Internet Engineering Task Force (IETF)
Request for Comments: 8055
Category: Standards Track
ISSN: 2070-1721

C. Holmberg
Ericsson
Y. Jiang
China Mobile

January 2017

Session Initiation Protocol (SIP) Via Header Field Parameter to Indicate Received Realm

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 by using a network realm value associated with the adjacent network.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8055.

Table of Contents

1. Introduction

1.1. General

When Session Initiation Protocol (SIP) [RFC3261] sessions are established between networks belonging to different operators or between interconnected networks belonging to the same operator (or enterprise), the SIP requests associated with the session might traverse transit networks.

Such transit networks might provide different kinds of services. In order to provide such services, 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 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 by 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 identify the network because IOIs are not defined for enterprise networks.

The following sections describe use cases where the information is needed.

1.2. Use Case: Transit Network Application Services

The Third Generation Partnership Project (3GPP) TS 23.228 [TS.3GPP.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 on a 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 different 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 policies 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. Such a mechanism might be based on, for instance, receiving the SIP request on an authenticated Virtual Private Network (VPN), on a specific IP address, or on a specific network access.

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: A 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 the 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: A JSON Web Signature, as defined in [RFC7515].

5. Via 'received-realm' Header Field Parameter

5.1. General

The Via 'received-realm' header field parameter value is represented as a combination of an operator identifier whose 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 detached from 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 colon 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.

The operator identifier value is case insensitive.

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.

NOTE: The "alg" parameter values for specific algorithms are listed in the IANA JSON Web Signature and Encryption Algorithms sub-registry of the JSON Object Signing and Encryption (JOSE) registry. Operators need to use algorithms for which an associated "alg" parameter value has been registered. The procedures for defining new values are defined in [RFC7518].

Example:

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

5.4. JWS Payload

The following 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, encoded in JSON NumericDate format [RFC7519].
- The "sip_callid" claim has the 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 the 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.

- The "sip_via_opid" claim has the value of the operator identifier part of the Via 'received-realm' header field parameter of the Via header field, in the SIP message, to which the 'received-realm' header field parameter is attached.

Example:

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

5.5. JWS Serialization

As the JWS Payload is not carried in the 'received-realm' parameter, in order to make sure that the sender and the receiver construct the JWS Payload object in the same way, the JSON representation of the JWS Payload object MUST be computed as follows:

- All claims MUST be encoded using lowercase characters.
- The claims MUST be in the same order as listed in Section 5.4.
- All claims except "sip_date" MUST be encoded as StringOrURI JSON string value [RFC7519].
- The "sip_date" claim MUST be encoded as a JSON NumericDate value [RFC7519].
- The JWS Payload MUST follow the rules for the construction of the thumbprint of a JSON Web Key (JWK) as defined in Section 3, Step 1 only, of [RFC7638].

Example:

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

NOTE: Line breaks are for display purposes only.

5.6. Syntax

5.6.1. 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].

5.6.2. ABNF

```
via-params     =/ received-realm
received-realm = "received-realm" EQUAL LDQUOT op-id COLON jws RDQUOT
op-id          = token
jws            = header ".." signature
header         = 1*base64-char
signature      = 1*base64-char
base64-char    = ALPHA / DIGIT / "/" / "+"
```

EQUAL, COLON, token, LDQUOT, RDQUOT, ALPHA, and DIGIT are as defined in [RFC3261].

NOTE: The two adjacent dots in the 'jws' part are due to the detached payload being replaced by an empty string [RFC7515].

5.7. Example: SIP Via Header Field

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

NOTE: Line breaks are for display purposes 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 Public Switched Telephone Network (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 as the operator identifier (Section 5.2) part of the header field parameter, to the Via header field added to the SIP request.

In addition, the SIP entity MUST also calculate a JWS (Section 5.4) and add the calculated JWS Header and JWS Signature as the 'jws' part of the Via header field parameter.

6.3. Behavior of a SIP Entity Consuming the 'received-realm' Value

When a SIP entity receives a Via 'received-realm' header field parameter and intends to perform actions based on the header field parameter value, it MUST first recalculate 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-realm' header field parameter. The SIP entity MAY also take additional actions (e.g., rejecting the SIP request) based on local policy.

7. Example: SIP INVITE Request and Response

This section shows an example of a SIP INVITE request and the associated response, which contains a Via header field (inserted into the request and removed from the response by the T_EP SIP proxy) with a 'received-realm' header field parameter.

```
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 created by [RFC3968]. The syntax is defined in Section 5.6. The required information is:

Header Field	Parameter Name	Predefined Values	Reference
Via	received-realm	No	RFC 8055

8.2. JSON Web Token Claims Registration

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

Claim Name: sip_from_tag
Claim Description: SIP From tag header field parameter value
Change Controller: IESG
Reference: RFC 8055, RFC 3261

Claim Name: sip_date
Claim Description: SIP Date header field value
Change Controller: IESG
Reference: RFC 8055, RFC 3261

Claim Name: sip_callid
Claim Description: SIP Call-Id header field value
Change Controller: IESG
Reference: RFC 8055, RFC 3261

Claim Name: sip_cseq_num
Claim Description: SIP CSeq numeric header field parameter value
Change Controller: IESG
Reference: RFC 8055, RFC 3261

Claim Name: sip_via_branch
Claim Description: SIP Via branch header field parameter value
Change Controller: IESG
Reference: RFC 8055, 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 'received-realm' Via header field parameter is inserted, signed, verified, and consumed within an operator network. The operator MUST discard parameters received from another network, and the parameter MUST only be inserted by SIP entities that are able to verify from which adjacent upstream network a SIP request is received.

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 entities signing and adding the JWS Signature to the 'received-realm' Via header field parameter of a SIP message and to network entities verifying and consuming the parameter value.

The operator MUST use a key management policy that protects against unauthorized access to the stored keys within nodes where the keys associated with the JWS Signature are stored and that protects against cryptoanalysis attacks using captured data sent on the wire.

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

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

10. References

10.1. 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>.

[RFC7638] Jones, M. and N. Sakimura, "JSON Web Key (JWK) Thumbprint", RFC 7638, DOI 10.17487/RFC7638, September 2015, <http://www.rfc-editor.org/info/rfc7638>.

10.2. Informative References

[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>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <http://www.rfc-editor.org/info/rfc7518>.

[TS.3GPP.23.228] 3GPP, "IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228 14.1.0, September 2016, <http://www.3gpp.org/ftp/Specs/html-info/23228.htm>.

Acknowledgements

Thanks to Adam Roach and Richard Barnes for providing comments and feedback on the document. Francis Dupoint performed the Gen-ART review.

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
China

Email: jiangyi@chinamobile.com