Toward Standardization of Authenticated Caller ID Transmission

Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn

Abstract

With the cost of telecommunication becoming as cheap as Internet data, the telephone network today is rife with telephone spam and scams. In recent years, the U.S. government has received record numbers of complaints on phone fraud and unwanted calls. Caller ID is at the heart of stopping telephone spam — a variety of apps and services, including law enforcement, rely on caller ID information to defend against unwanted calls. However, spammers are using spoofed caller IDs to defeat call blockers, to evade identification, and to further a variety of scams. To provide a solution to this problem, this article proposes a standardized authentication scheme for caller ID that enables the possibility of a security indicator for telecommunication. The goal of this proposal is to help prevent users from falling victim to telephone spam and scams, as well as provide a foundation for future and existing defenses to stop unwanted telephone communication based on caller ID information.

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. Phone fraud and voice phishing, or vishing, is also becoming a significant and rapidly growing problem. Many of these telephone scams and spam today are disseminated using an autodialer, which automatically dials telephone numbers and either connects the call to a live person or plays a recorded message (aka robocalls).

Despite various products and services aimed at stopping telephone spam, scams, and robocalls, complaints about illegal calls have reached record high levels in recent years. According to recent U.S. government reports, the number of phone fraud complaints in the United States more than doubled in just a matter of two years from 2013 to 2015 [1]. During the 2016 fiscal year, the national Do-Not-Call Registry faced a near 50 percent surge in the number of consumer complaints about unwanted telemarketing calls, and the total number of complaints that year has grown to more than 5.3 million [2]. In the United States, more than 75 percent of the reported fraud and identity theft attempts are now communicated over the phone [1].

At the root cause of this issue, not only has telephone spam become economically viable due to VoIP and autodialers, but illegal callers today have access to various technologies aimed at circumventing call blockers and evading identification. Among them, a practice known as *caller ID spoofing* is particularly effective at defeating call blockers, evading identification, and furthering a variety of scams. According to a 2013 consumer poll, 22 percent of U.S. smartphone users used a call blocking app or a feature to block calls on their device [3]. However, a malicious caller can easily bypass caller ID blacklisting by spoofing any number not blacklisted. As most telephone spam defenses today (including law enforcement) rely on user feedback, caller ID spoofing has also made user feedback completely irrelevant.

Abuse of Caller ID Spoofing

Caller ID spoofing is often used in a variety of phone scams. For example, there are several bank verification scams where the spammer spoofs the caller ID of a credit card issuing bank [4], and mimics audio from the credit card issuer's interactive voice response system to scam his/her recipients [5]. The audio recording tells the victims that their credit cards have been deactivated due to fraud, and the companies are in urgent need of verifying the victims' personal information to reactivate their accounts. 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. A malicious caller could spoof a known number to commit crimes, such as making phishing calls, making fake purchase orders, or sending police to a person's address for harassment [6]. As a result, true owners of spoofed caller IDs could end up in trouble.

Because of the prevalence of caller ID spoofing, it has led to many becoming overly suspicious of phone calls, even when they are for legitimate urgent and critical information. In a recent revelation about Russian cyberattacks on the Democratic National Committee (DNC), the DNC blew off FBI's repeated hack warnings because the workers could not differentiate a real FBI agent call from an impostor [7].

Overview of Caller ID

Since its introduction in the 1990s, caller ID service has now become ubiquitous in almost every form of telephone service. Today, caller ID is also used in other telephone services, such as SMS and MMS, and, with the prevalence of smart-

Digital Object Identifier:
10.1109/MCOMSTD.2017.1700019

The authors are with Arizona State University.

