Prevention of Toll Frauds against IP-PBX

James Yu
DePaul University
Chicago, IL 60604

Abstract – This research is motivated by a toll fraud case against an enterprise IP-PBX, and further investigation of an asterisk server log shows a growing threat of VoIP attacks against enterprise IP-PBX. Although the Session Initiation Protocol (SIP) has a comprehensive security measures, its implementations are optional and VoIP administrators could be confused about which security measures are required for their specific environments. This study identifies several vulnerabilities in the VoIP implementation, and hackers could explore the vulnerabilities to launch various security attacks. Based on the analysis of the log data and the protocol, this study proposes several counter measures to prevent the security attacks for different VoIP implementations.

Key-Words —VoIP, SIP, Registration Hijacking, Toll Fraud, PRS

I. INTRODUCTION

THE ubiquity of Internet Protocol (IP) and economics of IP-PBX make Voice over IP (VoIP) a cost-effective alternative to the legacy PBX or key system. An Infonetics report estimated the service market of VoIP is $68B in 2013, and expected to grow to $88B in 2018 [1]. The growth of IP-PBX seats (end-user ports) is estimated at 35% annually. However, there is also an increase in the phone fraud. A 2011 survey shows that phone fraud was estimated at $4.96B which is more than double the credit card fraud $2.40B [2]. In the same report, toll fraud is a major fraud category where hackers explore the vulnerability of the system for financial gain.

The increased use of IP-PBX in the enterprise environment makes it a new target of security attacks. In the taxonomy of VoIP security, researchers classify security requirements as follows [3][4][5]:

- *Confidentiality* – the communication is between the sender and the intended receiver. The security measure is to protect and prevent eavesdropping of the communication.
- *Integrity* – the content of the communication does not change during the communication. The security measure is to protect both signaling traffic and bearer traffic. In the case of bearer traffic, it needs to protect both the header and payload content.
- *Authentication* –both the caller and the callee are authentic users as they are claimed in the call messages and content. Authentication is assured by the server.
- *Availability* – this is the case of protecting against Denial of Service (DoS) attack.

Toll Fraud is an issue in the category of *authentication* where a hacker falsifies the caller ID and makes a call from the caller system for financial gains. Researches on toll fraud can be classified as fraud detection and fraud prevention. An example of fraud detection is to study real-time Call Detail Record (CDR) and identify anomalies in CDR [6]. This research is from a network perspective on fraud prevention. A major incentive of toll fraud by hackers is for immediate financial gain. Hackers explore the potential IP-PBX vulnerabilities and try to access it to make long distance (toll) calls. We can further categorize toll frauds into two categories:

1. The first category is that hackers gain access to enterprise IP-PBX and use it as a gateway for commercial use. A SANS report published a case where a hacker created several phone companies and route toll calls of his customers to multiple *hacked* IP-PBX. He made over $1M by charging his customers before being caught [7].
2. The 2nd category is the fraudulent use of Premium Rate Sharing Service (PRS). In the U.S., this is the 900- calls where each call is charged a high premium and the callee (receiver) gets a share of the service premium. Due to many frauds of the 900- calls, Federal Communication Commission (FCC) has a strict regulation. As a result, the frauds of 900- calls have been significantly reduced. However, the case of International Premium Rate Sharing (IPRS) is a new threat of phone fraud.

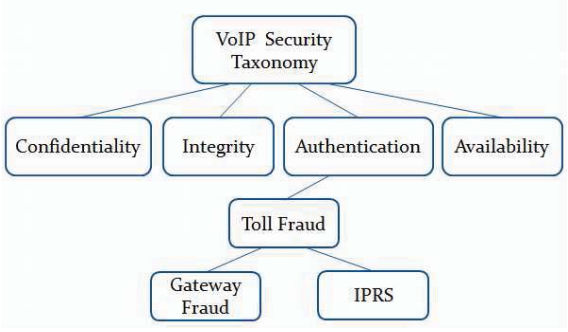

Figure 1. Taxonomy of VoIP Security

An example of the phone bill of IPRS fraud is given below:

Itemized Phone Bill

		Time	Charge $$
2522160333	07/20/11 9:49 p Somalia	19.8	16.6657
2522160333	07/20/11 10:15 p Somalia	16.8	14.1406
2522160333	07/20/11 10:32 p Somalia	17.4	14.6456
2522160333	07/20/11 10:49 p Somalia	20.7	17.4232
2522160333	07/20/11 11:10 p Somalia	20.7	17.4232
2522160333	07/20/11 11:31 p Somalia	11.9	10.0162
2522160333	07/20/11 11:44 p Somalia	16.6	13.9722

