Network Working Group
Request for Comments: 4238
Category: Standards Track

G. Vaudreuil
Lucent Technologies

October 2005

Voice Message Routing Service

Status of This Memo

Copyright Notice

Abstract

Voice messaging is traditionally addressed using telephone number addressing. This document describes two techniques for routing voice messages based on a telephone number. The complete service uses the Voice Profile for Internet Mail (VPIM) Directory service to lookup a VPIM email address with a telephone number and confirm that the address is both valid and associated with the intended recipient. However, this service will take time to become widely deployed in the near term. This document also describes a basic send-and-pray service that routes and delivers messages using only the ENUM telephone number resolution service and the existing DNS mail routing facilities.

Table of Contents

1. Design Goals

This profile is intended to provide a range of functional capabilities for message routing based on one of two mechanisms. The most complete service should use the ENUM address resolution service to determine the VPIM directory, and then use LDAP to retrieve the VPIM-specific email address that will be used for message routing.

The more basic send-and-pray message service uses only the ENUM service and MX records to route the message to the intended recipient's domain. The intelligence to further route the message to the intended recipient is placed within the message routing system of the recipient's domain.

The basic mechanism may be used even when there is a VPIM directory service available. The basic service is useful when LDAP queries are not available, such as may be the case for disconnected mobile terminals or because of firewall or information security policies.

The basic mechanism should facilitate the routing of VPIM messages to a suitable internal destination with a minimum of configuration. It is an important goal to avoid any content-processing to determine the nature of the message and its internal destination. At a minimum, it should be possible to establish a simple mail forwarding rule that

sends all inbound VPIM messages to a designated system, while facilitating the routing of FAX, SMS, or other telephone-addressed messages to other potentially different systems.

It is a goal that the mechanisms outlined in this document be extensible for all store-and-forward, telephone-number addressed messaging services.

It is a goal that the VPIM directory discovery and VPIM directory query steps occur within the timing constraints for user interfaces in PSTN networks. 95% of the time, that constraint can be a two-second response.

2. The Complete Service

For the complete VPIM message routing service, the sending client SHOULD query the VPIM directory for the VPIM-specific email address. The client SHOULD use the ENUM service to retrieve the identity of the VPIM Directory to query. The client should then query that server for the email address and any additional attributes desired.

2.1. Specification of Service "E2U+VPIM:LDAP"

* Service Name: E.164 to VPIM LDAP URL

* URI Type: "LDAP:"

* Type: VPIM

* Subtype: LDAP

* Functional Specification: See sections 3.2 through 3.3

* Intended Usage: COMMON

* Author: Greg Vaudreuil (gregv@ieee.org)

* Security Considerations:

  o Malicious Redirection

    One of the fundamental dangers related to any service such as this is that a malicious entry in a resolver’s database will cause clients to resolve the E.164 into the wrong LDAP URL. The possible intent may be to cause the client to connect to a rogue LDAP server and retrieve (or fail to retrieve) a resource containing fraudulent or damaging information.

- Denial of Service

  By removing the URL to which the E.164 maps, a malicious intruder may remove the client's ability to access the LDAP directory server.

2.2. VPIM Directory Discovery

The VPIM directory server is found by using the ENUM protocol and querying for the VPIMDIR service associated with the telephone number of the recipient.

The DNS query name is created as described by [ENUM]. The telephone number used for the directory location MAY contain additional sub-address information as additional digits.

Example:

```
Query: 2.1.2.1.5.5.5.3.1.6.1.e164.arpa
Responses:
  IN NAPTR  10 10 "U" "E2U+VPIM:LDAP" \
   "!^.*$!ldap://vdir1.Zcorp.com/telephoneNumber=\1!" .

  IN NAPTR  10 20 "U" " E2U+VPIM:LDAP" \
   "!^.*$!ldap://vdir2.Zcorp.com/telephoneNumber=\1!" .
```

It is recommended that VPIMDIR servers be deployed in a redundant configuration. NAPTR weight fields provide the ability to give two records indicating the same service and preference a different weight. The same weight can be specified for random distribution between the two servers. See [NAPTR-1, NAPTR-2, NAPTR-3, NAPTR-4]

2.3. Address Query

Once the VPIM directory is discovered, the client SHOULD issue an LDAP query for the vPIMrFC822Mailbox, that is, the address that SHOULD be used as the value for both the RFC 822 To: field and the SMTP RCPT command. See [VPIMDIR].

3. The Basic Service

The basic service relies upon NAPTR rewrite rules to mechanically construct a valid VPIM-specific email address. In the recipient's domain, the constructed address may be further routed using intradomain mail routing techniques.

To facilitate a full range of intradomain routing options, the constructed email address indicates that the message is a VPIM message. For ease of processing in the recipient's intradomain mail routing system, the indication that the message is a VPIM message SHOULD be in the domain name portion.

Note that there is no assurance the constructed address is valid, nor that the constructed address corresponds to the intended recipient. Because no capabilities information is provided about the recipient, messages sent with this mechanism SHOULD be sent using only the media and content types of the VPIM V2 profile.

