A Mechanism to Authenticate Caller ID

Jikai Li[1(✉)], Fernando Faria[1], Jinsong Chen[2], and Daan Liang[3]

[1] Computer Science Department, The College of New Jersey, Ewing, NJ 08628, USA
{jli,fariaf1}@tcnj.edu

[2] Princeton, Princeton, NJ 08540, USA
jsch@live.cn

[3] Department of Civil, Environmental, and Construction Engineering Department,
Texas Tech University, Lubbock, TX 79409−1023, USA
daan.liang@ttu.edu

Abstract. Caller ID displayed on the phone is supposed to provide accurate information of the caller. However, with the help of computer and Voice over Internet Protocol (VoIP), it is easy to spoof a Caller ID. The users of spoofing caller ID can be school district office, hospital, law enforcement, telemarketers etc. Although caller ID spoofing has legitimate uses, it imposes real threats to the receiver of the call when it is abused. In today's world, it is important to restore the credibility of the incoming caller ID. In this work, we propose a mechanism that can authenticate certified caller IDs, which can be authentic or legitimately-spoofed. The proposed scheme involves caller, receiver of the call, and a third-party to exchange short information. It is caller and receiver's discretion to adopt this scheme. The proposed scheme does not change switch or signaling protocol. The proposed scheme can be naturally integrated into current system. An Android-based application was developed to test the idea.

Keywords: Caller ID · Spoofing · Fake · Authentication · Trusted

1 Introduction

Caller ID (Caller Identification) displayed on landline phone, smartphone, VoIP phone, is widely used to identify the caller. People uses caller ID to recognize and identify the calls from emergency service, schools, hospitals, banks, colleagues, friends, relatives etc. Business, such as some banks, uses the displayed caller ID as an authentication measure to activate credit cards. However, the impression that caller ID can authenticate the caller is misleading. The caller ID displayed on phone can be easily faked in today's network. In a caller ID spoofing, the shown caller ID on the receiver's device is not the original caller's ID. Currently, fake caller ID or caller ID spoofing extensively exists in our daily life. Some of these caller ID spoofing are legitimate, many of them are not. The legitimate caller ID spoofing can provide privacy to the callers and convenience to the receivers. For example, the schools or the hospitals with an on-site Private Branch Exchange (PBX), such as Asterisk PBX [1], supporting dozens or hundreds distinctive phone numbers, the outward calling caller ID can be configured to be the single business number instead of the originator's caller ID. When a teacher of the school calls a

Á. Rocha et al. (eds.), *Recent Advances in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 570, DOI 10.1007/978-3-319-56538-5_75

student's parents, the displayed caller ID can be set to be the school's caller ID. Similarly, when a doctor of the hospital calls a patient, the receiver's device may show the caller ID of the hospital. The receiver uses the unique business caller ID to easily identify the institute of the caller. In this case, the receiver does not need to know the phone numbers behind the PBX, these numbers may change over time while the business number is stable for long period. In addition to provide convenience, the legitimate caller ID spoofing can provide privacy to the caller. For example, the law enforcement personnel, such as police, can use caller ID spoofing to protect their actual caller ID to be released.

Just like many other things, caller ID spoofing can be a double-edged sword. It can be easily abused and cause harmful results. In the last several years, there are callers spoofed the caller ID of Internal Revenue Service (IRS) of United States. They made unsolicited calls to the victims and claims to be IRS and request immediate payment of taxes via either credit card or wire transfer [2–4]. Many times, the scammers spoof the IRS toll-free number on the caller ID. There are more than 90,000 complaints about the IRS phone scam and caused millions of dollar loss [4]. In 2006, it is reported that Paris Hilton used caller ID spoofing to hack into other people, many of them are celebrities, voicemail accounts [5]. In 2015, there is report that scammer use caller ID spoofing to pose as police and demand the receivers to transfer money to the scammers [5].

