Retargeting Security in the Session Initiation Protocol (SIP)
draft-xu-yang-retargeting-security-00.txt

Abstract

As a SIP request is processed along its route to the destination, the initial request-URI can be altered without callers' notice or consent. The caller may concern both the final call recipient's identity and the authorities of the SIP intermediaries that alter the request-URI. Especially when the caller does not know the final call recipient, simply giving his/her identity to the caller will not help the caller to decide the legitimacy of the call. Without a secure retarget mechanism, the end-to-end security of SIP cannot be guaranteed. This document proposes a security mechanism to provide
the caller with credentials of SIP intermediaries that retarget a request and the final recipient's identity through response.

Conventions used in this document

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 [i].

Related response: final responses that define the security attributes of existing or future dialogs. The related responses include the 2xx response that carries the callee's identity, the 3xx response that carries the callee's new contact addresses, and the 496 or 493 response that carries the security key for future dialogs.

Table of Contents

1. Introduction...................................................2
2. Definitions....................................................4
3. Overviews of solution........................................4
4. Behavior........................................................5
   4.1 User Agent Behavior.......................................5
   4.2 Proxy Behavior...........................................5
   4.3 Redirector behavior......................................6
5. Criteria for recording and checking request-URI changes.......7
6. Formal Syntax..................................................7
7. Message Examples.............................................8
8. IANA considerations........................................13
   8.1 Header....................................................13
   8.2 Optional Tag.............................................13
9. Security Considerations......................................13
References....................................................................14
Acknowledgments..................................................14
Author's Addresses...............................................14
Intellectual Property and Copyright Statements.................15

1. Introduction

As a SIP request is processed in intermediaries, the initial request-URI can be altered with one or more targets identified via location service. This process, so-called Retargeting, is often done without caller's notice or consent. Since the current standards do not provide a mechanism for a UAC to constrain or authorize SIP intermediaries as what should be performed, and to authenticate the final call recipient's identity through SIP response, the UAC does not know where a request goes, how a request reaches a particular UAS and who this UAS is [5].

Yang                   Expires - November 2007               [Page 2]
In some circumstance, users are more interested in how a request reaches a particular UAS, e.g., when Alice calls Bob and Bob redirects calls to Carols, Alice wants to make sure that it is Bob that designated the delegation agent. It is also useful in the calling center when a call is redirected to a special handling agent, especially when the agent is outside the original domain. The UAC can determine the URI that a request has eventually reached and determine whether the chain of trust is broken during request retargeting, e.g., the request is retargeted in some suspicious domains.

Although connected identity [2] has proposed to use mid-dialog requests, e.g., an UPDATE method or re-INVITE method, to transfer the updated calling and called party’s identity based on RFC4474, several issues are still not resolved.

(1) The response identity problem. The handling of responses such as 493 Undecipherable and 3xx is fraught with risks if the identity of the sender of the response cannot be identified. Consider the following scenario mentioned in [5]: If Alice’s request to Bob is retargeted to Carol and Carol does not possess the private key corresponding to Bob’s public key, she would send some sort of failure response code (perhaps a 493 Undecipherable). According to the manner suggested in RFC3261, Alice might re-initiate the session using Carol’s certificate received in the body of 493 response. Here, Alice has no way of knowing if Carol is actually an attacker who sends a 493 in order to bid-down the security for the ensuing RTP session.

(2) If sometimes (1) can sometimes be avoided with connected identity [2], it means more rounds of message exchange. For example, a session only consists of an INVITE and a 3XX, or a MESSAGE with encrypted message body, [2] seems over weighted.

(3) If the target is redirected to an unknown domain, then secure retargeting is more important because of the unanticipated respondent problem, and the caller more trust the initial call recipient’s domain and its retargeting process than the new respondent.

Other cases such as in the session border controller scenario, where a UA cannot differentiate malicious man-in-the-middle attack and legitimate SBC, the secure retargeting helps to distinguish these cases if required.

To achieve end-to-end security, we feel that the response identity problem cannot be omitted, and it has to be solved with the secure retargeting. It is essential for the protocol to provide a mechanism to feed the caller with (1) the retargeting information, (2) the credential of the intermediate server that retargets a request to a
different Request-URI, and (3) the final recipient identity. This document proposes such a mechanism.

2. Definitions

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.

Related response: final responses that define the security attributes of existing or future dialogs. The related responses include the 2xx response that carries the callee’s identity, the 3xx response that carries the callee’s new contact addresses, and the 496 or 493 response that carries the security key for future dialogs.

