SIPCORE Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 23, 2017

C. Holmberg
Ericsson
J. Jiang
China Mobile

September 19, 2016

Via header field parameter to indicate received realm
draft-holmberg-dispatch-received-realm-03.txt

Abstract

This specification defines a new Session Initiation Protocol (SIP) Via header field parameter, "received-realm", which allows a SIP entity acting as an entry point to a transit network to indicate from which adjacent upstream network a SIP request is received, using a network realm value associated with the adjacent network.

Status of This Memo

This Internet-Draft will expire on March 23, 2017.

Copyright Notice

Table of Contents

1. Introduction

1.1. General

When SIP sessions are established between networks belonging to different operators, or between interconnected networks belonging to the same operator (or enterprise), the SIP requests might traverse transit network.

Such transit networks might provide different kind of services. In order to do that, a transit network often needs to know to which operator (or enterprise) the adjacent upstream network, from which the SIP session initiation request is received, belongs.

This specification defines a new Session Initiation Protocol (SIP) Via header field parameter, "received-realm", which allows a SIP entity acting as an entry point to a transit network to indicate from which adjacent upstream network a SIP request is received, using a network realm value associated with the adjacent network.

NOTE: As the adjacent network can be an enterprise network, an Inter Operator Identifier (IOI) cannot be used to identity the network, as IOIs are not defined for enterprise networks.

The following sections describe use-case where the information is needed.

1.2. Use-Case: Transit Network Application Services

The 3rd Generation Partnership Project (3GPP) TS 23.228 specifies how an IP Multimedia Subsystem (IMS) network can be used to provide transit functionality. An operator can use its IMS network to provide transit functionality e.g. to non-IMS customers, to enterprise networks, and to other network operators.

The transit network operator can provide application services to the networks for which it is providing transit functionality. Transit application services are typically not provided per user basis, as the transit network does not have access to the user profiles of the networks for which the application services are provided. Instead, the application services are provided per served network.

When a SIP entity that provides application services (e.g. an Application Server) within a transit network receives a SIP request, in order to apply the correct services it needs to know the adjacent upstream network from which the SIP request is received.

1.3. Use-Case: Transit Network Routing

A transit network operator normally interconnects to many diferent operators, including other transit network operators, and provides transit routing of SIP requests received from one operator network towards the destination. The destination can be within an operator network to which the transit network operator has a direct interconnect, or within an operator network that only can be reached via one or more interconnected transit operators.

For each customer, i.e. interconnected network operator for which, the transit network operator routes SIP requests towards the requested destination a set of transit routing polices are defined. These policies are used to determine how a SIP request shall be routed towards the requested destination to meet the agreement the transit network operator has with its customer.

When a SIP entity that performs the transit routing functionality receives a SIP request, in order to apply the correct set of transit routing policies, it needs to know from which of its customers, i.e. adjacent upstream network, the SIP request is received.

2. Applicability

The mechanism defined in this specification MUST only be used by SIP entities that are able to verify from which adjacent upstream network a SIP request is received.

The mechanism for verifying from which adjacent upstream network a SIP request is received is outside the scope of this specification.

3. 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 BCP 14, RFC 2119 [RFC2119].

4. Definitions

SIP entity: SIP User Agent (UA), or SIP proxy, as defined in RFC 3261.

Adjacent upstream SIP network: The adjacent SIP network in the direction from which a SIP request is received.

Network entry point: A SIP entity on the border of network, which receives SIP requests from adjacent upstream networks.

Inter Operator Identifier (IOI): A globally unique identifier to correlate billing information generated within the IP Multimedia Subsystem (IMS).

JWS: JSON Web Signature, as defined in RFC 7515.

5. Vie 'received-realm' header field parameter

5.1. General

The Via 'received-realm' header field parameter value is represented as a combination of an operator identyfier, which value represents the adjacent network, and a serialized JSON Web Signature (JWS) [RFC7515]. The JWS Payload consists of the operator identifier and other SIP information element values.

The procedures for encoding the JWS and calculating the signature are defined in [RFC7515]. As the JWS Payload information is found in other SIP information elements the JWS payload is not included in the serialized JWS conveyed in the header field parameter, as described in Appendix F of [RFC7515]. The operator identifier and the serialized JWS are separated using a comma character.

5.2. Operator Identifier

The Operator Identifier is a token value that represents the adjacent operator. The scope of the value is only within the network that inserts the value.