This is the case that a hacker intruded into an enterprise IP-PBX, and then made continuous international calls to many African countires (one of them is Somalia.) It is apparent that the hacker had a program to automatically generate calls, and each call lasted for 10-20 minutes. The fraud case started at 06:00pm and continued until 06:00am next morning. Because the calls were made at night, the users were not aware of this fraud case. The hacker then tried it again the next day. It took several days for the phone compnay to identify the fraud and cut the phone service. However, the company already accumulated a phone bill of thousands of dollars. After the first fraud case, the company implemented a strict dialing plan to prevent international calls. Any 011 prefix dialing was blocked. However, the North American Numbering Plan (NANP) includes many Carribbean countires which follow the NXX-XXX-XXXX dialing plan. The dialing plan to any NANP country is the same as a US domestic call. As a result, this company was hacked again with another large phone bill to a Carribbean country.

The purpose of this research is to study the vulnerability of VoIP implementations, and develop protective measures to prevent toll fraud against IP-PBX in an enteprise environment.

II. VoIP Networks

An example of IP-PBX for an enterprise environment is illustrated in Figure 2.

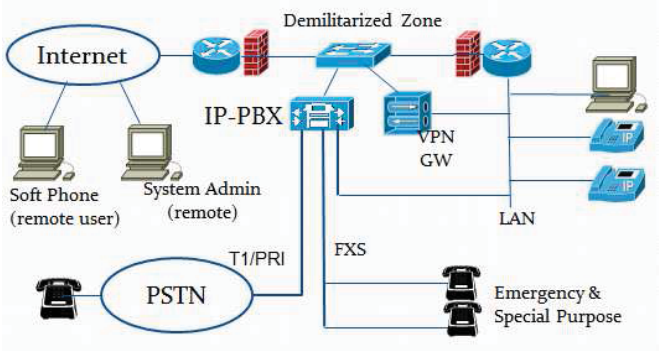

Figure 2. IP-PBX for an Enterprise environment.

An IP-PBX has the functions of both Session Initiation Protocol (SIP) proxy and gateway, and it usually has the four physical interfaces:

1. LAN ports – a LAN port connects to an Ethernet switch which connects to the enterprise Local Area Network (LAN). IP phones and workstation with soft phone are connected to the LAN.
2. WAN (Internet) port – a WAN port connects to the public Internet. The purpose of WAN port is to support remote clients and remote system administration. For security protection, the WAN connection terminates at the demilitarized s zone (DMZ) which is protected by a firewall.
3. Foreign Exchange Subscriber (FXS) lines – An IP-PBX usually has one to four FXS ports. This is to support emergency calls (e.g., E911) or special use (such as Fax).
4. PSTN interface – an IP-PBX may use either Foreign-Exchange-Office (FXO) lines or T1/E1 lines to connect to the Public Switch Telephone System (PSTN). In a typical office environment, we usually follow an engineering rule of 1:8 where one FXO line serves up to 8 users. For example, a small office of 30 staff would subscribe to four FXO lines. If a company needs more than 10 FXO lines, a T1 would be more economical. A T1/PRI (Primary Rate Interface) trunk has 23 B- channels and could support an office up to 184 users.

VoIP is an *application* on IP-based data network, and all security measures of IP network are applicable to VoIP [8]. This is the reason that IP-PBX needs to be positioned at DMZ and relies on firewall to protect typical threats against data network. We also observe a growing trend toward *all* IP networks in an enterprise environment, which is to use SIP trunking to replace FXO/T1 connections to PSTN. The SIP trunking configuration is illustrated in Figure 3.

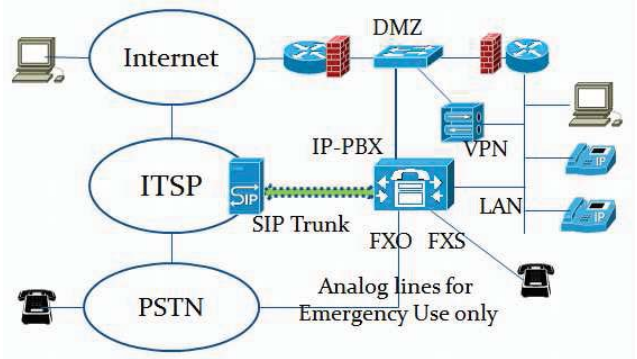

Figure 3. SIP Trunking Configuration

A SIP trunk is not a physical connection, but a secured IP tunnel from the enterprise to an Internet Telephony Service Provider (ITSP). Both signaling and bearer traffic is sent on this IP tunnel to the ITSP which routes the bearer traffic to PSTN. The pricing of each SIP trunk is comparable to an FXO line. Some of the advantages of SIP trunk are (a) simpler device configuration, (b) more scalable for service growth, and (c) lower toll cost. A disadvantage is service availability and reliability of emergency calls (e.g., E911).

