SIP Working Group
Internet-Draft
Intended status: Informational
Expires: August 18, 2008

J. Elwell
Siemens

February 15, 2008

SIP E.164 Problem Statement
draft-elwell-sip-e164-problem-statement-00

Status of this Memo

Copyright Notice

Abstract

SIP has long supported the use of both email-style addresses (user@host) and telephone-style addresses (number@host) in the "From:" address. A significant number of SIP deployments use the latter style with E.164 numbers. This document describes the problems that occur when such E.164 numbers are used in SIP.

Table of Contents

1. Introduction

The use of phone numbers with SIP was introduced with the TEL URL scheme [RFC3966]. In particular, this covered the use of E.164 numbers [ITU.E164.1991], as used in the public switched telephone network (PSTN). In RFC 3966, domain names were not used with fully-qualified E.164 phone numbers.

SIP URIs always have domain names. In SIP [RFC3261], a translation between SIP URIs and TEL URLs was described. When translating from a SIP URI to a TEL URL, the domain name from the SIP URI is simply dropped. When translating in the other direction (or simply generating a SIP URI from an E.164 number) it is not clear how to populate the domain name.

2. Discussion

2.1. Domain part of a SIP URI

When an E.164 number is represented as a SIP URI, it includes a domain part. Unfortunately there is no clear definition of what the domain part should contain. On the one hand, it is clear that, in common with any SIP URI, the domain denoted by the domain part should at least be able to route the request onwards towards the destination. Therefore if a SIP URI containing an E.164 number is the target of a SIP request, the request can be routed to the domain given in the domain part and that domain will be able to route the request onwards.

However, this still leaves scope for putting different values into the domain part, subject to the identified domain being able to route requests onwards towards their correct destinations. It has been suggested that the domain part should be the domain that "owns" the E.164 number, but the concept of ownership is unclear. Does an enterprise domain "own" the E.164 numbers assigned to it? Does a

public service provider "own" the E.164 numbers assigned to an enterprise that it serves? What if the enterprise obtains services associated with these numbers from multiple public service providers? Does a service provider "own" E.164 numbers assigned to an end user? Who is the "owner" in number portability situations?

In practice, for a given E.164 number, different domain names tend to be used, although such use is perhaps not the original intent of [RFC3261]. For example, a service provider might always use its own domain name, regardless of whether the URI represents a number assigned to one of its users, a number assigned to a different service provider but served by that first service provider, or some

other number. A service provider that hosts enterprise users might use the service provider's own domain name rather than that of the hosted enterprise. An ENUM look-up on an E.164 number might yield a SIP URI with a domain via which the user of that number can be reached, but not necessarily the end domain of the user. When E.164 numbers are represented as SIP URIs in fields of SIP messages, the domain part often changes as the message progresses through different domains. These considerations have a number of consequences.

2.2. E.164 numbers as From: URIs

When a UA receives an E.164 number represented as a SIP URI in a From header field, what does this say about the source of the request? Of course, it should indicate that the request originated at a user who has a right to use that E.164 number and who can be reached by submitting a request targeted at that E.164 number. However, the domain part means very little. At the most it means that the request has, at some stage, passed through the domain, and that a return request to that E.164 number can be routed via that domain. The request did not necessarily originate at that domain, but could simply have transited that domain. For example, a request could originate with the following From URI:

sip:+123456789@example1.com;user=phone

The request then passes through the service provider domain example2.com, which changes it to:

sip:+123456789@example2.com;user=phone

Furthermore the domain in the received From URI is not necessarily the "owner" of that E.164 number.

Similar considerations apply to E.164 numbers received as SIP URIs in the P-Asserted-Identity header field [RFC3325].

In the PSTN world there is a concept of user-provided and network-provided caller numbers. The two can differ when the user-provided number has been provided by an enterprise network (PBX) and denotes the particular enterprise user, whereas the network-provided number (the only one that the public network is able to authenticate) is the default number for the enterprise. It depends on the particular operator whether a network delivers the user-provided number, the network-provided number of both to the called user. The user-provided number is more useful for making a return call. If a SIP service provider modifies the From URI to provide the equivalent of a network-provided number, the domain part might no longer reflect the true identity of the originator of the request.

2.3. Authenticating a From: URI

SIP Identity [RFC4474] provides a means of authenticating a SIP URI in the From header field. The Identity header field contains a signature that can be generated only by the domain that appears in the SIP URI in the From header field. This means the request must have originated at or passed through that domain. If a domain changes the From URI, any existing Identity signature will be invalidated and should be removed, but of course that domain can insert its own Identity signature, signing the new From URI.