3. Overviews of solution

The fundamental functionality provided by the secure retargeting mechanism is the ability to collect credentials of intermediate servers that retarget requests and capture the associated request-URI change. The original request-URI, modified request-URI and the Identity of the server that does the request-URI modification are recorded in a new header for SIP messages: Target-Info. The signature used for validating headers including the Target-Info header is conveyed in the Identity header, and the reference to the certificate of the signer is conveyed in the Identity-Info header, as described in RFC 4474. An additional index parameter is added to each of the above header to group related information for a single retargeting server.

In applications that concentrate on sending callers target change for successfully established dialogs, the Target-Info header is added to 2xx, 3xx and responses that would change the secure attribute of a future dialog, such as the 496 and 493 responses. In this specification, these responses are called related responses.

If a caller wants intermediaries to provide credentials of retargeting on related responses, she/he MUST insert a new option tag target-info in the request to initiate a session.

To shield the network configuration and reduce computation overhead, proxies on the border of a trusted network SHOULD eliminate intermediate retargeting process information for routing and other purposes. There, the Authentication Service proxy SHOULD be logically configured on the network border. When the Authentication Service proxy received an incoming request with target-info in the Supported header and the related response indicating that request-URI
is changed within the trusted network, the proxy MUST insert Identity and Identity-Info headers in the response before forwarding the response to an untrusted network. Given secure connections exist between trusted network elements, the proxy SHOULD merge multiple Target-Info headers inserted within the trusted network into a single Target-Info header, which only records the last changed request-URI and the original request-URI received by the trusted network.

4. Behavior

4.1 User Agent Behavior

When issuing an INVITE request, a UAC that wishes to learn the intermediate target change MUST include a Target-info option tag in the Supported header field.

When receiving a response with Target-Info, Identity and Identity-Info header, the UAC inspects the signature in the Identity headers and validates related header fields and the message body.

Since each Target-Info provides an old and changed request-URI, and the last Target-Info provides the identity of the sender of the response, the Target-Info headers can form a trace of request-URIs when request is routed to the destination. For adjacent Target-Info pairs, the changed request-URI in the prior Target-Info MUST equal to the old or current request-URI in the next Target-Info.

The criteria for judging a request-URI change or for detecting a missing request-URI change segment are specified in section 6.

4.2 Proxy Behavior

For proxies that do not retarget requests, no behavior change is required.

The following is the behavior of a proxy that has performed or is about to perform retargeting.

When a proxy server receives a request with a Target-info option tag in the Supported header filed, if the proxy server is about to change the request-URI but is not able to provide authentication service for the future related response, the proxy SHOULD return a 420 Not Supported response. If the authentication service is provided in a centralized server, the proxy MUST be able to create a secure connection with the central authentication service.

When a proxy server receives a redirect response, before retargeting the request to the request-URI extracted from the contact header, the
proxy server MUST first verify whether the redirect response is directly received from a trust domain, or whether the contact header of the response is verifiable from the Identity and Identity-Info header. Here, the proxy delegates the process of authentication of the response to the caller. A proxy server MUST not forward any related response that comes from an untrust domain and does not have an Identity and Identity-Info header.

If the response comes from an untrust domain but has an unverifiable Identity and Identity-Info header, the proxy SHOULD forward the response upstream to the caller. If the response is a result of retargeting performed at the proxy, the proxy MUST insert a Target-Info header, and then use the domain key to sign the hash of the canonical string generated from certain components of the response before forwarding.

If the proxy performs a sequential or parallel search, the proxy SHOULD exhaust verifiable contact headers first.

If several proxies within a trust domain perform retargeting, then each of these proxies SHOULD insert a separate Target-Info header. If network privacy is enforced, e.g., when the consent framework [3] conceals the detailed user location, the border proxy MUST omit privacy sensitive request-URI changes within the domain. In a transition domain, only the original request-URI received by the domain and the last changed request-URI when the request left the domain are kept in the Target-Info header. In the destination domain, only the original request-URI received by the domain is left in the Target-Info header. While security always causes overhead, the proper network configuration can significantly reduce it. Centralized authentication service on a border proxy is one example.

The Target-Info header MUST be signed before sending the related response out of the trust domain.

4.3 Redirector behavior

If the redirect service only serves the proxy in the trust domain, then there is no behavior change.

Otherwise, when a redirector receives a request with the Target-info option tag in the Supported header filed, it SHOULD insert a Target-Info, Identity and Identity-Info header for the redirect response, or do so through an authentication service. If the redirect service only serves the proxy in the trust domain, then there is no behavior change.

Otherwise, when a redirector receives a request with the Target-info option tag in the Supported header filed, it SHOULD insert a
Target-Info, Identity and Identity-Info header for the redirect response, or do so through an authentication service.

