Secure Calls and Caller ID Spoofing Countermeasures

Towards building a Cyber Smart Societies

Junaid Chaudhry
Department of Computer Science
Innopolis University, Kazan, Russia
j.chaudhry@innopolis.ru

Shafique Ahmed Chaudhry
Department of Compute Science,
Dhofar University, Salalah, Oman.
shafique@du.edu.om

***Abstract*—Caller Identification (CallerID) is a service provided by the service providers that enables the receiver of the call to know who is trying to call him. Now a days, the caller ID service is used by many public and private organizations to contact their customers in order to exchange private information for authentication purposes. The unified caller ID for all the outgoing series of call connections, establishes an initial chain of trust between the caller and the callee. However, an increasing trends is observed where faking/spoofing the callerID has become a common trend. Cyber criminals spoof their caller IDs in order to gain call pickup trust from the user and build on to that initial trust to steel user data over phones. The faked callerID can cause roamers to spread and panic among public too. It is also used to defame organizations and particular people. In this paper, we aim at analyzing the existing methods to prevent the callerID spoofing along with their shortcoming and propose the model for caller ID verification that might be used to verify the identity of the caller.**

Keywords—callerIdentification; spoofing; telecommunication networks; cyber crimes; SSL7; signaling;

I. Introduction

The Plain Old Telephone Systems (POTS) are based on "circuit switched" PSTN technology; where individual connections (aka circuits or channels) are made in order to establish a phone call session between the caller and callee. With the advent of astronomical growth in the subscribers, competition among service providers, and VoIP technology, on one hand has reduced the cost of using telephony but on the other hand, it has given raise to many malfunctions that criminals can use in order to exploit different components of the system i.e. subscribers and service providers alike.

In order to regulate the ever expanding telecommunication industry, ITU introduced Signaling System Number 7 (SSL7) where calls are initiated and ended with standard control signals [1]. The same standard is followed in the delivery of short messaging service (SMS) too however, verification of the presented ID feature is not available so far. Another hurdle in caller ID verification is that the call routing information is kept transparent from the receiver signaling unit (typically a local exchange) hence the problem of caller verification still stands. In the scenario of establishing calls to a different network, only the point code of the originating switch will be used rather than the number of originator which means in reverse dialing mode, call will still be spoofed.

While PSTN networks are "circuit switched" the IP traffic aims for the "shortest path". This brings the infrastructure cost to a fraction of conventional telephony networks. Lower costs come with a a few downsides however. The advent of Session Initiation protocol (SIP) has reduced the network costs. The interactive voice response records are created on the fly at SIP application servers and SIP URIs are presented to the receiver exchanges which poses a challenging situation for SIP-SS7 gateways in call path. Hence delivering calls to the clients with vulnerable caller IDs. Among countless voice of IP clients, H.323 [2], and IAX2 [4] are widely used with their own security flaws [3] and adaptability issues.

In mobile networks the IMSI/MEID is assigned a subscriber number that is used for sim card validation which intern fed to CNAM service. In some counties, the CNAM service is *username* based, in others its mainly an extension of IMSI number. In VoIP infrastructure, the SIP URI is presented but SIP B2BUA strips the URI and assigns it SIP proxy without verifying the information. The SIP proxy forwarding happens for every hop without client verification which discloses inherent weakness in the SIP standards.

In this paper, we enumerate different methods of caller ID spoofing and perform a comparative analysis of these techniques. Based on our findings, we identify solution areas and we propose solutions that could be used in order to strength the Identification security in the telecommunication networks. We also present a domain name system based method that we plan to use as a building block for our caller ID spoofing solution. We propose that all IP-based traffic should be verified through SIP proxy and hence can be rejected or accepted based on the confidence shown on its routing patters. As we suggest service providers to tighten up the screws in their infrastructure, the DNS-based service that we are working on is entirely client-based and does not cost extra to the service provider.