The objective of security protection is to allow *normal* use of the network and to prevent *misuse* of the network. The scope of normal use includes the following:

1. Internal users (LAN side) can make and receive calls internally, and also make and receive calls to and from PSTN.
2. Remote users (Internet side) have the same capability as internal users, including making and receiving calls to and from PSTN. One important *built-in* VoIP feature is global *voice* Virtual Private Network (VPN). A user can keep his/her local phone number regardless of his/her physical location in the world.
3. Administrator have the capability to monitor the system either from the LAN side or through the public Internet.

The security measure against toll fraud should support *normal* use of phone services and protect *fraudlent* use from both internal and external hackers.

III. Hacking Scenarios and Prevention

In the legacy PBX system, toll frauds are usually from stolen pass codes that allow unauthorized access to PBX for free toll calls. If an IP-PBX has an interface to the Internet with a public IP address, it opens the door for a new wave of hacker attacks.

A. *Hacking and Intrusion Attempt*

In our VoIP lab, we have installed multiple asterisk servers for our VoIP course [9], and one of the servers has a public IP address for students to make proxy-based SIP calls. About half of our students are distance learning students, so the lab environment is accessible to these students via the public Internet. The server does not have PSTN interfaces, so it would not have an issue with toll fraud. To investigate the potential threat of the VoIP attack, we studied the Asterisk log and noticed an alarming attacking rate of the following pattern:

```
[Mar 14 03:00:25]Registration from '"7121" <sip:7121@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:00:36]Registration from '"7957" <sip:7957@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:00:47]Registration from '"7957" <sip:7957@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:00:59]Registration from '"7955" <sip:7955@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:01:11]Registration from '"7955" <sip:7955@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:01:24]Registration from '"7937" <sip:7937@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:01:37]Registration from '"7937" <sip:7937@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:01:49]Registration from '"7734" <sip:7734@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:01:58]Registration from '"7734" <sip:7734@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:02:11]Registration from '"7774" <sip:7774@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:02:22]Registration from '"7774" <sip:7774@140.192.40.4>' failed for '212.129.38.252
[Mar 14 03:05:24]Registration from '"7633" <sip:7633@140.192.40.4>' failed for '212.129.38.252'
[Mar 14 03:05:24]Registration from '"7633" <sip:7633@140.192.40.4>' failed for '212.129.38.252'
[Mar 14 03:05:24]Registration from '"7633" <sip:7633@140.192.40.4>' failed for '212.129.38.252'
[Mar 14 03:05:24]Registration from '"7633" <sip:7633@140.192.40.4>' failed for '212.129.38.252'
[Mar 14 03:05:24]Registration from '"7633" <sip:7633@140.192.40.4>' failed for '212.129.38.252'
[Mar 14 03:05:24]Registration from '"7633" <sip:7633@140.192.40.4>' failed for '212.129.38.252'
[Mar 14 03:05:24]Registration from '"7633" <sip:7633@140.192.40.4>' failed for '212.129.38.252'
[Mar 14 03:05:24]Registration from '"7633" <sip:7633@140.192.40.4>' failed for '212.129.38.252'
[Mar 14 03:05:24]Registration from '"7633" <sip:7633@140.192.40.4>' failed for '212.129.38.252'
```

Figure 4. Asterisk Log of VoIP Intrusion Attempt

The log data shows that hackers first check the open SIP port (UDP port 5060). When they find a VoIP server with this port open, they will try every possible extension to explore the VoIP system and they will also try many passwords for each extension. Our Asterisk server is available during the academic quarter only, and its Internet connection is disabled after the class is over. The attacking rates of the fall quarter of 2014 and the winter quarter of 2015 are illustrated in Figures 5a and 5b. Note that we experienced 8.67 million intrusion attempts in one day (03/14/2015) (Figure 5b). Although these are all failed attempts, the amount of hacker traffic affects the normal operation of the server and our network. This intrusion data shows a more serious case (many more intrusion attempts) than other researches which used a honeypot approach to trap and analyze the attacking data [10][11].

