STIR Signaling

IETF 88 (Vancouver)
November 6, 2013
Cullen Jennings
First principles

Separate the work into two buckets:

1) Signaling
   What fields are signed, signer/verifier behavior, canonicalization

2) Credentials
   How signers enroll, how verifiers acquire credentials, how to determine a credential’s authority for identity

• These are separable and modular pieces of work
  More consensus today on (1) than on (2) ?
  Could be separate drafts
  Could have only one approach to (2), or maybe more
The rest of this talk is just about (1), the signaling itself
Signature Fields

Signature over a concatenation of To, From and Date

• From
  Signer and verifier must be able to recognize a TN
  If TN, sign only the canonicalized TN (more later)

• Date (straightforward, replay protection)

• To
  Sign TN only if there’s a TN?
    Does a TN in the To also need a canonicalization pass? Probably
  Calls may be retargeted/forwarded in transit
  How can a verifier know that a call is destined for them?
    Mostly useful for replay protection
Additional Protection (1)

• ... and one proposal added an optional field to the end

• RFC4474bis defines a **Identity-Reliance** header
  
  If present, the signature in Identity-Reliance is signed over with the From, To and Date

• Signer can opt to include it or not

• Verifier always checks the From/To/Date/I-R signature, but doesn’t have to check the signature in Identity-Reliance itself
  
  However, no one can fool the verifier into thinking the signer did not provide I-R if main signature survives
Additional Protection (2)

- The motivation here is provide a way to link the identity protection to **integrity protection** over other parts of the message.
  - Won’t be useful in all environments, but might be in some.
- Most of what we want to protect is in the body.
  - Protecting keying material fingerprints
    - This is our best story for how to actually secure SIP media
    - MESSAGE-like cases where body is content
- Ultimately, all we need to decide now is whether to allow this point of **extensibility**
  - With the opt-in properties on the last slide
  - Identity-Reliance is just an example
Canonicalization (1)

• Proposal: **Identity is in the From**, always
  Some discussion about alternate headers (PAI)
    More to talk about there?
  Some services have a reply-to semantic
  But, the From header field value is what UAs render

• Intermediaries may tweak numbers in transit
  No bounds on intermediary behavior
  Some behaviors might make canonicalization impossible
    In that case, it just doesn’t work
    If this takes off, hopefully policies will make this easy

• Both the signer and verifier must canonicalize
  Must arrive at the same result, or the verifier will fail it
Canonicalization (2)

• So how do we do it?
  Strip special characters, append a country code if missing (crib from ENUM procedures?)
  End up with a format like:
    +17004561000 (should we include the +)
What if country code can’t be inferred (at either side)?
  Two possible options:
    Guess that it’s from this nation and append a cc, if the call is international, it fails
    Leave it without a country code and don’t include a +?
What about special numbers?
  Especially if we’re canonicalizing To as well
  Short codes, emergency codes, many corner cases
Just TNs, or other URIs?

- Signers and verifiers must be able to recognize a TN in the From
  Potentially non-trivial, we can’t depend on user=phone or a +
  
sip:67463@shortcode.com
  So, STIR implementations will necessarily be aware of non-TN URIs

- The proposals so far favor doing both
  For the **signaling module**, what would we do differently, really?

- How much new work is there for non-TNs?
  RFC4474 has a good story about this
  Once you fix the signature fields, as above
  DANE support is the only new wrinkle
  But the dns: URI could go in Identity-Info…
Replacing RFC4474

• Use Identity as the name of the header (or not)?
• We do want people to use the results of STIR rather than RFC4474
  But, we want to keep all the response codes and related apparatus
    428 “Use Identity” – verifier requires signed Identity
    436 “Bad Identity” – verifier couldn’t verify it

• Punt on Identity-Info as part of the credential piece