2471-2825/17/$25.00 © 2017 IEEE

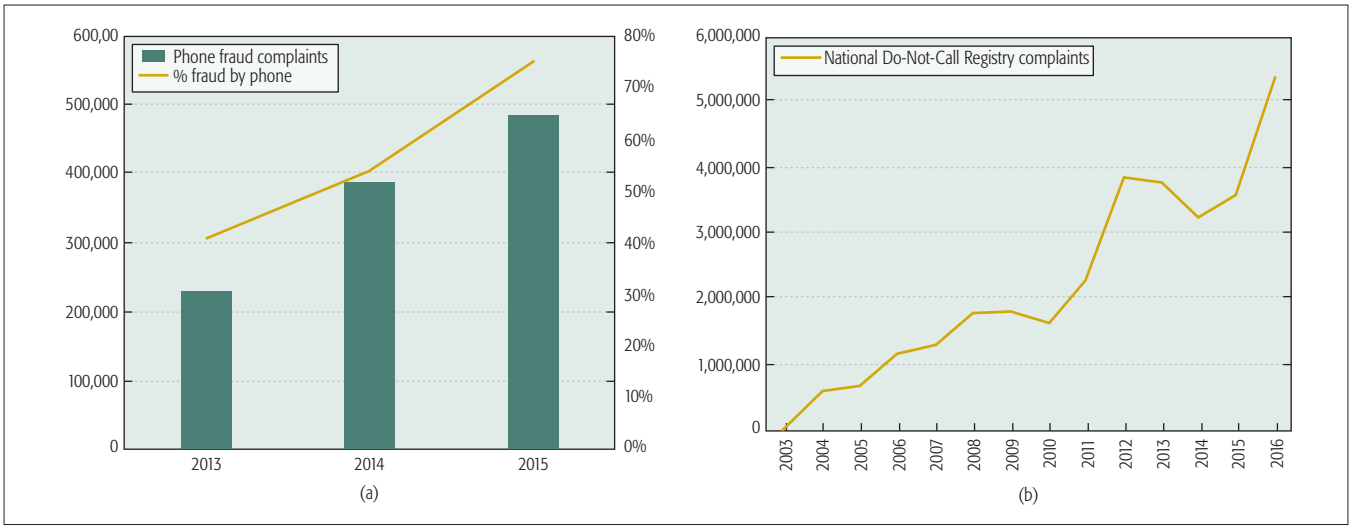

FIGURE 1. Recent U.S. government statistics on phone fraud and call complaints: a) phone fraud complaints each year received by the FTC Consumer Sentinel Network [1]; b) call complaints each year received by the National Do-Not-Call Registry [2].

phones, many apps and services also rely on caller ID for identification.

The core process of providing caller ID is known as Calling Line Identification Presentation (CLIP), which was first defined in International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) Recommendation Q.731.3 [8] for the Signaling System No. 7 (SS7) network in 1993. The SS7 network is the backbone infrastructure for most of the world's PSTN telephone calls. Even as the telephone backbone moves toward being carried by an IP packet-based infrastructure, Q.731.3 still plays a major role in providing caller ID for telecommunications and will continue to do so for many years to come.

In all major existing call signaling protocols (SS7, H.323, and SIP), caller ID is either provided by the originating exchange or by the calling party. In SS7 and SIGTRAN (the IP version of SS7), caller ID is defined by the calling party number (CPN) parameter, where the parameter is an optional part of the initial address message (IAM). The IAM is sent to the destination exchange as part of the basic call procedures according to Q.764 [9] to initiate a call. 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 (e.g., mobile or landline).

How Caller ID Spoofing Works

In the process of providing caller ID, the originating exchange can control what caller ID number is sent on a call-by-call basis. As the PSTN is traditionally regarded as a closed network of SS7 exchange switches between trusted operators, usually only an SS7 switch operator or a private branch exchange (PBX) owner has the ability to customize the caller ID. Since it was prohibitively expensive for individuals and small businesses to gain switch-level access to the SS7 network, in most telephone services, their caller IDs are typically managed by the caller's telephone carrier.

However, with growing access to the PSTN from the Internet, there are now many Internet telephone service providers (ITSPs) that provide telephone services over an Internet connection. With ITSPs, individuals and businesses are no longer limited to telephone services from their local telephone service providers. With an Internet connection, a malicious caller now has access to a world of ITSPs that can provide features such as caller ID customization/spoofing.

