TOWARD AUTHENTICATED CALLER ID TRANSMISSION: THE NEED FOR A STANDARDIZED AUTHENTICATION SCHEME IN Q.731.3 CALLING LINE IDENTIFICATION PRESENTATION

Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn
Arizona State University
{tu, doupe, zzhao30, gahn}@asu.edu

ABSTRACT

The rising prevalence of phone fraud is hurting consumers and businesses. With about a half million reports each year in the United States, phone fraud complaints have more than doubled since 2013. In the current calling line identification presentation scheme, the caller ID is trivially spoofed. Scammers are using spoofed caller IDs to trick their victims into answering unwanted calls and further a variety of scams. To provide a solution to this problem, this paper proposes an authentication scheme that provides the possibility of a security indicator for the current Q.731.3 calling line identification presentation supplementary service. The goal of this proposal is to help prevent users from falling victim to phone impersonation scams, as well as provide a foundation for future defenses to stop unwanted calls based on the caller ID information. This work will help to guide the future development of a standardized scheme in authenticating SS7 identities.

Keywords— Caller ID, calling line identification, spoofing, fraud, scam, authentication, verification, standardization

1. INTRODUCTION

With the introduction of IP access to the Public Switched Telephone Network (PSTN), today the PSTN is rife with telephone spam, namely voice, voicemail, and SMS spam. Voice phishing, vishing, or phone fraud is a significant and rapidly growing problem in many countries, including the US [1] and UK [2].

To deal with this issue, governments, including the US [3] and UK [4], have enacted laws to restrict most forms of unwanted telephone calls. Furthermore, some governments have established regulatory agencies and telephone number registries that allow consumers to explicitly opt out of unwanted calls [5, 6].

In addition to government efforts, there are also consumer and business products that are made to defend against unwanted calls. In the consumer market, there are physical call-blocking devices for landline telephones, and various smartphone apps, that can block unwanted calls from offending caller IDs. Among business and network operators, there is a also supplementary network feature known as MCID (Malicious Call Identification) that allows the destination operator to request identification of the offending calling party.

Despite various efforts to reduce telephone spam, scam and robocalls, complaints on illegal calls has been making record numbers in recent years. According to a recent US government report, the number of phone fraud complaints in the US more than doubled in just a matter of two years from 2013 to 2015 [1]. The rise of phone scam is troubling, as billions are lost to phone scams each year [7]. In the US, more than 75% of the reported fraud and identity theft attempts are made over the phone [1]. Today, the US government receives about 200,000 robocall complaints every month, and the total number of reported complaints on illegal calls totaled more than 3.5 million in 2015 [8].

Clearly, all these countermeasures have so far failed at reducing the growth of telephone spam. According to a recent research [9], illegal callers today have access to various technologies aimed at circumventing call blockers and preventing identification. Among them, a practice known as *caller ID spoofing* is particularly effective at defeating call blockers, avoiding identification, and further a variety of scams.

To show an example of how caller ID spoofing is used in phone scams, one type of phone fraud that occurs frequently is the credit card verification scam, where the spammer spoofs the caller ID of a bank, and uses audio recorded directly from the credit card issuer to scam his recipients. The audio recording tells the recipients that their credit cards have been suspected of fraud, and is in need of verifying their personal information to reactivate their account. Of course, the true motive of this scam is to steal the recipients' credit card and personal information.

Furthermore, caller ID spoofing can also frame true owners of spoofed caller IDs with illegal behavior. When a malicious caller spoofs a known number to commit crimes, such as making scam calls or illegal purchase orders, or deceiving police into raiding a compound [10], true owners of spoofed caller IDs often end up questioned by law enforcement, and receive unfriendly calls for wrongdoings that have nothing to do with them.

The telephone number in North America and many other regions follows a numbering format that identifies the region code, central office code, and subscriber number [11]. If the telephone number is spoofed, law enforcement would lose key information that could identify and locate the offender. As most telephone spam defenses today (including law enforcement) rely on user feedbacks, caller ID spoofing has made identification and user feedbacks completely irrelevant.

2. THE RISE OF CALLER ID SPOOFING

The caller ID is a generic name for a supplementary service offered by the called party's telephone company that presents the calling party's telephone number to the called party's user equipment during an incoming call. It helps the called party to decide whether to answer a call based on the caller's phone number, and, to call back the caller if the call could not be answered. Since its introduction in the 1990s, the caller ID service has now become ubiquitous in almost every telephone service. Today, the caller ID number is also used in other telephony services, such as the SMS and MMS, and, with the prevalence of smartphones, many smartphone apps and services also rely on the caller ID for identification.

However, because the PSTN was traditionally regarded as a closed trusted network, it was designed with little security in mind. Telephone companies rely on the trust in other operators to play by the rules. In the process of providing the caller's telephone number, the originating exchange can control what caller ID number is sent on a call-by-call basis.

Traditionally, a caller would need to gain control of a SS7 switch in order to have the capability to customize the caller ID. In consumer telephony services, the caller ID is typically managed by the caller's Local Exchange Carrier (LEC), preventing general users from spoofing the caller ID. It was also prohibitively expensive for individuals and small businesses to gain switch level access to the SS7 network, which kept the number of people with caller ID spoofing capability small.

