SIP
Internet-Draft
Intended status: Informational
Expires: August 21, 2008

D. Schwartz
XConnect
H. Kaplan
Acme Packet
K. Darilion
enum.at
H. Tschofenig
Nokia Siemens Networks

February 18, 2008

E.164 Ownership Problem Statement
draft-schwartz-sip-e164-ownership-00.txt

Status of this Memo

Copyright Notice

Abstract

When a call travels end-to-end relayed from the PSTN to SIP then problems occur with E.164 number ownership. Additionally, there are security challenges when the PSTN-VoIP gateway has to authenticate

and authorize the calling party. Without addressing these two aspects the overall security story is weak or non-existent. This document aims to investigate these two aspect; it does, however, not investigate current E.164 number handling with RFC 4474 ("SIP Identity"). Such an analysis is provided by other documents already.

Table of Contents

1. Introduction

RFC 4474 [3] defines a mechanism whereby an authentication service asserts the identity of a SIP UAC and determines whether he or she is authorized to use that identity. The authentication service then computes a hash over some particular headers, including the From header field and the bodies in the message. This hash is signed with the certificate for the domain and inserted in the 'Identity' header field in the SIP message. The proxy also inserts a companion header field, Identity-Info, that tells the verifying party how to acquire its certificate, in case it is not yet known already.

When the verifier receives the SIP message, it verifies the signature provided in the Identity header, and thus can determine whether the domain indicated by the host portion of the AoR in the From header field authenticated the user, and permitted the user to assert that From header field value.

The use of phone numbers with SIP was introduced with the TEL URL scheme [5] whereby domain names were not used with the phone numbers. SIP URIs always have domain names. In SIP [2], a translation between SIP URIs and TEL URLs is 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 [13]) it is not clear how to populate the domain name.

When SIP Identity [3] is applied to E.164 numbers then there is the question what the identity assertion actually means. Additionally, the usage of the domain for an E.164 number causes problems, as described in [7]. This document will, however, not focus on this aspect. Instead, we investigate the overall end-to-end security story and the ownership problem for E.164 numbers.

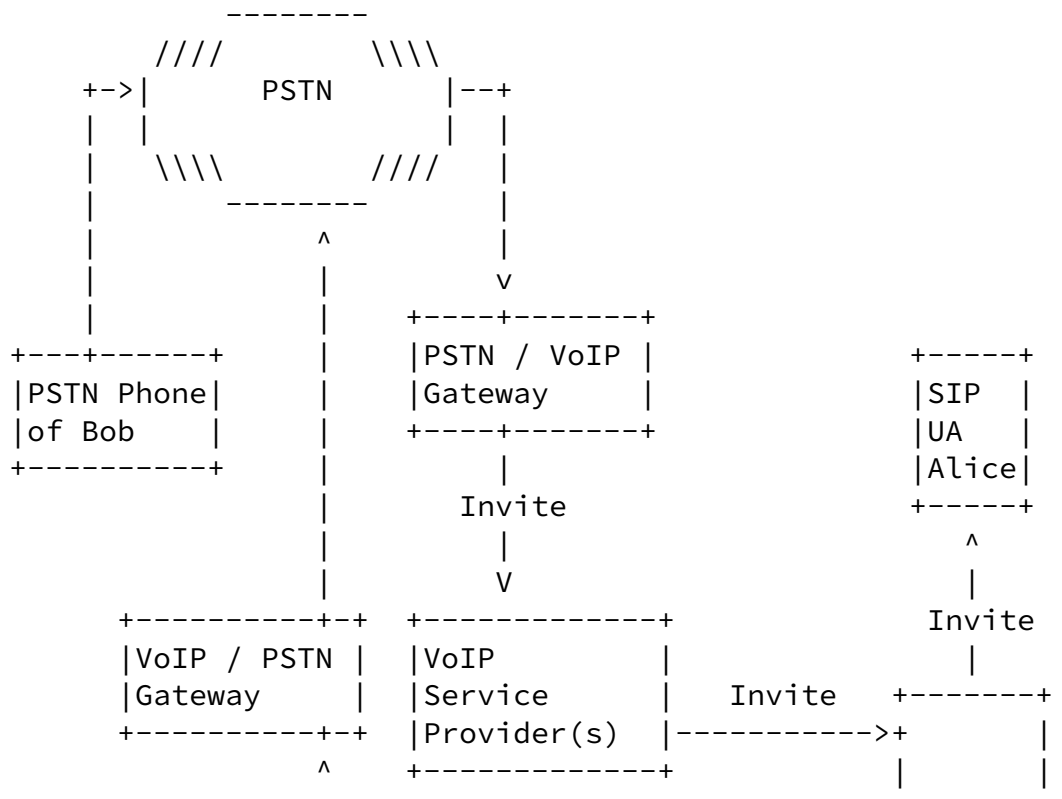
2. Terminology

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

3. The End-to-End Picture

Consider Figure 1 where two end points, Bob and Joe, initiate calls to Alice. Alice is using an IP-based phone and the same is true for

Joe. The call of Joe and Bob towards Alice traverse the PSTN; Bob is using a PSTN phone and the call enters the Internet via a PSTN/VoIP gateway. Joe's call traverses the PSTN, for example, because Joe's VoIP provider does not have a peering agreement with the called party domain and uses the PSTN as a way to interconnect VoIP networks. This is a common way of interacting between VoIP providers today.