To spoof a caller ID, the caller's originating exchange would declare the CPN parameter with false information. In the United States and many other jurisdictions, the caller's telephone service provider does not have any legal obligation to ensure that the caller ID is verified before it is transmitted. Even in jurisdictions that forbid telephone service providers from providing falsely declared caller IDs, with Internet access to an untrustworthy telephone service provider, it is easy for a malicious caller to start a call request from a different origin and transmit a fake caller ID.

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

At the heart of the issue, there is a lack of authenticity and accountability in the transmission of telephone identities. The PSTN has transformed from a closed trusted ecosystem to a diverse global ecosystem, so mutual trust can no longer be relied on to guard against the abuses of trust in caller ID transmission. Addressing this issue requires the core protocol to provide a mechanism to ensure authenticity and accountability. This is why we advocate for a standardized caller ID authentication scheme. By providing authentication to the caller ID, authenticity and accountability of the caller ID can be ensured. However, viable deployment of authenticated caller ID transmission requires mutual interoper-

To provide a solution to this problem, we drew inspiration from the Internet. The Internet is widely known for its exposure to intrusion and man-in-the-middle attacks from untrusted parties around the world. In such a relatively untrusted environment, solutions were developed to combat identity spoofing.

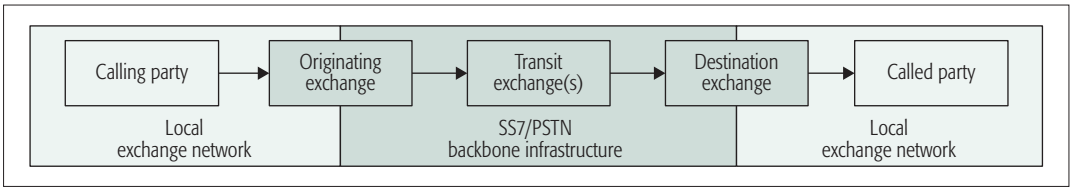

Figure 2. An overview of call routing.

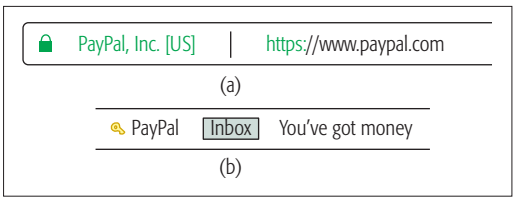

Figure 3. Examples of existing security indicators in HTTP and email communication: a) an example of an HTTPS security icon in Google Chrome; b) an example of an authentication icon in Gmail.

ability. Therefore, standardization is the key to building a telephone ecosystem that could rely on the assurance of caller IDs.

Solution: Security Indicators

To provide a solution to this problem, we drew inspiration from the Internet. The Internet is widely known for its exposure to intrusion and man-in-the-middle attacks from untrusted parties around the world. In such a relatively untrusted environment, solutions were developed to combat identity spoofing.

In the Internet ecosystem, HTTP and email communication are arguably the most popular types of communication used today. In HTTP communication, the universally recognized padlock indicator with the name of the company displayed in the address bar of modern web browsers (e.g., the one shown in Fig. 3a) provides users with immediate trust in the website's domain and entity name identity.

In email communication, the key-shaped security indicator of the email sender (e.g., the one shown in Fig. 3b) in some email clients provides users with immediate trust in the identity of the email sender.

An example of a possible caller ID security indicator for an incoming call is shown in Fig. 4. The security indicator can be similarly attached to other forms of telecommunication such as SMS and MMS.

These security indicators are crucial for informing the user that the information is from a verified source. The availability of the security indicator provides an immediate indication of the authenticity of the sender's identity. The recognizability of the security indicator icon provides an immediate understanding of the functionality of the indication. By simply recognizing an icon, users are able to protect themselves from phishing and impersonation scams. The prevalence of security indicators promotes awareness that the user should only trust senders that are verified, which would inspire users to be more vigilant of calls and messages from unverified sources.

