Toll-Fraud Protection, Detection and Prevention

Abdulrazaq Alsuhail Almutairi
Information and Computer Center
The Public Authority for Applied Education and Training
State of Kuwait

Abstract

Voice over Internet Protocol (VOIP) is a type of technology that enables users to make calls through the internet. It works by converting sound into digital voice communication and then transferring it through the internet. Such technology offers several benefits like low cost calls, portability, and integrability with software. Many businesses these days depend on VOIP technology in handling their voice communications. Although there are many benefits of such technology, it has become one of the areas targeted by hackers, intent on causing financial damage to businesses. One of the attacks carried out is called toll-fraud, where attackers get access to a victim's account then make calls without paying for such calls. In this paper, different approaches are proposed to monitor and prevent such types of attacks.

1. Introduction

Many businesses these days have employed Voice over Internet Protocol (VoIP) as an alternative to the traditional public switching telephone network (PSTN). VoIP is also known as internet telephony. The usage of VoIP is associated with many advantages. VoIP software facilitates business activities more than PSTN. Such software may include messaging, conference calls, video, caller identification, and dynamic identity services. Uys [1] describes the main advantages of using VoIP as follows:

> *"The main advantages of using VoIP are the result of the non-reservation of lines for communication purposes and the transmission of packets of data along with other data packets on the data network. This translates into cost savings and effective network utilization, which can result in further benefits due to the digitization of the process."*

In addition, it provides flexibility in the way that the telephony system can be used from different geographic locations, as it operates through the internet. It also offers scalability benefits in the way that the telephony system can easily and rapidly scale up and down when adding or removing new people.

Although there are benefits and advantages of using VoIP technology, it can result in toll-fraud. Toll-fraud, which is also known as long-distance fraud, is an unauthorized access to communications services to make calls charged to an unsuspecting entity. Fraudsters typically use a compromised IP-PBX server or IP-phone to gain access to special services numbers that carry a per minute or per call charge. Based on a survey conducted in 2013 by the Communications Fraud Control Association (CFCA) [2], losses associated with toll-fraud across businesses worldwide was around $46.3 billion, an increase of 15% from 2011. In the same context, Pearce [3] said:

> *"Many businesses aren't aware of the potential threat and unwelcome costs that they may face by not securing their phone system. Figures show that a single Toll Fraud attack can cost an organization around £10,000, which can have a devastating impact, especially on small businesses."*

In this paper, three different approaches are proposed to limit the impact of toll-fraud attacks. One of these approaches is to restrict making calls based on a specified daily limit. The second approach is based on measuring the volume of calls over a specified period. The third approach is IP geographic-based, where calls are allowed based on geographic location of the call originator.

The second section of this paper provides a brief background to different VoIP security threats. The third section goes through the first approach. The fourth section walks through the second approach, while the fifth section discusses the third approach. The sixth section provides the results of evaluating the proposed approach. The seventh section discusses the related work. The last section presents the conclusion and future work.

2. Background

2.1. IP-PBX

An IP-PBX (Internet Protocol Private Branch Exchange) is a VOIP system telephone acting as a switchboard that employs IP (Internet protocol) to carry telephone calls through computer networks rather than using traditional phone lines. The IP-PBX system comprises VoIP phones, an IP-PBX server and a VoIP Gateway (optional). The IP-PBX server works as a proxy server: SIP clients, being either soft phones or hardware, register with the IP-PBX server, and when they wish to make a call, they ask the IP-PBX to establish the connection. The IP-PBX has a directory of all phones/users and their corresponding SIP address and thus is able to connect an internal call or route an external call, via either a VoIP gateway or a VoIP service provider, to the desired destination [4].

2.2. SIP Overview

SIP (Session Initiation Protocol) is a signalling protocol for session management. It used with VoIP as it is designed for real-time transmission. SIP is not responsible for transmitting the voice data. It is mainly used for initiating, coordinating and terminating a communication session between two endpoints. For example, the ringing of a phone, the busy tone and termination of a call are all functions the SIP protocol provides [5]. SIP has the advantage of an ability to redirect calls through User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) over other VoIP protocols that support only UDP.

