T and Gizmo) show that they are vulnerable to a number of VoIP exploits that essentially violate the VoIP users' basic trust that their calls will reach their intended destinations only. Specifically, a MITM (man-in-the-middle) can 1) detour any chosen Vonage and AT&T VoIP call via anywhere on the Internet; 2) redirect any selected Vonage and AT&T VoIP call to any third party without authorization; 3) manipulate and set the call forwarding setting of any selected Gizmo VoIP subscriber without authorization. Such an unauthorized call diversion capability enables a new attack, called *voice pharming*, against VoIP users, where the attacker transparently diverts selected VoIP calls to the bogus IVR (interactive voice response) or bogus representative. In other words, voice pharming can cause selected VoIP callers to interact with the bogus IVR or representative even if they have dialed the correct phone numbers. Therefore, even the most meticulous VoIP caller could be tricked into giving out sensitive information (e.g., SSN, credit card number, PIN) to the adversary. To mitigate such imminent threats to current VoIP users, all segments along the VoIP path need to be protected and trustworthy. Our experience shows that enforcing TLS or IPSEC between the SIP phone and SIP servers could be an effective first step toward mitigation.

SecureComm 2008, September 22–25, 2008, Istanbul, Turkey.

1. INTRODUCTION

VoIP has experienced phenomenal grow in the past few years, and more and more people, businesses are relying on VoIP for their voice communication needs. A recent study by ABI [4] predicted that the number of residential VoIP subscribers worldwide will increase from current 38 million to more than 267 million by 2012. The Radicati Group [35] predicted that 74% of all corporate telephone lines worldwide will be VoIP by 2009.

One of the most basic and fundamental requirements of any VoIP services is that they must be reliable and trustworthy. When people subscribe or use any VoIP service, they have actually put a lot of implicit trust on it. For example, when people make phone calls, they intuitively trust that their calls will reach the intended callee once they dial the correct phone number and no one but the intended callee will receive their calls. When people talk over the established phone session, they trust that their conversation and any PIN number pressed will reach the intended receiver unaltered. In addition, people would expect that their calls will not be wiretapped without proper legal authorization. Based on this trust, voice communication has been used for exchanging many critical and sensitive information (e.g., emergency 911 calls, calls to customer service of financial institutions). The general public are used to giving out their SSN, credit card number and PIN when they interact with the interactive voice response (IVR) system before they are connected to a service representative of their financial institution. Furthermore, people are comfortable to give out their credentials (e.g., SSN, account number, authentication code) to the service representative of their financial institution over the phone even if they don't personally know the service representative.

To exploit people's trust in telephone service, phishing attacks are evolving from traditional web-based into sophisticated phone scams called voice phishing (i.e., vishing) [18, 46]. Instead of asking people to visit some bogus web site, voice phishing lures them into dialing some bogus phone number (given by a bogus email or phone call) and giving out their credentials. Recent voice phishing attacks on PayPal and Santa Barbara Bank & Trust [28, 22] urged people to call a bogus phone number (805-xxx-xxxx) and input their 16-digit credit card numbers. To help the general pub-

lic avoid being victim of such voice phishing scams, Secure Computing [46] advises people only call the phone number on the back of their credit card or on their bank statement. The Anti-Phishing Working Group [2] also advises the public to call the company on telephone as a way to avoid phishing scams. All these suggest that despite voice phishing attack, phone call remains one of the most trusted ways to communicate with organizations (e.g., emergency response center) or unknown person (e.g., bank teller) remotely. While people may not trust the unsolicited incoming calls and the callers, the general public simply trust that their phone call will reach the intended callee (e.g., police, financial institution, service representative) once they dial the genuine phone number (e.g., 911). Such a basic trust of voice communication is fundamental to the normal operation of our society, and any compromise of such a basic trust of phone call would disrupt the daily lives of millions of people.

While traditional PSTN (Public Switched Telephone Network) calls have been shown to be quite trustworthy, it is not clear how secure and trustworthy the currently deployed VoIP systems are. Although a number of potential threats to VoIP have been presented [27, 14, 26], most of them have never been validated empirically with currently deployed VoIP systems. Thus there is a wide-spread doubt on whether those potential threats to VoIP are actual [33]. In addition, most existing VoIP security analysis has been focused on the threats to the VoIP infrastructure (e.g., denial-of-service attack on VoIP servers) rather than the VoIP users. There exists a substantial gap in the understanding of the potential impact of VoIP exploits on the VoIP users. In this paper, we seek to fill this gap by investigating the trust issues of currently deployed VoIP systems and their implications to the VoIP users.

We have empirically investigated leading VoIP services by Vonage, AT&T and Gizmo, and we have found that they are vulnerable to a number of exploits that essentially violate the VoIP users' basic trust that their calls will reach the intended callee only. Specifically, a MITM (man-in-the-middle) could 1) detour any chosen VoIP call through any remote device; 2) transparently redirect any selected VoIP call to any phone chosen by the attacker; 3) transparently manipulate and set the call forwarding setting of any selected VoIP subscriber. Such unauthorized VoIP call diversion enables a new class of attack, called *voice pharming* attack, against VoIP users. Similar to pharming attack [31], voice pharming aims to collect victims' confidential information (e.g., SSN, credit card number, PIN) by diverting victims' phone calls to bogus IVR (interactive voice response) or bogus representative. Compared with voice phishing (i.e., vishing) [54], voice pharming attack is particularly dangerous in that it could cause the victims talk to bogus representative or interact with bogus IVR of chosen institution (e.g., Citibank) even if they have dialed the correct phone numbers. Therefore, even the most meticulous caller could be tricked into giving out sensitive information (e.g., SSN, account number, PIN). Note none of these attacks require the knowledge of the secret password shared between the VoIP phone and the VoIP servers, and they could be launched from anywhere along the VoIP path on the Internet. Therefore, current VoIP users are susceptible to identity theft and financial lost due to the lack of trust of currently deployed VoIP. To mitigate such imminent threats to current VoIP users, all segments along the VoIP path need to be protected and trustworthy. Our experience shows that enforcing TLS or IPSEC between the SIP phone and SIP servers could be an effective first step toward mitigation.

The rest of this paper is organized as follows: Section 2 overviews the SIP signaling protocol and its security mechanisms. Section 3 describes the VoIP threat model and our investigation methodology. Section 4 empirically demonstrates the unauthorized VoIP call diversion vulnerability of leading deployed VoIP services. Section 5 discuss the implications of the unauthorized VoIP call diversion vulnerability. Section 6 discusses potential mitigation strategies against the unauthorized call diversion and voice pharming attack. Section 7 presents related works on VoIP security. Section 8 concludes the paper.

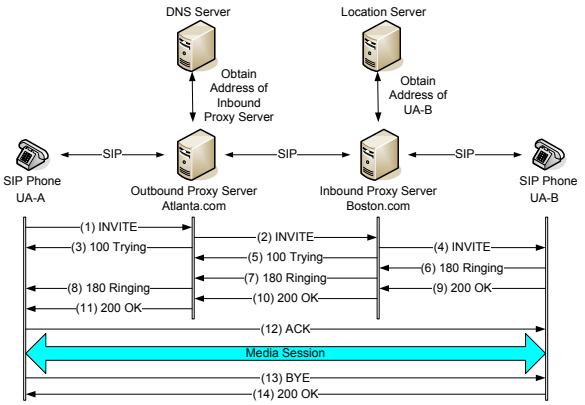
2. VOIP SIGNALING AND SIP OVERVIEW

Given that signaling is fundamental to any VoIP services, we briefly overview VoIP signaling. Existing VoIP signaling protocols include Session Initiation Protocol (SIP) [40], H.323 and Media Gateway Control Protocol (MGCP) [1]. SIP is a RFC standard from the Internet Engineering Task Force (IETF), and it is a generic signaling protocol for establishing sessions in an IP network. H.323, on the other hand, is an ITU standard that was originally designed to provide multimedia communication over LANs, and it is suited for interworking between IP and ISDN. MGCP [1] is a signaling protocol for controlling telephony gateways from external call control elements called media gateway controllers or call agents. Schulzrinne and Rosenberg [44] argued that SIP is superior to H.323 in extensibility and scalability aspects although they provide approximately the same services. Currently SIP is the dominant signaling protocol for VoIP.