To provide a consistent caller ID service, it is necessary that all carriers follow a set of consistent policy, regulations, and laws. However, that is not the case in today's telecommunication network. The Truth in Caller ID Act of 2009 passed by US congress prohibits transmitting misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value [7]. In other words, it is legal to do caller ID spoofing as long as the caller has no intention to defraud, harm, or wrongfully obtain anything of value. In Canada, it only requires the telemarketers to accurately identify themselves. Each individual violation is can lead to fines up to $1,500 [8]. Other than this requirement, it is totally legal to do caller ID spoofing in Canada. In United Kingdom, the caller can only spoof the phone number allocated to the caller or the phone number with explicit permission of the third party [9].

If the originator of the call and the receiver of the call are inside two different carriers' networks and the originator's carrier does not prohibit or detect caller ID spoofing, then no matter what regulation or legislation the receiver's carrier follows, the receiver will get limited information of the call ID from the carrier. If there is no extra effort made on the receiver side, practically caller ID spoofing will be unavoidable to the receiver sooner or later.

There are several different ways to do caller ID spoofing. VoIP makes caller IP spoofing extremely easy. Spoofcard [10] has its own smartphone app. After installing the app, the users of SpoofCard can buy the credits online and make call directly on their own smartphones. SpoofCard allows the user not only spoof the caller ID, but also change the voice of the caller and add background sounds. SpoofCard calims they have more than 750,000 users. Other call ID spoofing service, like SpoofTel [11] and Spoof My Phone [12], allows the user make caller ID spoofing online.

Several existing works address the fake caller ID detection and caller ID authentication issues. A proposed mechanism CallerDec [13] does caller ID verification based on either Short Message Service (SMS) or a phone call. When receiver receives a phone call, the receiver contacts the displayed caller ID via either SMS or phone call to verify whether the phone call is real or not. CallerDec is relatively easy to implement. All the modification should be on user's side. It does not need to change carrier's infrastructure. However, this mechanism is vulnerable to DoS attack. For example, if the attacker continuously sends a lot of calling requests to different receivers and these requests have the same fake caller ID (the victim's caller ID), the receivers will either send SMS or call back to the fake caller ID (the victim). As the verification requests number increases, the victim's phone can be easily overwhelmed. The work in [14] proposes to use certified caller ID that is supported by the carrier. The work in [15] proposes to use a validating system that works directly with the originator node and the terminating node. Both [14, 15] integrate the caller ID validating as part of the network infrastructure, the implementation of these mechanism requires extensive system upgrade of current network infrastructure. The work in [16] uses the idea similar to trademark registration. It proposes to setup jurisdiction office for each area, this office provides authentication to the callers of the area. However, if the caller calls a phone number in the area that the caller does not register, then there will be no authentication service to the caller. For example, if the caller calls from Canada to a phone number in United States, and the caller registers in Canada but not in United States, the receiver of the call in US will not get caller ID authentication. The mechanism proposed in [17] detects spoofing caller by tracing back an incoming call to its gateway that does Session Initiation Protocol (SIP) and SS7 ISDN User Part (SIUP) conversion. The gateway verifies whether the caller ID is spoofed. To implement this mechanism, the PBX that servicing the displayed callerID must be compatible with the proposed mechanism. In other words, if some PBX is not compatible with this mechanism, the receiver of the call cannot detect whether it is a spoofing call.

In this paper, we propose a solution, Trusted Caller ID (TCI), to provide caller ID authentication. This authentication scheme does not involve extensive service infrastructure change. It is an optional service to the users that need authenticate their caller IDs. TCI can authenticate not only the regular caller ID, but also the legitimate caller ID spoofing. In fact, the legitimate caller ID spoofing users, such as schools and hospitals, can not only continue use caller ID spoofing, but also authenticate their caller ID.

The rest of the paper is organized as follows: Sect. 2 discusses how of caller ID works in telephony network and how caller ID spoofing happens in today's network. Section 3 discusses our proposed solution to provide authentication to the caller IDs. Section 4 highlights the advantages of this approach and discuss the future work.

