                    PASSporT Extension for Diverted Calls
                    draft-ietf-stir-passport-divert-01.txt

Abstract

   This document extends PASSporT, which conveys cryptographically-
   signed information about the people involved in personal
   communications, to include an indication that a call has been
   diverted from its original destination to a new one. This
   information can greatly improve the decisions made by verification
   services in call forwarding scenarios.

Status of This Memo

Copyright Notice

the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

[1](#). Introduction

PASSporT [I-D.ietf-stir-passport] is a token format based on JWT
[RFC7519] for conveying cryptographically-signed information about
the people involved in personal communications; it is used with STIR
[I-D.ietf-stir-rfc4474bis] to convey a signed assertion of the
identity of the participants in real-time communications established
via a protocol like SIP. This specification extends PASSporT to
include an indication that a call has been diverted from its
originally destination to a new one.

Although the STIR problem statement [RFC7340] is focused on
preventing the impersonation of the caller's identity, which is a
common enabler for threats such as robocalling and voicemail hacking
on the telephone network today, it also provides a signature over the
called number as the authentication service sees it. As
[I-D.ietf-stir-rfc4474bis] Section 12.1 describes, this protection
over the contents of the To header field is intended to prevent a
class of cut-and-paste attacks. If Alice calls Bob, for example, Bob
might attempt to cut-and-paste the Identity header field in Alice's
INVITE into a new INVITE that Bob sends to Carol, and thus be able to
fool Carol into thinking the call came from Alice and not Bob. With
the signature over the To header field value, the INVITE Carol sees
will clearly have been destined originally for Bob, and thus Carol
can view the INVITE as suspect.

However, as [I-D.ietf-stir-rfc4474bis] Section 12.1.1 points out, it
is difficult for Carol to confirm or reject these suspicions based on
the information she receives from the baseline PASSporT object. The

common "call forwarding" service serves as a good example of the fact
that the original called party number is not always the number to
which a call is delivered. The address in the To header field value
of SIP requests is not supposed to change, accordingly to baseline
[RFC3261], as it is the Request-URI that is supposed to be updated
when a call is retargeted, but practically speaking some operational
environments do alter the To header field. There are a number of
potential ways for intermediaries to indicate that such a forwarding
operating has taken place. The History-Info header field [RFC7044]
was created to store the Request-URIs that are discarded by a call in
transit. The SIP Diversion header field [RFC5806], though historic,
is still used for this purpose by some operators today. Neither of
these header fields provide any cryptographic assurance of secure
redirection, and they can both capture minor syntactical changes in
URIs that do not reflect a change to the actual target of a call.

This specification therefore extends PASSporT with an explicit
indication that original called number in PASSporT no longer reflects
the destination to which a call is likely to be delivered.
Verification services and the relying parties who make authorization
decisions about communications may use this indication to confirm
that a legitimate retargeting of the call has taken place, rather
than a cut-and-paste attack.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED",
"SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT
RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as
described in [RFC2119].

3. PASSporT 'div' Claim

This specification defines a new JSON Web Token claim for "div" which
indicates a previous destination for a call during its routing
process. When a retargeting entity receives a call signed with a
PASSporT, it may act as an authentication service and create a new
PASSporT containing the "div" claim to attach to the call (without
removing the original PASSporT). Note that a new PASSporT is only
necessary when the cannical form of the "dest" identifier (per the
canonicalization procedures in [I-D.ietf-stir-rfc4474bis] Section 8)
changes due to this retargeting. "div" is typically populated with a
destination address found in the "dest" field of PASSporT received by
the retargeting entity. These new PASSporT generated by retargeting
entities MUST include the "div" PASSporT type, and an "x5u" field
pointing to a credential that the retargeting entity controls. The
new PASSporT will look as follows:

```
{ "typ":"passport",
  "ppt":"div",
  "alg":"ES256",
  "x5u":"https://www.example.com/cert.pkx" }
```

A PASSporT claims object containing "div" is populated with a
modification of the original token before the call was retargeted: at
a high level, the original identifier for the called party in the
"dest" array will become the "div" claim in the new PASSporT. If the
"dest" array of the original PASSporT contains multiple identifiers,
the retargeting entity MUST select only one them to occupy the "div"
field in the new PASSporT. and in particular, it MUST select an
identifier that is within the scope of the credential that the
retargeting entity will specify in the "x5u" of the PASSporT header
(as described below).