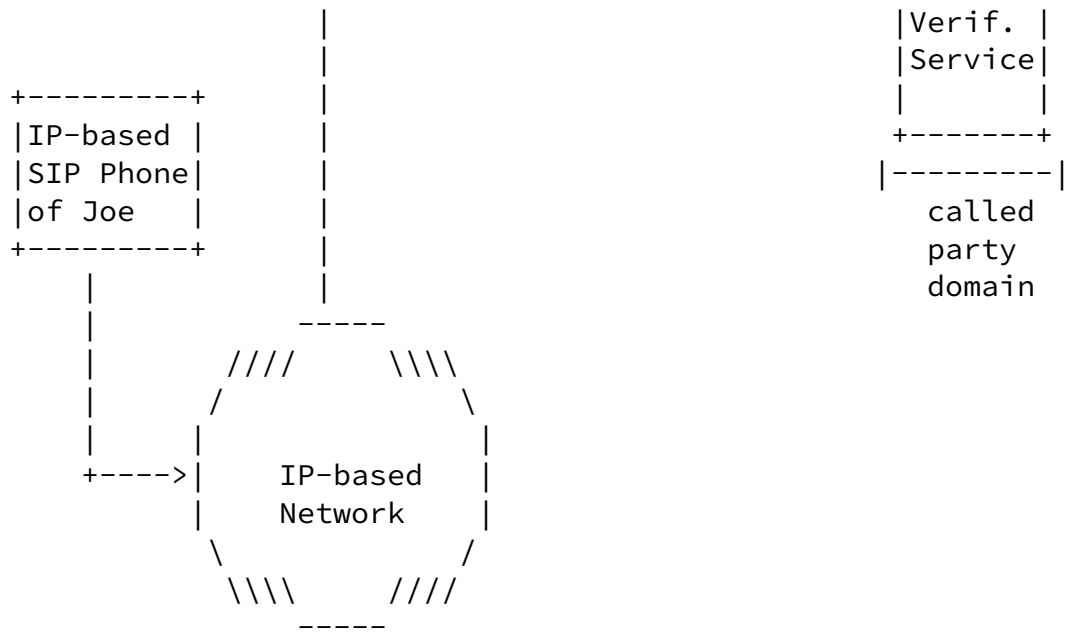


Figure 1: PSTN to SIP Communication

Figure 1 raises two important questions:

1. How does the authentication service (for example an entity that is co-located with the PSTN/VoIP gateway) authenticate and authorize the calling party?
2. How does the verification service determine ownership of an E.164 number?

Section 4 investigates the first question in more detail whereas Section 5 addresses the second question.

4. Authenticating and Authorizing the Calling Party Identity

RFC 4474 rightfully makes some important assumptions about the behavior of the authentication service that contribute significantly to the security of the overall system. While some assumptions seem to be obvious for SIP usage, they are less obvious when considering them in relationship with a PSTN interworking. Section 4 of [3] says:

"The authentication service authenticates Alice (possibly by

sending a Digest authentication challenge) and validates that she is authorized to assert the identity that is populated in the From header field. This value may be Alice's AoR, or it may be some other value that the policy of the proxy server permits her to use.

...

The proxy, as the holder of the private key of its domain, is asserting that the originator of this request has been authenticated and that she is authorized to claim the identity (the SIP address- of-record) that appears in the From header field. "

The crutial question therefore is: In the generic case is the authentication service able to authenticate the caller-ID used in the PSTN and to authorize it's usage?

There are problems with this step:

1. The PSTN builds on a walled garden with a chain-of-trust security model. This is "nice" as long as the participating parties are indeed honest. Unfortunately, this is not true anymore (and has not been the case for a long time already) [add-references-to-examples]. Caller-ID spoofing is common and even transit providers are not trustworthy either.

2. A call originated on the PSTN is often times routed to a PSTN/VoIP gateway. That PSTN gateway is operated by the owner of the called number, rather than the owner of the calling number.

5. Verifying Ownership: What does it mean?

Imagine a verification service at Alice's VoIP provider network receives a SIP message with an 'Identity' and an 'Identity-Info' header.

How would this verification service determine whether the signer of the message is indeed authorized to claim ownership?

Ownership is an artificial construct but one could compare it with an

oracle that returns the name of a domain when asked who is authoritative for using a particular E.164 number.