2 Background

The Public Switched Telephone Network (PSTN) includes the circuit-switched telephone networks, which includes telephone lines, optic fibers, cellular networks, microwave links, satellite links, undersea cables, etc. When a landline or cellular phone user makes a phone call using PSTN, also known as Plain Old Telephone Service (POTS), a connection is setup between the caller and the receiver. Typically, this connection is circuit switched. VoIP, unlike PSTN, provides communication service over Internet. In United States, PSTN is regulated by Federal Communications Commission (FCC). However, FCC claims that VoIP is information service instead of telecommunication service. Thus, FCC has limited rights to regulate VoIP. Being lack of regulation over VoIP is one of the reasons that illegitimate caller ID spoofing is rampant now.

Caller ID is supported by both PSTN and VoIP applications. Typically, Caller ID includes two pieces of information. One is the caller ID number and the other one is the caller ID name. When the caller makes the phone call, the caller's phone number is transmitted to the called party's device. Usually, this happens before the phone is answered. In addition to displaying the caller's phone number, the called party's device may also display the name of the caller. This service is called CNAM. The caller ID spoofing can make the caller's phone number to be a fake one, or the displayed name to be a fake one, or both the caller's phone number and the displayed name to be fake. In the following discussion, we introduce how caller's phone number and name can be faked.

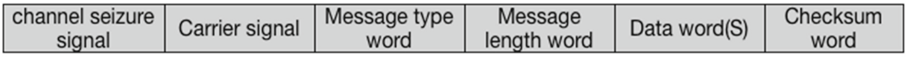
There are three kinds of phone users today. They are POTS, cellular network, and VoIP users. If the calling party is a POTS user, the local switch will generate the caller ID for this call. The caller ID generated by local switch includes caller ID phone number, but may or may not include caller ID name. Generally speaking, because the POTS caller does not have direct access to the local switch and cannot modify the configuration of the caller ID on the local switch, the POTS caller cannot fake the caller ID. However, if the calling party is behind a PBX, it is possible that PBX can do the caller ID spoofing. PBX is connected to the local switch via Primary Rate Interface (PRI). The local switch of PSTN usually just passes the caller ID received from PBX to PSTN [18], even the caller ID is fake. If the calling party is a cellular network user, typically, the International Mobile Subscriber Identity (IMSI) stored on the Subscriber Identification Module (SIM) card (installed on phone) is used by the switching center to identify the ID of the calling party. It is difficult for a cellular caller to hack either the SIM card or the caller ID configuration in the switching center. Similar to the caller of POTS (except the one with PBX), the caller of cellular network has limited chance to fake caller ID either.

Unlike POTS and cellular network, it is relatively easy to setup/configure/fake caller ID in VoIP. Signaling protocols of VoIP network, such as H.323 [19], MGCP [20], Session Initiation Protocol (SIP) [21], and SKINNY [22], control the VoIP conversation. All these protocols support caller ID. For example, when Eve uses SIP-based VoIP to call Bob and spoofs Alice's caller ID. The INVITE message from Eve to Bob may contain the following information:

```
To: Bob < sip:bob@biloxi.com>
From: Alice < sip:alice@atlanta.com > ;tag = 1928301774
Call-ID: a84b4c76e66710@pc33.eve.com
```

The first line of the above information contains receiver's name (Bob) and his SIP Uniform Resource Identifier (URI), which is sip:bob@biloxi.com in this example. The second line contains the caller name (Alice) and caller's SIP URI, which is sip:alice@atlanta.com. The name and SIP URI are used by the receiver to display caller name and caller number. However, the name and SIP URI can be faked by VoIP caller. There is no authentication for the second line in SIP. The lack of authentication of the second line makes SIP (and other similar signaling protocols) vulnerable to caller ID spoofing. The third line of the above information contains a globally unique identifier for this call [21].