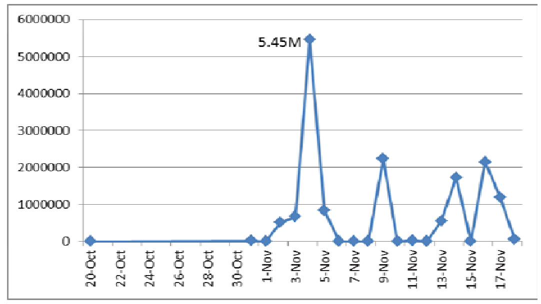

Figure 5a. Daily SIP Intrusion Attempts in Fall 2014

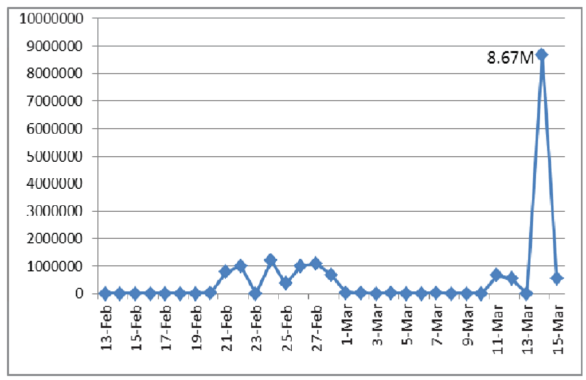

Figure 5b. Daily SIP Intrusion Attempts in Winter 2015

We also checked the source location of IP addresses of those SIP intrusion attempts, and the results are given in Figure 6.

```
Attempts  IP               Country

 7938129  62.210.245.11    FR
 1795703  195.154.38.225   FR
 1784133  195.154.42.18    FR
 1575740  195.154.41.250   FR
 1303322  212.129.38.252   FR
 1227472  212.83.128.50    FR
 1009644  62.210.245.132   FR
   57656  209.126.100.162  US  MO    Saint Louis
   21344  195.154.38.97    FR
   19860  195.154.33.127   FR
   10573  85.25.214.254    DE
    1580  37.75.213.132    PS
```

Figure 6. SIP Intrusion Source in Winter 2015

From our analysis, we concluded that this is similar to Distributed Botnet attacks [12]. The hacker builds a botnet and recruits an army of bots from multiple sources. When the hacker finds a potential target, he/she will send SIP

registration requests to find a valid, unsecured phone number. If he/she finds one, his/her Command and Control Center will make hundreds of automated IPRS calls from which the hacker would share the premium.

B. SIP Registration and Session Hijacking

According of the SIP standard (RFC 3261), the password for SIP clients is optional. A SIP client (e.g., IP Phone) is first registered with a SIP proxy server. After the success of registration, the SIP client can make a call request via the INVITE message. The message flow of registration and call is captured in the wireshark packet trace as illustrated in Figure 7. Note that the call setup time (INIVTE to 180 Ringing) is

$$10.009 - 9.795 = 0.214 \text{ (sec)} = 214 \text{ ms}$$

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.106	140.192.40.4	SIP	Request: REGISTER
3	0.096954	140.192.40.4	192.168.0.106	SIP	Status: 200 OK (1
6	9.795298	192.168.0.106	140.192.40.4	SIP/SDP	Request: INVITE si
8	10.009022	140.192.40.4	192.168.0.106	SIP	Status: 180 Ringin
9	27.064595	140.192.40.4	192.168.0.106	SIP/SDP	Status: 183 Sessio
11	27.070765	140.192.40.4	192.168.0.106	SIP/SDP	Status: 200 OK |
13	27.105583	192.168.0.106	140.192.40.4	SIP	Request: ACK sip:2
555	32.536903	192.168.0.106	140.192.40.4	SIP	Request: BYE sip:2
557	32.567092	140.192.40.4	192.168.0.106	SIP	Status: 200 OK |
558	46.526187	192.168.0.106	140.192.40.4	SIP	Request: REGISTER
560	46.570758	140.192.40.4	192.168.0.106	SIP	Status: 200 OK (0

Figure 7. SIP Registration and Call Flow (no password)

If an IP-PBX is open to the public Internet and one of the phones (SIP client) is not password protected, a hacker can easily find this phone through exhaustive search. Also note that an *easy-to-guess* password is the same as no password because hackers will try hundreds of common-used passwords for each account.