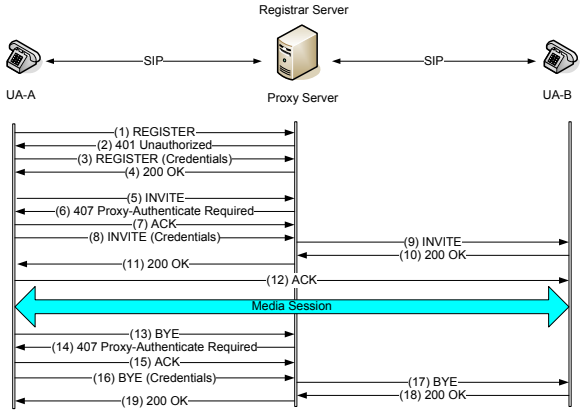
According to RFC-3261 [40], SIP is a general purpose, application layer signaling protocol used for creating, modifying, and terminating multimedia sessions (e.g. VoIP calls) among Internet endpoints. SIP defines the signaling interaction between: *user agent* (UA), *proxy server*, *redirect server*, *registrar server* and *location server*. An UA represents an endpoint of the communication (i.e., a SIP phone). Based on its role in the communication, an UA could be either UA client or UA server. The proxy server is the intermediate server that acts on behalf of UA to forward the SIP messages to its destination. The registrar server handles the UA's registration request. The location server maintains the location information of the registered UAs. The redirect server provides the UA client with an alternative set of contact addresses on behalf of the UA server.

Based on client-server model, SIP uses *request* and *response* messages to establish sessions between two or more endpoints. The endpoint that functions as client or server in the SIP signaling is called *user agent client* (UAC) or *user agent server* (UAS) respectively. To establish, manage or tear down a VoIP session, UAC will send to SIP server or UAS a SIP request messages identified by one of the six SIP method names: `INVITE`, `ACK`, `BYE`, `CANCEL`, `REGISTER` and `OPTIONS`. Upon receiving SIP request message, the SIP server or UAS will, when appropriate, reply with a SIP response message identified by a status code that indicates the status or result of the action taken upon the corresponding SIP request message.

In SIP network, each user is identified by a SIP *Uniform Resource Identifier* (URIs), which is similar to an e-mail ad-



(a) SIP Message Flow without Digest Authentication



(b) SIP Message Flow with Digest Authentication

Figure 1: SIP Message Flows for Call Setup and Tear Down with and without Digest Authentication

dress. Suppose there are two UAs *UA-A* and *UA-B* belong to domain *Atlanta.com* and *Boston.com* respectively, both of which have their own proxy servers. Figure 1(a) shows the SIP message flow of a typical and successful call setup and tear down without authentication.

The SIP security is largely based on existing security mechanisms for HTTP and SMTP. SIP [40] recommends using TLS [7] or IPsec [19] to protect the SIP signaling path in SIP networks. It suggests using S/MIME[36] to protect the integrity and confidentiality of SIP messages. However, it is difficult to protect the whole SIP message from end-to-end since intermediate SIP servers need to examine and change certain fields of the SIP messages while they are transferred. SIP mandates that all SIP proxy, redirect server and registration server must support TLS [7] and HTTP digest based authentication [12]. However, UAs are required to support HTTP digest based authentication [12] only.

Based on HTTP digest authentication [12], SIP authentication provides anti-replay protection and one-way authentication to SIP messages. It can be used by a SIP UAC, SIP UAS, SIP proxy or registrar server to prove that it knows the shared secret password. Figure 1(b) shows the typical SIP authentication of call registration, call setup and termination. When a SIP server (e.g., proxy, registrar) receives a SIP request (e.g., `INVITE`, `REGISTER`, `BYE`), the SIP server challenges the UAC with either a `401 unauthorized` or a `407 proxy-authentication required` message. Upon receiving the `401` or `407` response, the UAC applies specific digest algorithm (e.g., MD5 [39]) to SIP message fields *request-URB*, *username*, *password*, *realm*, *nonce* to get a hash value. Then the UAC resend the SIP request with the hash value as part of the credential to authenticate the SIP request.

3. VOIP THREAT MODEL AND INVESTIGATION METHODOLOGY

3.1 VoIP Threat Model

Since VoIP is an application upon IP, it is susceptible to many known attacks on the Internet and its applications. For example, VoIP servers may be vulnerable to denial of service attack, and the VoIP traffic may be mislead or corrupted by DNA cache poisoning. In this paper, we leave aside those vulnerabilities that are general to the Internet protocols and instead focus on the vulnerabilities that are

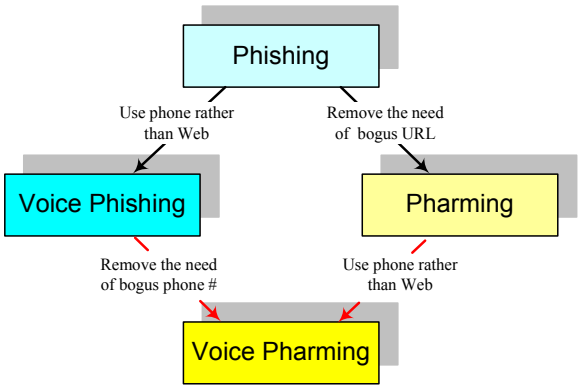


Figure 2: "Evolutional" Relationship between Phishing, Voice Phishing, Pharming and Voice Pharming

specific and inherent to VoIP protocols.

We assume there exists an active adversary in the VoIP signaling and/or media path who may observe, modify, drop and even spoof the VoIP traffic. In addition, the attacker may have one or more accomplices on the Internet and they could target any device in the path from the caller to the callee. Unlike most previous works [38, 41, 48, 49, 57, 56] on VoIP security, our focus is on those attacks that target selected, individual end users (i.e., subscribers) of the SIP-based VoIP systems rather than the VoIP infrastructure (e.g., SIP proxy, registrar servers). Since these attacks normally do not affect other end users and the VoIP servers, they are less likely to be noticed or detected by the VoIP service provider. Nevertheless, these attacks pose imminent threat to millions VoIP subscribers.

Specifically, we consider a new attack against the VoIP users: *voice pharming* attack, which subverts the victims' VoIP calls and divert them to bogus IVR or representative. Like phishing [32], pharming [31] and voice phishing [54] attacks, voice pharming aims to trick the victims into giving out their confidential information (e.g., SSN, credit card number, PIN) to the adversary. Similar to voice phishing, voice pharming exploits people's trust in voice communication. However, it eliminates the bogus phone number used in voice phishing via transparent call diversion, just like pharming eliminates the bogus URB used in phishing via trans-

parent Web traffic diversion. Therefore, voice pharming can be thought as a decedent of voice phishing and pharming, both of which are derived from phishing. Figure 2 shows the "evolutional" relationship between phishing, voice phishing, pharming and voice pharming.

