PASSporT Extensions

IETF 99 (Prague) STIR WG

July 2017

draft-ietf-stir-passport-divert-00

- A feature many people have asked about
  - How do we handle **retargeting**?
  - To header field of SIP is signed by PASSporT
    - Original value may be lost with retargeting
- We define a special Identity header track it
  - With its own “ppt” – “**div**” for “divert”
- Different from History-Info and Diversion?
  - Yes, as it is signed by the original destination domain
  - Moreover, it only captures “major” changes
    - Thanks to our canonicalization procedures
- Useful for things like **SIPBRANDY** where integrity protection for retargeting matters

Inverting the signer

- *A diverting auth service takes an existing PASSporT, moves the "dest" to "div," and populates "dest" with the new target*
- An Identity header with "div" always points to some prior Identity header
  - Though that header may in turn contain a div…
  - Chains back to an original assertion
- Instead of signing for the "orig" value, the auth service for "div" signs the "dest"
  - So relying parties get a direct cryptographic attestation that the original destination domain authorized the new target

Original vs. Divert Passport

Header:

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

Original PASSporT

Claims:

```
{ ”orig":{“uri”:”alice@example.com”},
  ”dest":{“uri”:”firsttarget@example.com”}, <- original target
    "iat": 1443208345 }
```

Header:

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

Added when retargeting

Claims:

```
{ ”orig":{“uri”:”alice@example.com”},
  ”dest":{“uri”:”secondtarget@example.com”},  <- new target
  "iat": 1443208345,
  “div”:{“uri”:”firsttarget@example.com”} }  <- original target
```

Issues

- It’s pretty straightforward, this seems relatively baked
- Do we need a reason?
  - That is, a cause for the retargeting to be recorded
  - Any actual security value for the threat model?
- Has some interesting interactions with out of band
  - Turns out we probably really need it for that

draft-ietf-stir-passport-rcd-00 (formerly cnam)

- Adds a “rcd” array to PASSporT
  - Baseline include a “nam” key-value pair containing a display-name
- But the “rcd” element is richer than just Caller-ID
  - Scope: anything rendered to the called user to help them decide to pick up the phone or not - extensible
  - Could include information about organizations
    - Government, bank, etc.
    - Maybe some fields in Henning’s Caller-Info parameters
  - Location, potentially
    - Likely by reference rather than by value
  - Other rich data associated with the originating persona
    - Social network data, crowdsourced reputation, and so on
    - Creates an IANA registry allowing allocation of more related elements

First and Third

- Operates in two modes
- Without "**ppt**"
  - This signifies that an originating authentication service provides the caller name
    - Same entity that signs for the originating number
- With "**ppt**"
  - This signifies that a third party provides the assertion
    - *Different* entity than signs for the originating number
      - Signature can come from someone that doesn't own the TN
      - Instead the "iss" field identifies who generated it
    - Different Identity header field as well

“rcd” without “ppt”

Header:

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

Claims:

```
{ ”orig":{“tn”:"12155551212”},
  ”dest":{“tn”:"12155551213”},
      "iat": 1443208345,
  “rcd”:{“nam:”Alice Atlanta”} }
```

“rcd” with “ppt”

Header:

```
{ "typ":”passport",
  "alg":”ES256“,
  "ppt":”rcd“,
  "x5u":"https://www.example.org/cert.pkx" }
```

Third Party Signer

Claims:

```
{ ”orig":{“tn”:"12155551212”},
  ”dest":{“tn”:"12155551213”},
     "iat": 1443208345,
  “rcd”:{“nam:”Alice Atlanta”} }
```

Issues: LoA

- How do you know who's behind a phone number?
  - Carriers know their direct customers, but not reseller's customers
  - Should a given extension at an enterprise display the name of the organization or the individual or both?
  - Individuals populate names in their address books, claim them in SIP From headers
- Do we need a way to express confidence in names and RCD?
- There is something similar in SHAKEN
  - "Attest" levels of A, B, C - could adapt to RCD

Other Issues

- Richer information can be more personal
  - Privacy issues with carrying a “rcd” payload
  - Confidentiality required for these PASSporTs?
    - We have a story for this developing in OOB
- What is the interface for third-person “rcd”?
  - Out of band?
  - There are some interactions with OOB here…
- Need to make sure information propagates down to end user devices…