However, with the recent rise of IP access to the PSTN, cheap IP-based client protocols (such as SIP [12]) are replacing the expensive traditional bulk telephone services (such as ISDN). Cheap and accessible Voice-over-IP (VoIP) bulk telephony services are now becoming the norm.

The PSTN is also moving toward being carried by the IP infrastructure (such as SIGTRAN [13]), however, the core SS7 signaling protocols have not changed to ensure compatibility with legacy systems. Telephone companies still relied upon trust in other switch operators to play by the rules. With growing IP access to the PSTN, the SS7 network is no longer exclusive to traditional telephone carriers. Today, there are now many internet telephony service providers (ITSPs) that provide bulk telephony services over an Internet connection. With the popularity of the cloud business model, access to SS7 switch level capability is becoming more available to untrusted parties. Some ITSPs *sell customizable caller ID as a service feature*, along with mass distribution technologies such as voice broadcasting, voicemail broadcasting, and SMS broadcasting, all provided over an Internet connection.

Further complicating matters, the Internet provides plenty of opportunities for a malicious caller to evade law enforcement through geography and technology. With an Internet connection, a spammer can now cost-effectively distribute outbound calls from an overseas location, beyond the jurisdiction of law enforcement. To further prevent identification, the spammer can hide behind virtual private networks (VPNs) and Tor networks to distribute the calls anonymously.

The PSTN has transformed from a closed national ecosystem to an open global ecosystem, therefore mutual trust and local laws can no longer be relied upon to materially guard against the abuse of SS7's inherent insecurities. There is a lack of accountability in phone identities. This is why we advocate for a standardized caller ID authentication scheme for the PSTN. By securing the caller ID, not only would consumers benefit from being able to distinguish between verified and unverified caller IDs, it provides a foundation for many telephony spam defenses (including law enforcement).

With the growing prevalence of phone fraud, calls from billing, government, and banking institutions would also greatly benefit from providing authenticity of their caller IDs, such that their customers would feel greatly assured doing business over the phone. Authenticated caller IDs may also be useful for immediate customer identity verification, without relying on (possibly stolen or guessable answers of) security questions to verify the identity of customers. As there are also scam calls that spoof the caller IDs of existing customers, which the malicious callers then trick the institution into emptying their customers' bank account [14].

However, for any viable deployment of such feature, it requires ITU-T standardization to ensure mutual interoperability. Therefore, standardization is key to building a PSTN ecosystem that could rely on the trust of caller IDs.

3. HOW CALLER ID SPOOFING WORKS

The SS7 process of providing the caller ID or calling party number (CPN), is known as Calling Line Identification Presentation (CLIP). In CLIP, the CPN is sent along with a call request using the initial address message (IAM) to the destination exchange of the called party. The relevant details of CLIP are defined in ITU-T Recommendation Q.731.3 [15], Q.81.1 [16], Q.951.3 [17], and I.251.3 [18].

The CPN is either provided by the originating local exchange or by the calling party, where the CPN parameter is inserted in the initial address message, which is sent as part of the basic call procedures according to Recommendation Q.764 [19]. The IAM routes through transit exchange switches until it reaches the destination exchange of the called party, in which the called party's local exchange carrier would convert and retransmit the CPN to a specific caller ID format for the called party's user equipment during the incoming call setup process.

The parameter value of the CPN is placed within the optional part of the initial address message. The IAM follows the ISUP (ISDN User Part) message format as defined in Q.763 [20]. The CPN parameter follows a structured binary coding format as defined in Q.763.3.10 [20].

To spoof the caller ID, the caller's originating exchange or the calling party will declare the CPN parameter with false information. In the US and many other jurisdictions, the caller's telephone service provider does not have any legal obligation to ensure that the caller ID number is genuine before it is transmitted. Even in jurisdictions that forbid telephone service providers from providing falsely declared caller ID information, with Internet access to an untrustworthy telephone service provider, it is easy for a malicious caller to start the call request from a different origin, and transmit the false caller ID to the destination exchange of the called party.

4. WHY SECURITY INDICATORS MATTER

In the internet ecosystem, the HTTP and email are arguably the most popular types of communication used today. In HTTP communication, the universally recognized padlock indicator displayed in the address bar of modern web browsers (such as the one shown in Fig. 1) provides users with immediate trust in the web site's domain name identity.

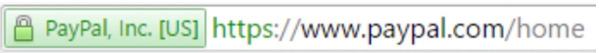

PayPal, Inc. [US] https://www.paypal.com/home

Figure 1: An example of HTTPS security indicator in Google Chrome with extended verification

In email communication, the key-shaped security indicator of the email sender (such as the one shown in Fig. 2) in email clients provides the users with immediate trust in the identity of the email sender.