SIP has two components: User Agents and SIP servers. User Agents represent endpoints of the SIP system (IP Phone). User agents may either represent an agent client or an agent server. A user agent client starts a session by sending a SIP request and a user agent server responds to the request by accepting, terminating or forwarding the request. A SIP server handles requests for transferring, security, authentication, and call routing. There are three types of SIP servers including SIP proxy servers, SIP registrar servers, and SIP redirect servers.

3. VOIP Security Threats

3.1. Social Threats

Social threats directly target humans. For example, misconfiguration, or bad protocol interactions in VoIP give the opportunity to perform attacks that misrepresent the identity of malicious parties to users. Such attacks may then proceed to the next phases such as phishing, or theft of service [6].

3.2. Scanning a VoIP Network

Scanning a network is a step that precedes some attacks. If an attacker targets an individual component of VoIP infrastructure, they need to locate them in the network, then try to obtain as much information as possible about the targeted component and infrastructure. VoIP infrastructure includes elements other than just VoIP phones and servers. Attackers normally focus only on devices running VoIP services, due to the availability and security of VoIP networks relying so heavily on supporting the infrastructure. The attacker then moves to the next phase. For example, if an attacker manages to locate and disqualify the TFTP (Trivial File Transfer Protocol) server, several models of phones trying to download configuration files on boot-up might crash or stall [7]. Another example of such kinds of threats is Registration hijacking. The attacker performs a scan looking for IP addresses that have an open SIP (session initiation protocol) port 5060. The attacker then scans this port targeting a valid extension on the PBX. Once found, a brute force attack will be launched to crack the registration password for that extension. Once the user-name and password are obtained, the attacker can use them to register their own Sip phone and make calls.

3.3. PBX Control

It has become very common to find a web application used as a PBX administrative control rather than proprietary programming applications. There are scenarios where, if an attacker manages to gain access to that web interface due to security holes in the web page such as cross site forgery, or cross site scripting, they will have full control of the PBX, all options, and capabilities. The attacker at this point will be able to generate calls and remove any restrictions in place to make calls to premium destinations.

3.4. End-Point Control

Many modern IP-based handsets are often managed by a web interface. Some of those handsets give the option to generate calls through their web interface. If an attacker takes control of an endpoint, they will be able to access the interface and generate calls directly from the PBX.

4. Proposed Approaches

4.1. Overview

Most of the VoIP security threats are based on security holes around network and web-based applications. Attackers try to develop approaches to break security controls. In this paper, three different approaches are proposed to protect VoIP systems from Toll-fraud attacks. These approaches are based on assessing how a VoIP account is used in terms of time, call charges, and geographic locations.

4.2. Charges-Based Traffic Monitoring

This approach is based on assessing average daily charges of calls made. The idea behind setting a daily limit is to monitor irregular activities in terms of call charges. The daily spending limit is calculated according to the following formula:

$$DailyLimit = \frac{M}{\mathrm{N}} \sum_{n=1}^{N} C_n$$

Where:

A: Magnification factor is greater than one.
N: Number of days that represent the assessment period.
C: Call charges on day n.

The daily limit is regularly updated (e.g. on a weekly basis) to reflect changes on the VoIP account spending behaviour. The approach monitors the spending after terminating each call. If the total call charge exceeds the daily limit, the VoIP account will be suspended.

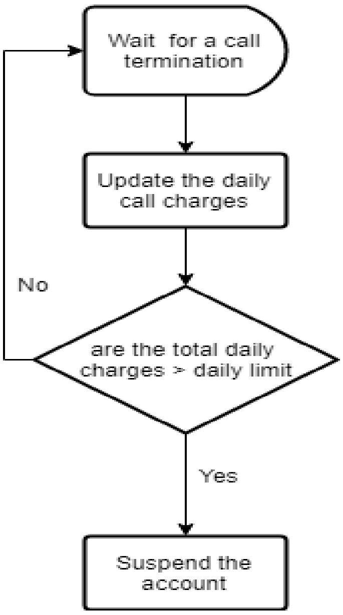
Wait for a call termination
Update the daily call charges
No
are the total daily charges > daily limit
Yes
Suspend the account

