

Network Working Group
Internet-Draft
Intended status: Informational
Expires: June 3, 2013

A. Cooper
CDT
H. Tschofenig
Nokia Siemens Networks
J. Peterson
NeuStar
B. Aboba
Microsoft
November 30, 2012

Secure Call Origin Identification
draft-cooper-iab-secure-origin-00.txt

Abstract

A number of parties have suggested creating mandates such that networks receiving voice calls would be capable of securely identifying the call origin. This document provides insights about the capabilities and limitations of supporting call origin identification in a secure and privacy- friendly way in the PSTN and for IP-based real-time communications.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 3, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

Internet-Draft

Secure Origin

November 2012

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Secure Origin Challenges in the PSTN	3
3.	Secure Origin Challenges for VoIP	4
4.	Secure Origin Challenges for Real-Time Communication on the Web	5
5.	Conclusion	6
6.	Security Considerations	7
7.	Informative References	7
	Authors' Addresses	7

Internet-Draft

Secure Origin

November 2012

1. Introduction

A number of parties have suggested creating mandates such that networks receiving voice calls would be capable of securely identifying the call origin [ID-62]. These proposals are primarily motivated by concerns over fraudulent calls and the associated economic impact that spoofed or fraudulent origin identification can have on telecommunications settlement agreements. Concerns have also been raised about ensuring secure origin identification for law enforcement and abuse tracking purposes.

Support for caller identification in the public switched telephone network (PSTN) has been developed to meet existing regulatory needs and for other purposes, but it has limitations. As real-time communication has become IP-based, it has become significantly more difficult to identify the origin of real-time communication for a number of reasons. Furthermore, to the extent that new mandates are being suggested to require origin identification for all IP traffic -- real-time or not -- it is unclear how such identification would be accomplished given the complexity and diversity of today's IP network traffic. This document provides insights about the capabilities and limitations of supporting call origin identification in a secure and privacy-friendly way in the PSTN and for IP-based real-time communications.

2. Secure Origin Challenges in the PSTN

The problems facing origin identification are not limited to the Internet. In the traditional public switched telephone network, information about the calling party is often missing from signaling messages. This is because, per the ITU-T and related national specifications (beginning with Q.761), the calling party number field of a call establishment message (IAM) is an optional parameter. There remain a number of legitimate reasons today why the origin of a telephone call might be absent from call establishment signaling:

because of interworking with a legacy (pre-SS7) network or a private branch exchange which lacks the capability to identify subscribers, for example, or because the call has been handled by an interexchange carrier using calling cards that require the customer to dial a relay number. So long as there are legitimate reasons why the calling party number might be missing from a call, and the parameter remains optional in the SS7 standards, carriers will sometimes fail to provide origin identification in the telephone network. Parties who want to obscure their identity can rely on equipment or carriers that do not provide the calling party number.

Whether or not the calling party number should be trusted, if it is

present, is a separate but related question. Private branch exchanges that signal calls via ISDN (Q.931) can provide an arbitrary calling party number in their own call establishment message (SETUP), and some operators translate those numbers directly to the calling party number field of SS7. Due to the transitive trust inherent in the SS7 network, there is no way for the recipient of a call to determine how trustworthy the calling party number field is: effectively, all carriers in the telephone network necessarily trust the origin identification provided by any carrier. These difficulties have been exacerbated by the widespread deployment of Internet gateways. For these gateways, it is almost always better to supply no calling party number to the SS7 network than it is to accept a number provided by Internet signaling. Because some gateways do accept the numbers provided by Internet callers, however, this further weakens the trustworthiness of calling party number information on the telephone network. These concerns are not limited to calls either: text messages have similar problems resulting from email-to-text gateways.

Our ability to solve origin identification for Internet calling depends on solving it for the telephone network, as Internet telephony solutions inevitably exchange traffic with the telephone network. Given the inherent limitations of SS7 standards for origin identification, the transitive trust properties of the telephone network, and the widespread acceptance of calls without origin identification in the telephone system today, the prospects are very doubtful for remedying this problem by simply mandating that carriers provide origin identification.

3. Secure Origin Challenges for VoIP

Standards for Voice Over IP (VoIP) originally focused on Session Initiation Protocol (SIP) and Extensible Messaging and Presence Protocol (XMPP)-based systems, with SIP becoming a popular foundation for many proprietary VoIP systems. SIP provides a number of different mechanisms for asserting the identity of a caller, including "P-Asserted-Identity" (PAI) [[RFC3325](#)], "SIP Cert" [[RFC6072](#)] and the "SIP Identity" mechanism [[RFC4474](#)]. PAI and SIP Identity allow SIP application servers in the network to insert caller information into the 'From' header of outgoing calls.

However, not all calls will necessarily identify the calling party in any way, and there are no standardized requirements to use any particular caller identification solution. Anonymous calls and calls made from outbound-only calling services generally do not contain identity information. In addition, in some situations, calls made through relay services may identify the relay as the calling party

rather than the original caller.

