dispatch	J. Rosenberg	
Internet-Draft	jdrosen.net	
Intended status: Standards Track	C. Jennings	
Expires: April 28, 2011	Cisco	
	M. Petit-Huguenin	
	Stonyfish	
	October 25, 2010	

TOC

Session Initiation Protocol (SIP) Extensions for Blocking VoIP Spam Using PSTN Validation
draft-rosenberg-dispatch-vipr-sip-antispam-03

Abstract

Verification Involving PSTN Reachability (ViPR) is a new technique for inter-domain federation of SIP calls. ViPR makes use of the PSTN as an introduction mechanism to verify the correctness of mappings from phone numbers to domains. The PSTN introduction mechanism can also be used as a technique for blocking spam - a SIP caller is only authorized when its calling domain has previously called that same number over the PSTN. This document describes an extension to SIP which enables authorization of SIP calls based on a prior PSTN introduction.

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 April 28, 2011.

Table of Contents

---

1. Introduction

TOC

The anti-spam tickets described in this specification are the key security mechanism in ViPR for mitigation of SPAM. The domain originating a call inserts a ticket in the SIP INVITE sent to the other domain. The Border Element in the domain receiving the call (see Figure 1 (Architecture)) can check the ticket to ensure that this originating domain has been authorized by the terminating domain. This document relies heavily on the concepts and terminology defined in [VIPR-OVERVIEW] (Rosenberg, J., Jennings, C., and M. Petit-Huguenin,

"Verification Involving PSTN Reachability: Requirements and Architecture Overview," October 2010.) and will not make sense if you have not read that document first.