5. Criteria for recording and checking request-URI changes

The criteria of justifying a request-URI change depend on the request-URI scheme and the portion of the request-URI involved in a change.

If a GRUU [4] request-URI is used, each request-URI change MUST be recorded.

If the tel URI scheme is used, adding or deleting international or area code MAY be considered as a target change.

The username change in a sip URI MUST be considered as a target change.

In the same trust domain, the host portion of a request-URI may be changed several times. In the destination domain, the host portion of a request-URI is often detailed to a specific host address. As specified in section 4, the authentication service MAY choose to conceal such detailed retargeting information. In the same trust domain, only receiving last modified host portion of the request-URI is recorded. In the destination domain, only the receiving user name and host portion of the request-URI is recorded.

The user's involvement MAY be required for some ambiguous target change. The UA can list suspicious target changes via GUI.

6. Formal Syntax

The Target-Info header carries the following information, with the mandatory parameters required.

target change: A mandatory parameter contains either the current target or a pair of targets that reflect the target change.

retarget-server: A mandatory parameter captures the server name that performs the retargeting.

index: A mandatory parameter that groups related Target-Info, Identity and Identity-Info headers. The index starts at one. Each subsequent index increases by one.

Target-Info=ÂTarget-InfoÂ HCOLON (target-change|current-target) COMMA retarget-server COMMA index
Retargeting Security                 May 2007

target-change=previous-target COMMA changed-target COMMA index
previous-target = ÂpreviousÂ EQUAL request-URI
changed-target = ÂchangedÂ EQUAL request-URI

current-target = ÂcurrentÂ EQUAL request-URI

reTARGET-server = ÂserverÂ EQUAL name-addr

index = ÂindexÂ EQUAL 1*DIGIT

request-URI = name-addr

The Identity and Identity-Info header defined in RFC 4474 are also
updated with the additional index parameter.

Identity = "Identity" HCOLON signed-identity-digest COMMA index

Identity-Info = "Identity-Info" HCOLON ident-info *(SEMI ident-
info-params) COMMA index

The signed-identity-digest is a signed hash of a canonical string
generated from certain components of a SIP response. To create the
content of the signed-identity-digest, the authentication service
MUST use the elements of a SIP message placed in a bit-exact string
specified in RFC 4474, and the added Target-Info header specified in
this document, separated by a vertical line, Â|Â or %x7C, character:

digest-string = digest-string = addr-spec "|" addr-spec "|" callid
"|" 1*DIGIT SP Method "|" SIP-date "|" [ addr-spec ] "|" message-body
Â|Â Target-Info

The Target-Info above refers to the local added Target-Info

7. Message Examples

It is expected that most retargeting happen in destination domain, in
which the authentication service signs and forwards the response from
the final call recipient back to the caller.

In the following example, we describe a simple case when UA Alice
initiates an INVITE to Bob and the INVITE is redirected in the
destination domain. We assume the destination proxy, the destination
redirector, and the final call recipient Bob are all in the same
trust domain.

Yang                   Expires - November 2007               [Page 8]
F1: UA Alice -> Proxy destination

INVITE sip:bob@destination.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.source.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@destination.com>
From: Alice <sip:alice@atlanta.source.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Supported: target-info
Contact: <sip:alice@pc33.atlanta.source.com>
Content-Type: application/sdp
Content-Length: 147

v=0
o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
s=Session SDP
c=IN IP4 atlanta.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

F2: Proxy destination -> Redirector destination

INVITE sip:bob@destination.com SIP/2.0
Via: SIP/2.0/UDP proxy.destination.com;branch=z9hG4bKnashds8
Via: SIP/2.0/UDP pc33.atlanta.source.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@destination.com>
From: Alice <sip:alice@atlanta.source.com>;tag=1928301774
Call-ID: a84b4c76e66710

CSeq: 314159 INVITE
Max-Forwards: 70
Supported: target-info
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@atlanta.source.com>
Content-Type: application/sdp
Content-Length: 147

v=0
o=Alice 2890844526 2890844526 IN IP4 atlanta.example.com
s=Session SDP
c=IN IP4 atlanta.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

F3: Redirector destination

Since both the destination proxy and redirector are in the same trust domain, no security-retargeting headers are generated. Otherwise, the redirector MUST insert security-retargeting headers and the proxy MUST verify these headers before retargeting the request to contact addresses specified in the returned 3xx response.

302 Temporarily Moved
Via: SIP/2.0/UDP proxy.destination.com;branch=z9hG4bKnashds8
Via: SIP/2.0/UDP pc33.atlanta.source.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@home.destination.com>
From: Alice <sip:alice@atlanta.source.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:bob@home.destination.com>
Content-Type: application/sdp
Content-Length: 0

F4: Proxy destination -> UA Bob

The destination proxy changes the request-URI to bob@home.destination.com.

