rfc4474bis-05

STIR Interim

October 9 2015

Jon

What we did since -04

- General clean-up
- Removed Identity-Reliance, for Identity-Extension
  - Identity-Extension now can appear multiple times in a message
- Bolstered the Security Considerations
  - With special reference to RFC7375
- Instructions were to prepare for Last Call
- But I’m really going to talk about first principles today instead

The Revised Sec Considerations

- Explains why we sign what we sign
  - TN or “identity field” in From/PAI
  - Date header field value
  - To header field’s TN or “identity field”
  - SIP Method (INVITE, MESSAGE, etc)
    - Optionally, any media security parameters in SDP
    - Optionally, any Identity-Extension headers
- What we use to sign (the credential) is a separate question
  - Outside the scope of RFC4474bis

Signing From or PAI

- Sometimes, the TN/identity field lives in PAI (RFC3325)
  - So that should be signed instead of the From
    - From may not include anything useful in those cases
- Existing text:
  - Allows the canonical format to draw from the PAI
  - In PAI-using networks, verifiers should be able to reconstruct the canon
- I’ve heard this is insufficient
  - My reasoning: in Spec(T) environments today where you send PAI, recipients know that you’re supposed to use PAI
    - There’s no indicator to say “use PAI instead of From” today
  - If there’s something broken here, PAI has been broken for 15 years
- Privacy leak?
  - Only when “canon” is used
  - How bad? Fixes? (put “canon” in the PAI header instead?)

Signing Date and To

- Detects cut-and-paste attacks
- If we only signed the identity field in the From, then an attacker could cut-and-paste into a new SIP request
- **Date** creates a window of validity for the identity assertion
  - If it is replayed after that window, it will be detected
  - If replayed within the window, detectable by keeping state
- **To** prevents replay within the window to a new target
  - Eve receives a call from Alice, immediately places a new call to Bob cut-and-pasting Alice's identity assertion
  - Including the **To** value lets Bob detect this call was for Alice
    - However, due to potential retargeting, this is not unambiguous

Signing the Method

- The SIP Method protects against other cut-and-paste attacks
  - Eve captures an INVITE, and replays its identity assertion in a MESSAGE, say
  - Eve captures an INVITE, and replays its identity assertion in a re-INVITE with new SDP sending media elsewhere
- Value of this is somewhat peripheral to robocalling
  - Perhaps more meaningful for voicemail hacking or vishing
  - If we’re desperate to reduce complexity, this could go
    - Not that this introduces a ton of complexity
- It does however does make the signature SIP-specific
  - More on that in a moment..

Optionally protecting media keys

- Came in the wake of PERPASS (BCP 188)
  - We took a hum, there was a good consensus to do it
- There are impersonation attacks where this matters
  - Ultimately, some baiting attacks can still cut-and-paste and potentially cause confusion
  - With media security, the attacker will be able to ring your phone, but not to convincingly impersonate any media
- And if you don’t care about media security?
  - If your environment doesn’t use SRTP, this costs you one thoughtless byte: “|”
  - From a complexity standpoint, this adds virtually nothing

Optionally signing anything else

- Motivated by CNIT and extensibility in general
- Defined a new Identity-Extension header
  - If present, contains a signature over fields in the SIP request
    - Which fields? Determined by the extension
    - Extensions identified with an IANA namespace
  - For CNIT, could be display-name, or anything else
- Identity-Reliance collapsed into this to reduce complexity in the signature

Should this be SIP specific?

- This was a charter decision we made in 2013
  - Do a SIP-specific version first, only then think about “out-of-band” or “gateway” indications
- Could we collapse these into one identity assertion?
  - Sure, we could have all along
- Remove SIP specific elements (Method)
  - Need to manage Identity-Info and extensions in some way
- Even if we make the identity assertion generic (not SIP-specific)
  - We still need to specify how to handle it in SIP
    - What status code do you send when the sig is broken?
      - Or when you don’t know the signing cert?
      - Or when you require a sig and there isn’t one?
    - We have to meet a minimum interoperability bar
      - Still needs to be a SIP-specific specification somewhere in the mix

Header or Body?

- We chose a header, back in RFC4474
  - Architecturally, wanted intermediaries to be able to add it without being B2BUAs
  - Though yes, many intermediaries are already B2BUAs
- Header worries me less now than it did then
  - There are some big headers out there in the wild
- Ultimately there should be one place to stick it in SIP
  - A specification should define this for the sake of interoperability
  - If it isn’t SIP-specific, we should obligate using protocols to provide similar specifications

That’s it

- We need to decide where we go from here