A Minimalist Approach to Direct Peering
draft-mahy-speermint-direct-peering-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 9, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document describes a concrete example of a peering convention for domains and federations of domain which use SIP for communications, especially in conjunction with E.164 addresses (telephone numbers). This convention makes use of direct SIP and media communication between the operator of the initiating and receiving administrative domains.
Table of Contents

1. Conventions .................................. 3
2. Introduction ................................. 3
3. Overview .................................. 3
4. Procedures .................................. 4
   4.1. Initiating Peer ........................... 4
       4.1.1. Analyzing target address ............ 4
       4.1.2. User ENUM lookup .................. 4
       4.1.3. Carrier ENUM lookup ............... 5
       4.1.4. Target by routing table ............ 5
       4.1.5. SIP DNS resolution .................. 5
       4.1.6. Setup TLS connection ............... 6
       4.1.7. Send the SIP request ............... 6
   4.2. Receiving Peer ........................... 7
       4.2.1. Publish ENUM records ............... 7
       4.2.2. Publish SIP DNS records .......... 7
       4.2.3. Verify TLS connection .............. 8
       4.2.4. Receive SIP requests .............. 8
       4.2.5. Record Routing ...................... 8
5. Security Considerations .................... 9
6. IANA Consideration .......................... 9
7. References .................................. 9
   7.1. Normative References .................... 9
   7.2. Informational References ............... 10
Author’s Address .............................. 10
Intellectual Property and Copyright Statements ................ 11
1. Conventions

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 RFC-2119 [3].

2. Introduction

The Session PEERing for Multimedia INTerconnect (SPEERMINT) Working Group is chartered to document conventions for routing real-time sessions, such as VoIP telephone calls, at the application layer. The speermint terminology document [16] describes this as "layer 5 peering". This document will use the term "peering" to describe this layer 5 peering.

This document describes a concrete example of a peering convention. This example approach is intentionally minimalistic in its approach, and leaves many issues as local policy decisions. This "less is more" philosophy hopefully encourages addition of new features only when the vast majority of peers would benefit from them. The author hopes that the example will facilitate discussion about speermint requirements. This approach is also summarized in the consolidated use cases document [17].

3. Overview

The approach described here assumes that the initiating peer first discovers a SIP [2] target URI handled by the receiving peer, then sends SIP requests directly to the receiving peer.

When the initiating peer receives a request to contact a resource addressed in its domain using an "external" telephone number (one for which the peer is not responsible), the peer first consults "User" ENUM [1] records, then carrier ENUM [14] records, and finally it may optionally consult a local routing table to determine the appropriate target URI. Requests to im: or pres: resources in external domains can resolve to SIP URIs using the procedures defined in RFC 3861 [8]. Requests which already address a SIP URI in an external domain need no additional peer discovery.

Once the initiating peer discovers a SIP URI corresponding to the receiving peer, the initiating peer finds the correct SIP server for the receiving peer according to the DNS resolution procedures for SIP in RFC 3263 [2]. Peers send all SIP messages to each other over a TLS [5] protected channel and use the SIP Identity [12] mechanism to verifiably assert an identity for the sender of most messages.
Note that in a federation of domains, the initiating peer role can be logically decomposed. Domain A1 can forward requests to domain A2, so that A2 actually opens a TLS connection to the receiving peer. Likewise, the receiving peer function can be similarly decomposed. How functions are distributed between or among domains or nodes is not subject to this specification as long as the requirements described in this document are met.

4. Procedures

4.1. Initiating Peer

4.1.1. Analyzing target address

Before the initiating peer is even aware that it will peer, it receives a request to communicate. If the target address does not represent a resource inside the initiating peer’s administrative domain or federation of domains, the request may need to be sent to a peer. How the peer determines a resource is external is the subject of local policy. Note that the peer is free to consult any manner of private data sources to make this determination, including for example those using ENUM technology with private roots.

If the request is for an im: or pres: URI type, the initiating peer follows the procedures in [8]. If the highest priority supported URI scheme is sip: or sips:, the initiating peer skips to SIP DNS resolution. Likewise, if the target address is already a sip: or sips: URI in an external domain, the initiating peer skips to Section 4.1.5.

If the target address corresponds to a specific E.164 address, the peer may need to perform some form of number plan mapping according to local policy. For example, in the United States, a dial string beginning "011 44" could be converted to "+44", or in the United Kingdom "00 1" could be converted to "+1". Once the peer has an E.164 address, it can continue to the next step.