Having a security indicator for telecommunication would also be an effective solution against telephone spam. Apps and services can be built on top of the security indicator to analyze whether a call comes from an untrusted source to more effectively block unwanted callers. According to a recent comprehensive survey of various telephone spam countermeasures [10], solutions based on caller ID analysis are close to being overall ideal. If caller ID spoofing can be effectively prevented, caller ID analysis will be able to satisfy the criteria of being usable, deployable, and robust.

With the growing prevalence of phone fraud, calls from billing, banking, government, and law enforcement organizations would also benefit from providing authenticity of their caller IDs, as their recipients would be certain that the caller is real and not an impostor, and therefore feel more assured receiving communication over the phone.

Caller ID Authentication

The main communication service used in the telephone network is voice; in addition, SMS and MMS service are popular among mobile telephone users. There is a caller identity authentication standard proposal for the Session Initiation Protocol (SIP) [11]. Authenticating the SIP caller identity is insufficient to provide authenticated transmission of caller identity for the majority of existing domestic and international telephone networks [12]. This article focuses on authenticating the caller ID for telephone calls in the SS7 network. The proposed authentication process can be modeled to provide authenticated transmission of telephone identities for other forms of telecommunication.

The current caller ID transmission scheme has two fundamental insecurities:

1. A lack of verification and authentication of the declared caller ID
2. A lack of integrity protection of the transmitted caller ID

The current calling line identification presentation scheme allows the CPN to be declared arbitrarily. 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 principles of a prospective caller ID authentication scheme must address the aforementioned fundamental security flaws:

1. Ensuring that the caller ID is verified and authenticated. That is, it can only be produced by the calling party or the originating exchange before transmission.
2. Ensuring that the caller ID is guarded against unwanted modification during transit. Furthermore, it is crucial that the users of caller ID authentication enjoy the same user experience as before.

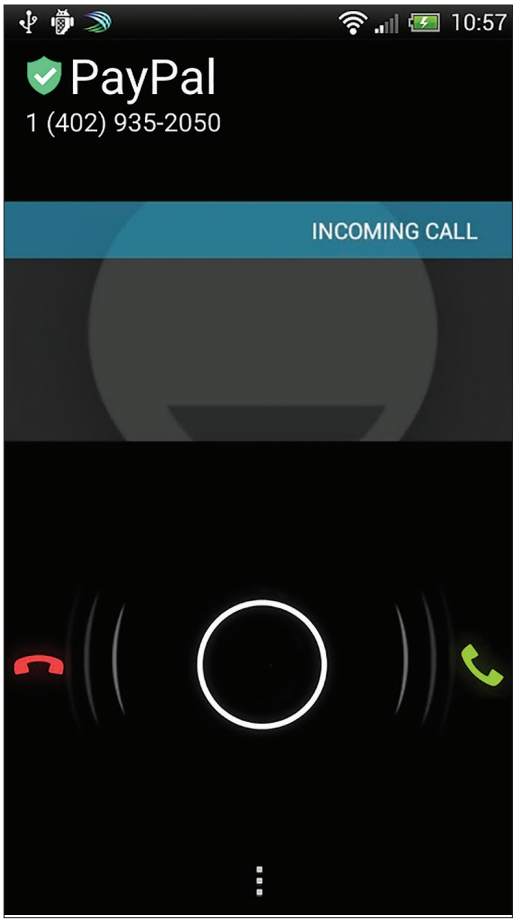

Figure 4. An example of the proposed caller ID security indicator for an incoming call.

3. It must also be able to coexist with the existing call control signaling protocols.

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 be used to secure the caller ID, is ill suited for the PSTN. The PSTN primarily uses the SS7 protocol stack to service telephone calls, whereas SSL/TLS was mainly designed to encrypt data communication, which has significant transport and latency overhead. After establishing an initial end-to-end connection with a TCP three-way handshake, the SSL/TLS process requires two additional round-trips (four-way handshake) to establish a secure connection. In the SS7 call request, this "handshake" is a one-way forward transmission (as shown in Fig. 5), where the originating exchange sends an initial address message to the destination exchange to reduce the delays of initiating a call. Implementing the SSL/TLS scheme for SS7 would require all exchange switches to support the multi-way handshake process, which not only requires critical changes, but could potentially add significant delays to the call request process. In addition, SSL/TLS is designed for a client-server web 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").