Figure 1. Charges-Based Traffic Monitoring

4.3. Duration-Based Traffic Monitoring

This approach is based on assessing the daily duration of calls to specific destinations. For example, a VoIP account may be used normally to make local calls with an average of two hours a day, and five minutes for international calls. The proposed approach will suspend the account if this account reaches the daily threshold for international calls (e.g. seven minutes). The monitoring process in this approach is based on a profile that defines the maximum call limit for each group of destinations. The threshold for each group is calculated as follow:

$$DurationThreshold = \frac{M}{\mathrm{N}} \sum_{n=1}^{N} T_n$$

Where:
M: Magnification factor is greater than one.
N: Number of days that represent the assessment period.
T: Total duration of calls made to destinations included in the group.

The monitoring process as shown in Figure 2 will first match the call with a destination group (e.g. Local destinations, West Asia destinations) and then check the total duration against the set threshold of the destination group to decide whether to suspend the account or not.

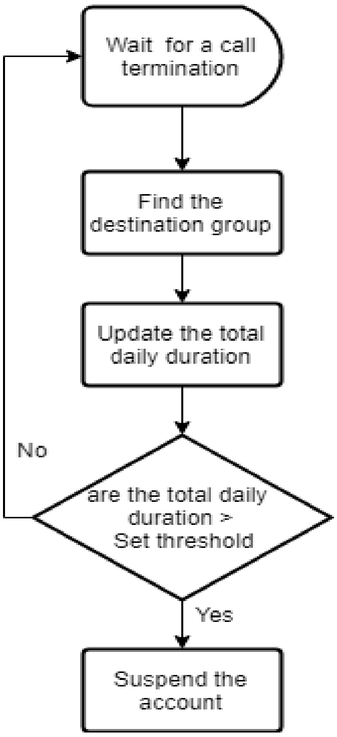
Wait for a call termination
Find the destination group
Update the total daily duration
No
are the total daily duration > Set threshold
Yes
Suspend the account

Figure 2. Duration-Based Traffic Monitoring

4.4. IP Geographic-Based Profile

VoIP accounts are used within some geographic locations. By restricting the use of VoIP accounts from specified locations, fraudsters will be blocked from carrying out toll-fraud from an IP address geographically outside the list of specified locations. In other words, calls made from countries not in a white list will be considered suspicious. For example, a VoIP account is used only in two countries: Kuwait and the United Kingdom. If that account is compromised and used to make calls from an IP address classified as an IP address based in Lithuania, the call will be considered suspicious and blocked. The approach can be extended to limit calls to be made only from specific IP addresses. Figure 3 shows the logic of restricting the calls based on the geographic-based profile.

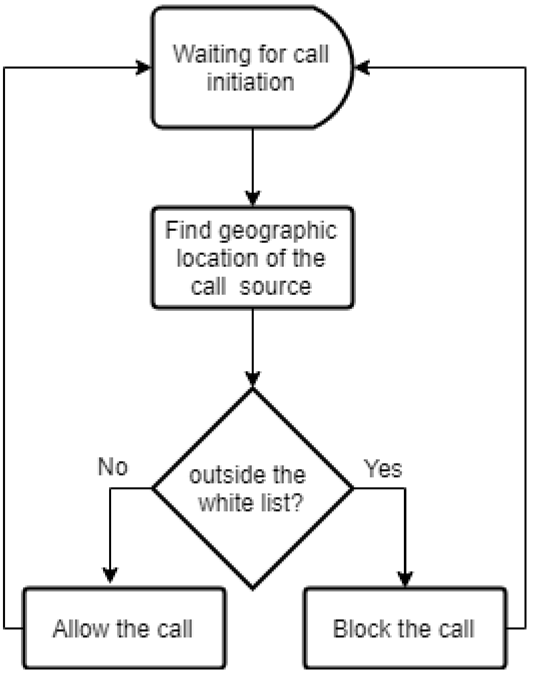
Waiting for call initiation
Find geographic location of the call source
outside the white list?
No
Yes
Allow the call
Block the call

Figure 3: IP Geographic-Based Approach

5. Experiment

5.1. Experiment Settings

The experiment has been carried out using a hosted IP-PBX (asterisks based). The system has been used with each approach separately. The approaches have been used as follows:

- *Charges-Based Traffic Monitoring:*

$$DailyLimit = \frac{1.7}{7}\sum_{n=1}^{7} C_n$$

The Daily limit was $4.00

- *Duration-Based Traffic Monitoring:*

$$DurationThreshold = \frac{2}{7}\sum_{n=1}^{7} T_n$$

The Duration-Threshold was 45 minutes/day.