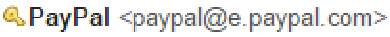
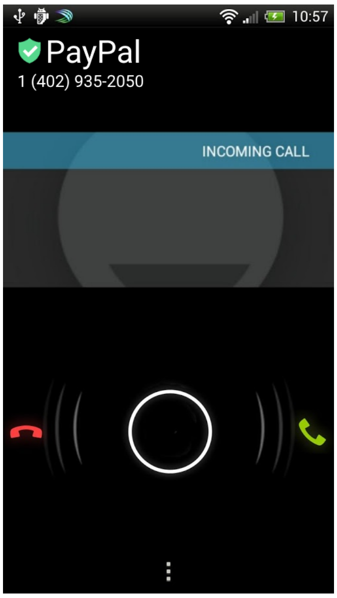

PayPal <paypal@e.paypal.com>

Figure 2: An example of email security indicator in Gmail


10:57

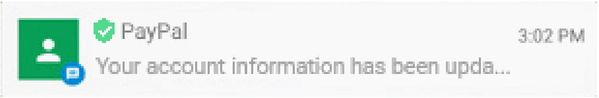
PayPal

1 (402) 935-2050

INCOMING CALL

Figure 3: An example of proposed caller ID security indicator for an incoming call

These security indicators are crucial to informing the user that the information is from a verified source. The distinctive appearance of the security indicator provides an immediate cue of the authenticity of the sender's identity. The universality of the security indicator symbol provides an immediate cue of the functionality of the indication. By examining the authenticity of certificates that underpin the security indicator, users are able to protect themselves from phishing and impersonation scams.


PayPal 3:02 PM

Your account information has been upda...

Figure 4: An example of proposed caller ID security indicator for an incoming SMS

This is why having a security indicator can be an effective solution against caller ID spoofing. Examples of possible caller ID security indicators for incoming call and SMS are shown in Fig. 3 and 4. By having assurance in the security indicator, users can quickly determine if the sender is authentic by recognizing an icon. Furthermore, the prevalence of security indicators promotes awareness that the user should only trust senders that are verified, which may inspire them to be more vigilant of calls and messages from unverified sources.

5. DESIGNING THE CALLER ID AUTHENTICATION SCHEME

Before we discuss the technical detail of designing the underlying caller ID authentication scheme behind the security indicator, we first present an overview of the parties involved in the transmission of a call request.

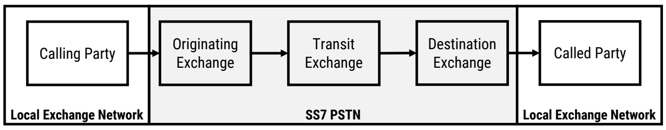


Figure 5: An overview of the parties involved in the transmission of a call request

Calling Party is the party initiating the call request with an user equipment (UE) or software client that connects with the originating exchange.

Originating Exchange is a switch in the PSTN that generates and transmits the IAM to the destination exchange pertaining to the call request from the calling party.

Transit Exchange is an interconnecting switch in the PSTN that helps to route the messages from the originating exchange to the destination exchange.

Destination Exchange is the terminating switch in the PSTN that receives the IAM and sets up the call with the called party.

Called Party is the party with an user equipment or software client of the intended called party for the call request.

In general, the sequences within a local exchange network define how user equipment interacts with the local exchange carrier during a call setup, and the sequences within the PSTN define how SS7 switches interact with each other during a call setup. More details of basic call control and signaling procedures can be found in Q.764.2 [19].

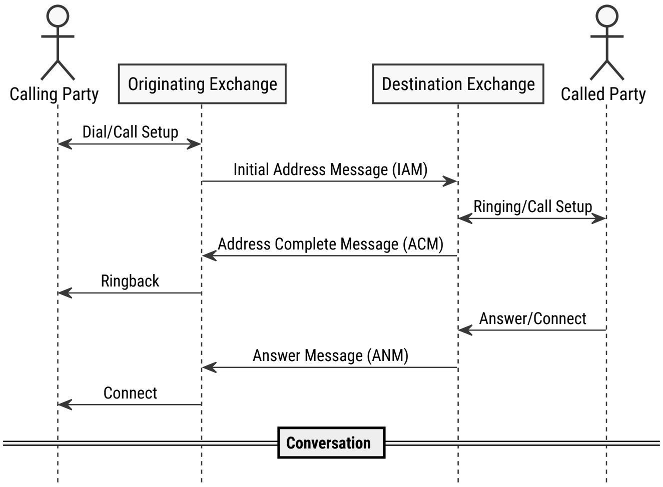


Figure 6: A simplified sequence of basic call control signaling

The current SS7 calling line identification presentation scheme has two fundamental insecurities: (1) a lack of verification of the declared caller ID and (2) a lack of integrity of the transmitted caller ID. The current calling line identification presentation scheme allows the CPN to be declared arbitrarily. Furthermore, there are currently no mechanisms to protect the CPN from unwanted modification during transmission. Even if the caller has proven that she indeed owns that phone number, an actor (perhaps in association with the caller) along the transit link may still intercept and alter the caller ID number.

Therefore, the design goal of a prospective caller ID authentication scheme must address the aforementioned fundamental security flaws, allowing the CPN to be verified before transmission, and making sure that the CPN is authenticated and can only be produced by the calling party or the originating exchange. The authentication scheme must provide a process that ensures the verified CPN can protect its integrity and guard against unwanted modification during transit. It must also be able to coexist with the existing call control signaling protocols for deployability.