Different countries use different standards to transmit caller ID in PSTN. For example, US, Canada, Australia, New Zealand, and China use Bellcore FSK; Ireland, Spain, Norway uses ETSI FSK; UK uses SIN227; Finland, Denmark, Iceland, Netherlands, and Sweden use DTMF. Figure 1 shows the message containing caller ID in Bellcore FSK.



channel seizure signal	Carrier signal	Message type word	Message length word	Data word(S)	Checksum word

Fig. 1. Message containing call ID in Bellcore FSK

For both PSTN and VoIP, there are several facts about caller ID worth noting. First, when the calling party initiates a phone call, the caller ID created on the calling side includes caller number and an optional caller name. Second, if the calling party uses PBX or VoIP, it is relatively easy to fake both caller number and caller name, or one of these two. Third, when caller number is receiver by the carrier of the receiver, it is simply passed to the receiver. However, when the caller name is passed to the carrier of the receiver, the carrier may forward the name directly to the receiver directly, or discards the caller name and uses the caller number to search the database and find the corresponding registration name. For example, when caller ID < 1609123456, Alice > is received, the carrier may forward this caller ID to the receiver. Or, the carrier uses phone number 1609123456 to search the registration database and find out Eve is the billing name of this phone number, then it forward < 1609123456, Eve > to the receiver.

3 Trusted Caller ID

The proposed Trusted Caller ID (TCI) is based on the observation that the current carriers have little, if there is any, economic motivation to verify or authenticate caller ID. In addition to that, the regulation/legislation of different countries and different protocols used by carriers make upgrade current telephone switches difficult. More importantly, even though we want to detect/prevent illegitimate caller ID spoofing, any new mechanism should NOT block the legitimate caller ID spoofing, such as the ones from schools and hospitals.

In the following discussion, we assume Alice is the calling party and Bob is the receiving party. Eve is the calling party with caller ID spoofing. In the proposed TCI mechanism, there is a third-party, called Phone Call Authority (PCA), which provides phone call and caller ID authentication service. In TCI, caller ID authentication service is optional. If Alice wants to authenticate her caller ID, she first contacts PCA to authenticate her caller ID. If the authentication only includes the caller number, PCA can send a verification code to the phone number via SMS. Alice types this verification code in app to activate the authentication. If Alice wants to authenticate both phone number and caller name, she needs to provide proper documentation to prove the she is the owner of the phone number and the caller name. Figure 2 shows the relationships between the caller, receiver, carriers, and PCA. As Fig. 2 shows, PCA does not belong to any carrier. If Alice needs her caller ID authentication service, Alice need to register with PCA only once.

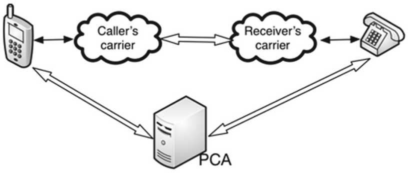


Fig. 2. The layout of callers, receivers and PCA

In the following discussion, P_A represents the phone number of Alice, similarly P_B represents the phone number of Bob. We use N_A to represent the name of Alice. Figure 3 illustrates how TCI works when a legitimate phone call is made. The calling party, Alice, first registers her caller ID with one PCA. There can be multiple PCA available to choose, Alice should have no pre-assigned commitment to any particular PCA. Theoretically speaking, she can pick anyone she likes. When Alice registers her caller ID with PCA, she can choose whether register only P_A, or both P_A and N_A. Once the registration is finished, all future phone calls made by Alice can be authenticated by that particular PCA.