The new target for the call selected by the retargeting entity
becomes the value of the "dest" array of the new PASSporT. The
"orig" value MUST be copied into the new PASSporT from the original
PASSporT received by the retargeting entity. The regargeting entity
SHOULD retain the "iat" value from the original PASSporT, though if
in the underlying signaling protocol (e.g. SIP) the retargeting
entity changes the date and time information in the retargeted
request, the new PASSporT should instead reflect that date and time.
No other extension claims should be copied from the original PASSporT
to the "div" PASSporT.

So, for an original PASSporT of the form:

```
{ "orig":{"tn":"12155551212"},
  "dest":{"tn":"12155551213"},
  "iat":1443208345 }
```

If the retargeting entity is changing the target from 12155551213 to
12155551214, the new PASSporT with "div" would look as follows:

```
{ "orig":{"tn":"12155551212"},
  "dest":{"tn":"12155551214"},
  "iat":1443208345,
  "div":{"tn":"121555551213"} }
```

After the PASSporT header and claims have been constructed, their
signature is generated per the guidance in [I-D.ietf-stir-passport] -
except for the credential required to sign it. While in the ordinary
construction of a PASSporT, the credential used to sign will have
authority over the identity in the "orig" claim (for example, a
certificate with authority over the telephone number in "orig" per
[I-D.ietf-stir-certificates]), for all PASSporTs using the "div" type

the signature MUST be created with a credential with authority over
the identity present in the "div" claim. So for the example above,
where the original "dest" is "12155551213", the signer of the new
PASSporT object MUST have authority over that telephone number, and
need not have any authority over the telephone number present in the
"orig" claim.

4. Using 'div' in SIP

This section specifies SIP-specific usage for the "div" PASSporT type
and its handling in the SIP Identity header field "ppt" parameter
value. Other using protocols of PASSporT may define behvaior
specific to their use of the "div" claim.

4.1. Authentication Service Behavior

An authentication service only adds an Identity header field
containing the "div" PASSporT type to an SIP request that already
contains at least one Identity header field; it MUST NOT add a "div"
request to an INVITE that contains no other Identity headers fields.
Note that the authentication service doing so does not remove or
replace any existing Identity header fields, it simply adds a new
one. When adding an Identity header field with a PASSporT object
containing a "div" claim, SIP authentication services MUST also add a
"ppt" parameter to that Identity header with a value of "div". The
resulting compact form Identity header field to add to the message
might look as follows:

```
Identity: ..sv5CTo05KqpSmtHt3dcEiO/1CWTSZtnG3iV+1nmurLXV/HmtyNS7Ltrg9dlxkWzo
    eU7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI3d7SyN21yNDo2ER/Ovgtw0Lu5csIp
    pPqOg1uXndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs=; \
    info=<https://biloxi.example.org/biloxi.cer>;alg=ES256;ppt="div"
```

A SIP authentication service typically will derive the new value of
"dest" from a new Request-URI that is set for the SIP request before
it is forwarded. Older values of the Request-URI may appear in
header fields like Diversion or History-Info; this document specifies
no specific interaction between the "div" mechanism and those SIP
header fields. Note as well that because PASSporT operates on
canonicalized telephone numbers and normalized URIs, many smaller
changes to the syntax of identifiers that might be captured by other
mechanisms (like History-Info) that record regargeting will likely
not require a "div" PASSporT.

4.2. Verification Service Behavior

[I-D.ietf-stir-rfc4474bis] Section 6.2 Step 5 requires that
specifications defining "ppt" values describe any additional verifier
behavior. The behavior specified for the "div" value of "ppt" is as
follows.

In order to use the "div" extension, a verificiation service needs to
inspect all of the valid Identity header field values associated with
a request, as an Identity header field value containing "div"
necessary refers to an earlier PASSporT already in the message. In
particular, the verification service must find a PASSporT associated
with the call, one created earlier, that contains a "dest" claim with
a value equivalent to the "div" claim in the current PASSporT. It is
possible that this earlier PASSporT will also contain a "div", and
that it will in turn chain to a still earlier PASSporT stored in a
different Identity header field value. Ultimately, by looking at
this chain of transformations and validating the associated
signatures, the verification service will be able to ascertain that
the appropriate parties were responsible for the retargeting of the
call to its ultimate destination; this can help the verification
service to determine that original PASSporT in the call was not
simply used in a cut-and-paste attack. This will help relying
parties to make any associated authorization decisions in terms of
how the call will be treated - though, per [I-D.ietf-stir-rfc4474bis]
Section 6.2.1, that decision is a matter of local policy.