Voice pharming attack essentially exploits people's long time trust that their calls will reach the intended callees once they dialed correct phone numbers (e.g., 911). If the attacker could somehow transparently divert the victim's VoIP call to a phone number or device he has chosen, all current VoIP users are susceptible to identity theft and financial lost due to voice pharming attack. Therefore, it is critically important to investigate if the calls of currently deployed VoIP systems can be transparently diverted by the attacker.

3.2 Investigation Methodology

In this paper, we take the role of active adversary, and we seek to find the vulnerabilities in both VoIP signaling and media protocols that would enable the attacker to transparently divert selected VoIP calls. Specifically we will focus on SIP [40] and RTP [43].

We observe that SIP messages can not be simply encrypted end-to-end due to the need to let any intermediate SIP proxies to legitimately change/add certain fields (e.g., `request-URI`, `via`) of the SIP messages. This makes the SIP signaling vulnerable to the *man-in-the-middle* (MITM) attack where an adversary is able to read, insert and modify at will, the SIP messages between two communicating parties without either party knowing that the SIP messages between them have been compromised.

Among all the hops in the SIP signaling path, the link between the end SIP phones and the immediate SIP servers (e.g., SIP proxy, registrar) is the weakest due to the following reasons:

- While the SIP specification [40] requires all the SIP-compliant SIP servers (e.g., proxy, registrar) to support TLS [7] hop-by-hop encryption among themselves, it does not require the UAs (i.e., SIP phone) to support any hop-by-hop encryption. Therefore, the SIP signaling between the deployed SIP phones and the deployed SIP servers is likely in clear text.

- A SIP phone is usually many router hops away from its immediate SIP servers. For example, our Vonage SIP phone has accessed 4 different Vonage SIP servers with IP addresses `69.59.242.84` (Los Angeles, CA), `69.59.252.35` (Philadelphia, PA), `69.59.227.87` (Holmdel, NJ) and `69.59.232.42` (Washington DC), which are 9 to 13 router hops away from our Vonage SIP phone. Our AT&T SIP phone has accessed AT&T SIP server with IP address `12.194.224.134` (Bridgeton, Missouri), which is 12 router hops away. This means that a SIP phone is likely to be of hundreds (or even thousands) of miles away from its SIP server. Such a long distance across the public Internet gives the adversary many opportunities to play MITM along the path of SIP messages. Specifically, compromised edge routers (e.g., gateway to certain institution) would allow the MITM to target specific group of people more accurately.

- A SIP phone could easily change its location and IP address. This gives the MITM more room to create spoofed SIP messages and makes it harder for the SIP server to filter out spoofed SIP messages. Now people are used to accessing wireless routers in airports, restaurants, conferences, libraries, and other public places, an attacker could easily become the MITM by setting up malicious wireless routers in these areas that offer free Internet access.

Therefore, the SIP messages to and from any SIP phone on the public Internet are subject to tampering by any device along the path between the SIP phone and the SIP server. Furthermore, the RTP stream is subject to MITM attack if it is not carried in secure channel (e.g., IPsec).

4. INVESTIGATING CURRENTLY DEPLOYED VOIP SYSTEMS

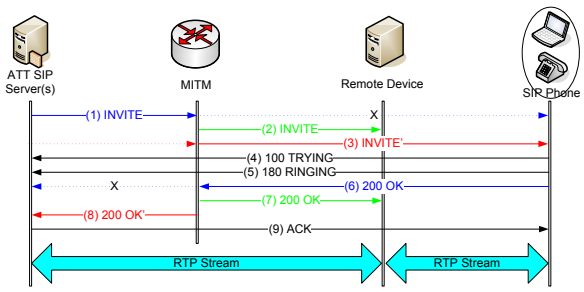
In this section, we examine the currently deployed VoIP systems and seek to find out what the active adversary could do to transparently divert selected VoIP calls. We choose to use the VoIP services of Vonage, AT&T and Gizmo [15] in our empirical investigation. According to Telephia's recent survey [55], Vonage and AT&T are the no. 1 (53.9%) and the no. 2 (5.5%) respectively in US VoIP market share. Gizmo, on the other hand, "is the best-known open-standards softphone project" [21]. Note all the VoIP exploits in our investigation were against our own phones rather than the VoIP infrastructure. At no time did we send any traffic to affect any other VoIP subscribers or violate any service agreement.

4.1 Transparent Detour of Selected VoIP Calls on the Internet

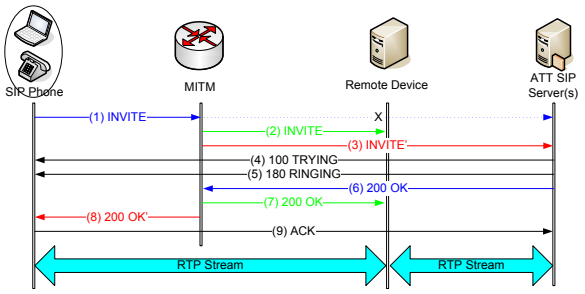
In this subsection, we show how an active adversary could detour any selected SIP-based VoIP call through any remote device chosen by the adversary. The goal of the remote transparent detour is to divert the RTP voice stream of the selected call through an arbitrary node (the remote device) on the Internet before it reaches its final destination.

During the SIP call setup process, the caller and callee can choose where (i.e., at what IP, on what port) they want to receive the upcoming RTP voice stream and they inform the other party about their choices via the `INVITE` and `200 OK` messages respectively. Since the RTP endpoint information (i.e., IP address, port number) is specified in the SDP part of `INVITE` and `200 OK` messages which is not protected by the SIP digest authentication at all, the active adversary is free to manipulate the RTP endpoint information. Due to performance consideration, some VoIP service providers (e.g., Vonage) may choose to use different servers for the SIP signaling and the RTP voice stream. Consequently, SIP phone will initiate its RTP stream to any IP address and port number specified in the SDP part of the `INVITE` or `200 OK` messages. On the other hand, the SIP server may remember the IP address of any registered SIP phone. However, the SIP server can not insist on sending its RTP stream to the registered IP address due to the need to support the SIP phones behind NAT. All these enable a MITM to divert any chosen RTP voice stream through any remote device on the Internet.

We have explored the transparent VoIP call detour in 4 scenarios: 1) a PSTN phone calls 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. We assume there is a MITM between the

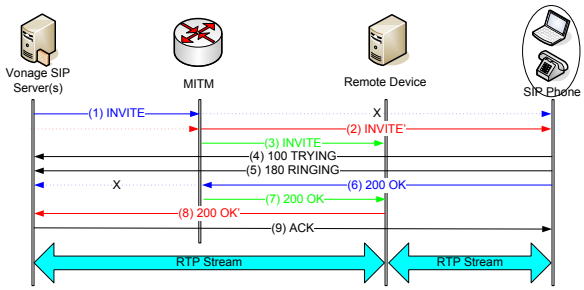


(a) PSTN Phone Calls AT&T SIP Phone

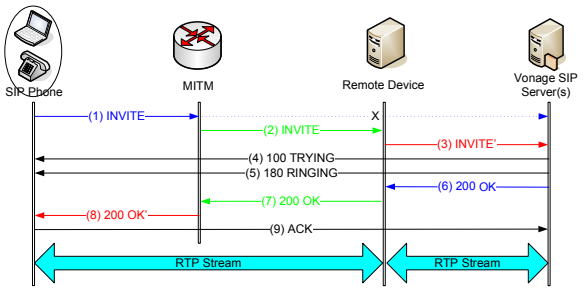


(b) AT&T SIP Phone Calls PSTN Phone

Figure 3: SIP Message Flows of Transparent Detour of Calls between an AT&T SIP Phone and a PSTN Phone



(a) PSTN Phone Calls Vonage SIP Phone



(b) Vonage SIP Phone Calls PSTN Phone

Figure 4: SIP Message Flows of Transparent Detour of Calls between a Vonage SIP Phone and a PSTN Phone

SIP phone and the SIP signaling server and the MITM is collaborating with a remote device. By careful manipulation of the SDP part of the `INVITE` and `200 OK` messages, we are able to divert the RTP voice streams in all of the 4 above mentioned scenarios through arbitrary node on the Internet.