C. SIP Authentication

To prevent the above attacking scenario, the SIP standard provides an authentication procedure. A password is provisioned for each SIP account and the password is configured on both the server and the client. The registration process and the call flow diagram are captured in the wireshark packet trace as illustrated in Figure 8. The highlighted messages are authenticated. Note that the call setup time (INVITE to 180 Ringing) is

$$(18.460 - 18.147) = 0.313 = 313 \text{ ms}$$

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.106	140.192.40.4	SIP	588	Request: REGISTER sip:140.192.40.4 (1 bi
3	0.032525	140.192.40.4	192.168.0.106	SIP	584	Status: 401 Unauthorized |
4	0.135334	192.168.0.106	140.192.40.4	SIP	742	Request: REGISTER sip:140.192.40.4 (1 bi
6	0.167877	140.192.40.4	192.168.0.106	SIP	631	Status: 200 OK (1 binding) |
11	18.147348	192.168.0.106	140.192.40.4	SIP/SDP	990	Request: INVITE sip:20370140.192.40.4 |
12	18.182377	140.192.40.4	192.168.0.106	SIP	597	Status: 407 Proxy Authentication Required
13	18.182781	192.168.0.106	140.192.40.4	SIP	364	Request: ACK sip:20370140.192.40.4 |
14	18.186305	192.168.0.106	140.192.40.4	SIP/SDP	1155	Request: INVITE sip:20370140.192.40.4 |
16	18.460265	140.192.40.4	192.168.0.106	SIP	531	Status: 180 Ringing |
18	39.749511	140.192.40.4	192.168.0.106	SIP/SDP	856	Status: 183 Session Progress |
21	39.760445	140.192.40.4	192.168.0.106	SIP/SDP	842	Status: 200 OK |
33	39.865245	192.168.0.106	140.192.40.4	SIP	634	Request: ACK sip:20370140.192.40.4 |
2105	60.470602	192.168.0.106	140.192.40.4	SIP	591	Request: SUBSCRIBE sip:20360140.192.40.4
2109	60.502533	140.192.40.4	192.168.0.106	SIP	585	Status: 401 Unauthorized |
2121	60.605349	192.168.0.106	140.192.40.4	SIP	750	Request: SUBSCRIBE sip:20360140.192.40.4
2516	64.540309	192.168.0.106	140.192.40.4	SIP	674	Request: BYE sip:20370140.192.40.4 |
2519	64.574150	140.192.40.4	192.168.0.106	SIP	523	Status: 200 OK |

Figure 8a. Caller Side (Wireshark Packet Trace)

No.	Time	Source	Destination	Protocol	Info
1	0.00000000	192.168.0.20	140.192.40.4	SIP	Request: REGISTER sip:140.
3	0.03128200	140.192.40.4	192.168.0.20	SIP	Status: 401 Unauthorized |
4	0.03843000	192.168.0.20	140.192.40.4	SIP	Request: REGISTER sip:140.
6	0.07162900	140.192.40.4	192.168.0.20	SIP	Status: 200 OK (1 bindin
11	16.8360960	140.192.40.4	192.168.0.20	SIP/SDP	Request: INVITE sip:2037@1
13	17.0105860	192.168.0.20	140.192.40.4	SIP	Status: 180 Ringing |
15	24.1985060	192.168.0.20	140.192.40.4	SIP/SDP	Status: 200 OK |
17	24.2291050	140.192.40.4	192.168.0.20	SIP	Request: ACK sip:2037@192.
868	32.7948650	140.192.40.4	192.168.0.20	SIP	Request: BYE sip:2037@192.
870	32.8391460	192.168.0.20	140.192.40.4	SIP	Status: 200 OK |

Figure 8b. Callee Side (Wireshark Packet Trace)

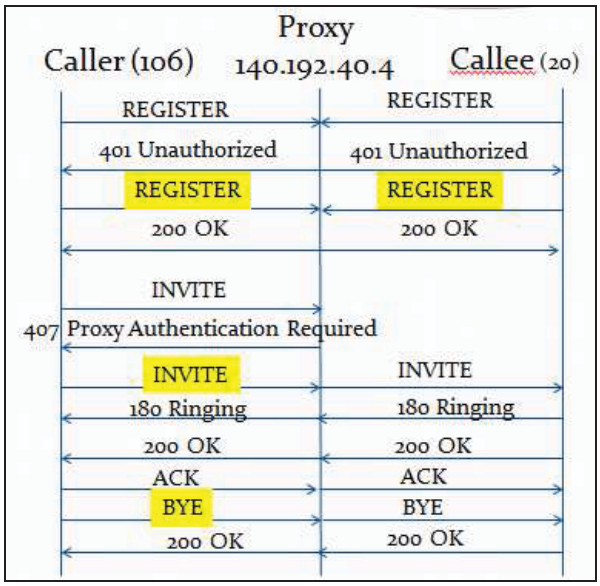

Figure 8c. SIP Registration and Call Flow

As llustrated in Figure 8, the authentication follows a *three-way* hand-shaking procedure for the registration process. The 1st REGISTER message from the client is a request, and the server responds with a challenge (401 Unauthorized). The client then resends the REGISTER message with a response to the challenge. The password is not sent in the authentication process, and the password is used to decrypt the challenge and to encrypt the response on the client side. There is a unique *nonce* value generated on the server for each challenge-response. It should also be noted that this registration process is repeated every 60 seconds as shown in Figure 8. The authentication process is also applied to each call. When a client makes a call request, it also uses the three-way hand-shaking process to authenticate each call request. The nonce value, generated on the server, is used as a challenge in the 407 Proxy Authentication Required message. This nonce value is used for the next INVITE message to authenticate the call.