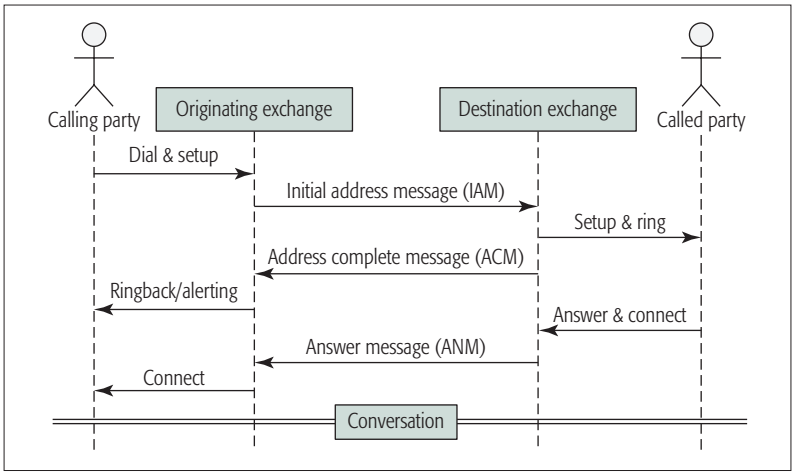

Figure 5. An overview of the existing call request transmission process.

Therefore, we need to design an authentication scheme better suited for the PSTN. This article presents the high-level idea of a suitable caller ID authentication scheme, further technical details of which were published in the *Proceedings of ITU Kaleidoscope 2016 — ICTs for a Sustainable World* [13].

Proposed Scheme

The central idea of the scheme is to introduce a public key infrastructure (PKI) scheme for the PSTN. The high-level architecture of the proposed scheme is shown in Fig. 6. The scheme will have CAs certify, issue, and revoke caller ID certificates (CICs) for the calling parties that have proven ownership of their respective telephone numbers. After successfully obtaining the CIC, the calling party's originating exchange can then use the caller ID certificate to generate an authenticated call request by extending the existing initial address message. Upon receiving an IAM call request, the destination exchange then checks for the presence and validity of authenticated call request parameters and presents the validated caller ID using a security indicator during the call setup to the called party.

The role of each actor with regard to the caller ID authentication scheme is as follows.

Certificate Authority: an entity in the PSTN that verifies phone number ownership and issues caller ID certificates to a requester that successfully provides proof of phone number ownership. The CA is a trusted third party, trusted by both the calling party and the called party relying on the certificate. The CA is also responsible for revoking caller ID certificates if needed.

Calling Party: sets up a call request with the originating exchange for the called party. Under the caller ID authentication scheme, the calling party or the originating exchange may initiate a request to obtain a caller ID certificate from the CA.

Originating Exchange: obtains and stores the caller ID certificate from the CA for the calling party's phone number. Upon a call request, the originating exchange generates an authenticated IAM on behalf of the calling party and transmits it to the destination exchange.

Destination Exchange: receives the authenticated IAM and checks the validity and authen-