3.1. Specification of Service "E2U+VPIM:Mailto:"

* Service Name: E.164 to VPIM MailTo: URL
* URI Type: "Mailto:"
* Type: VPIM
* Subtype: MAILTO
* Functional Specification: See sections 4.2 through 4.4
* Intended Usage: COMMON
* Author: Greg Vaudreuil (gregv@ieee.org)
* Error Conditions:
  - E.164 number not in the numbering plan
  - E.164 number in the numbering plan, but no URLs exist for that number
  - E2U+VPIM:Mailto Service unavailable
* Security Considerations:
  - Malicious Redirection

    One of the fundamental dangers related to any service such as this is that a malicious entry in a resolver's database will cause clients to resolve the E.164 into the wrong email URL. The possible intent may be to cause the client to send the information to an incorrect destination.

- Denial of Service

  By removing the URL to which the E.164 maps, a malicious intruder may remove the client's ability to access the resource.

- Unsolicited Bulk Email

  The exposure of email addresses through the ENUM service provides a bulk mailer access to large numbers of email addresses where only the telephone number was previously known.

3.2. Address Construction

Construct a VPIM email address using the address rewrite rules of the NAPTR records associated with the VPIM service.

3.3. Interdomain Message Routing

The interdomain routing of a constructed VPIM address is mechanically indistinguishable from existing email routing. No changes to the infrastructure are required. The sending system consults the Domain Name System for an MX record corresponding to the domain name and forwards the message to the indicated system.

3.4. Intradomain Message Routing

Within the recipient's domain, the message may be further routed to the appropriate messaging system. Two general mechanisms may be used to further route the message to the intended system within a network.

Note: This section is strictly informational. The mechanisms for intradomain routing are an internal matter for the domain and do not affect the protocol. It is only necessary that the addresses created by the NAPTR rewrite rules have meaning to the domain advertising them. However, a convention for the creation and use of such addresses may be useful.

3.4.1. Directory-Enabled Routing

Various proprietary directory mechanisms provide a means for an inbound mail router of the recipient's domain to send a message to the appropriate internal mail host. In many cases, the local part of the address is used to query for an internal mail address. That internal mail address is substituted for the SMTP RCPT address and used to deliver the message to the recipient mailbox. Note that the mailbox does not need to have any knowledge of the mechanically-constructed telephone number-based address.

Example address: +12145551212@sp.net

3.4.2. Service-based Mail Routing

Alternately, a mail gateway may simply send all voice messages into a separate messaging system. That system may be a single voice messaging server or a service-specific gateway into a larger telephone number-based voice-messaging network.

Such a mail gateway may be provisioned with a simple rule or small set of rules to forward all messages of a given service type to a pre-defined server. This rule would check for the service name "VPIM" as a prefix to the constructed domain name to reroute messages.

Example address: +12145551212@VPIM.sp.net

4. Security Considerations

There is little information disclosed to the sender of the message that is not already disclosed using standard email protocols. The ability to use this protocol to probe for valid addresses is identical to the sending of test messages and waiting for a non-delivery notification in return.

4.1. Unsolicited Bulk Email

However, the use of ENUM records to create routable email addresses from telephone numbers provides bulk-emailers the capabilities to send email to a large set of recipients where only the telephone number is known or where telephone numbers are guessed.

4.2. DNS-based Attacks

Both the complete and basic services rely upon the DNS to provide the information necessary to validate a recipient or send a message. The message sender is a casual, unauthenticated use of the indicated servers, and relies upon the DNS for accurate information. If the DNS is compromised, an attacker can redirect messages by providing a malicious email address or indicating a rogue directory with malicious LDAP URL’s. Use of DNS Security protocols [DNSSEC] substantially reduces the risk of a domain being hijacked. If the E.164 zone is secured with DNSSEC, then the attack is precluded if the client can trust the key used to sign the zone. DNS security does not protect against the LDAP service being independently compromised. Further discussion on the risk to this LDAP service is provided in [VPIMDIR].

5. IANA Considerations

This specification registers the E2U+VPIM and E2U+Voice services according to the specifications and guidelines in RFC 3761 [ENUM] and the definitions in this document.

6. References

6.1. Normative References

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

[NAPTR-1] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS", RFC 3401, October 2002.

[NAPTR-2] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm", RFC 3402, October 2002.

[NAPTR-3] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.

[NAPTR-4] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)", RFC 3404, October 2002.

[VPIMDIR] Vaudreuil, G., "Voice Messaging Directory Service", RFC 4237, October 2005.

6.2. Informative References

[VPIMV2] Vaudreuil, G. and G. Parsons, "Voice Profile for Internet Mail - version 2 (VPIMv2)", RFC 3801, June 2004.

[DNSSEC] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

Author's Address

Please send comments on this document to the VPIM working group mailing list <vpim@ietf.org>.

Gregory M. Vaudreuil
Lucent Technologies
9489 Bartgis Ct
Frederick, MD 21702

EMail: GregV@ieee.org

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.