Figure 3 shows the SIP message flows of the transparent detour of calls between an AT&T SIP phone and a PSTN phone. Note these SIP message flows differ from that of normal calls. First, the MITM intercepts the `(1) INVITE` message toward either SIP phone or the SIP server and send a copy (message `(2) INVITE`) to the remote device. This is to inform the remote device about the IP address and port number of the upcoming RTP stream selected by the caller side so that it can forward the RTP stream to the caller side. Second, the MITM modifies the SDP part of the intercepted `INVITE` message such that the IP address and port number for RTP will be that of the remote device. This essentially tells the callee side to send the RTP voice stream to the remote device. Then the MITM sends the modified `(3) INVITE` message to its original destination. The MITM will not intercept any `100 TRYING` or `180 RINGING` message. When the callee side accepts the call and sends the `(6) 200 OK` message to the caller side, the MITM intercept it and send a copy (message `(7) 200 OK`) to the remote device. This would informs the remote device about the IP address and port number of the upcoming RTP stream selected by the callee side. Such a information is necessary for the remote device to relay the received RTP voice stream. Then the MITM changes the IP address and port number in the SDP part of the intercepted `(6) 200 OK` message to that of the remote device and send the modified `(8) 200 OK` message to its original destination. This would trick the caller into sending the RTP voice stream to the remote device. Once the caller side responds with the `(9) ACK` message, the SIP call setup completes. Now the caller and callee will send their RTP voice streams to the remote device, which will relay the received RTP streams to their original destination and functions as a transparent proxy between the caller and callee.

When we apply the above attack procedures to the calls to and from our Vonage SIP phone, we see mixed result. While the Vonage SIP phone is tricked into sending its RTP voice stream to the remote device, the Vonage RTP server does not send out any RTP voice stream at all. It appears that the Vonage server checks the RTP stream IP address in the SDP part of the received `INVITE` or `200 OK` messages and refuses to send out any RTP stream if the it is different from the registered IP address of the SIP phone. This means that the MITM could not change the RTP stream IP address in the SDP part of the `INVITE` or `200 OK` message if he wants the call established. It seems that Vonage's SIP-based VoIP service is robust against the transparent detour attack.

After further research, we have found that while the Vonage SIP server validates the RTP stream IP address in the SDP part of the received `INVITE` or `200 OK` messages, it actually sends the RTP stream to the source IP address of the `INVITE` or `200 OK` message. This is necessary for the Vonage VoIP service to support SIP phone behind NAT where the registered SIP IP address is private.

Based on this finding, we have changed the SIP message flow of our transparent detour exploit. Figure 4 shows the SIP message flows of the transparent detour of calls between

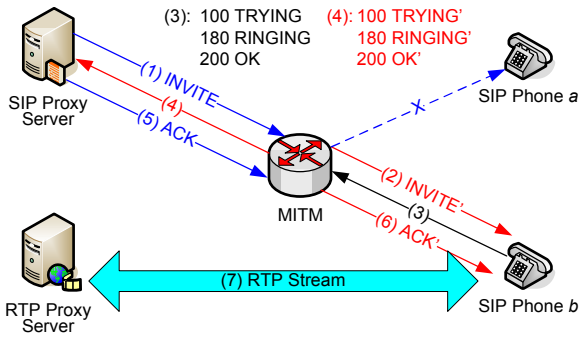


Figure 5: Unauthorized Call Redirection via MITM

a Vonage phone and a PSTN phone. The key difference between figure 3(a) and figure 4(a) is who will send message `200 OK` to the SIP server. When MITM intercepts message `(6) 200 OK` from the Vonage SIP phone, it sends a copy (message `(7) 200 OK`) to the remote device. Instead of letting the MITM to send out the modified `200 OK` message to the Vonage SIP server, the remote device will modify the RTP stream port number only and send the modified message `(8) 200 OK'` to the Vonage server. Since the RTP stream IP address in the SDP part of message `(8) 200 OK'` is not changed, message `(8) 200 OK'` will pass the check by the Vonage server. The Vonage server will send the RTP stream to the source IP address of message `(8) 200 OK'`, which is that the remote device. The key difference between figure 3(b) and figure 4(b) is who will send the `INVITE` message to the SIP server. For VoIP calls from Vonage SIP phone to PSTN phone, the MITM does not send the intercepted message `(1) INVITE` to the Vonage server, but rather let the remote device to modify the RTP port number in the SDP part of message `(2) INVITE` message and send the modified message `(3) INVITE` to the Vonage server. This would cause the Vonage SIP server to send its RTP stream to the remote device.

In summary, the MITM can transparently detour the RTP voice stream of any selected Vonage and AT&T SIP calls through any remote device on the Internet and let the original caller and callee establish the VoIP call. In this case, the remote device will have access to all the voice streams between the caller and the callee.

4.2 Transparent Redirection of Selected VoIP Calls

In this subsection, we explore how the active adversary could transparently redirect any selected VoIP call to any third party chosen by the adversary. As a result, the caller will be connected to the third party rather than the original callee. However, the caller will think he has reached the original callee while he has actually reached the third party. On the other hand, the original callee has never received the call from the caller.

4.2.1 *Callee Side Call Redirection*

When a caller wants to initiate a call via SIP, he sends an `INVITE` message to the callee, who is identified by the `request-URI` field in the `INVITE` message. Although the `request-URI` field is part of the SIP digest authentication, the SIP digest authentication is only applied to those `INVITE` messages from the SIP phone to the SIP servers. In other words, any `INVITE` messages from the SIP proxy to the SIP phone are not authenticated with the digest. Therefore, the MITM in between the SIP proxy and the SIP phone could freely change the `request-URI` field and redirect the SIP calls to any other SIP phone.

We have explored such call redirection attack at the callee side of our Vonage and AT&T SIP phones, and we are able to transparently redirect calls between our Vonage phone and AT&T phone. Figure 5 illustrates SIP message flows of the call redirection attack. When some one wants to call phone a, he sends an `INVITE` message to phone a. The MITM at the callee side intercepts the `INVITE` message and modifies the `request-URI`, `To` fields, the IP address and the port number of the `INVITE` message, and send the modified `INVITE` message to phone b. When phone b responds with `100 TRYING`, `180 RINGING` or `200 OK` messages, the MITM intercepts them and modifies the `To` field, the IP address and the port number. Then the MITM forwards the modified SIP message from phone b to the SIP proxy of phone a – pretending that those messages were from phone a. When the SIP proxy acknowledges the receipt of `200 OK`, it sends out `ACK` message to phone a. The MITM intercepts it and send the modified `ACK` message to phone b. This will establish the call between the caller and phone b instead of phone a.