4.1.2. User ENUM lookup

If an external E.164 address is the target, the initiating peer consults the public "User ENUM" rooted at e164.arpa, according to the procedures described in RFC 3761. The peer MUST query for the "E2U+ sip" enumservice as described in RFC 3674 [11], but MAY check for other enumservices. The initiating peer MAY consult a cache or alternate representation of the ENUM data rather than actual DNS queries. Also, the peer MAY skip actual DNS queries if the initiating peer is sure that the target address country code is not
If an im: or pres: URI is chosen based on an "E2U+im" [15] or "E2U+pres" [4] enumserver, the peer follows the procedures for resolving these URIs to URIs for specific protocols such as SIP or XMPP as described in the previous section.

4.1.3. Carrier ENUM lookup

Next the initiating peer checks for a carrier-of-record in a carrier ENUM domain according to the procedures described in [14]. As in the previous step, the peer MAY consult a cache or alternate representation of the ENUM data in lieu of actual DNS queries. The peer first checks for records for the "E2U+sip" enumservice, then for the "E2U+pstn" enumservice as defined in [13]. If a terminal record is found with a sip: or sips: URI, the peer skips to Section 4.1.5, otherwise the peer continues processing according to the next section.

4.1.4. Target by routing table

If there are no user ENUM records, and the initiating carrier cannot discover the carrier-of-record or if the initiating peer cannot reach the carrier-of-record via SIP peering, the initiating peer still needs to deliver the call to the PSTN or reject the call. Note that the initiating peer MAY still send the call to another carrier for PSTN gateway termination by prior arrangement. If so, the initiating peer rewrites the Request-URI to address the gateway resource in the target carrier’s domain and MAY forward the request on to that carrier using the procedures described in the remainder of these steps.

4.1.5. SIP DNS resolution

Once a sip: or sips: in an external domain is selected as the target, the initiating peer MAY apply local policy to decide whether forwarding requests to the target domain is acceptable. If so, the initiating peer uses the procedures in RFC 3263 [6] Section 4 to determine how to contact the receiving peer. To summarize the RFC 3263 procedure: unless these are explicitly encoded in the target URI, a transport is chosen using NAPTR records, a port is chosen using SRV records, and an address is chosen using A or AAAA records. Note that these are queries of records in the global DNS.

When communicating with a public external peer, entities compliant to this document MUST only select a TLS-protected transport for communication from the initiating peer to the receiving peer. Note
that this is a single-hop requirement. Either peer MAY insist on using a sips: URI which asserts that each hop is TLS-protected, but this document does not require protection over each hop.

Some operators have complained that the TLS is not practical to deploy in this context. The traditional objection to using TLS is that it is difficult to build SIP intermediaries which can handle more than on the order of 10,000 or 100,000 simultaneous TCP connections. This objection is not relevant in this context, since the end-user user agents are still free to use any transport inside their administrative domain, and the number of simultaneous TCP connections between peers who have recently exchanged traffic is expected to be on the order of 100 to 1000 connections per peer.

### 4.1.6. Setup TLS connection

Once a transport, port, and address are found, the initiating peer will open or find a reusable TLS connection to the peer. The initiating provider MUST verify the server certificate which SHOULD be rooted in a well-known certificate authority. The initiating provider MUST be prepared to provide a TLS client certificate upon request during the TLS handshake. The client certificate MUST contain a DNS or URI choice type in the subjectAltName which corresponds to the domain asserted in the host production of the From header URI. The certificate SHOULD be valid and rooted in a well-known certificate authority.

Note that the client certificate MAY contain a list of entries in the subjectAltName, only one of which has to match the domain in the From header URI.

### 4.1.7. Send the SIP request

Once a TLS connection between the peers is established, the initiating peer sends the request. When sending some requests, the initiating peer MUST verify and assert the senders identity using the SIP Identity mechanism.