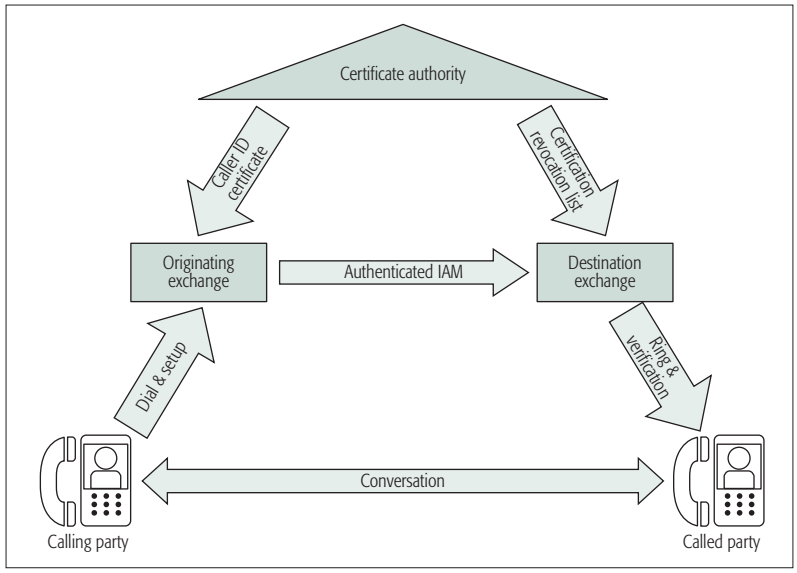

FIGURE 6. High-level overview of the proposed scheme

ticity of the call request, and sets up the call with the called party with a security indicator showing the caller ID verification status. The destination exchange may also forward the authenticated IAM to the called party to allow verification to be performed at the terminal for better security.

Called Party: receives the call/ring request with a verification status or authenticated IAM. The terminal displays an incoming call with a security indicator.

The processes of the authentication scheme can be logically divided into two parts: caller ID verification and authenticated call request.

In the caller ID verification process, the goal is for a CA to verify a calling party's ownership of a phone number (i.e., the phone number actually routes to the calling party) and then issue a certificate. The verification process can take advantage of the fact that *receiving* a call or message is proof of phone number ownership in the PSTN. In the actual process, more steps are involved to ensure the authenticity of the CA's identity and the integrity of the certificate request. The calling party/originating exchange will thus need to generate a public-private key pair and store the private key securely. After proving to the CA that the calling party/originating exchange is really the owner of the phone number and the public key, the public key of the calling party is signed by the CA with attributes indicating phone number ownership information, turning it into a caller ID certificate.

Although verification of a caller ID can also be done directly by the called party, where the called party can check for the authenticity of a caller ID by simply calling/messaging back the calling party's phone number, as proposed in previous works [14, 15], this type of scheme adds delays to each communication and is repetitive for each call request. A PKI certification model eliminates the need for a connection-oriented, repetitive callback verification on every call request.

In the authenticated call request process, the goal is for a certified calling party to generate an authenticated call request so the called party trusts that the CA has guaranteed the caller ID really belongs to the calling party. When initiating a call request, the calling party's originating exchange will generate an extended IAM that includes some additional parameters which authenticate the call request. These additional parameters are designed to prove that the caller ID is authentic, and the request is transient and unique (non-repeatable) to guard against "cut and paste" or replay attacks by a man-in-the-middle or malicious calling party. Upon receiving the extended IAM, the destination exchange checks the authenticity and validity of the call request and sets up the call with the called party with a security indicator showing the caller ID verification status. The destination exchange may also forward the extended IAM to the called party to allow verification to be performed at the terminal for better protection against man-in-the-middle attacks.

The authenticated call request process does not change the existing one-way process of transmitting the call request using the IAM, which is what enables a call request to be delivered quickly and thus can be implemented without adding perceivable delay to the existing user experience of initiating a call.

To ensure transit compatibility, the extended IAM would include a *Parameter Compatibility Information* parameter to instruct the existing transit exchanges to transparently forward the extended parameters to the destination exchange. The specifics of Parameter Compatibility Information can be found in Q.764 (12/99) section 2.9.5.3.2 [9].

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

Security Considerations

Even as we outline the 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 mobile phone theft, or using a malware to steal the private key. Furthermore, having a valid caller ID certificate does not imply that the caller should *always* be trusted. As a critical security measure, the CA must also be able to deal with revocations of a previously issued certificate.

Learning from the pains of revoking certificates on the Internet, where using a certificate revocation list (CRL) [16] has the disadvantage of distributing bulky lists for large numbers of revocations, and the alternative Online Certificate Status Protocol (OCSP) [17] has the disadvantage of requiring the receiving party to open a real-time connection with the CA, potentially stalling the communication, we need to explore a more suitable approach for handling certificate revocations in the PSTN.

With that in mind, first, 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, it will severely affect the user experience. It is important that the authentication scheme does not cause perceivable 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. The downside of CRL is that it does not receive real-time revocation updates; however, the risks can be mitigated by having the originating exchange or calling party choose to use shorter-term certificates, and by having the destination exchange choose to update the revocation list more frequently.