When designing an authenticated caller ID scheme, an immediate idea is to model it after the SSL/TLS protocol of the Internet. However, this design, although can guarantee the authenticity and integrity of caller IDs, is ill-suited for the PSTN. After establishing an initial end-to-end connection with a TCP 3-way handshake, SSL/TLS authentication requires two additional round-trips (4-way handshake) to establish a secure connection. However, in a typical SS7 call request, this handshake is a one-way process, where the originating exchange sends an initial address message to the destination exchange to present the calling party's phone number identity. Implementing a naive SSL/TLS scheme would require SS7 call requests to support the multi-way handshake process, which is hard to adapt for the current SS7 scheme, and could potentially add delay to the call request process. In addition, SSL/TLS is designed for a client-server environment, which requires the server ("called party") to first acquire a certificate from a certificate authority (CA), whereas in the PSTN scenario, we are mainly concerned with authenticating the client ("calling party"). Finally, SSL/TLS is also designed to encrypt the data communication, which adds transport and processing overhead, whereas in our case, the primary goal is sender identity authentication instead of encrypting the conversation.

Therefore, we need to design an authentication scheme better suited for the PSTN. Designed as an initial reference, we propose a caller ID authentication scheme, which will guide and shape an authenticated calling line identification presentation process for the SS7 ecosystem.

The high-level idea of the protocol is that it takes advantage of the fact that *receiving* a message is proof of phone number ownership in the PSTN. The originating exchange or calling party first verifies with a certificate authority that the originating exchange or calling party actually owns the CPN by sending a message through the PSTN routing mechanism, and is issued a caller ID certificate. The originating exchange can then use this caller ID certificate to generate an authenticated call request by extending the parameters within the optional part of the IAM. The destination exchange or called party's user equipment then checks the validity of the authenticated call request, and presents the validated caller ID using a security indicator during the call setup to the called party.

The role of each actor with regards to the caller ID authentication scheme is as follows:

Certificate Authority is an entity in the PSTN that verifies phone number ownership and issues caller ID certificates to requesters that successfully provided proof of phone number ownership.

Calling Party sets up a call request with the originating exchange for the called party.

Originating Exchange obtains a caller ID certificate from the certificate authority for the calling party's phone number, if acquired, generates and transmits an authenticated IAM upon a call request from the calling party to the destination exchange.

Transit Exchange helps to route the IAM to the called party's destination exchange as usual.

Destination Exchange receives the authenticated IAM and checks the validity and authenticity of the call request, and it sets up the call with the called party with a security indicator showing the caller ID verification status.

Called Party receives the call request showing a security indicator.

The processes of the authentication scheme can be divided into 2 parts: Caller ID Verification and Authenticated Call Request.

In Caller ID Verification, the core process is sequenced as follows:

Prerequisites to the process: (1) the CA's public key P_S is publicly known, and (2) the CA has his private key Q_S.

1. Originating exchange or calling party generates a public-private key pair for the calling party's phone number, P_A and Q_A.

2. Originating exchange sends calling party's phone number *From*$_A$ and public key P_A to the CA.
3. CA creates an encrypted nonce *ENonce*$_S$ by first generating a random nonce *Nonce*$_S$ and then encrypting it with the calling party's public key. *ENonce*$_S$ = Encrypt(P_A)$\{$*Nonce*$_S\}$. This ensures that only someone with the calling party's private key can decrypt *ENonce*$_S$.
4. CA signs the *ENonce*$_S$ to create a signature *ENonce-Sig*$_S$. This is to safeguard the authenticity of the nonce during transmission.
5. CA sends *ENonce*$_S$ and *ENonce-Sig*$_S$ to calling party's telephone number *From*$_A$. The phone number should route to the originating exchange or calling party.
6. Originating exchange verifies the signature *ENonce-Sig*$_S$ to ensure CA's identity.
7. If *ENonce-Sig*$_S$ is verified, the originating exchange decrypts *ENonce*$_S$ with private key Q_A to obtain *Nonce*$_S$.
8. Originating exchange sends decrypted *Nonce*$_S$ to CA, proving that the originating exchange/calling party is really the owner of the phone number and public key.
9. CA verifies *Nonce*$_S$ and, if valid, sets a short expiration time *Expiry*$_A$ and generates a caller ID certificate (CIC) for the calling party *CIC*$_A$ by signing the calling party's phone number *From*$_A$, public key P_A, and *Expiry*$_A$ using the CA's private key.
10. CA sends *CIC*$_A$ to originating exchange.

A sequence diagram of the Caller ID Verification process is shown in Figure 7.

In actual deployment, there can be several CAs, allowing different users, such as in different networks or regions, to verify with an appropriate CA.