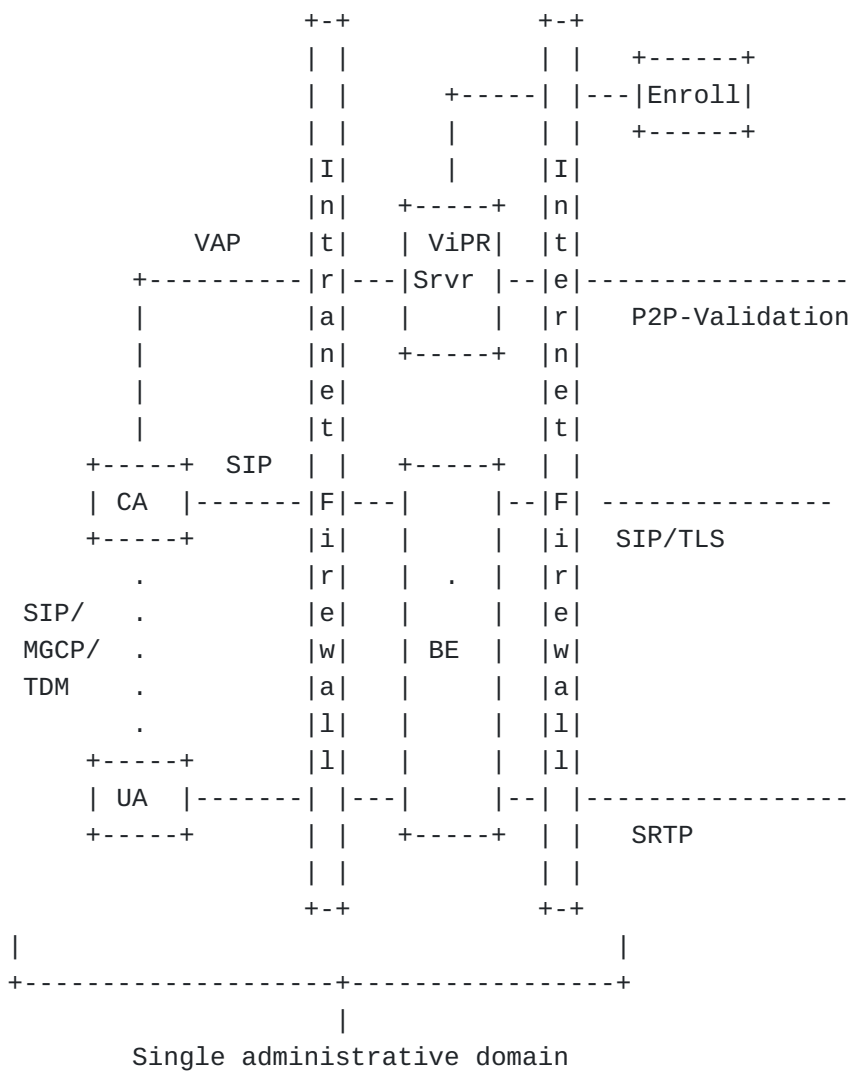

Figure 1: Architecture

2. Terminology

TOC

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 [RFC2119] (Bradner, S.,

"Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

---

3. Terminating Side Procedures

TOC

The Border Element will receive the TLS ClientHello which begins the TLS handshake. The Border Element will present its own configured cert. Once TLS handshaking is complete, the Border Element notes the domain from the SubjectAltName on the other side of the TLS connection, and associates it with that connection.

Next, the Border Element will receive an INVITE. This INVITE will contain a ticket in the X-Cisco-ViPR-Ticket header field value. The Border Element extracts this header field. This call flow assumes it is present. The Border Element parses it, and obtains the epoch value encoded in the ticket. This is matched against the current epoch value for the configured password. If they match, processing continues. The Border Element verifies the signature is correct. Next, it examines the start and stop time of the validity. If the current time is between the start and stop times, the check is passed. Next, the Border Element checks the granted-to domain in the ticket. It compares that domain against the domain name in the SubjectAltName of the peer on the other side of the TLS connection, as noted above. Next, it takes the Request-URI of the SIP INVITE. That will be of the form sip:+number@domain. If it is not in that form, and if the number does not begin with a plus, the request is dropped. The value, including the plus, is then compared to the number in the ticket. If it is equal, the check has passed. The Border Element leaves the header field in the request, but forwards to the Call Agent.

In addition, the Border Element will typically be configured to apply its SIP message validation logic, and enforce restrictions on the sizes of various SIP header fields. This provides an additional layer of security in case malicious SIP messages are sent.

The Border Element will also apply port forwarding in the case of NAT, so that the incoming request is forwarded to the appropriate Call Agent node.

The Call Agent will receive incoming SIP INVITEs. The Request-URI of the INVITE will contain an E.164 number as indicated by a leading plus. If the Request-URI is not an E.164, the request must be rejected with a 403. Only E.164 numbers can be accepted on a ViPR trunk.

---

4. Originating Side Procedures

TOC

The routes stored to other domains in the Call Agent will each store a ticket to utilize with calls to that route. The Call Agent learns about

these routes and the information needed to construct the ticket from the VAP protocol (Rosenberg, J., Jennings, C., and M. Petit-Huguenin, "Verification Involving PSTN Reachability: The ViPR Access Protocol (VAP)," October 2010.) [VIPR-VAP]. When sending a SIP request to one of these domains, the Call Agent MUST include the ticket in any dialog forming request or request that is not in an existing dialog.

---

5. Tickets

TOC

This ticket is a sequence of characters. These MUST be placed into a X-Cisco-ViPR-Ticket SIP header field value. Consequently the format for this header field is:

```
Ticket = "X-Cisco-ViPR-Ticket" HCOLON ticket-val
ticket-val = 1*(alphanum / "-" / "_" / ".")
```

This header field MUST be utilized in all dialog forming requests and all out-of-dialog requests. It is not utilized in responses. The ticket-value is a modified base64 encoded version of an object that is composed of a series of TLVs. Each TLV is a 16 bit type, a 16 bit length, and a variable length value. The length field refers to the length of the value portion of the TLV, measured in bytes. The following TLV types are defined:

1. Ticket Unique ID: This TLV has a type of 0x0001. It contains a 128 bit ID that has a unique identifier for this ticket. The value MUST contain a 128 bit UUID defined by [RFC4122] (Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace," July 2005.). This TLV MUST be present. However at this time it is used for diagnostic purposes only.

2. Salt: This TLV has a type of 0x0002. It contains a value which MUST be at least 32 bits, and contains a random number. Its presence ensures that each ticket contains sufficient randomness. This TLV MUST be present.

3. Validity: This TLV has a type of 0x0003. It contains two 64 bit NTP times. The first is the start of the validity of the ticket, the next is the end time for the validity of the ticket. This TLV MUST be present.