Second, unlike domain certificates, which are typically valid for years at a time, in PSTN, we recommend that the CA issue short-term caller ID certificates to limit the expiration period. There are two reasons for 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 CA would only need to revoke unexpired certificates within the bounded period. Of course, the downside of having short-term certificates is that caller ID certificates must be renewed frequently. However, unlike domain certificates, which can last for hours due to Domain Name Service (DNS) propagation delay, caller ID certificate renewals could be completed within seconds as the process of verifying a telephone number can be fully automated. Furthermore, because the number of future certificate renewals is largely predictable, 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.

Finally, we recommend the CA issue caller ID certificates for conditional usage, limiting the usage to a specific method of contact or capability of the calling terminal, such as by whitelisting/blacklisting features including SMS, MMS, call forwarding, and so on. This further reduces the risk from a caller identity theft by containing the threat to limited methods of contact. For instance, it is unlikely that a customer support phone would need to contact individuals using SMS or MMS; hence, a successful theft of the company's caller identity would force the attacker to use voice when contacting the victims, which could make the scam sound suspicious.

Local Deployment Considerations

Having 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 exchange call setup format (e.g., POTS, GSM, SIP). Hence, for a local exchange network to support the caller ID verification scheme, some type of modification/extension to the local call setup format is required, since each SS7 call request will need to be converted to a local call setup format. An immediate thought is to implement the caller ID verification status as a simple indicator flag/parameter added to the local exchange call setup format. However, there are some risks in such an implementation. We would like to provide some discussion on how a conversion of an authenticated call request should be implemented.

In mobile telephone services, caller ID is typically a parameter within a 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 (e.g., GSM), 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. Instead, the presentation of caller ID verification status should be implemented as a forwarding 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, namely the plain old telephone service (POTS), caller ID is a parameter within the header message encoded in Single Data Message Format (SDMF) or Multiple Data Message Format (MDMF), transmitted to the called party in frequency shift keying (FSK) signal. Assuming that the connection to the central office exchange is secure (e.g., 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, and, as a result, the verification status flag would be vulnerable to being spoofed by the malicious caller. Hence, in such cases, the caller ID verification status should also be implemented as a forwarding of the extended IAM parameters to protect the integrity of the authenticated call request.

Therefore, in summary, when implementing the presentation of caller ID verification status to the called party, only in scenarios where:

1. The local exchange network connection is secured
2. The identity of the local exchange carrier is authenticated
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 caller ID verification status should be implemented as a forwarding of the extended IAM parameters to allow the called party's user equipment to perform verification of the call request.

Conclusion

This article proposes a standardized authentication scheme for the caller ID that enables the possibility of a security indicator for SS7 telecommunication. The goal of this proposal is to help prevent users from falling victim to telephone spam and scams, as well as provide a foundation for future and existing defenses to stop unwanted telephone communication based on caller ID information.

With the growing prevalence of phone fraud, calls from billing, banking government, law enforcement organizations would also benefit from providing authenticity of their caller IDs, as their recipients would be certain that the caller is real and not an impostor, therefore feel better assured receiving communication over the phone.

The goal of this proposal is to help prevent users from falling victim to telephone spam and scams, as well as provide a foundation for future and existing defenses to stop unwanted telephone communication based on caller ID information.

Acknowledgment

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

References

[1] FTC, "Consumer Sentinel Network Data Book for Jan.–Dec. 2015," 2016.

[2] FTC, "National Do Not Call Registry Data Book for Fiscal Year 2016," 2016.

[3] Marketwired, "From Stalkers to Spam, WhitePages Study Breaks Down Reasons Americans Block Calls," http://www.marketwired.com/press-release/from-stalkers-to-spam-whitepages-study-breaks-down-reasons-americans-block-calls-1900134.htm.

[4] A. Johnson, "Scammers Can Fake Caller Id Info — Consumer Information," https://www.consumer.ftc.gov/blog/scammers-can-fake-caller-id-info, 5 2016, accessed Apr. 3, 2017.