With regards to the caller ID certificate format, the certificate could be based on ITU-T X.509 format [21], and the telephone number in the certificate could be based on international E.164 format [22]. The required critical extension field for the X.509 certificate could be as follows (in RFC5280 style [23]):

```
Extensions ::=
    SEQUENCE {intlPhoneNumber  E.164}
E.164 ::== PrintableString (SIZE (3..15))
```

In Authenticated Call Request, the core process is sequenced as follows:

Prerequisites: (1) the originating exchange has CA's public key P_S, and (2) the originating exchange has caller ID certificate *CIC*$_A$ and his private key Q_A.

1. Originating exchange generates an IAM for the call request as usual.
2. Originating exchange generates an IAM Signature *IAM-Sig*$_A$ by signing all enclosed fields in the IAM along with current the current UTC timestamp *Time*$_A$.

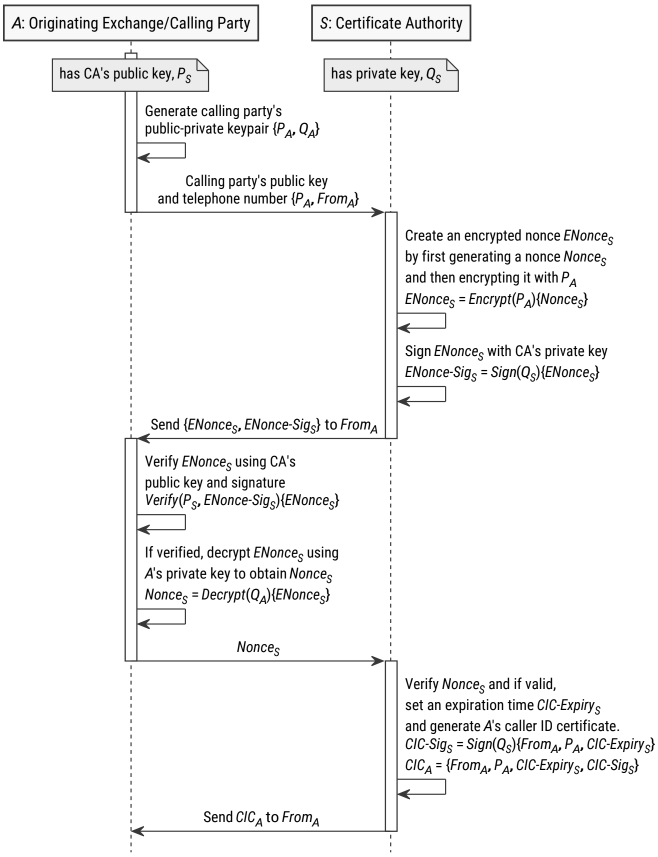

A: Originating Exchange/Calling Party
S: Certificate Authority
has CA's public key, P_S
has private key, Q_S
Generate calling party's
public-private keypair {P_A, Q_A}
Calling party's public key
and telephone number {P_A, $From_A$}
Create an encrypted nonce $ENonce_S$
by first generating a nonce $Nonce_S$
and then encrypting it with P_A
$ENonce_S$ = Encrypt(P_A){$Nonce_S$}
Sign $ENonce_S$ with CA's private key
$ENonce$-Sig_S = Sign(Q_S){$ENonce_S$}
Send {$ENonce_S$, $ENonce$-Sig_S} to $From_A$
Verify $ENonce_S$ using CA's
public key and signature
Verify(P_S, $ENonce$-Sig_S){$ENonce_S$}
If verified, decrypt $ENonce_S$ using
A's private key to obtain $Nonce_S$
$Nonce_S$ = Decrypt(Q_A){$ENonce_S$}
$Nonce_S$
Verify $Nonce_S$ and if valid,
set an expiration time CIC-$Expiry_S$
and generate A's caller ID certificate.
CIC-Sig_S = Sign(Q_S){$From_A$, P_A, CIC-$Expiry_S$}
CIC_A = {$From_A$, P_A, CIC-$Expiry_S$, CIC-Sig_S}
Send CIC_A to $From_A$

Figure 7: Sequence diagram showing the core steps to obtain a caller ID certificate

The inclusion of a UTC timestamp ensures that the call request is transient and unique with regards to time and destination, in order to guard against "cut and paste" and replay attacks.

3. Originating exchange attaches the UTC timestamp *Time*$_A$, IAM Signature *IAM-Sig*$_A$, and Caller ID Certificate *CIC*$_A$ in the optional part of the IAM and sends the extended IAM to the destination exchange.
4. Destination exchange obtains the extended IAM and checks if *CIC*$_A$ is valid, expired or revoked.
5. If the *CIC*$_A$ is valid, verify IAM signature against all the enclosed fields.
6. If the IAM signature is valid, check if the UTC timestamp is valid (within a reasonable delay and clock drift), and check if the called party number is correct.
7. Setup the call request with the called party and present a security indicator for the verification result.
8. Destination exchange sends address complete message (ANM) with verification result back to the originating exchange.

A sequence diagram of the Authenticated Call Request process is shown in Figure 8.