There are various owership verification steps that got used in the IETF within other protocols. RFC 4474 [3], for example, uses the following verification step for SIP URIs:

> "6. Verifier Behavior
>
> Step 2:
>
> The verifier MUST follow the process described in Section 13.4 to determine if the signer is authoritative for the URI in the From header field.
>
> 13.4. Domain Names and Subordination
>
> When a verifier processes a request containing an Identity-Info header, it must compare the domain portion of the URI in the From header field of the request with the domain name that is the subject of the certificate acquired from the Identity-Info header."

This is a concept of referential integrity where information of the protocol (in this case the identity) is matched against information from the certificate. Still, the signer and the verifier need to have a trust anchor in common. There are additional aspects about the detailed matching procedure that are described in Section 13.4 of [3].

Unfortunately, this simple authorization check cannot be used with

E.164 numbers because of the missing domain concept in the identifier itself and because of number portability.

A couple of other ownership approaches have been used in IETF protocols. A few examples below:

Return Routability Check: A form of check is to exploit the topological properties of identifier routing and the possible

placements of adversaries with respect to a certain message interaction. RRT and various other forms fall into that category. An example can be found in [9].

Authorization Certificates:

A form of check is to use authorization certificates. The basic idea is that one would trust the entity that creates the authorization certificate (most likely in a hierarchical form) then you also trust its content. SIP-SAML (see [8]) and [12] belong to this category. When the identity of the certificate is constructed in a suitable way then together with a delegated signing the same effect could be accomplished.

Distributed Databases:

Another form of mechanism is to use an out-of-band database lookup, for example using the DNS, in order to verify that the entity which uses the private key for creating the SIP Identity header is authorized to attach the corresponding public key to the this distributed database. The identity would be used for the lookup to the database and the security of the system relies on ensuring that only those entities add the public key that are also owner of the corresponding E.164 number. An example of such an approach can be found in [15]. The usage of TRIP [11] (with extensions with information about E.164 numbers that are authorized for usage by a specific provider) has been discussed as well.

Cryptographic Addresses and Hash Chains:

These mechanisms utilize a temporal property by creating a binding between the public key (or values from a hash chain) and the identity be verified by re-computing the hash value and by comparing the hash with the identifier. These mechanisms have found some excitment with protocol work at lower layers (see, for example, [10]).

It is quite obvious that each mechanism has different scalability, security and deployment properties.

6. Security Considerations

With the work on this subject it is important to keep two quotes in mind:

- "The security of a system is as good as the weakest link."
- "If you think cryptography is the solution to your problem, you don't know what your problem is." --- Roger Needham

We are still in an early phase to properly understand the problem domain even though there are a couple of TECHNICAL solution proposals available to address the ownership question. These technical approaches do, however, not help when there is no deployment incentives. These approaches also do not help with the security of the overall system when the identity of the calling party cannot be verified by the authentication service.

As such, it is too early to conclusively argue that an RFC 4474 alike authentication service should actually attempt to offer a solution for E.164 numbers even though they are heavily used in today's networks.

7. Contributors

We would like to thank the following individuals for their contributions to this document:

- Dan Wing
- John Elwell
- Kai Fischer

8. IANA Considerations

There are no IANA considerations with this document.

9. Acknowledgments

Add your name here.

10. References

10.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] 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.

[3] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[4] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007.

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

[6] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761, April 2004.

10.2. Informative References

[7] Elwell, J., "SIP E.164 Problem Statement", draft-elwell-sip-e164-problem-statement-00 (work in progress), February 2008.

[8] Tschofenig, H., Hodges, J., Peterson, J., Polk, J., and D. Sicker, "SIP SAML Profile and Binding", draft-ietf-sip-saml-03 (work in progress), November 2007.

[9] Wing, D., "SIP E.164 Return Routability Check (RRC)", draft-wing-sip-e164-rrc-01 (work in progress), February 2008.

[10] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[11] Rosenberg, J., Salama, H., and M. Squire, "Telephony Routing over IP (TRIP)", RFC 3219, January 2002.

[12] Bellovin, S., Ioannidis, J., Keromytis, A., and R. Stewart, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec", RFC 3554, July 2003.

[13] ITU-T, "The international public telecommunication numbering plan", Recommendation E.164, May 1997.

[14] Peterson, J., "A Privacy Mechanism for the Session Initiation

Protocol (SIP)", RFC 3323, November 2002.

[15] Darilion, K., "E.164 Ownership using Public Keys stored in ENUM", Info draft-darilion-sip-e164-enum-00.txt, Feb 2008.

Authors' Addresses

David Schwartz
XConnect
Malcha Technology Park
Jerusalem, 96951
Israel

Email: dschwartz@xconnect.net

Hadriel Kaplan
Acme Packet
71 Third Ave.
Burlington, MA 01803
USA

Phone:
Fax:
Email: hkaplan@acmepacket.com
URI:

Klaus Darilion
enum.at GmbH
Karlsplatz 1/9
Wien A-1010
Austria

Phone: +43 1 5056416 36
Email: klaus.darilion@enum.at
URI: http://www.enum.at/

Hannes Tschofenig

Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.com

Full Copyright Statement

Intellectual Property

specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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