4.2.2 *Caller Side Call Redirection*

We have also been able to transparently redirect selected VoIP calls at the caller side. In this case, the MITM intercepts the SIP messages from the victim caller, and pretends to be the SIP server by responding with spoofed SIP messages. The message flow in this case is similar to that show in Figure 5.

4.3 Manipulating and Hijacking Call Forwarding Setup

Call forwarding is a feature that allows the telephone subscribers to specify where the incoming calls will be forwarded. For example, people can setup call forwarding so that they can receive calls to their office phones with their cell phones while they are away from their offices.

Now we describe two attacks that would allow attacker to transparently manipulate the phone number to which the calls to the victim will be forwarded to. Unlike attacks described in sections 4.1 and 4.2, the attacks on call forwarding setup exploit the vulnerabilities of the media stream (e.g., RTP) rather than that of the signaling protocols (e.g, SIP). Therefore, these attacks could work even if the VoIP signaling is fully protected.

4.3.1 *Manipulating Vonage Call Forwarding Setup*

The call forwarding of Vonage VoIP phones can be setup by dialing a special number `*72`. The caller will be prompted to input the phone number to which the incoming calls (to the subscriber's phone) will be forwarded to. The input phone number will be transferred via RTP event packets to the Vonage RTP server. After the RTP server receives the call forwarding number, it will acknowledge the call forwarding number and ask the subscriber for confirmation. Once the subscriber confirms the input call forwarding number, the call forwarding will take effect immediately.

Assume the MITM is in between the SIP phone and Vonage RTP server, it could modify the call forwarding number to any phone number (including international phone numbers) and trick the subscriber into believing that the call for-

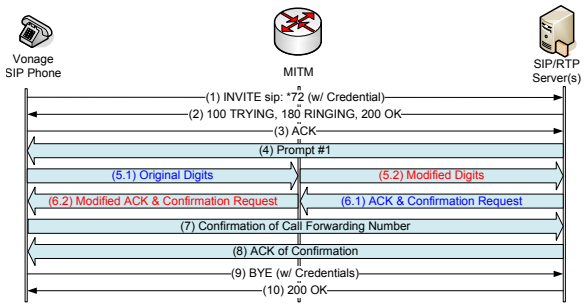


Figure 6: Manipulating Vonage Call Forwarding Setup via Man-in-the-Middle (MITM) in between SIP Phones and Vonage Servers

warding has been setup with the number he/she has chosen. Figure 6 shows the SIP and RTP message flows of the Vonage call forwarding setup manipulation attack. Messages (1) (2) and (3) show the authenticated call setup sequence for call to `*72`. Once the call to `*72` has been established, the Vonage RTP server will send the caller voice prompt "`For in country call forwarding, please enter ..., for international call forwarding, please enter ...`" in RTP (represented by message `(4) Prompt #1`) and wait for caller's response.

Once the caller inputs the call forwarding number, the SIP phone will send the call forwarding number in RTP event packets (represented by message `(5.1) Original Digits`) to the Vonage RTP server. The MITM intercepts the RTP event packets, and send the modified call forwarding number in the bogus RTP event packets (represented by message `(5.2) Modified Digits`) to the RTP server.

Note the MITM could change the number of digits of the call forwarding number. For example, the MITM could change the call forwarding number from an 11-digit domestic phone number (`1-xxx-xxx-0416`) to a 15-digit international phone number (`011-44-xxx-xxx-3648`). This means the MITM needs to send more bogus RTP event packets than the original RTP event packets from the caller. To maintain the correct RTP seq# and extended seq# in the RTP stream, the MITM needs to drop some normal RTP packets, which essentially contains background noise in between the keystrokes by the caller. This will make sure the RTP server accepts the modified bogus RTP (event) packets.

The RTP server will acknowledge the bogus call forwarding number it received and ask the caller for confirmation: "`you have entered 011-44-xxx-xxx-3648, press 1 to ...`" (represented by message `(6.1) ACK & Confirmation Request`). To prevent the caller from knowing the bogus call forwarding number received by the RTP server, the MITM needs to intercept the original acknowledgement and confirmation request and send the caller the modify acknowledgement and confirmation request (message `(6.2) Modified ACK & Confirmation Request`) so that the caller will hear the original call forwarding number (`1-xxx-xxx-0416`) he/she entered. After that, the MITM could let the rest RTP stream pass without modification.

We have experimented the above attack on Vonage call forwarding setup with our Vonage VoIP account. The caller have chosen to forward incoming call to an US domestic number (`1-xxx-xxx-0416`), the MITM have successfully and transparently changed the call forwarding number to an international phone number (`011-44-xxx-xxx-3648`). As a result, subsequent incoming calls to our Vonage VoIP phone have been forwarded to the international phone number `011-44-xxx-xxx-3648`.

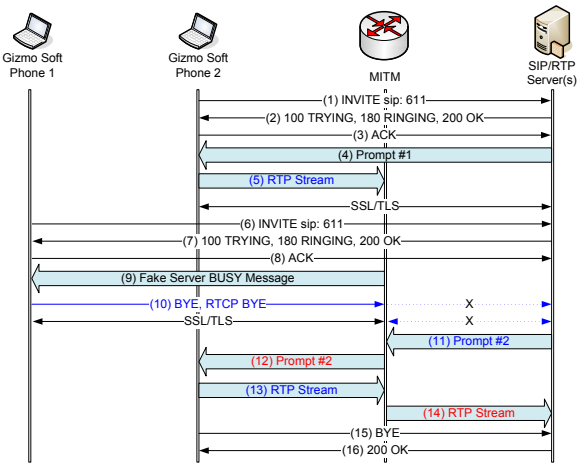


Figure 7: Hijacking Gizmo Call Forwarding Setup via Man-in-the-Middle (MITM) in between Gizmo Soft Phones and Gizmo Servers

4.3.2 Hijacking Gizmo Call Forwarding Setup

In section 4.3.1, we have shown that a MITM can transparently modify the call forwarding number to any preselected phone number while keeping the caller thinking that the call forwarding has been setup with the number he/she has chosen. In fact, the MITM can hijack the call forwarding setup session completely and let the attacker impersonate the VoIP subscriber and setup the call forwarding for the victim. We choose to use Gizmo, a popular SIP soft phone system, to demonstrate such hijacking attack on call forwarding setup.

To setup the call forwarding for a Gizmo phone number, the Gizmo subscriber dials `611` from his/her Gizmo soft phone to begin a call forwarding setup session. The Gizmo caller will be prompted to input the call forwarding number after the session to `611` has been established. Similar to the Vonage RTP server, the Gizmo RTP server will acknowledge the received call forwarding number and ask the Gizmo caller for confirmation. Once the Gizmo caller confirms the number, the call forwarding will take effect immediately.

Assume the victim uses Gizmo soft phone 1, the attacker uses Gizmo soft phone 2, and the MITM is in between the Gizmo soft phone 1 and Gizmo SIP, RTP servers. The MITM could let the attacker at Gizmo soft phone 2 hijack the call forwarding setup session between Gizmo soft phone 1 and Gizmo RTP server and configure the call forwarding of Gizmo soft phone 1. At the same time, the victim at Gizmo soft phone 1 will hear a bogus voice message: `the number you are trying to reach is busy`. This would make the victim think that the call forwarding setup server is busy and the call forwarding has not been setup. Figure 7 shows the SIP and RTP message flows of the hijacking of the Gizmo call forwarding setup session.