The rest of the paper is organised as follows: we first analyse the problem definition in both mobile, cellular and tradition PSTN networks. We also analyse the solutions of these problems proposed in academia in the related work section. We

discuss the proposed scheme and present the architecture of the target application that we aim at building as a part of this research. In the end we conclude our paper with analysis of strengths and weaknesses of the research by analysing the scope.

.

II. Problem Description

A. Spoofing a VoIP call

The SIP URI that is presented at call set up time in INVITE message to the callee is set up by the caller that could be either SIP URI or some other URI that the originator of call wants. The SIP proxy has the option to forward the CallerID as-it-is, the Direct Inward Dial (DID) number, or up to the PBX to set up the caller ID [5]. There is an option to forward the call to the receiver as *anonymous*. An example of such setting is set below:

Remote-party-ID:
Anonymous<sip:anonymous@anonymous.invalid>;
tag=98765xy

It is up to the service provider at the receiver's end to reject those calls with "*non-regulated*" caller IDs. It is possible however that the privacy settings at the originator's end are masked by the B2BUA. In either case, the service providers should comply with the regulations and consumer protection. Filtering and different numbering schemes are used by the service providers with "*recognized SIP Carriers*" and those who present DID numbers but its a practice not followed by the most. Typically voice over IP services can be classified into three different classes: 1- SIP trunking, 2- DID providence providers, 3- Full stack. These services can be both central or can be in geographically distributed locations with different sets of local regulations to follow. The SIP users can use multiple service providers to receive or make calls which is called "split horizoning". In case of split horizoning the incoming and out bound calls take totally different routes which makes caller ID an even harder problem to solve. It is often observed that the outgoing calls are from a spoofed number that actually intern premium rate number . So in case of dial back, premium rate numbers serve as revenue generators for the cyber criminals.

International dialing is a very lucrative market with abundance of revenue on offer. The VoIP provides cheaper solutions to the service providers. The international SIP carriers provide services in multiple countries as both point of presence (POP) or both termination and DID services. This has given rise to outsourced parties that have connections with multiple carriers and serve as transit point for many. In their business, interoperability is crucial hence enforcement of regulations is not up to the standards.

So we can single out three areas which are hard to solve from a strategic perspective: 1- international nature of the problem that puts on a set of problems that need international relations to play a major role in resolution of this problem, 2- technical issues play another major role in the resolution of the problem, 3- telecommunication market has turned such corners where cost cutting is considered sole way of revenue generation while compromising on quality and privacy.

B. Abuse of Tracking and Privacy

Some might argue over the issues of privacy and tracking issues due to vivid importance being given to caller ID spoofing and disambiguation efforts. If we consider, there are two areas to tracking phone calls: 1- meta-data related to the calls e.g. originator, destination, duration of calls, etc. 2- contents of the call e.g. voice packets and its contents [3].

On traditional PSTN networks the user calls tracking data is contained for billing purposes. It is mainly the originator's number that is traced for calls and their duration with respect to the destination. Most propriety VoIP services charge their customers for their services for making calls on the fixed infrastructure. Anonymity is an extra service which is requested at a price on top of regular rates. In case of SIP service providers the unregulated B2BUAs that forward calls can spoof caller IDs.

The SIP to SIP calls it is the call originator gateway that sets the caller ID for the originator. Because its direct SIP proxy to SIP proxy interaction there is no need for B2BUA or BGCs and direct IP address of caller is presented to the receiver as caller ID. Hence its easier to recognize but harder to prove in real time.

III. Related Work

The problem of Caller ID spoofing has taken the center stage in recent years due to huge losses that people has faced in the form of financial value, breach of privacy, and reputation. In [6] the authors debate on the steting up a honey pot for Smap over Internet Telephony (SPIT) and propose an algorithm to mitigate the denial of service attacks. However, we believe that deployment of a honey pot for voice traffic is a big net that is casted over all the voice traffic of a service provider which may effect the quality of service of legitimate users too. This is the reason why we propose minimal physical changes to the already present infrastructure and let giving control to the end users. In [7] a swarm intelligence based web-of-trust solution is proposed which in our opinion, works for a closed group of community but it hardly is feasible for out-of-bound calls, international calls, and call that are out of the circle of trust.