5.3. JWS Header

The following header parameters MUST be included in the JWS.

- The "typ" parameter MUST have a "JWT" value.

- The "alg" parameter MUST have the value of the algorithm used to calculate the JWS.

NOTE: Operators need to agree on the set of supported algorithms for calculating the JWT signature.

Example:

```
{
        "typ":"JWT",
        "alg":"HS256"
}
```

5.4. JWS Payload

The followoing claims MUST be included in the JWS Payload.

- The "sip_from_tag" claim has the value of the From 'tag' header field parameter of the SIP message.

- The "sip_date" claim has the value of the Date header field in the SIP message, quoted and encoded in JSON NumbericData format [RFC7519].

- The "sip_callid" claim has have value of the Call-ID header field in the SIP message.

- The "sip_cseq_num" claim has the numeric value of the CSeq header field in the SIP message.

- the "sip_via_branch" claim has value of the Via branch header field parameter of the Via header field, in the SIP message, to which the received-realm header field parameter is attached.

All claims MUST be encoded using lower case characters.

All claims except "sip_date" MUST be encoded as StringOrURI JSON string value [RFC7519].

The sip_date claim MUST be encoded as a JSON NumericData value [RFC7519]

Example:

```
{
        "sip_from_tag":"1928301774",
        "sip_date":"1472815523",
        "sip_callid":"a84b4c76e66710@pc33.atlanta.com",
        "sip_cseq_num":"314159",
        "sip_via_branch":"z9hG4bK776asdhds"
}
```

5.5. Syntax

5.5.1. General

This section describes the syntax extensions to the ABNF syntax defined in [RFC3261], by defining a new Via header field parameter, "received-realm". The ABNF defined in this specification is

conformant to RFC 5234 [RFC5234]. "EQUAL", "LDQUOT", "RDQUOT" and "ALPHA" are defined in [RFC3261]. "DIGIT" is defined in [RFC5234].

5.5.2. ABNF

```
        via-params     =/ received-realm
        received-realm = "received-realm" EQUAL operator-id COLON jws
        operator-id    = token
        jws            = LDQUOT header "." "." signature RDQUOT
        header         = *base64-char
        signature      = *base64-char
        base64-char    = ALPHA / DIGIT / "/" / "+"
```

EQUAL, COLON, token, LDQUOT, RDQUOT, ALPHA and DIGIT as defined in RFC 3261.

5.6. Example

```
     Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776;
     received-realm=myoperator:"eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1N..
           dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk"
```

NOTE: Line breaks for display purpose only

6. User Agent and Proxy behavior

6.1. General

This section describes how a SIP entity, acting as an entry point to a network, uses the "received-realm" Via header field parameter.

6.2. Behavior of a SIP entity acting as a network entry point

When a SIP entity, acting as a network entry point, forwards a SIP request, or initiates a SIP request on its own (e.g. a PSTN gateway), the SIP entity adds a Via header field to the SIP request, according to the procedures in RFC 3261 [RFC3261]. In addition, if the SIP entity is able to assert the adjacent upstream network, and if the SIP entity is aware of a network realm value defined for that network, the SIP entity can add a "received-realm" Via header field parameter, conveying the network realm value, to the Via header field added to the SIP request.

When the SIP entity adds a "received-realm" Via header field parameter to a SIP request, it MUST also calculate a Hash-based

message authentication code (HMAC) [RFC2104] value from the parameter value, using a secret key which is shared between the SIP entity and any SIP entity which will use the parameter value. The HMAC is then added to the parameter.

When the receiver decodes the JWT, it MUST compare the JWT claims with the corresponding SIP header field information. If there is a mismatch, the receiver MUST discard the received-realm header field parameter.

6.3. Behavior of a SIP entity consuming the received-network value

When a SIP entity receives a Via 'received-network' header field parameter, and intends to perform actions based on the header field parameter value, it MUST first re-calculate the JWS and check whether the result matches the JWS received. If there is not a match the SIP entity MUST discard the received 'received-network' header field parameter. The SIP entity MAY take also take additional actions (e.g. rejecting the SIP request) based on local policy.