Due to the one-way process of transmitting the authenticated call request in the IAM, the call verification process can be implemented adding negligible delay to the existing call

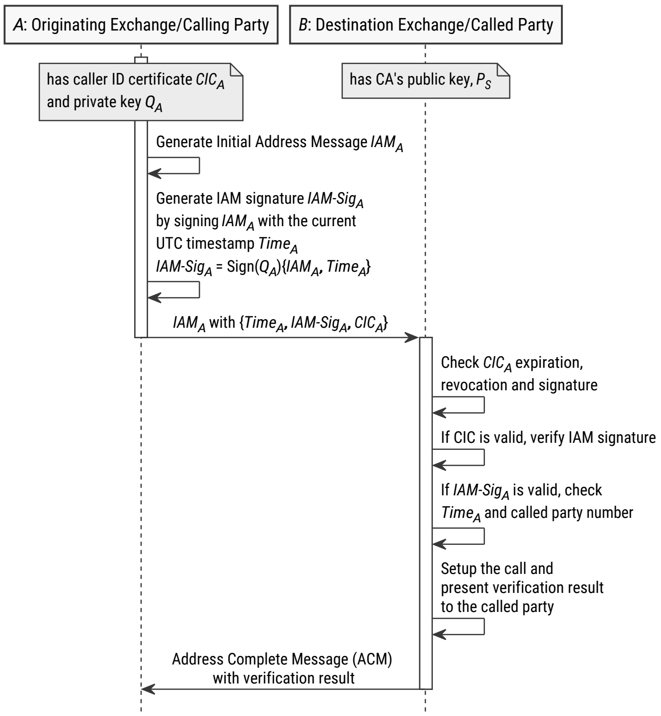

A: Originating Exchange/Calling Party
B: Destination Exchange/Called Party
has caller ID certificate CIC_A and private key Q_A
has CA's public key, P_S
Generate Initial Address Message IAM_A
Generate IAM signature $IAM\text{-}Sig_A$ by signing IAM_A with the current UTC timestamp $Time_A$
$IAM\text{-}Sig_A$ = Sign(Q_A){IAM_A, $Time_A$}
IAM_A with {$Time_A$, $IAM\text{-}Sig_A$, CIC_A}
Check CIC_A expiration, revocation and signature
If CIC is valid, verify IAM signature
If $IAM\text{-}Sig_A$ is valid, check $Time_A$ and called party number
Setup the call and present verification result to the called party
Address Complete Message (ACM) with verification result

Figure 8: Sequence diagram showing the core steps to initiate an authenticated call request

setup process.

The existing parameters of the IAM is listed in Q.763 [20] Table 32. The proposed extended IAM parameters could be as follows in Table 1.

Table 1: Extended IAM parameters proposed

Parameter	Type	Length (octets)
UTC Timestamp	Optional Part	4-?
Signature Algorithm	Optional Part	1-?
Signature	Optional Part	16-?
Caller Identity Certificate	Optional Part	32-?

To ensure transit compatibility, the extended IAM would include a *Parameter Compatibility Information* parameter to instruct the existing transit exchanges to transfer the extended IAM parameters transparently to the destination exchange. The specifics of the Parameter Compatibility Information parameter can be found in Q.764.2.9.5.3.2 [19].

To inform the originating exchange that the authenticated call request has successfully pass verification at the destination exchange, we also recommend including a *Request Verification Status* parameter in the optional part of the address complete message to provide a feedback on the verification result. This would be useful for the originating exchange to determine if the extended IAM has been successfully verified by the destination exchange and make corrections if needed.

After the last step, the called party decides whether to answer the call request based on the caller ID and the verification result.

5.1. Security Considerations

Even as we outlined the reference scheme to authenticate the caller ID, we also need to assume that there is a constant threat of malicious actors stealing the caller's identity, such as by seizing control of the caller's phone number, or stealing the private key of the caller ID certificate. Cell phone theft is an ever-prevalent issue, and many users simply do not secure their cell phones. Furthermore, having a valid caller ID certificate does not imply that the caller should always be trusted. As a critical security measure, the certificate authority therefore must also be able to deal with revocations of a previously-issued certificate.

Learning from the pains of maintaining and distributing revoked certificates on the Internet, where Certificate Revocation Lists (CRLs) [24] have the disadvantage of being unboundedly bulky for a large number of revocations, and the alternative Online Certificate Status Protocol (OCSP) [25] has the disadvantage of requiring the receiving party to open a real-time connection with the issuer, potentially stalling the communication, therefore, we need to explore a different approach to handle certificate revocations in the PSTN. Furthermore, in many cases, we also need to assume that the victims of identity theft may not realize that they have been compromised, therefore revoking a certificate after an incident may not help.

With that in mind, we will provide some additional discussion on how certificate revocations should be handled in the PSTN. First, we recommend having the CA issue short-term caller ID certificates to limit the expiration period. We recommend limiting the certificate expiration to no more than 72 hours (inspired by the typical time needed to settle an automated clearing house transaction in the US). The certificate requester can request to have a certificate with an even shorter expiration. There are two notable benefits to having short-term certificates. First, it reduces the risk from a successful theft of the certificate private key or phone number by containing the impersonation threat within a bounded period. Second, it significantly reduces the size of revocation lists as the CAs would only need to assert or revoke unexpired certificates within a bounded period. Of course, the downside of having short-term certificates is that the caller ID certificates must be renewed frequently. However, unlike the Internet domain certificates where it can take hours due to a manual process and DNS propagation delay, caller ID certificate renewals would not have this problem because the process of verifying a telephone number can be fully automated and completed within seconds. Furthermore, because the amount of future certificate renewals is largely predictable, the CAs would be able to pre-adjust the quality of service to meet future demands, and perhaps even pre-generate some caller ID certificates to further improve service efficiency.