It should be noted that this SIP authentication process is a one-way procedure. It is for the proxy server to authenticate the clients, but it does not support clients to authenticate the proxy server. In Figure 8, there is no authentication for any message on the callee side (except for registration). This one-way authentication has a potential issue of Denial of Service (DoS) attacks. If a call is terminated by the caller, the SIP BYE message is authenticated by the same nonce value of the original call. However, if a call is terminated by the callee, the SIP BYE message is not authenticated as illustrated in Figure 9.

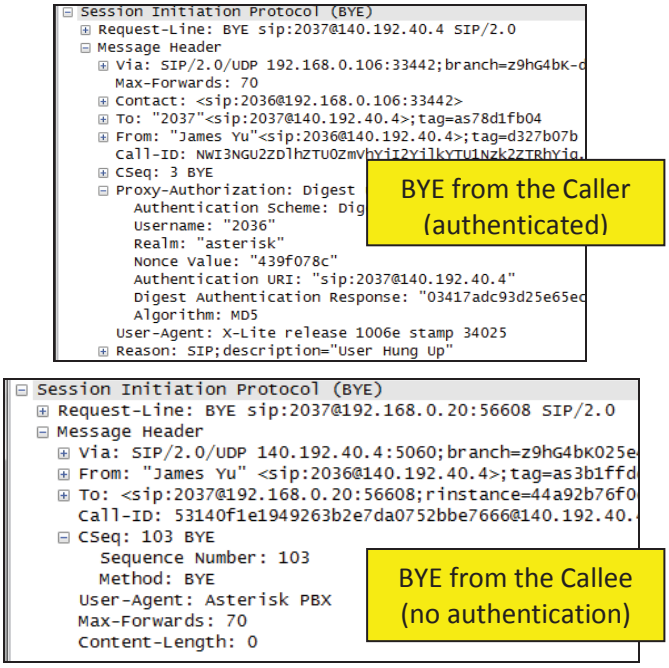

Figure 9. SIP BYE Message

Because this SIP messages on the callee side are not encrypted, a hacker could sniff the traffic from the network. The hacker could *impersonate* as a callee and send a BYE message to the proxy server. Without authentication, the proxy simply relays the BYE message to the caller and terminates the call. Abdelnur identified another vulnerability in SIP where an authenticated user could obtain credentials of other legitimate users and make fradulent calls from their accounts [13]. This is an example of internal hacking by legitimate users.

D. SIP over TLS

In the previous section, we identified three vulnerabilities of the SIP authentication process: (a) not a mutual authentication, (b) unauthorized call termination, and (c) weakness in protecting user credentials. These three issues could be addressed by SIP over Transport layer Security (TLS) which is also specified in RFC 3621 [15]. The procedure of SIP over TLS, aka as SIPS, is the same as HTTP over TLS, aka HTTPS. Shen and his colleagues did a thorough performance analysis of SIPS overhead [16]. According to their study, the most secured case of TLS mutual authentication would reduce the call capacity (calls per seconds) from 460 cps down to 60 cps. Although this reduction seems significant, a capacity of 60 cps is equivalent to 216,000 Busy Hour Calls (BHC). Assuming a user makes an average of four calls during *busy* hour, this capacity could support an enterprise of 54,000 users. Therefore, the performance issue is not a concern of using SIP over TLS.

IV. VoIP Security Protection

Given the severity of hacker attacks on the VoIP, our first recommendation is that if an IP-PBX has a direct connection to PSTN, the IP-PBX should not have a public IP address.[1] We recommend to move IP-PBX out of the DMZ and to put it behind the 2nd firewall as illustrated in Figure 10.