A hybrid solution is proposed in [8] where authors use a different channel of communication by using the cellular networks to inform about the legitimacy of a call or not. This type of approach is post-emptive where attackers have already got through to the end user and communication should be made to the user before or upon arrival of the call establishment packets. A covert channel based caller ID spoofing detection methods is proposed in [9] where authors try to verify the identity of the user at call arrival time. They propose an Android-based solution that can be installed at the client end and incoming call arrivals are monitored. They also propose to use the reverse calling features in order to verify the identity of the caller at call time. There are three problems with this approach: 1- busy channels, 2- unassailable incompatibility, 3- extra cost of receiving a call when it could have been a cost free

procedure. Moreover, in situation of split horizon, the user might never be able to verify the identity of the original caller.

In [10] the authors propose the use of identity cards in order to verify their identity as originators of SIP traffic. In other words, all SIP vendors are assumed to be complying with this assumption. As discussed above, due to the three challenges discussed in the previous section, this solution may be useful for one geographical location for all local bound traffic but can not be implemented on the out of area traffic, transit traffic, or DID services provided by the international service providers that are looking to establish local interchange presence points. In [11] the authors propose a framework that mandates per hop authentication for SIP traffic. As we discussed in the earlier sections, the proposition requires international and inter organizational coherence and should be backed up by the blanket laws in geographical regions.

IV. Proposed Methodology

While there are a variety of solutions proposed for the problem of caller ID spoofing, some suggest changes in the service providers infrastructure and the others suggest specialized applications of both centralized and distributed nature. We suggest the use of enabling technology of the Internet on which all IP traffic relies; that is the domain name servers (DNS). Internet consists of all items that are connected with each other through an Internet protocol address (IP address) and as discussed earlier, the voice over IP data and signaling passes to the destination: whether PSTN or another VoIP client, over IP networks.

In [12] the authors emphasize on standardization of caller identification policies in order when calls are made from the caller to a user that is a subscriber of the same network. In this situation, the CNAM stays the same as the one registered in the Home Location Register (HLR) of the service provider for that particular user and the control for call set up is context switching among base station system, in some cases and the between MSS and BSS, within the network of the service provider. The call set up and context switching principle stays very same when inter-service provide calls are a made within a country. The confusion arises when, 1-a VoIP call is made from within the same country of the callee, and 2-a VoIP call is made from overseas.

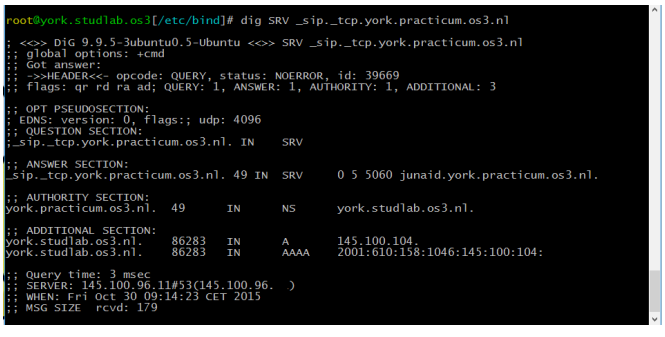

Fig. 1. Example of a the SRV record *implemented*

In this paper we address the VoIP caller issues and track the DNS records for that SIP proxy. We use repro1.8 [13] server developed by Resiprocate. After deployment on a cluster of servers we obtained the SRV records from the SIP proxy and analysed the SRV records and forwarded the results to the receiver of the call. At this stage, we have left it up to the user to determine the validity of the caller ID. In future work, we aim at providing more presentable information to the user about the SRV records and switching information of user call context in the real time.