Second, we recommend having the CA issue caller ID certificates for conditional usage, such as by limiting the usage to a specific method of contact, or by excluding features such as call forwarding, SMS, MMS, etc. This further reduces the risk from a successful identity theft by containing the threat to limited methods of contact. For instance, it is unlikely that a customer support department would need to contact individuals using SMS or MMS, hence, a successful theft of the bank's caller identity would force the attacker to use a live human or synthesized voice when contacting their victims, which could make the impersonation scam sound suspicious.

Finally, we recommend using CRL over OCSP when verifying revoked certificates. A phone call is more urgent compared to email and web communication, if a phone call is stalled by the certificate verification process, the calling party may assume that the called party cannot answer and hang up. It is important that the authentication scheme does not cause significant delays, otherwise some users may even choose to abandon security verification. CRL has an advantage over OCSP in this regard, because the revocation list can be cached at the destination exchange for immediate verification. Of course, the downside of CRL is that it does not receive real-time revocation updates, however, we believe that the risks can be mitigated by having the originating exchange or calling party choose to use even shorter-term certificates, and by having the destination exchange choose to update the revocation lists more frequently.

5.2. Local Deployment Considerations

As we outlined the process to verify the calling party number at the destination exchange, we also need to consider how the security indicator for the caller ID verification status would be transmitted and presented to the called party.

At the destination exchange, the local exchange carrier would present the caller ID verification status in a local call setup format (e.g., POTS, GSM, CDMA, UTMS, SIP, etc.). Each local exchange carrier would decide on the implementation of this presentation scheme, since they have full control over the vertical stack of network standards within their own network. An immediate thought is to simply implement the caller ID verification status as an indicator flag added to the existing caller ID format. However, this can be risky, we will provide some additional discussion on how it should be implemented.

In mobile telephone networks, popular technologies of which include the GSM (Global System for Mobile Communications), CDMA (Code Division Multiple Access), and LTE (Long Term Evolution). In these technologies, the caller ID is typically a parameter within the SETUP message transmitted to the called party's user equipment via an encrypted wireless signal. Assuming that the wireless transmission is well encrypted, a key consideration here is whether the identity of the base station is authenticated. In technologies that provide mutual authentication between the mobile phone and the base station, the presentation can be implemented as a flag indicator parameter, after performing the call verification at the destination exchange. However, in technologies where base station authentication is missing or flawed, the local exchange network should not use the flag indicator approach, because the verification status flag would be vulnerable to being spoofed by an attacker that could spoof a base station. If the call request can be spoofed by a fake base station (such as an IMSI-catcher), the verification status flag can also be spoofed by the fake base station. Instead, the presentation of caller ID verification status should be implemented as a full conversion of the extended IAM parameters, transmitted to the called party, to allow the called party's user equipment to perform verification of the authenticated call request.

In landline telephone services, the most popular technology of which is the POTS (Plain Old Telephone Service), the caller ID is a parameter within the header message encoded in SDMF (Single Data Message Format) or MDMF (Multiple Data Message Format), transmitted to the called party's telephone terminal in FSK (Frequency Shift Keying) signal between the first and second ring. Assuming that the connection to the central office exchange is secure (such as from physical protection), a key consideration here is whether the call request header is integrity protected. In POTS, the call request header is potentially vulnerable to "Orange box" attacks, where a malicious caller is able to alter the SDMF/MDMF header with spoofed FSK signals, as a result, the verification status flag would be vulnerable to being spoofed by the malicious caller. Hence, in such cases, the conversion should also be implemented as a full conversion of the extended IAM parameters to ensure that only the bona fide calling party can produce the authenticated call request.

Therefore, in summary, when implementing the presentation of the caller ID verification status at the local exchange network, only in scenarios where (1) the local exchange network connection is secured, (2) the identity of the local exchange carrier is authenticated, and (3) the call request header is integrity protected, should the local exchange carrier implement the presentation of verified caller ID as an indicator flag, otherwise, the conversion should be implemented as a full conversion of the extended IAM parameters to allow the called party's user equipment to perform verification of the call request.

6. RELATED WORKS

Peterson et al. [26] recently proposed an identity authentication mechanism for end users that originate SIP (Session Initiation Protocol) requests. The scheme proposes having the SIP proxies generating and inserting a PASSporT object [27] (a type of identity token) in the Identity header of every SIP request. Other than transport protocol and data format differences, the scheme uses a similar identity-token based mechanism in authenticating and verifying the caller identity. However, Peterson et al's proposal requires TLS connection for every communication, for reasons mentioned before, is difficult to adapt to the PSTN.