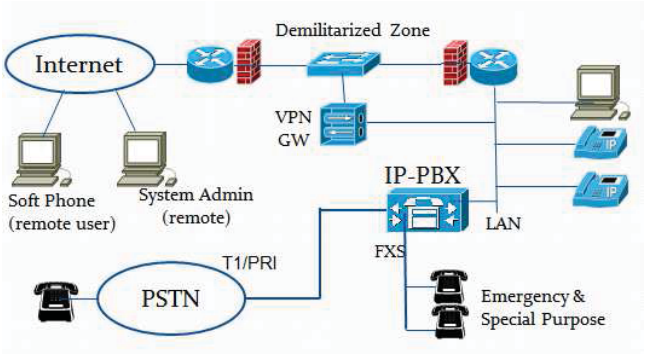

Figure 10. Secured IP-PBX for an Enterprise

Without a public IP address, external hackers cannot access the IP-PBX, and we prevent any threat of external intrusion attempts or attacks. However, we still need to support remote users and remote administration over the public Internet. Our recommendation is to require remote users to access the internal IP-PBX via IP-VPN. The protocol stacks of VoIP over IP-VPN are given in Figure 11.

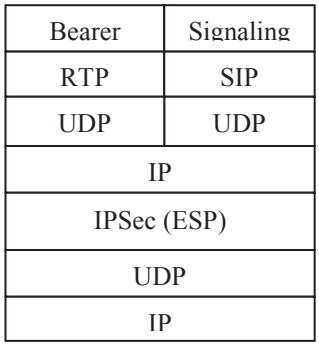

Figure 11. Protocol Stacks of VoIP over IP-VPN

Our lab test, which is based IPSec/ESP (Encapsulating Security Payload), shows that the performance overhead of ESP on the client is low, and the set up time (270 ms) is comparable to non-VPN cases. There is no performance overhead on IP-PBX as it does not *see* IP-VPN. A remote user over IP-VPN is the same as a local user from the IP-PBX perspective.

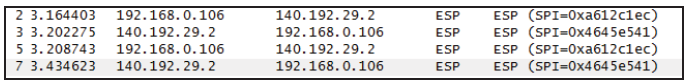

Figure 12. Encrypted SIP messages
(Invite, Status 407, Invite and180 Ringing)

We also recommend that all SIP clients must be password protected. This could be an administration issue to manually configure passwords on individual clients. Fortunately, most VoIP servers (including Asterisk) support the generation of client configuration files and

[1] In some environment, its *public-like* IP address is not routable on the Internet. It is considered the same as a private IP address.

then automatically distribute these files to the clients. This step is essential for the provisioning of the VoIP service. It is possible and also acceptable to set up test accounts without passwords, but it should be limited during testing only. When an IP-PBX is in the production environment, administrator should conduct regular audits to assure that all SIP accounts are password protected and have not-easy-to-guess passwords.

In the case SIP trunking service, the IP-PBX requires a public IP address to connect to the SIP proxy server managed by the ITSP. In this case, SIPS (SIP over TLS) should be required for *signaling* traffic, and Secured RTP (SRTP, RFC 3711) should be required for *bearer* traffic. If the ITSP does not support SIPS or SRTP, the enterprise should use a security measure comparable to SIPS and SRTP. For example, an IP-VPN tunnel based on IPSec and L2TP provides a strong security protection comparable to SIPS and SRTP. It should be noted that this public IP address on IP-PBX is for the ITSP only. The firewall policy should prevent any other service or any other external connection using this IP address.

The enterprise also needs to consider hacking/abuse within the network (LAN side). We recommend to use Virtual LAN (IEEE 802.1Q) to segregate voice and data traffic [17], and also to implement Quality of Service (802.1p) to give priority to voice traffic over data traffic. This design prevents internal hackers from sniffing voice traffic. The network administrator could also monitor traffic on individual voice ports on the Ethernet switch. If a voice port has unusual traffic spike, it would trigger a security alert for further investigation. In our lab environment, we use mrtg (www.mrtg.org) to monitor the lab traffic, and an example of our monitoring chart is illustrated in Figure 13.

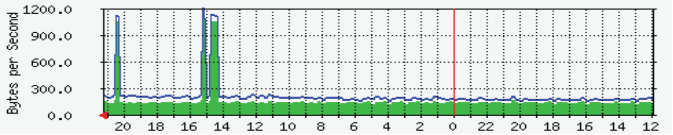

Figure 13. Monitoring VoIP Traffic on Individual Ports

Other recommendations of security counter-measures are given as follows:

1. Disable non-service related ports [18]. This is a standard practice of hardening a server.
2. Restrict international calls to designated phone numbers. As discussed earlier, international calls are not limited to 011 calls. They are many NANP countries, and administrator needs to identify their area codes and to restrict calls to these countries [19].
3. Constantly monitor Call Detail Record (CDR) to identify unusual usage patterns. A CDR is created after each call, and it contains the billing information of the call. Administrator should not wait until the phone bill; instead, administrator should monitor CDR and identify abnormal events.