V. Conclusion

In this paper, we proposed a domain name server based solution for the problem of caller ID. This solution does not require any infrastructure level changes at the service provider's end rather uses the information from the domain name servers in order to display the SIP "switching" the user and let him/her decide about the validity of the caller. We also discussed some areas of improvement for he service providers and aim at improving on our scheme in future.

Acknowledgment

The authors would like to acknowledge the contribution of Innopolis University, Dhofar University, and University of Amsterdam for their assistance in conduction of the research.

References

[1] Yi-Bing Lin, "Signaling System Number 7," in *Potentials, IEEE* , vol.15, no.3, pp.5-8, Aug/Sep 1996

[2] Lie-Liang Yang; Hanzo, L., "A residue number system based parallel communication scheme using orthogonal signaling. II. Multipath fading channels," in *Vehicular Technology, IEEE Transactions on* , vol.51, no.6, pp.1547-1559, Nov 2002

[3] Yi-Bing Lin; Meng-Hsun Tsai, "Eavesdropping Through Mobile Phone," in *Vehicular Technology, IEEE Transactions on* , vol.56, no.6, pp.3596-3600, Nov. 2007 doi: 10.1109/TVT.2007.901060

[4] Spinsante, S.; Gambi, E.; Bottegoni, E., "Security solutions in VoIP applications: State of the art and impact on quality," in *Consumer Electronics, 2008. ISCE 2008. IEEE International Symposium on* , vol., no., pp.1-4, 14-16 April 2008

[5] Chow, Stanley T.; Gustave, Christophe; Vinokurov, Dmitri, "Authenticating displayed names in telephony," in *Bell Labs Technical Journal* , vol.14, no.1, pp.267-282, Spring 2009 doi: 10.1002/bltj.20367

[6] Vennila, G.; Shalini, N.S.; Manikandan, M.S.K., "Performance analysis of VoIP spoofing attacks using classification algorithms," in *Applications and Innovations in Mobile Computing (AIMoC), 2014* , vol., no., pp.193-198, Feb. 27 2014-March 1 2014

[7] Seedorf, J.; d'Heureuse, N.; Niccolini, S.; Cornolti, M., "Detecting Trustworthy Real-Time Communications Using a Web-of-Trust," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* , vol., no., pp.1-8, Nov. 30 2009-Dec. 4 2009

[8] Sachin, P.T.; Tamrakar, S., "VOIP and data storage in wireless GSM modem over MANET area," in *Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), 2013 International Conference on* , vol., no., pp.31-36, 25-26 March 2013

[9] Mustafa, H.; Wenyuan Xu; Sadeghi, A.R.; Schulz, S., "You Can Call but You Can't Hide: Detecting Caller ID Spoofing Attacks," in *Dependable Systems and Networks (DSN), 2014 44th Annual*

IEEE/IFIP International Conference on , vol., no., pp.168-179, 23-26 June 2014

[10] Falk, R.; Fries, S.; Hof, H.J., "Protecting Voice over IP Communication Using Electronic Identity Cards," in *Advances in Human-Oriented and Personalized Mechanisms, Technologies and Services (CENTRIC), 2010 Third International Conference on* , vol., no., pp.5-10, 22-27 Aug. 2010

[11] Feng Cao, "SeCReT: A Security Framework for Enhancing Chain of Response Trust in Session Initiation Protocol," in *Internet Surveillance and Protection, 2006. ICISP '06. International Conference on* , vol., no., pp.29-29, 26-28 Aug. 2006

[12] Chow, Stanley T.; Gustave, Christophe; Vinokurov, Dmitri, "Authenticating displayed names in telephony," in *Bell Labs Technical Journal* , vol.14, no.1, pp.267-282, Spring 2009

[13] Repro SIP Server: http://www.resiprocate.org/About_Repro, last accessed 15/10/2015.