Credentials Roadmap

STIR WG

IETF 90 (Toronto)

Sean Turner (turners@ieca.com)

The Path Forward

- Signaling protocol is coming along
  - But for credentials, we have big choices
- Two concrete proposals to date:
  - draft-kaplan-stir-cider
  - draft-peterson-stir-certificates
  - Both -00s. Read either? (show of hands)
- Are going to choose between them?
  - Possible to proceed with both
  - Signing mechanism designed to be agnostic
    - However, that would require compatible keying

draft-peterson-stir-certificates-00

- Attempt to provide a certificate-based STIR credential system
  - Still a lot to fill in, but this is the high-level idea
- Defines attributes for telephones numbers and number ranges
- Defines ways of acquiring the certs
  - Largely follows the Identity-Info paradigm
- Sketches techniques for real-time cert validation

draft-kaplan-stir-cider-00

- (trying to characterize this fairly, not mine)
- DNS based approach
  - Creates an ENUM-like tree
  - Designed for ease of discovery, lightweight retrieval
  - Also reuses existing ENUM stacks
    - Some modifications required
- Keys for each number
  - Potentially multiple keys per number

How to choose?

- There is basis for comparison
  - Key uniqueness (multiple keys per TN?)
  - Enrollment mechanisms (“golden root”?)
  - Credential acquisition (which protocol(s)?)
  - Rollover, expiry (easier with one or the other?)
  - Public or private credentials (requirement?)
  - Delegation (including partial delegation)
- Other important considerations?
- Do these give us enough to make a decision?

Choices or Hums

- Do we have consensus to do one, or both?
  - Or do we need another choice?
    - Possible to skin either of these cats differently
- If not, what's our path to get there?

- (detailed issues follow, time permitting)

DETAILED ISSUES

Which credentials do verifiers need?

- Can we uniquely identify the needed credential based on TN alone?
  - Depends on how many authorities there are
- How many authorities and delegates per number?
  - Some kind of hint needed to disambiguate
    - Identity-Info
    - CIDER “public key index value”

Enrollment

- Document assumes a threefold method
  - Direct assignment
    - From numbering authorities, regulators, etc.
  - Delegation from above
    - From other number holders
  - Proof of possession
    - Last time here, we had “no opposition” to going forward with that
- Is there a “golden root”

Verifier Credential Acquisition

- Different methods of acquiring certs
  - Push (e.g., credential arrives with a SIP request)
    - MIME multipart body
  - Pull (e.g., verifier acquires credential on receipt of request)
    - Either dereferencing Identity-Info URI
    - DNS: or creating a fetch based on the originating number
      - For certs, current recommendation is to use EST (RFC7030)
  - Prefetch (verifier gets top 500 keys) with pull
    - SIP SUBSCRIBE/NOTIFY mentioned in the text
  - Others? Probably – no need to choose one (but MTI?)
    - DANE? If you there's a DNS tree…

Expiry, Revocation and Rollover

- All credentials will have a lifetime
  - Ordinary rollover
    - Sometimes keys will be compromised before their expiry
  - But telephone numbers change owners, get ported, transfer normally
- Some sort of real-time checking required
  - DNS gets this for free (presuming no caching)
  - For certs, pull method could encompass this check
    - As could the prefetch
  - OCSP checks, but adds some overhead
    - More investigation to be done here

Open Issue: Handling Ranges

- But some entities will have authority over multiple numbers
  - Administrative domains could control millions of numbers
    - In non-continuous ranges
  - Includes service providers, enterprises, resellers, etc.
- Ideally, a service provider should not have to have one credential per number
  - The draft contains new syntax for number ranges

Open Issue: Partial Delegation

- Authority over numbers conflates many powers
- Should it be possible to delegate authority over services?
  - e.g., my SMS provider can sign my texts (MESSAGE), but my voice provider signs my INVITEs
    - Yes, example is kind of contrived
    - Can I give my SMS provider a text-specific cert that would not enable to them to sign voice calls?
- Too complex? Do we need this?

Open Issue: Private Key Provisioning

- How do signers acquire and manage private keys?
  - Self-generated and provisioned at the authority?
  - Generated by the authority and downloaded to devices?
- Intermediaries and enterprises
  - Provision keys for number blocks, sign on behalf of calls/texts passing by
  - May possess many keys
- What's the right tool to accomplish this?

Open Issue: Public or Confidential Credentials?

- How much information are we willing to make public?
  - Should credentials advertise a subject (e.g., "AT&T")
    - Okay when a call is received to know the originating carrier?
      - Receiving user vs. receiving carrier may be different
    - More seriously, can an attacker mine a public database to reveal who owns *all* numbers?
  - Will we introduce VIPR-like privacy leaks?
- Can we restrict access to the credentials?
  - Identity-Info, say, could have short lived, unguessable URLs
  - How important is endpoint verification?
    - Does trust become transitive if endpoints rely on intermediary verifiers?