In addition, the identifier syntax used in SIP varies from email-address-style identifiers to ones that use E.164 telephone numbers. Because of the security shortcomings of the PSTN described above, SIP-based services that seek to make authentication and identification guarantees cannot do so purely with E.164 numbers. Such guarantees would require a universal move toward email-style identifiers.

Even in a SIP-only environment, the choice of syntax, made separately by different implementers and users, impacts the security mechanisms that can be used for attesting to the authenticity of the identifier. Without any form of cryptographic identity assertion, the 'From' header can be easily forged, and headers are often stripped or modified by intermediaries in transit. Attempts at enhancing the integrity protection of SIP identity have not seen wide deployment.

Finally, SIP supports a number of privacy mechanisms that allow SIP users to shield their identities from the network and the called party [[RFC3323](#)] [[RFC5767](#)] [[RFC5379](#)]. SIP privacy has valid uses; for example, it enables users to avoid exposing their identity to

destinations that might make them a target for unsolicited advertising or other undesirable consequences. As in the PSTN, parties that do not wish to disclose their identities can use services that support this functionality.

[4.](#) Secure Origin Challenges for Real-Time Communication on the Web

While SIP and XMPP were originally designed to facilitate interoperable real-time communications between systems developed by different vendors, the last 10 years have seen the rise of a new platform for deployment of applications: the world wide web. Web applications that run in a secure execution environment inside a web browser are now commonplace. As a result, real-time communications -- including voice and video telephony -- are migrating to the web as well.

This new trend in application development enables real-time application to be downloaded on-demand and executed within the browser utilizing new interfaces in the browser platform to interact with the microphone, camera, and other sensors. The integration of real-time communication into the huge web ecosystem opens a number of new possibilities that were previously only possible with proprietary browser plug-ins.

This migration to the web does not eliminate the challenges

associated with providing secure call origin identification; in some ways, it even serves to complicate the situation. While web servers have a common and widely used means of authenticating themselves -- public key-based authentication infrastructure for use with SSL -- no single client-side authentication mechanism has emerged to authenticate users sitting in front of their browsers. Instead, a variety of technologies have been deployed, often with applicability only in narrow sectors.

Enterprise networks, for example, often use hardware tokens to authenticate employees. Banking web sites often require one-time secrets in combination with knowledge-based security. Many consumer-focused web sites tend to rely on insecure password-based authentication. With so many web sites requiring authentication, Web Single-Sign-On (WebSSO) deployments have emerged to attempt to create

a uniform authentication mechanism. But while individual identity providers offering such WebSSO solutions offer security benefits and great convenience for end users, they too are typically limited as far as the scope of web sites that can rely on them for authentication. Relying web sites, likewise, usually only support a single or limited set of identity providers. Consequently, users are confronted with islands on the web that use different identity technologies.

Because web-based real-time applications extends the existing web ecosystem, they also inherit its identity management ecosystem, a system that is still in flux. With new technology being developed every day it is unlikely that a single identity management technology will dominate in the near future. Furthermore, because of the technological differences between web identity management and caller identification in SIP and other previously developed real-time communication technologies, the seamless flow of identity information across these technologies will likely remain elusive for the foreseeable future.

[5.](#) Conclusion

Every calling technology presents significant challenges to the secure identification of the caller. The interoperation of all of these technologies -- from legacy pre-SS7 telephone networks to cutting edge web-based calling services -- further complicates the task of identifying the origin of a call in a trusted and interoperable way. While industry efforts are underway to address some of these challenges, a uniform origin identification system is unlikely to emerge, regardless of potential regulatory mandates.

[6.](#) Security Considerations

This document describes, at a high level, some of the security challenges of providing trustworthy call origin information. There are further detailed privacy and security aspects related to call origin identification that will be addressed in a future version of this document.

7. Informative References

- [RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", [RFC 3323](#), November 2002.
- [RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", [RFC 3325](#), November 2002.
- [RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", [RFC 4474](#), August 2006.
- [RFC5379] Munakata, M., Schubert, S., and T. Ohba, "Guidelines for Using the Privacy Mechanism for SIP", [RFC 5379](#), February 2010.
- [RFC5767] Munakata, M., Schubert, S., and T. Ohba, "User-Agent-Driven Privacy Mechanism for SIP", [RFC 5767](#), April 2010.
- [RFC6072] Jennings, C. and J. Fischl, "Certificate Management Service for the Session Initiation Protocol (SIP)", [RFC 6072](#), February 2011.
- [TD-62] Council Working Group to Prepare for the 2012 World Conference on International Telecommunications, "CWG-WCIT12 Temporary Document 62 Rev.2 - Draft Compilation of Proposals with Options for Revisions to the ITRs", 2012, <<http://files.wcitleaks.org/public/T09-CWG.WCIT12-120620-TD-PLN-0062R2.pdf>>.

Alissa Cooper
CDT
1634 Eye St. NW, Suite 1100
Washington, DC 20006
USA

Email: acooper@cdt.org

Hannes Tschofenig
Nokia Siemens Networks

Email: hannes.tschofenig@gmx.net

Jon Peterson
NeuStar

Email: jon.peterson@neustar.biz

Bernard Aboba
Microsoft

Email: bernard.aboba@gmail.com