- *IP Geographic-Based Profile:*

The system was configured to allow making calls only from the UK.

5.2. Experiment Results

The results obtained from the experiment as shown in Table 1 have shown that the charges-based traffic monitoring approach is effective when compromised VoIP accounts are used to make calls to destinations at a high rate (e.g. premium numbers). On the other hand, the duration-based approach is effective with low rate destinations. It has also found that IP geographic-based profiles may fail, if an attack is carried out from geographic locations included in the white list.

Table 1. Experiment Results

Approach	**High Rate Destinations ($2.00/minute)**	**Low Rate Destinations ($0.05/minute)**
Charges-Based	The account has been suspended after making two minutes call	The account has been suspended after eighty minutes calls.
Duration-Based	The account has been suspended after making $90.00 call	The account has been suspended after making $2.25 call
IP Geographic-Based profile	Calls have been blocked when they were made only outside the UK.	

6. Related Works

Cortes and Pregibon [9] proposed an approach based on the use of fraudulent signatures, which are regularly updated. Those signatures are added to a training data set then used with a supervised machining learning algorithm to create a toll-fraud detection model. The main disadvantage of this approach is the high dependency on the regular update of fraudulent signatures.

Murad and Pinkas [10] proposed an approach that profiles normal behaviour form. The normal behaviours are extracted using a clustering algorithm with a cumulative distribution distance function. Toll-fraud is detected if the standard deviation of the overall profile is exceeded. This approach is very close to the work presented in this paper. The main difference is not considering the geographic location as a parameter in detecting toll-frauds.

7. Conclusion and Future Work

Each of the proposed approaches is effective for certain scenarios. It will be more effective to combine the use of all of the proposed approaches in this paper to cover most of the toll-fraud scenarios. For example, the IP geographic-based profile will represent the first defence line, as it blocks calls made from geographic locations not included in the configured white list. In case VoIP accounts are used to make calls from geographic locations included in the white list, charges-based and duration-based approaches will be in place to suspend the compromised account.

Future work will involve using artificial intelligence algorithms to set a daily limit, duration threshold, and configure the white list rather than setting them manually.

8. References

[1] Uys, L., (2009)., Voice over internet protocol (VoIP) as a communications tool in South African business, African Journal of Business Management, vol.3 , pp. 89-94.

[2] Communications Fraud Control Association, (2013). Global Fraud Loss Survey, Available at: http://www.ntvoiceanddata.co.uk [Accessed 15th Jan 2018].

[3] Equations Voice and Data Communication (2016), PRESS RELEASE: Small businesses urged to protect themselves from telephone Toll, Available at: http://equationsvoiceanddata.co.uk [Accessed 21st March 2018].

[4] Jiang, W. et al., (2010), Towards Junking the PBX: Deploying IP TelephonyProceeding, Proceedings of the 11th international workshop on Network and operating systems support for digital audio and video, pp. 177-185.

[5] Handley, M., (1999), SIP: session initiation protocol. Requestfor Comments 2543, Internet Engineering Task Force.

[6] Keromytis, A., (2009) A Survey of Voice over IP Security Research. In: Prakash A., Sen Gupta I. (eds) Information Systems Security. ICISS 2009. Lecture Notes in Computer Science, vol.5905.

[7] Konstantinos, F., (2007), Voice over IP Security: Threat Analysis and Countermeasures, University of London.

[8]Cortes, C., Pregibon, D. & Volinsky, C., (2003). Computational Methods for Dynamic Graphs. Journal of Computational and Graphical Statistics 12: 950-970.

[9]Murad, U. & Pinkas, G., (1999). Unsupervised Profiling for Identifying Superimposed Fraud. Proc. of PKDD99