Note that although changing the From URI can be a reason for generating a new Identity signature, also the converse is true. An Identity signature can be invalidated because other signed information (e.g., IP addresses and ports in SDP) has changed, and because a domain can sign only when its own domain name is in the From URI, it must change the From URI before signing.

2.4. Using a received From: URI

Even when authenticated, a received From URI can only indicate a domain through which a request has passed, not necessarily the domain

in which it has originated. This can be an issue if the UAS expects it to indicate a particular originating domain but in fact it indicates the domain of an intermediate service provider. For example:

> Suppose the UAS has a white list of particular URIs or domains from which it accepts communications. The domain at which a request originated might be in the white list, but if the From URI indicates another domain through which the request passed, the check against the white list might fail.
>
> Requests from the same originating domain but all routed through different intermediate domains might all arrive with different From URIs. Attempts to correlate these requests will probably fail.
>
> Any attempt by a UAS to correlate a received URI with that of a known communication partner and as a result provide relevant information to the user will fail if URIs are compared but the domain part of the received URI is different from that expected.
>
> If a user expects a particular communication to be to/from a particular domain (e.g., the user's bank), yet the authenticated From URI in an received request indicates a service provider's domain, the user might not be prepared to proceed with that communication, or might proceed but withhold information of a

> sensitive nature.

Some of these issues can be resolved if the domain part is ignored and only the E.164 number is used for comparison. However, the last of these issues is a far more serious problem: the user expects a communication partner to be from a particular domain (the E.164 number is not necessarily an important factor). Seeing that domain in the From: URI, coupled with authentication by means of the Identity header field, would satisfy the user's expectation. Seeing a different domain, that of an intermediate service provider, which may or may not be known to the user, would not satisfy the user's expectation. The user might not be prepared to accept the unexpected URI and might decide not to proceed with the communication.

This last point is particularly important when the media are to be

secured using SRTP. As a basis for this security, the communication partner with which encrypted and integrity-protected RTP packets are exchanged must be authenticated as the expected or an acceptable communication partner. If this involves knowing the domain of the communication partner, then it is important that the From URI indicates the domain of the partner and not that of some intermediate service provider. If the Identity signature also covers the fingerprint of the certificate used by the partner for establishing SRTP keys, then this binds the secure media stream to the From URI. If the From URI is not acceptable, the media stream cannot be regarded as secure.

3. Summary of problem

A SIP URI containing an E.164 number received in a From header field is not a reliable source domain of a request, even when authenticated by means of the Identity header field. Only the E.164 number itself can be considered reliable, and only the E.164 itself is suitable for comparing with known identities at the destination (e.g., in a white list, in an address book). The inability to depend on the domain part of an E.164 SIP URI is a serious deficiency in some situations.

4. Requirements

A solution addressing the problem must satisfy the following requirements:

REQ1: When a UAS receives a SIP request originated by a user identified by an E.164 number, the UAS must receive a SIP or SIPS URI containing that E.164 number and containing the originator's domain in the domain part.

REQ2: When a UAS receives a SIP request that includes a SIP or SIPS URI identifying the originating user, if that URI contains an E.164 number that number alone, when placed in a TEL URI, must be suitable for routing a request back to the originating user.

REQ3: When a UAS receives a SIP request that includes a SIP or SIPS URI identifying the originating user, if that URI contains an E.164 number and the originating domain it must be possible to

include in the request cryptographic evidence from that originating domain that binds secure media to that SIP URI.

REQ1 is in principle met by the From URI, but not if it is modified by intermediate domains between the originating domain and the UAS. Obviously elimination of such practices would in theory be sufficient to satisfy REQ1, but this might not be achievable. Therefore it might require new techniques.

REQ2 requires new techniques.

REQ3 can in theory be met by the Identity header field, but this is true only if intermediate domains do not modify the From URI or other signed information, such as IP addresses and ports in SDP (these are often changed by Session Border Controllers, SBCs) and contact URIs (these too are often changed by SBCs and other B2BUAs). Therefore to solve this in a way that will work in most practical situations requires new techniques.

5. IANA Considerations

None; this document is informational.

6. Security Considerations

[[This section will be completed in a later version of this document.]]

7. Acknowledgements

The author thanks Dan Wing for encouraging the writing of this document.

8. Informative References

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for

Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

[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.

[ITU.E164.1991] International Telecommunications Union, "The International Public Telecommunication Numbering Plan", ITU-T Recommendation E.164, 1991.

Author's Address

John Elwell
Siemens Enterprise Communications GmbH & Co KG
Hofmannstrasse 51
D-81379 Munich
Germany

Phone: +44 115 943 4989
Email: john.elwell@siemens.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).