First, the attacker at Gizmo phone 2 calls `611`, and establishes a session with the Gizmo RTP server. Messages `(1)` `(2)` and `(3)` show the call setup sequence between Gizmo soft phone 2 and the Gizmo SIP server. Then the Gizmo RTP server will send Gizmo soft phone 2 voice prompt in

RTP (represented by message `(4) Prompt #1`). At the same time, the Gizmo soft phone 2 will start sending RTP stream to the negotiated UDP port (6824) at the Gizmo RTP server. The MITM temporarily blocks the RTP stream from the Gizmo soft phone 2 (represented by message `(5) RTP Stream`).

We notice that Gizmo soft phone 2 and the Gizmo RTP server has established some SSL/TLS connection during the call establishment phase, which appears to be some secure out-of-band management channel. The MITM does not block the SSL/TLS connection between them. The purpose of establishing the session between Gizmo phone 2 and the Gizmo RTP server is to facilitate the quick hijacking of the `611` call session between Gizmo soft phone 1 and the Gizmo RTP server. In theory, we can establish the session between Gizmo phone 2 and the Gizmo RTP server on the fly, but this will incur some extra delay in the call hijacking.

Now once the victim calls `611` from Gizmo soft phone 1, Gizmo soft phone 1 will establish a separate `611` call session with the Gizmo server as shown in messages `(6)`, `(7)` and `(8)`. To hijack the established `611` call session between Gizmo soft phone 1 and the Gizmo RTP server, the MITM first sends Gizmo soft phone 1 some bogus voice message in RTP: `the number you are trying to reach is busy` (shown as message `(9) Fake Server BUSY Message`). After the victim caller at Gizmo soft phone 1 hangs up, Gizmo soft phone 1 will send SIP `BYE` and RTCP `BYE` messages to the Gizmo SIP and RTP servers respectively. To keep the Gizmo server thinking that its session with Gizmo soft phone 1 is alive, the MITM now blocks all the traffic from Gizmo soft phone 1 to the Gizmo server (as shown in message `(10) BYE, RTCP BYE`) and remembers the UDP port number (6454) the Gizmo RTP server uses for session with Gizmo soft phone 1.

At the same time, the Gizmo server sends voice prompt (message `(11) Prompt #2`) to Gizmo soft phone 1. Now the MITM diverts all the RTP traffic from the Gizmo RTP server to Gizmo soft phone 1 (represented by message `(11) Prompt #2`) to Gizmo soft phone 2 (represented by message `(12) Prompt #2`), and diverts all the traffic from Gizmo soft phone 2 to UDP port 6824 (represented by message `(13) RTP Stream`) to UDP port 6454 (represented by message `(14) RTP Stream`) at the Gizmo RTP server. This would allow the attacker at Gizmo soft phone 2 impersonate the victim caller at Gizmo soft phone 1 and freely setup any call forwarding number for the victim at Gizmo soft phone 1. The attacker at Gizmo soft phone 2 can terminate the hijacked `611` call forwarding setup session after setting up any call forwarding number he/she has chosen.

We have experimented the above hijacking attack on the Gizmo call forwarding setup with our Gizmo VoIP accounts, and we have been able to hijack the call forwarding setup session for our Gizmo phone number 1 and configure the call forwarding to an international phone number `011-44-xxx-xxx-1284` from our Gizmo phone number 2. As a result, subsequent incoming calls to our Gizmo phone number 1 have been transparently forwarded to the international phone number `011-44-xxx-xxx-1284`.

5. IMPLICATIONS OF UNAUTHORIZED CALL DIVERSION

In section 4, we have empirically demonstrated that a MITM could detour or redirect any selected Vonage and AT&T VoIP calls via or to anywhere on the Internet. In addition, the MITM could manipulate and hijack the call forwarding setup of selected Vonage and Gizmo SIP subscribers such that the attacker can control where the calls to the victims will be forwarded to. All these call diversion attacks essentially violate the VoIP users' basic trust that their calls will reach the intended callees only. Furthermore, such a call diversion capability enables the attacker to launch the voice pharming attack against targeted VoIP callers, where the selected VoIP calls are transparently transferred to the bogus IVR or representative even if the callers have dialed correct phone numbers. In this case, the victim callers have no easy way to tell if they have reached the bogus IVR or representative. Therefore, even the most cautious callers could be tricked into giving out their credentials (e.g., SSN, credit card number, PIN) to the adversary. Such a voice pharming attack, enabled by the unauthorized call diversion, could indeed shake the long time trust that the general public have in voice communication.

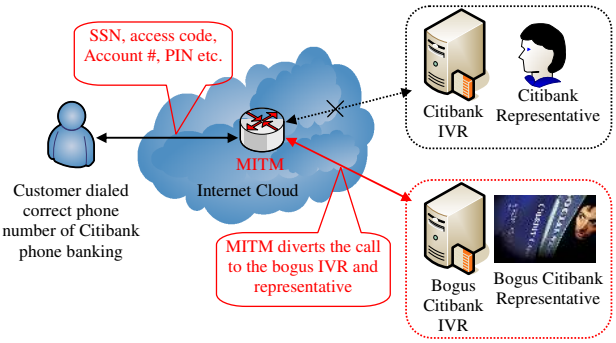


Figure 8: Hypothetical Voice Pharming Attack

5.1 Hypothetical Voice Pharming Attack

Citibank provides a phone banking service which allows its customers to have checks issued and paid to anyone by calling Citibank. Specifically, when a customer dials the Citibank phone banking phone number (1-800-374-9700), the IVR will prompt the caller to speak or enter his/her 9-digit SSN or personal taxpayer identification number. Then the IVR will ask for the telephone access code before allowing the caller to choose the available service options. After choosing the bill payment option, the caller will be connected to a Citibank service representative. To authenticate the caller, the service representative usually asks a few questions about the following information: (1) *debit card number*, (2) *checking account number*, (3) *phone PIN*, (4) *mother's maiden name*, (5) *the state on which the account was opened* and (6) *personal full name*. If the caller correctly answers the questions, the service representative would issue checks paying to anyone at any address the caller wants. One coauthor of this paper has successfully had one check issued, mailed and paid to another coauthor via Citibank phone banking.

Figure 8 illustrates a hypothetical voice pharming attack against Citibank phone banking. In order to launch voice pharming attack, the attacker needs to 1) setup a bogus IVR that sounds exactly the same as the real IVR; 2) redirect the calls toward Citibank phone banking to the bogus IVR and/or a phone the attacker uses. Setting up a bogus IVR is quite straight forward with VoIP technology. For example, the attacker could simply call the real Citibank IVR

via VoIP and record all the prompts as RTP traces. Then the attacker could construct the bogus IVR by replaying the collected RTP traces. Such a bogus IVR would have exactly the same voice as that of the real IVR. Now suppose the MITM is in a place (e.g, gateway, wireless router, firewall) that can intercept VoIP traffic, then it can check if there is any call toward any number of targeted financial institutions (e.g., 1-800-374-9700 of Citibank phone banking). By using the real-time call redirection attack described in section 4.2, the attacker could transparently divert the call to his bogus Citibank IVR. In addition, the attacker could pretend to be a Citibank service representative asking the caller the same questions (e.g, debit card number, mother's maiden name). Since the caller has dialed the correct phone number and has heard exactly the same voice menu, he/she simply has no way to tell if he/she is talking to a bogus IVR. Given that a bank customer usually does not know the bank representative personally, he/she can not tell if he/she is talking to a real bank representative or a bogus one. Therefore, voice pharming could let the attacker obtain all the information needed to impersonate the victim caller and gain financially (e.g., pay bill at the victim's expense).