7. Example

```
 Operator 1    T_EP                                 T_AS

 - INVITE ------>
   Via: SIP/2.0/UDP IP_UA
                 -- INVITE ---------------------------->
                    Via: SIP/2.0/UDP IP_TEP;branch=z9hG4bK776;
                     received-realm=myoperator:"eyJ0eXAiOiJKV1QiLA0KICJh
                     bGciOiJIUzI1N..dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW
                     1gFWFOEjXk"
                    Via: SIP/2.0/UDP IP_UA; received=IP_UA

                 <- 200 OK ----------------------------
                    Via: SIP/2.0/UDP IP_TEP;branch=z9hG4bK776;
                     received-realm=myoperator:"eyJ0eXAiOiJKV1QiLA0KICJh
                     bGciOiJIUzI1N..dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW
                     1gFWFOEjXk"
                    Via: SIP/2.0/UDP IP_UA; received=IP_UA

 <- 200 OK------
    Via: SIP/2.0/UDP IP_UA; received=IP_UA
```

8. IANA Considerations

8.1. 'received-realm' Via header field parameter

This specification defines a new Via header field parameter called received-realm in the "Header Field Parameters and Parameter Values" sub-registry as per the registry created by [RFC3968]. The syntax is defined in Section 5.5. The required information is:

Header Field	Parameter Name	Predefined Values	Reference
Via	received-realm	No	RFCXXXX

8.2. JSON Web Token Claims Registration

This specification defines new JSON Web Token claims in the "JSON Web Token Claims" sub-registry as per the registry created by [RFC7519].

Claim Name: "sip_from_tag"

Claim : SIP From tag header field parameter value

Change Controller: IESG

Specification Document(s): RFC XXXX, RFC 3261

Claim Name: "sip_date"

Claim Description: SIP Date header field value

Change Controller: IESG

Specification Document(s): RFC XXXX, RFC 3261

Claim Name: "sip_callid"

Claim Description: SIP Call-Id header field value

Change Controller: IESG

Specification Document(s): RFC XXXX, RFC 3261

Claim Name: "sip_cseq_num"

Claim Description: SIP CSeq numeric header field parameter value

Change Controller: IESG

Specification Document(s): RFC XXXX, RFC 3261

Claim Name: "sip_via_branch"

Claim Description: SIP Via branch header field parameter value

Change Controller: IESG

Specification Document(s): RFC XXXX, RFC 3261

9. Security Considerations

As the received-realm Via header field parameter can be used to trigger applications, it is important to ensure that the parameter has not been added to the SIP message by an unauthorized SIP entity.

The operator MUST change the key on a frequent basis. The operator also needs to take great care in ensuring that the key used to calculate the JWS signature value is only known by the network entry point adding the received-realm Via header field parameter to a SIP message and the entities that use the parameter value.

A SIP entity MUST NOT use the adjacent network information if there is a mismatch between the JWS value received in the SIP header field and the JWS calculated by the receiving entity.

A SIP entity MUST use different key values for each parameter value that it recognizes and use to trigger actions.

Generic security considerations for JWS are defined in [RFC7515].

10. Acknowledgements

Thanks to Adam Roach and Richard Barnes for providing comments and feedback on the document.

11. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from draft-holmberg-dispatch-received-realm-02

- JWT replaced with JWS.

- Appendix F of RFC 7515 applied.

Changes from draft-holmberg-dispatch-received-realm-01

- Define received-realm parameter value as a JSON Web Token (JWT).

Changes from draft-holmberg-dispatch-received-realm-00

- New version due to expiration of previous version.

Changes from draft-holmberg-received-realm-04

- Changed IETF WG from sipcore do dispatch.

- HMAC value added to the parameter.

Changes from draft-holmberg-received-realm-03

- New version due to expiration.

Changes from draft-holmberg-received-realm-02

- New version due to expiration.

Changes from draft-holmberg-received-realm-01

- New version due to expiration.

Changes from draft-holmberg-received-realm-00

- New version due to expiration.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <http://www.rfc-editor.org/info/rfc7515>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <http://www.rfc-editor.org/info/rfc7519>.

12.2. Informative References

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <http://www.rfc-editor.org/info/rfc2104>.

[RFC3968] Camarillo, G., "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)", BCP 98, RFC 3968, DOI 10.17487/RFC3968, December 2004, <http://www.rfc-editor.org/info/rfc3968>.

Authors' Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com

Yi Jiang
China Mobile
No.32 Xuanwumen West Street
Beijing Xicheng District 100053
P.R. China

Email: jiangyi@chinamobile.com