SHAKEN Framework for Proof of Possession of Telephone Numbers

Chris Wendt/David Hancock
TN-PoP Overview

• It is very common practice for enterprises and telephone providers/services and other trunking and wholesale consumers to want to originate a call onto the telephone network that is not owned by the service provider that is chosen.

• Reasons for this can be many:
  • Least Cost Routing
  • Redundant provider for failover
  • Intentional spoofing for application reasons:
    • Call centers
    • Calling services
    • Robocalling
    • 3rd Party Call Control
TN-PoP Problem Statement

• We want an efficient, secure, reliable mechanism that a customer of both the provider that owns the telephone number as well as the provider that ultimately originates the call can securely pass the prove of possession of that Telephone number from provider to provider without

  • complicated or time consuming mechanisms of querying databases

  • needing to pre-arrange/provision the potentially complicated relationships between TN providers and origination service providers
TN-PoP Solution

- Use a framework very similar to STIR/SHAKEN but extend it to wholesale and trunking customers.
- Protocols and mechanisms are very similar, however security relationship is from customer to provider rather than provider to provider.
TN-PoP Basic Flow

- **STI-PA**
  - Policy Administrator
  - SPC Token

- **Telephone Number Provider Admin API**
  - PoP Token

- **Telephone Number Provider ACME Proxy**
  - Certificate with TN
  - CSR with SPC Token

- **STI-CA**
  - Certification Authority
  - Certificate with TN
  - ACME

- **Customer PBX**
  - INVITE w/ PoP Identity header

- **Originating SP**
  - INVITE w/ shaken Identity header
  - Validate PoP Identity Header with Certificate
  - STI-CR
  - Certificate
  - STI-AS

- **Terminating SP**
  - Validate Shaken Identity Header
  - STI-VS
  - Replace PoP Identity header with Shaken Identity header
TN-PoP Discussion

- Customers get credentials they put in their PBX that support getting periodic PoP tokens to be used for SP ACME proxy service.
- Using ACME client and the PoP token, the PBX requests certificate that proves they own TN.
- TN-PoP ACME proxy service puts TN public key certificate in STI-CR.
- PBX gets certificate that is used for signing TN-POP identity header for INVITE sent to originating service provider.
- Originating service provider validates TN-POP identity header, if validation is successful, strips TN-POP identity header and sends INVITE to STI-AS with proper origID and full attestation.
- Call continues as with SHAKEN framework.
TN-PoP Discussion

• Porting:

  • Two options:
    • provider uses very short lived certificates (minutes/hours)
    • Perhaps (but not great for reason below) provider ported from
      removes availability of cert for TN from STI-CR

  • Proposal: We need to be comfortable with short term certs, otherwise
    any other revoking mechanism will cost industry in need to scale CAs
    (OSCP, etc) and transaction time