6. MITIGATION STRATEGIES

The root cause of the VoIP vulnerabilities (e.g., unauthorized call diversion) we have demonstrated is the lack of appropriate protection of the SIP messages and RTP traffic between the VoIP servers and the SIP phones. For example, the SIP specification [40] does not require the UAs (i.e., SIP phone) to support any hop-by-hop encryption. The mandatary SIP digest authentication only applies to two SIP messages (i.e., `INVITE` and `200 OK`) from the SIP phone to the SIP server. Furthermore, the SIP digest authentication only covers a few fields of SIP messages and leave many important fields (e.g., `request-URI`, `From`, SDP part) unprotected. This lack of integrity protection makes it difficult to detect any unauthorized modification of the SIP message and RTP traffic.

The key to mitigate the existing VoIP vulnerabilities is to ensure the integrity and authenticity of the SIP messages and RTP traffic between the appropriate VoIP servers and the SIP phone. This can be achieved by encrypting and/or authenticating appropriate fields of appropriate SIP messages and RTP traffic. However, protecting the integrity and authenticity of SIP is not trivial due to the special requirements and needs of the SIP protocol. For example, SIP requires certain fields (e.g., `request-URI`, `Via`) in the SIP messages to be visible to all intermediate SIP proxies for routing purpose. During the routing of SIP messages, some intermediate SIP proxies may need to change the `request-URI` field or add new `Via` field to the SIP message. All these make it infeasible to protect the SIP messages from end-to-end. Therefore, the integrity and authenticity of SIP messages have to be protected hop-by-hop.

While the attacker could, in theory, launch the call diversion (as well as the voice pharming) attacks from any hop along the path of VoIP traffic, it is easier for the attacker to launch the attack from the link between the victims' VoIP phones and their next hop VoIP servers (e.g., SIP proxy, RTP server). Therefore, it would be very helpful to fully protect the edge link of the VoIP path by enforcing hop-by-hop encryption between the VoIP phones and next hop VoIP servers. Specifically, enforcing SSL or TLS between the VoIP phones and the next hop VoIP servers would make it much more difficult for the attacker to launch the unauthorized call diversion and voice pharming attacks.

However, hop-by-hop encryption (e.g., SSL or TLS [7]) or authentication may still be vulnerable to the MITM attack [8, 25] unless both the communicating parties can reliably authenticate each other. While PKI (public key infrastructure) is able to provide strong mutual authentication, it is not clear if it is feasible to require every VoIP phone and server to support PKI.

7. RELATED WORKS

Most existing works on VoIP security are on the defense side. Arkko et al [3] proposed a new way for negotiating the security mechanisms (e.g., IPSec [19] and TLS [7] HTTP authentication [12]) used between a SIP UA and its next-hop SIP entity. Salsano et al [41] evaluated the performance of SIP digest authentication and showed that the processing overhead for implementing SIP digest authentication ranges from 77% to 156%. McGann and Sicker [26] analyzed several VoIP security tools and they showed that there exists large gap between known VoIP security vulnerabilities and the tool's detection capability.

Reynolds and Goshal [38] proposed a multi-layered protection against flooding type of denial-of-service (DoS) attack on VoIP network. They described a DoS detection method based on measuring the difference between the numbers of attempted connection establishments and the number of completed handshakes. Wu et al [57] proposed a stateful, cross protocol VoIP intrusion detection system called SCIDIVE, which detects BYE-attack via identification of the orphan RTP flows. If the attacker sends a `BYE` message to only one end of an established VoIP call, SCIDIVE is able to detect it since there is some orphan RTP flow left alive. However, SCIDIVE is not able to detect the case where the attacker sends `BYE` messages to both ends of the SIP session. Sengar et al. [49, 48] extended the cross protocol VoIP intrusion detection method by using Hellinger distance to detect flooding DoS attacks that may use a combination of SIP, RTP and IP streams. Specifically, the learning phase of their detection method learns the normal traffic pattern and the detection phase uses the Hellinger distance to detect abnormal deviations from the normal behaviors. However, none of these VoIP defense mechanisms is able to detect or prevent the unauthorized call diversion attacks we have demonstrated in this paper.

Geneiatakis et al. [14] looked the several potential security problems in SIP and listed several potential threats (e.g., DoS attack) to SIP and their remedies. However, they have not considered any of the transparent call diversion attacks we have demonstrated in this paper.

Zhang et al. [58] recently demonstrated that current VoIP users are vulnerable to billing attacks, which would allow the attack to incur overcharges to the victims on calls they have made.

Enck et al. [10] studied the security ramification of SMS (Short Messaging Services) of cell phone, and they showed that SMS of cell phone could be exploited to launch DoS attack on cellular networks. They suggested a number of methods to avoid such attacks, such as limiting message acceptance rates per phone number, separating voice and text data streams, resource provisioning, and making active phone lists difficult to obtain freely on the Internet.

Similarly, Racic et al. [34] showed that Multimedia Messaging Services (MMS) of cell phones can be exploited to surreptitiously drain cell phone's battery and they suggested using message and server authentication, information hiding at WAP gateway, MMS message filtering and improved PDP context management as mitigating techniques.

8. CONCLUSION

In this paper, we have empirically investigated the trust issues of currently deployed VoIP systems and their implications to the VoIP users. Our experiments show that leading deployed VoIP services (e.g., Vonage, AT&T, Gizmo) are vulnerable to unauthorized call diversion, 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: the voice pharming attack, which could trick the most cautious VoIP callers into giving out sensitive information (SSN, credit card number) to the adversary. Our results show that existing VoIP users are susceptible to identify theft and financial lost due to the lack of the trust of currently deployed VoIP systems.

To prevent such authorized call diversion and voice pharming attacks, all segments of the VoIP path need to be protected. Our experience shows that enforcing SSL or TLS between all the VoIP phones and their VoIP servers would make it much more difficult for the attacker to launch the unauthorized call diversion and voice pharming attacks.

Acknowledgement

The authors would like to thank the anonymous reviewers for their insightful comments that helped to improve the presentation of this paper. This work was partially supported by NSF Grant CNS-0524286.

9. REFERENCES

[1] F. Andreasen and B. Foster. Media Gateway Control Protocol (MGCP) Version 1.0. *RFC 3435, IETF*, January 2003.

[2] Anti-Phishing Working Group. Consumer Advice: How to Avoid Phishing Scams. http://www.antiphishing.org/consumer_recs.html

[3] J. Arkko, V. Torvinen, G. Camarillo, A. Niemi and T. Haukka. Security Mechanism Agreement for the Session Initiation Protocol (SIP). *RFC 3329, IETF*, January 2003.

[4] ABI Study Predicts 267 Million Residential VoIP Subscribers Worldwide by 2012. P. Barnard. http://www.tmcnet.com/voip/ip-communications/articles/4824-abi-study-predicts-267-million-residential-voip-subscribers.htm.

[5] S. A. Baset and H. Schulzrinne. An Analysis of the Skype Peer-to-Peer Internel Telephony Protocol. Columbia Technical Report CUCS-039-04, December 2004

[6] Report: Cable VoIP Market Set to Surge. M. Perez. http://www.voip-news.com/news/cable-voip-market-report-080406/.