INVITE sip:bob@home.destination.com SIP/2.0
Via: SIP/2.0/UDP proxy.destination.com;branch=z9hG4bKnashds8
Via: SIP/2.0/UDP pc33.atlanta.source.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@destination.com>
From: Alice <sip:alice@atlanta.source.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Supported: target-info
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@atlanta.source.com>
Content-Type: application/sdp
Content-Length: 147

v=0
o=Alice 2890844526 2890844526 IN IP4 atlanta.example.com
s=Session SDP
c=IN IP4 atlanta.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

F5: UA Bob -> Proxy destination

200 OK SIP/2.0
Via: SIP/2.0/UDP proxy.destination.com;branch=z9hG4bKnashds8
Via: SIP/2.0/UDP pc33.atlanta.source.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@destination.com>
From: Alice <sip:alice@atlanta.source.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:bob@home.source.com>
Content-Type: application/sdp
Content-Length: 147

v=0
o=Alice 2890844526 2890844526 IN IP4 atlanta.example.com
s=Session SDP
c=IN IP4 atlanta.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

F6: Proxy destination -> UA Alice

Assume secure communications exist between the destination proxy and
UA Bob and the destination proxy verifies UA Bob's identity through
HTTP change and response. Also assume that the privacy policy allows
the proxy to disclose the user location information to the caller.
200 OK SIP/2.0
Via: SIP/2.0/UDP proxy.destination.com;branch=z9hG4bKnashds8
Via: SIP/2.0/UDP pc33.atlanta.source.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@destination.com>
From: Alice <sip:alice@atlanta.source.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Target-Info: previous=bob@destination.com,
changed=bob@home.destination.com, current=bob@home.destination.com,
server=proxy.destination.com,index=1
Identity:ÂZYNBbHC00VMZr2kZt6VmCvPonWJMGrqTBqghoWeLxJfzB2alpxAr3VgrB0
SsSAaifsRdiOpoQZYCv2wrVghuhcsMbHWUSFxFI6p6q5TOQXHMz6uEo3s5jsSH49thyGn
FVcnyaZ++yR1BYQtLqWzJ+KvhPKbfU/pryhVn9yc6U=Â, index=1
Identity-Info: <https://desination.com/destination.cer>;alg=rsa-shal,
index=1
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:bob@home.source.com>
Content-Type: application/sdp
Content-Length: 147

v=0
c=IN IP4 destination.com
s=Session SDP
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

If assume that the privacy policy does not allow the proxy to
disclose the user location information to the caller, F6 should look
like this:

F6: Proxy destination -> UA Alice

200 OK SIP/2.0
Via: SIP/2.0/UDP proxy.destination.com;branch=z9hG4bKnashds8
Via: SIP/2.0/UDP pc33.atlanta.source.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@destination.com>
From: Alice <sip:alice@atlanta.source.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Target-Info: current= bob@destination.com,
server=proxy.destination.com,index=1
Identity:ÂZYNBbHC00VMZr2kZt6VmCvPonWJMGrqTBqghoWeLxJfzB2alpxAr3VgrB0
SsSAaifsRdiOpoQZYCv2wrVghuhcsMbHWUSFxFI6p6q5TOQXHMz6uEo3s5jsSH49thyGn
FVcnyaZ++yR1BYQtLqWzJ+KvhPKbfU/pryhVn9yc6U=Â, index=1
8. IANA considerations

This specification registers a new SIP header and a new option tag.

8.1 Header

This specification registers a new SIP header, according to the guidelines in Section 27.1 of RFC 3261.

Name: Target-Info

Description: This new header captures the request-URI change and the current request-URI.

8.2 Optional Tag

This specification registers a new optional tag, according to the guidelines in Section 27.1 of RFC 3261.

Name: target-info

Description: This option tag is used to indicate that a UA requires intermediate proxies that perform retargeting to add Target-Info, Identity and Identity-Info headers in the response.

9. Security Considerations

This document proposes a security mechanism to provide the caller with credentials of SIP intermediaries that retarget a request and the final recipient's identity through response.
References


Acknowledgments

Thanks to Mark Duffy for providing valuable comments.

Author’s Addresses

Xu Yang
Sonus Networks
7 Technology Park Drive
Westford, MA 01886
Phone: 978-614-8205
Email: cxuyang@sonusnet.com
Retargeting Security

May 2007

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is currently provided by the IETF Administrative Support Activity (IASA).