Reaves et al. [28] recently proposed an in-band modem for executing a TLS-inspired authentication protocol over the voice channel of the conversation. The modem is designed to overcome the challenges of low transmission bitrate due to voice codec and transmission losses. After the in-band modem established a data channel between the two parties over the voice channel, the scheme uses a cryptographic challenge-response based scheme to verify the caller's identity. The scheme can provide strong security guarantees comparable to the TLS. However, the verification process require both parties' telephone terminals to support read-write access and live processing of the voice signals, which would require significant computation power on both parties' telephone terminals. It could also invoke privacy fears due to voice recording capability, and potentially add significant delay prior to the voice conversation.

7. CONCLUSION

With increasing abuse of PSTN's insecurities from untrusted parties, telephone spam, phone fraud and caller ID spoofing is poised to increase significantly. To ensure a sustainable future for the PSTN, the SS7 is in critical need of an upgrade of its core robustness. As a first step, we propose a caller ID authentication scheme for Q.731.3 calling line identification presentation. This work will serve as an inspiration for future standards to specify the verification processes and formats in authenticating SS7 identities.

8. ACKNOWLEDGMENT

This work was supported in part by grants from the Center for Cybersecurity and Digital Forensics at Arizona State University.

REFERENCES

[1] Federal Trade Commission, "Consumer Sentinel Network Data Book for January - December 2015," 2016.

[2] Financial Fraud Action UK, "FFA - Fraud the Facts 2016," 2016.

[3] Federal Communications Commission, "Telephone Consumer Protection Act 47 U.S.C. 227," 1991.

[4] OFCOM: The Office of Communications, "Nuisance calls and messages," 2012.

[5] Federal Trade Commission, "National Do Not Call Registry," https://www.donotcall.gov/, 2016.

[6] TPS: Telephone Preference Service, "Register," http://www.tpsonline.org.uk/tps/number_type.html, 2016.

[7] TrueCaller, "Americans lost $8.6 billion in phone scams: Learn to protect yourself," http://www.truecaller.com/blog/americans-lost-86-billion-in-phone-scams-learn-to-protect-yourself, 2014.

[8] Federal Trade Commission, "National Do Not Call Registry Data Book for Fiscal Year 2015," 2016.

[9] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn, "SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephony Spam," in *Proceedings of the 37th IEEE Symposium on Security and Privacy*. IEEE, 2016.

[10] Jason Fagone, "The serial swatter," *The New York Times Magazine*, Nov 2015.

[11] NANPA : North American Numbering Plan Administration, "About the North American Numbering Plan," https://www.nationalnanpa.com/about_us/abt_nanp.html.

[12] Jonathan Rosenberg, Henning Schulzrinne, Gonzalo Camarillo, Alan Johnston, Jon Peterson, Robert Sparks, Mark Handley, and Eve Schooler, "Sip: session initiation protocol," Tech. Rep., 2002.

[13] K Morneault and J Pastor-Balbas, "Signaling System 7 (SS7) Message Transfer Part 3 (MTP3)-User Adaptation Layer (M3UA)," 2006.

[14] Dune Lawrence, "An Identity Thief Explains the Art of Emptying Your Bank Account," *Bloomberg Businessweek*, 2015.

[15] International Telecommunication Union, "Q.731.3 : Stage 3 description for number identification supplementary services using Signalling System No. 7 : Calling line identification presentation (CLIP)," 1993.

[16] International Telecommunication Union, "Q.81.1 : Stage 2 description for number identification supplementary services : Direct dialling-in," 1988.

[17] International Telecommunication Union, "Q.951.3 : Stage 3 description for number identification supplementary services using DSS 1 : Calling line identification presentation," 1993.

[18] International Telecommunication Union, "I.251.3 : Number identification supplementary services : Calling Line Identification Presentation," 1992.

[19] International Telecommunication Union, "Q.764 : Signalling System No. 7 - ISDN User Part signalling procedures," 1999.

[20] International Telecommunication Union, "Q.763 : Signalling System No. 7 - ISDN User Part formats and codes," 1999.

[21] International Telecommunication Union, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks," 2012.

[22] International Telecommunication Union, "E.164 : The international public telecommunication numbering plan," 2010.

[23] D Cooper, S Santesson, S Farrell, S Boeyen, R Housley, and W Polk, "Internet X. 509 Public Key Infrastructure Certificate and CRL Profile," *RFC5280*, 2008.

[24] Russell Housley, W Polk, Warwick Ford, and David Solo, "Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile," Tech. Rep., 2002.

[25] Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, "X. 509 Internet public key infrastructure online certificate status protocol-OCSP," Tech. Rep., 1999.

[26] Cullen Jennings, Jon Peterson, and Eric Rescorla, "Authenticated Identity Management in the Session Initiation Protocol (SIP) draft-ietf-stir-rfc4474bis-09," *IETF*, 2016.

[27] Chris Wendt and Jon Peterson, "Persona Assertion Token draft-ietf-stir-passport-03," *IETF*, 2016.

[28] Bradley Reaves, Logan Blue, and Patrick Traynor, "Authloop: End-to-end cryptographic authentication for telephony over voice channels," in *25th USENIX Security Symposium*. 2016, USENIX Association.