V. Conclusion

This research is motivated by a real case of toll fraud, and further study of the lab log shows an alarming and growing threat of VoIP attacks. This paper presents a detailed study of the authentication process in the VoIP protocol (SIP) and identifies several vulnerabilities of its use. Note that we did not identify issues with the protocol (SIP) itself, but its security features are optional in implementation. Our study shows that the use of security measures depends on the enterprise network configuration. For example, SIPS should be mandatory for IP-PBX with a public IP address. Certain security measure (e.g., password protection for clients) should be mandatory regardless of any environment.

It should be noted that the scope of our study is on the IP side, and it does not cover the protection on the PSTN side. Our conclusion is that an IP-PBX, if properly protected, could be as safe as any legacy PBX, but not better. The reason is that all attacks from the PSTN side are equally applicable to both IP-PBX and legacy PBX.

References

[1] Diane Myers, "2014 VoIP and UC Services and Subscribers," http://www.infonetics.com/pr/2014/2H13-VoIP-UC-Services-Market-Highlights.asp

[2] Wikepedia Phone Fraud http://en.wikipedia.org/wiki/Phone_fraud

[3] D. Butcher, X. Li, and J. Guo, "Security Challenge and Defense in VoIP Infrastructures," IEEE Transactions on Systems, Man, and Cybernetics, , Vol. 37-6, November 2007, pp. 1152-1162.

[4] Angelos D. Keromytis, "A Comprehensive Survey of Voice over IP Security Research," IEEE Communications Survey and Tutorial, Vol. 14-2, 2012 pp. 514-437.

[5] D. Hoffstadt et. al. "A comprehensive framework for detecting and preventingVoIP fraud and misuse," International Conference on Computing, Networking and Communications (ICNC), February 2014, pp. 807-813.

[6] Hofbauer, S. et. al., "A Lightweight Privacy Preserving Approach for Analyzing Communication Records to Prevent VoIP Attacks using Toll Fraud as an Example," IEEE 11th Intl. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom), June 2012, pp. 992 – 997.

[7] David Persky, "VoIP Security Vulnerabilities," SANS Institute, Fall 2007. http://www.sans.org/reading-room/whitepapers/ voip/voip-security-vulnerabilities-2036

[8] D. R. Kuhn, T. J. Walsh, and S. Fries, "Security Considerations for Voice over IP Systems," National Institute of Standard and Technology, 800-58, January 2005.

[9] Asterisk VoIP server. http://www.asterisk.org/

[10] Gruber, M. et. al., "Voice calls for free: How the black market establishes free phone calls - Trapped and uncovered by a VoIP honeynet," 11th Intl. Conf. on Privacy, Security and Trust (PST), July 2013, pp. 205 – 212

[11] Aziz, A. et. al., "A distributed infrastructure to analyse SIP attacks in the Internet," IFIP Networking Conference, June 2014, pp. 1-9.

[12] L. Zhang, S. Yu, Di Wu, P. Watters, "A Survey of Recent Botnet Attacks and Defenses," IEEE 10th International Conference on Trust, Security, and Privacy in Computing and Communications, November 2011, pp. 53-60.

[13] Abdelnur, H. et. al. "Abusing SIP Authentication," 4th Intl. Conf. on Information Assurance and Security, September 2008, pp. 237-242.

[14] A. N. Jaber, S.Manickam, S. Ramdas " A study of SIP trunk security and challenges," IEEE International Conference on Electronics Design, Systems and Applications (ICEDSA), November, 2012 pp. 239-243.

[15] G. Sonwane, B. Chandavarkar, "Security Analysis of Session Initiation Protocol in IPv4 andIPv6 Based VoIP Network," 2nd International Conference on Advanced Computing, Networking and Security (ADCONS), December 2013, pp. 187-192.

[16] Shen, C. et. al. "The Impact of TLS on SIP Server Performance: Measurement and Modeling," IEEE/ACM Transactions on Networking, Volume: 20 , Issue: 4, August 2012 , pp.1217 - 1230

[17] G. Sonwane, B. Chandavarkar, "Security Analysis of Session Initiation Protocol in IPv4 andIPv6 Based VoIP Network," 2nd International Conference on Advanced Computing, Networking and Security (ADCONS), December 2013, pp. 187-192.

[18] X. Wei, K. Sellal, Y. Bouslimani, "Security Implementation for a VoIP Server," International Conference on Computer Science & Service System (CSSS), August 2012 pp. 983-985.

[19] Countries of North American Numbering Plan (NANP) http://www.nanpa.com/pdf/NANP_Member_Country_Maps.pdf