[5] Numbercop, "Smishing & Vishing News? Weekly Summary 3/2-3/8," https://numbercop.tumblr.com/post/115252732893/weekly-summary-32-38, 4 2015, accessed Apr. 3, 2017.

[6] Julianne Pepitone, "'Swatting' Celebrities Is Far Too Simple," http://money.cnn.com/2013/04/14/technology/security/swatting-caller-id/, 4 2013, accessed Apr. 3, 2017.

[7] E. Lipton, D. E. Sanger, and S. Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times*, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html, 12 2016, accessed Apr. 6, 2017.

[8] ITU, "Q.731.3 : Stage 3 Description for Number Identification Supplementary Services Using Signalling System No. 7: Calling Line Identification Presentation (CLIP)," 1993.

[9] ITU, "Q.764 : Signalling System No. 7 — ISDN User Part Signalling Procedures," Dec. 1999.

[10] H. Tu *et al.*, "SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephony Spam," *Proc. 37th IEEE Symp. Security and Privacy*, 2016.

[11] C. Jennings, J. Peterson, and E. Rescorla, "Authenticated Identity Management in the Session Initiation Protocol (SIP)," IETF, 2016.

[12] E. Burgerand and J. Kieserman, "S2ercproject: Next Generation Calleridentification," https://s2erc.georgetown.edu/sites/s2erc/files/files/upload/stir_status_and_analysis.pdf, 6 2016, accessed Apr. 10, 2017.

[13] H. Tu *et al.*, "Toward Authenticated Caller ID Transmission: The Need for a Standardized Authentication Scheme in Q.731.3 Calling Line Identification Presentation," *Proc. ITU Kaleidoscope 2016 — ICTs for a Sustainable World*, Nov. 2016.

[14] N. J. Croft and M. S. Olivier, "A Model for Spam Prevention in IP Telephony Networks Using Anonymous Verifying Authorities," *Proc. Annual Info. Security South Africa Conf.*, 2005.

[15] H. Mustafa *et al.*, "You Can Call but You Can't Hide: Detecting Caller ID Spoofing Attacks," *Proc. Conf. Dependable Systems and Networks*, 2014.

[16] R. Housley *et al.*, "Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," tech. rep., 2002.

[17] M. Myers *et al.*, "X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP," tech. rep., 1999.

Biographies

Huahong Tu (tu@asu.edu) is a Ph.D. candidate in the School of Computing, Informatics, and Decision Systems Engineering and a research assistant at the Center for Cybersecurity and Digital forensics at Arizona State University. His research focuses on security for network and communication protocols, authentication schemes, identity management, and systems engineering. He was a recipient of the Best Paper Award in the *Proceedings of ITU Kaleidoscope 2016* and a recipient of the Graduate Fellowship Award from the Fulton Schools of Engineering at Arizona State University.

Adam Doupé (doupe@asu.edu) is an assistant professor in the School of Computing, Informatics, and Decision Systems Engineering and the associate director of the Center for Cybersecurity and Digital forensics at Arizona State University. His research interests include vulnerability analysis, web security, mobile security, network security, and hacking competitions. In 2017 he received the NSF CAREER award and the Best Teacher Award of the Fulton Schools of Engineering, Arizona State University.

Ziming Zhao (zzhao30@asu.edu) is an assistant research professor in the School of Computing, Informatics, and Decision Systems Engineering, Arizona State University. His current research interests include system and network security. He received his Ph.D. degree in computer science from Arizona State University in 2014.

Gail-Joon Ahn [SM] (gahn@asu.edu) is a professor in the School of Computing, Informatics, and Decision Systems Engineering, Ira A. Fulton Schools of Engineering at Arizona State University. His research has been supported by the National Science Foundation, the Department of Defense, the Office of Naval Research, the Army Research Office, the Department of Justice, and the private sector. He is a recipient of the Department of Energy Early Career Investigator Award. He received his Ph.D. degree in information technology from George Mason University, Fairfax, Virginia, in 2000.