Note that Identity header fields are not ordered in a SIP request,
and in a case where there is a multiplicity of Identity header fields
in a request, some sorting may be required to match divert PASSporTs
to their originals.

5. Using 'div' in STIR out-of-band

When storing a PASSporT with "div" at a Call Placement Service (CPS)
for STIR out-of-band [I-D.ietf-stir-rfc4474bis] scenarios, clients
should include an "opt" element within "div". "opt" contains the full
form of the original PASSporT from which the "div" was generated. If
the diverting entity originally received that PASSporT encrypted, it
MUST decrypt it before storing it in "opt." The entire "div"
PASSporT would than be signed and re-encrypted normally for storage
at an out-of-band Call Placement Service (CPS).

A "div" PASSporT containing the "opt" would look as follows:

       { "orig":{"tn":"12155551212"},
         "dest":{"tn":"12155551214"},
         "iat":1443208345,
         "div":{"tn":"121555551213",
         "opt":"eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1I \
         joiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ
         kZXN0Ijp7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImlhdC \
         I6IjE0NDMyMDgzNDUiLCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifX0.r \
         q3pjT1hoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-cpFYpFYs \
         ojNCpTzO3QfPOlckGaS6hEck7w"} }

   The "opt" extension is not required for any unencrypted in-band
   PASSporT conveyance. For forward compatibility reasons, its use is
   not forbidden in those environments.

6. Extending 'div'

   Past experience has shown that there may be additional information
   about the motivation for retargeting that relying parties might
   consider when making authorization decisions about a call, see for
   example the "reason" associated with the SIP Diversion header field
   [RFC5806]. Future extensions to this specification might incorporate
   reasons into "div".

7. Acknowledgments

   We would like to thank Robert Sparks for contributions to this
   document.

8. IANA Considerations

   This specification requests that the IANA add a new claim to the JSON
   Web Token Claims registry as defined in [RFC7519].

   Claim Name: "div"

   Claim Description: New Target of a Call

   Change Controller: IESG

   Specification Document(s): [RFCThis]

9. Security Considerations

   This specification describes a security feature, and is primarily
   concerned with increasing security when calls are forwarded.
   Including information about how calls were retargeted during the
   routing process can allow downstream entities to infer particulars of

the policies used to route calls through the network. However,
including this information about forwarding is at the discretion of
the retargeting entity, so if there is a requirement to keep the
original called number confidential, no PASSporT should be created
for that retargeting - the only consequence will be that downstream
entities will be unable to correlate an incoming call with the
original PASSporT without access to some prior knowledge of the
policies that could have caused the retargeting.

10. Informative References

[I-D.ietf-stir-certificates]
          Peterson, J. and S. Turner, "Secure Telephone Identity
          Credentials: Certificates", draft-ietf-stir-
          certificates-14 (work in progress), May 2017.

[I-D.ietf-stir-oob]
          Rescorla, E. and J. Peterson, "STIR Out of Band
          Architecture and Use Cases", draft-ietf-stir-oob-00 (work
          in progress), July 2017.

[I-D.ietf-stir-passport]
          Wendt, C. and J. Peterson, "Personal Assertion Token
          (PASSporT)", draft-ietf-stir-passport-11 (work in
          progress), February 2017.

[I-D.ietf-stir-rfc4474bis]
          Peterson, J., Jennings, C., Rescorla, E., and C. Wendt,
          "Authenticated Identity Management in the Session
          Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-16
          (work in progress), February 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", BCP 14, RFC 2119,
          DOI 10.17487/RFC2119, March 1997,
          <https://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,
          <https://www.rfc-editor.org/info/rfc3261>.

[RFC5806] Levy, S. and M. Mohali, Ed., "Diversion Indication in
          SIP", RFC 5806, DOI 10.17487/RFC5806, March 2010,
          <https://www.rfc-editor.org/info/rfc5806>.

   [RFC7044] Barnes, M., Audet, F., Schubert, S., van Elburg, J., and
              C. Holmberg, "An Extension to the Session Initiation
              Protocol (SIP) for Request History Information", RFC 7044,
              DOI 10.17487/RFC7044, February 2014,
              <https://www.rfc-editor.org/info/rfc7044>.

   [RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure
              Telephone Identity Problem Statement and Requirements",
              RFC 7340, DOI 10.17487/RFC7340, September 2014,
              <https://www.rfc-editor.org/info/rfc7340>.

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

Author's Address

   Jon Peterson
   Neustar, Inc.
   1800 Sutter St Suite 570
   Concord, CA 94520
   US

   Email: jon.peterson@neustar.biz