4. Number: This TLV has a type of 0x0004. It contains a string which has an E.164 number, included the "+", which may be called using this ticket. The TLV has variable length. This TLV MUST be present.

5. Granting Node: This TLV has a type of 0x0005. It contains a 128 bit value which is the Node-ID of the node which granted the ticket. This TLV MUST be present.

6. Granting Domain: This TLV has a type of 0x0006. The domain which granted the ticket. A string, up to 256 characters, each of which must be a valid domain name character. The TLV has variable length. This TLV MUST be present.

7. Granted-To Domain: This TLV has a type of 0x0007. The domain to which the ticket is granted. A string, up to 256 characters, each of which must be a valid domain name character. The TLV has a variable length. This TLV MUST be present.

8. Epoch: This TLV has a type of 0x0008. It contains a 32 bit epoch value. It is used to select a key. This TLV MUST be present.

9. Integrity: This TLV has a type of 0x0009. It contains a 160 bit integrity value, computed using HMAC-SHA1. This TLV MUST be present and MUST be the last TLV in the object.

The base64 encoding uses the base64url encoding from RFC4648 (Josefsson, S., "The Base16, Base32, and Base64 Data Encodings," October 2006.) [RFC4648], with the exception of the pad character, which is a "." instead of an "=". This ensures that the output is a valid SIP token.
To compute the MAC, the following is done. First, the key is obtained. The key is actually a 128 bit key, configured into the system. The key, P, is then used to compute Km:
Km = HMAC-SHA1(P, S | Epoch)
Based on PBKDF2 from PKCS #5 (Kaliski, B., "PKCS #5: Password-Based Cryptography Specification Version 2.0," September 2000.) [RFC2898] with HMAC-SHA1 as PRF and iteration count of 1. Where S is the 32 bit salt and Epoch is the 32 bit Epoch, from the ticket. This produces a 160 bit Km. The MAC is then computed as another HMAC-SHA1, over the entire ticket up to but not including the Integrity itself, using Km as the key. This produces the 160 bit MAC.

---

6. Security Considerations

TOC

TBD

TOC

7. IANA Considerations

TBD - Register SIP Header
TBD - Form IANA registry for Ticket TLVs

---

8. Acknowledgements

TOC

Thanks to Patrice Bruno for his comments, suggestions and questions that helped to improve this document.

---

9. References

TOC

9.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2898]	Kaliski, B., "PKCS #5: Password-Based Cryptography Specification Version 2.0," RFC 2898, September 2000 (TXT).
[RFC4122]	Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace," RFC 4122, July 2005 (TXT, HTML, XML).
[RFC4648]	Josefsson, S., "The Base16, Base32, and Base64 Data Encodings," RFC 4648, October 2006 (TXT).
[VIPR-OVERVIEW]	Rosenberg, J., Jennings, C., and M. Petit-Huguenin, "Verification Involving PSTN Reachability: Requirements and Architecture Overview," draft-rosenberg-dispatch-vipr-overview-04 (work in progress), October 2010 (TXT).

9.2. Informative References

TOC

[VIPR-VAP]	Rosenberg, J., Jennings, C., and M. Petit-Huguenin, "Verification Involving PSTN Reachability: The ViPR Access Protocol (VAP)," draft-rosenberg-dispatch-vipr-vap-03 (work in progress), October 2010 (TXT).

Appendix A. Release notes

TOC

This section must be removed before publication as an RFC.

A.1. Modifications between rosenberg-03 and rosenberg-02

TOC

*Added terminology section.

*Nits

*Shorter I-Ds references.

*Changed issued-to to granted-to.

*Fixed the ABNF.

*The tickets is used in all dialog forming requests, not only INVITE.

*The Number TLV has a variable length.

*The Integrity TLV MUST be the last in the object.

*Fixed a discrepancy in the epoch length.

Authors' Addresses

TOC

	Jonathan Rosenberg
	jdrosen.net
	Monmouth, NJ
	US
Email:	jdrosen@jdrosen.net
URI:	http://www.jdrosen.net
	Cullen Jennings
	Cisco
	170 West Tasman Drive
	MS: SJC-21/2
	San Jose, CA 95134
	USA
Phone:	+1 408 421-9990
Email:	fluffy@cisco.com

	Marc Petit-Huguenin
	Stonyfish
Email:	marc@stonyfish.com