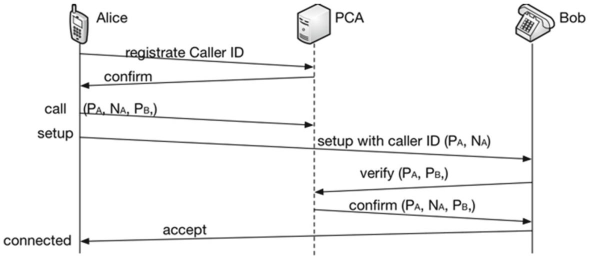


Fig. 3. The phone call and Caller ID is authenticated

When Alice calls Bob, Alice's device first sends the Alice's caller ID (P_A, N_A) and Bob's phone number (P_B) to PCA via data channel (Internet). Upon receiving the caller ID and Bob's phone number, PCA checks authenticity of (P_A, N_A). If they are authentic, (P_A, N_A, P_B) will be stored into a database, which maintains currently active phone calls. The entry of (P_A, N_A, P_B) will only stay in the database for a short period, such as two minutes. Later on, we will explain why. After the information of (P_A, N_A, P_B) was sent to PCA, the caller starts the regular calling setup process, which is facilitated by protocols, such as SS7, SIP, H.232, etc. During the connection setup process, the caller ID, (P_A, N_A), is delivered to the receiver. If there is no caller ID authentication service, (P_A, N_A) will be displayed as the caller ID on the receiver's device. In TCI, the receiver sends (P_A, P_B) to PCA to verify whether there is a call from P_A to P_B. If PCA does have the record of a call from P_A to P_B, it retrieves the registered caller name N_A, and replies back to Bob with (P_A, N_A, P_B), which indicates there is a valid call from P_A to P_B and the authenticated caller ID is (P_A, N_A). When Bob receives (P_A, N_A, P_B), he knows the call is not spoofed and the caller ID is (P_A, N_A). The call ID authentication happens during the period when the call connection is setup, this period usually is short. So the information of (P_A, N_A, P_B) stored in PCA is only valid for a short period, such as two minutes.

Figure 4 shows the situation when a caller ID spoofing is detected. In this example, Eve calls Bob with faked caller ID (P_A, N_A). When Bob receives the caller ID, he verifies the received caller ID (P_A, N_A) with PCA. Since PCA did not register this phone call, PCA sends a negative acknowledgement to Bob. Therefore, Bob can reject the call.

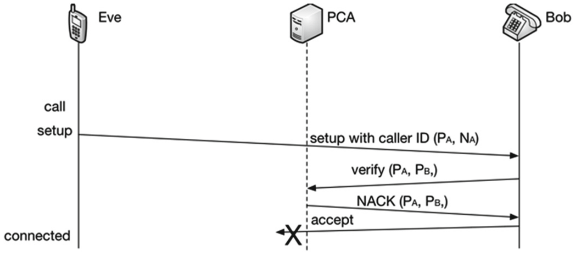


Fig. 4. Spoofing Caller ID is detected

As the above example shows, the proposed TCI can detect the spoofing caller ID. In fact, for the legitimate caller ID spoofing users, their calls also can be authenticated. For example, in Fig. 5, if the legitimate caller ID spoofing caller uses PBX to spoof the caller ID, the user can upgrade the PBX and make the PBX register the phone call information with PCA. Then, the phone call and the caller ID will be authenticated by PCA. Furthermore, if we make PBX delegate all the phones behind it, all the phone calls initiated behind the PBX will be authenticated by PCA. The phones behind PBX does not need to change any current configuration. The authentication process is transparent to the callers behind PBX. In this way, the current legitimate caller ID spoofing users (schools, hospital, law enforcements etc.) can continue to use caller ID spoofing. In addition to that, the legitimate caller ID spoofing can get authentication service.