The domain name in the URI of the From header MUST be a domain which was present in the certificate presented when establishing the TLS connection for this request, even if the user part has an anonymous value. If the From header contains the user URI parameter with the value of "phone", the user part of the From header URI MUST be a complete and valid tel: URI [9] telephone-subscriber production, and SHOULD be a global-number. For example, the following are all acceptable, the first three are encouraged:
The following are not acceptable:

From: "2125551212" <2125551212@example.net;user=phone>
From: "Anonymous" <anonymous@anonymous.invalid>

In addition, for new dialog-forming requests and non-dialog-forming requests, the request MUST contain a valid Identity and Identity-Info header as described in [12]. The Identity-Info header must present a domain name which is represented in the certificate presented when establishing the TLS connection over which the request is sent. The initiating peer SHOULD include an Identity header on in-dialog requests as well, if the From header field value matches an identity the initiating peer is willing to assert.

The initiating peer MAY include any SIP option-tags in Supported, Require, or Proxy-Require headers according to procedures in standards-track SIP extensions. Note however that the initiating peer MUST be prepared to fallback to baseline SIP functionality as defined by the mandatory-to-implement features of RFC 3261, RFC 3263, and RFC 3264 [7], except that peers implementing this specification MUST implement SIP over TLS using the sip: URI scheme, the SIP Identity header, and RFC 4320 [10] non-INVITE transaction fixes.

4.2. Receiving Peer

4.2.1. Publish ENUM records

The receiving peer SHOULD participate by publishing "E2U+sip" and "E2U+pstn" records with sip: or sips: URIs wherever a public carrier ENUM root is available. This assumes that the receiving peer wants to peer by default. Even when the receiving peer does not want to accept traffic from specific initiating peers, it MAY still reject requests on a case-by-case basis.

4.2.2. Publish SIP DNS records

To receive peer requests, the receiving peer MUST insure that it publishes appropriate NAPTR, SRV, and address (A and/or AAAA) records in the global DNS that resolve an appropriate transport, port, and address to a relevant SIP server. The transport actually used for external public peering MUST be TLS protected.
4.2.3. Verify TLS connection

When the receiving peer receives a TLS client hello, it responds with its certificate. The receiving peer certificate SHOULD be valid and rooted in a well-known certificate authority. The receiving peer MUST request and verify the client certificate during the TLS handshake.

Once the initiating peer has been authenticated, the receiving peer can authorize communication from this peer based on the domain name of the peer and the root of its certificate. This allows two authorization models to be used, together or separately. In the domain-based model, the receiving peer can allow communication from peers with some trusted administrative domains which use general-purpose certificate authorities, without explicitly permitting all domains with certificates rooted in the same authority. It also allows a certificate authority (CA) based model where every domain with a valid certificate rooted in some list of CAs is automatically authorized.

4.2.4. Receive SIP requests

Once a TLS connection is established, the receiving peer is prepared to receive incoming SIP requests. For new dialog-forming requests and out-of-dialog requests, the receiving peer verifies that the target (request-URI) is a domain which for which it is responsible. (For these requests, there should be no remaining Route header field values.) Next the receiving verifies that the Identity header is valid, corresponds to the message, corresponds to the Identity-Info header, and that the domain in the From header corresponds to one of the domains in the TLS client certificate.

For in-dialog requests, the receiving peer can verify that it corresponds to the top-most Route header field value. The peer also validates any Identity header if present.

The receiving peer MAY reject incoming requests due to local policy. When a request is rejected because the initiating peer is not authorized to peer, the receiving peer SHOULd respond with a 403 response with the reason phrase "Unsupported Peer".

4.2.5. Record Routing

The receiving peer MAY add a Record-Route header field value corresponding to itself. This insures that subsequent in-dialog requests are sent through a node associated with the receiving peer.
5. Security Considerations

This document does not introduce any new security concerns, but the overall security of a peering system using this mechanism is worth discussing separately. The security and privacy implications of using user and carrier ENUM are primarily discussed in RFC 3761 [1] and [14] respectively. User ENUM records are only added at the discretion of the user. Carrier ENUM records should be deployed for an entire number range so that no user-specific information can be gleaned. Note that in some countries, knowledge of the carrier-of-record for a specific phone number is not public knowledge.

This document requires peers use a TLS-protected channel and the SIP Identity mechanism. This section needs to be completed in more detail later.

6. IANA Consideration

This document requires no action by IANA.

7. References

7.1. Normative References


7.2. Informational References

draft-ietf-speermint-terminology-08 (work in progress),

[17] Uzelac, A., "VoIP SIP Peering Use Cases",
draft-ietf-speermint-voip-consolidated-usecases-02 (work in progress), June 2007.

Author’s Address

Rohan Mahy
Plantronics

Email: rohan@ekabal.com