[7] T. Dierks and C. Allen. The TLS Protocol. *RFC 2246, IETF*, January 1999

[8] Dsniff. http://www.monkey.org/ dugsong/dsniff/

[9] John E. Dunn. Expert scares world with VoIP hacking proof. http://www.techworld.com/security/news/index.cfm?newsid=10736

[10] H. Enck, P. Traynor, P. McDaniel and T. L. Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedgins of the 12th ACM Conference on Computer and Communications Security (CCS 2005)*, November 2005.

[11] Enterprise VoIP adoption in North America will more than double in 2010. http://www.voip-news.com/press-releases/enterprise-adoption-america-forecast-projection-021407/.

[12] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen and L. Stewart. HTTP Authentication: Basic and Digest Access Authentication. *RFC 2617, IETF*, June 1999.

[13] Sharon Gaudin. Pharming Attack Slams 65 Financial Targets. http://www.informationweek.com/showArticle.jhtml?articleID=197008230

[14] D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis and S. Gritzalis. SIP Security Mechanisms: A State-of-the-art Review. In *the Proceedings of the Fifth International Network Conference (INC 2005)*, pages 147–155, July 2005, Samos, Greece,

[15] Gizmo. http://gizmo5.com

[16] M. Handley and V. Jacobson. SDP: Session Description Protocol. *RFC 2327, IETF*, April 1998.

[17] Identity Theft Resource Center. http://www.idtheftcenter.org/

[18] R. Jaques. Cyber-Criminals Switch to VoIP 'Vishing'. http://www.vnunet.com/vnunet/news/2160004/cyber-criminals-talk-voip.

[19] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. *RFC 2401, IETF*, November 1998.

[20] Jeremy Kirk. 'Pharming' attack hits 50 banks. http://www.techworld.com/security/news/index.cfm?newsid=8102

[21] P. D. Kretkowski. VoIP: How Free Can It Be? http://www.voip-news.com/feature/voip-how-free-can-be-120307/

[22] Andrew Lavallee. Email Scammers Try New Bait in Voice 'Phishing'. http://www.post-gazette.com/pg/06198/706477-96.stm.

[23] Hank Layton. Phone Scammers Targeting Veterans, Patriot Guard. http://www.leavenworthtimes.com/articles/2008/01/07/news/news06.txt

[24] Jim Louderback. Security Holes Make VoIP a Risky Business. http://www.eweek.com/article2/0,1759,1591127,00.asp#talkback

[25] Man-In-The-Middle Attack. http://en.wikipedia.org/wiki/Man_in_the_middle_attack

[26] S. McGann and D. C. Sicker. An analysis of Security Threats and Tools in SIP-Based VoIP Systems. Second VoIP Security Workshop, 2005.

[27] G. Me, D. Verdone. An Overview of Some Techniques to Exploit VoIP over WLAN In *Proceedings of 2006 International Conference on Digital Telecommunications (ICDT 2006)*, August 2006.

[28] R. Naraine. Voice Phishers Dialing for PayPal Dollars. http://www.eweek.com/article2/0,1895,1985966,00.asp.

[29] Nuance Speaker Verification Delivers Biometric Security without Expensive Equipment or Special Hardware. http://www.nuance.com/news/pressreleases/2006/20060803_biometric.asp.

[30] J. Peterson. A Privacy Mechanism for the Session Initiation Protocol (SIP). *RFC 3323, IETF*, November 2002.

[31] Pharming. URL. http://en.wikipedia.org/wiki/Pharming

[32] Phishing. URL. http://en.wikipedia.org/wiki/Phishing

[33] B. Prince. Experts: Enterprises Must Focus on VOIP Security. http://www.eweek.com/article2/0,1895,2154629,00.asp

[34] R. Racic, D. Ma amd H. Chen. Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery. In *Proceedgins of the Second International Conference on Security and Privacy in Communication Networks (Securecomm 2006)*, August 2006.

[35] The Radicati Group. Corporate VoIP Market, 2005-2009. http://www.peterdehaas.net/2005/09/corporate_voip_.html

[36] B. Ramsdell, Editor. S/MIME Version 3 Message Specification. *RFC 2633, IETF*, June 1999.

[37] ITU-T Recommendation H.323v.4 Packet-based multimedia communications systems. November 2000.

[38] B. Reynolds and D. Ghosal. Secure IP Telephony Using Multi-layered Protection In *Proceedgins of the 2003 Network and Distributed System Security Symposium (NDSS 2003)*, Feburary 2003.

[39] R. Rivest. The MD5 Message-Digest Algorithm. *RFC 1321, IETF*, April 1992.

[40] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M Handley and E. Schooler. SIP: Session Initiation Protocol. *RFC 3261, IETF*, June 2002.

[41] S. Salsano, L. Veltri, D. Papalilo. SIP Security Issues: the SIP Authentication Procedure and Its Processing Load. In *IEEE Network*, 16(6), Pages 38–44, 2002.

[42] H. Schulzrinne. Internet Telephony. In *Practical Handbook of Internet Computing*, CRC, 2004

[43] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. *RFC 1889, IETF*, January 1996.

[44] H. Schulzrinne and J. Rosenberg. A Comparison of SIP and H.323 for Internet Telephony. In *Proceedings of International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV 1998)*, pages 83–86, Cambridge, England, July 1998.

[45] H. Schulzrinne and J. Rosenberg. Signaling for Internet Telephony. In *Proceedings of The 6th IEEE International Conference on Network Protocols (ICNP'98)*, October 1998.

[46] Secure Computing Corporation. Secure Computing Warns of New VoIP Based Phishing Scam; Credit Card and Banking Customers Warned to Be on Guard Against ID Theft By Phone. http://www.securecomputing.com/press_releases.cfm?ID=879984

[47] Larry Seltzer. Don't Believe That Lying Telephone. http://www.eweek.com/article2/0,1759,2004426,00.asp

[48] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia. Fast Detection of Denial of Service Attacks on IP Telephony. In *Proceedings of the 14th IEEE International Workshop on Quality of Service (IWQoS 2006)*, June 2006.

[49] H. Sengar, D. Wijesekera, H. Wang, and S. Jajodia. VoIP Intrusion Detection Through Interacting Protocol State Machines. In *Proceedgins of the 2006 International Conference on Dependable Systems and Networks (DSN 2006)*, June 2006.

[50] Skype - the Global Internet Telephony Company. http://www.skype.org

[51] Radu State. Remote eavesdropping with SIP Phone GXV-3000. http://www.voipsa.org/pipermail/voipsec_voipsa.org/2007-August/002424.html

[52] Fueled by VoIP Adoption, PBX Revenue to Exceed $7.5 Billion in 2011. J. Torres. http://ipcommunications.tmcnet.com/hot-topics/gateway/articles/4738-fueled-voip-adoption-pbx-revenue-exceed-75-billion.htm

[53] Bob Violino. After Phishing? Pharming! http://www.csoonline.com/read/100105/pharm.html

[54] Vishing. http://en.wikipedia.org/wiki/Vishing

[55] Vonage Is Still #1 In VoIP Market Share. http://www.voipnow.org/2006/07/vonage_is_still.html.

[56] X. Wang, S. Chen, and S. Jajodia. Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS 2005)*, pages 81–91, Alexandra, VA, November 2005. ACM.

[57] Y. Wu, S. Bagchi, S. Garg, N. Singh. SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments In *Proceedgins of the 2004 International Conference on Dependable Systems and Networks (DSN 2004)*, Pages 433 – 442, July 2004.

[58] R. Zhang, X. Wang, X. Yang, X. Jiang. Billing Attacks on SIP-Based VoIP Systems In *Proceedings of the 1st USENIX Workshop on Offensive Technologies (WOOT 2007)*, August 2007.