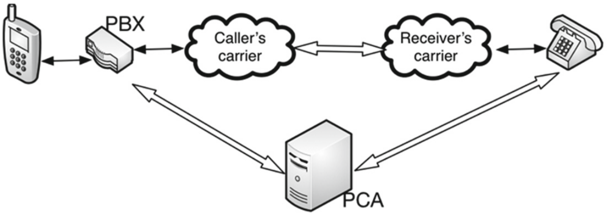


Fig. 5. Legitimate Spoofing Caller ID is supported by PCA

4 Conclusion

This paper discusses the caller ID spoofing problem. Caller ID is often used by the receiver to identify the caller. However, with the help of PBX and VoIP, it is easy to spoof a fake caller ID. In the spoofed caller ID, the caller number, or the caller name, or both the caller number and caller name can be fake. Caller ID spoofing does not always mean illegitimate activities. In fact, many legitimate users, such as schools, hospitals and law enforcements, use caller ID spoofing service as well. Therefore, to ban all caller ID spoofing services is unacceptable. The current telephony network is quite complicated, there are many different protocols and devices working together. The telephony industry has little motivation to overhaul its own network to provide caller ID spoofing detection or authentication service. The regulation policies and laws of different countries about caller ID spoofing are different. The discrepancy of the regulations/laws creates the space for illegitimate caller ID spoofing service. In this paper, we propose TCI, a mechanism that authenticates caller ID, including the legitimately spoofed caller ID. The service of TCI is optional to the phone users. Whoever needs authenticated caller ID service, that person register the phone number with PCA. After the registration, whenever the caller makes a phone call, the caller notifies the PCA of this ongoing activity. When the receiver receives the call, the receiver checks with PCA to see whether the call and the caller ID are authentic or not. Because TCI does not require comprehensive network upgrade. The caller who wants the authentication service need to upgrade the software of the calling device, which can be a phone or PBX. If the receiver wants to have authentication service, the receiver's device need to install the software. Otherwise, if the receiver does not need this service, the current phone can still receive the call as usual. Because of the flexibility provided by TCI, it is easy to phase TCI into current telephone network.

References

1. Customize Outgoing Caller Name and Caller ID. http://wiki.freepbx.org/display/FPG/Customize+outgoing+caller+name+and+caller+ID
2. Scam Phone Calls Continue; IRS Identifies Five Easy Ways to Spot Suspicious Calls. https://www.irs.gov/uac/newsroom/scam-phone-calls-continue-irs-identifies-five-easy-ways-to-spot-suspicious-calls
3. IRS Urges Public to Stay Alert for Scam Phone Calls. https://www.irs.gov/uac/irs-urges-public-to-stay-alert-for-scam-phone-calls
4. An IRS Warning About Phone ScamsHow to Avoid Becoming a Victim. https://www.irs.com/articles/irs-warning-about-phone-scams
5. Paris Hilton accused of voice-mail hacking. http://www.infoworld.com/article/2658949/security/paris-hilton-accused-of-voice-mail-hacking.html
6. Scammers Turn to Caller ID 'Spoofing' To Pose As Police. http://www.npr.org/2015/06/17/414997683/scammers-turn-to-caller-id-spoofing-to-pose-as-police
7. Truth in Caller ID Act of 2009. https://www.govtrack.us/congress/bills/111/s30/text
8. Caller ID Spoofing. http://www.crtc.gc.ca/eng/phone/telemarketing/identit.htm
9. Caller ID Spoofing: All You Need to Know. https://www.trapcall.com/blog/caller-id-spoofing/

10. SpoofCard. http://www.spoofcard.com
11. Spooftel. http://www.spooftel.com
12. Spoof My Phone. http://www.spoofmyphone.com
13. Mustafa, H., Xu, W., Sadeghi, A.R., Schulz, S.: End-to-end detection of caller ID spoofing attacks, IEEE Trans. Dependable Secure Comput. 99 (2016)
14. Kurapati, S., Mohan, R., Sadhasivam, K., Tyagi, S.: System and method for authentication of caller identification, US Patent 6324271 (2001)
15. Cai, Y.: Validating caller id information to protect against caller id spoofing, US Patent 20080159501 (2008)
16. Chow, S.T., Gustave, C., Vinokurov, D.: Authenticating displayed names in telephony. Bell Labs Tech. J. **14**(1), 267–282 (2009). Spring
17. Song, J., Kim, H., Gkelias, A.: iVisher: Real-Time Detection of Caller ID Spoofing. ETRI J. **36**(5), 865–875 (2014)
18. Caller ID. https://en.wikipedia.org/wiki/Caller_ID
19. H.323: Packet-based multimedia communications Systems. https://www.itu.int/rec/T-REC-H.323/en
20. Media Gateway Control Protocol (MGCP) Version 1.0. https://tools.ietf.org/html/rfc3435
21. SIP: Session Initiation Protocol (RFC 3261). https://www.ietf.org/rfc/rfc3261.txt
22. Signalling Connection Control Part User Adaptation Layer (SUA). https://tools.ietf.org/html/rfc3868