SIPNOC 2019
AT&T SHAKEN Deployment Case Study

Andy Jurczak
Principal Member of Technical Staff

12/03/2019
Agenda

• Current status of AT&T’s SHAKEN Deployment
• Implementation Insights
• Display: Trust & Intent
Current Status
AT&T STIR/SHAKEN Deployment Overview

• STIR/SHAKEN is operational in AT&T’s production network
  ➢ Currently deployed on AT&T’s VoLTE and Consumer VoIP (AT&T Phone) services
  ➢ Authenticating/verifying 100% of intra-AT&T traffic for above services
  ➢ Have begun the exchange of signed traffic with Comcast and T-Mobile
  ➢ Ongoing testing and rollout with additional service providers
  ➢ Tested with ATIS/Neustar Robocalling Testbed

• Manual exchange of self-signed root certificates
  ➢ Will be interfacing with STI-PA/CA for certificates

• Support SHAKEN Error Responses

• In house development of STI-AS, STI-VS, TN-CR, SKS
  ➢ 100% virtualized
Implementation Insights
• In reference model, signing is performed for all originating calls
• In practice, per call authentication is required, but per call signing is not
• Signing of intra-network calls result in unnecessary costs in terms of processing and call setup delay
AT&T only signs calls sent to other SHAKEN-enabled service providers

- Perform signing at the egress IBCF/SBC
- Dramatic decrease in signing resources
- Makes use of ATIS-1000082 API (to be discussed later)
Signing upon Egress for Inter-Network Calls: Issues

• Signing upon egress poses two issues:
  • Authentication is best performed upon origination
  • May not have origination information at egress (to be used in origid)
• If only signing inter-carrier calls, how are intra-carrier calls verified?
• Solution: “Tagging”
Tagging adds information to SIP Signaling used to sign and/or verify calls
Tagging performed upon origination, e.g. app server
Tagging:
  - Inserts Attestation level based on Authentication results
  - Inserts Origid based on origination source
  - Inserts verstat
    - Verstat=TN-Validation-Passed (if successfully authenticated)
    - Verstat=No-TN-Validation (if unable to authenticate)
SIP Headers used for Tagging are defined in 3GPP 24.229
  - Attestation-Info
  - Origination-Id
Tagging: Inter-carrier Call

- Tagging provides “attest” and “origid” claim data to be used when call is signed
- Origination-Ids can be unique, per SHAKEN standards and recommendations

INVITE after tagging:

```
INVITE sip:+17325551212@carrier.net;user=phone SIP/2.0
...
...  
Attestation-Info: A
Origination-Id: 2FB71193-D137-4DA1-9B34-E35CEA35498F
...```
Tagging provides “verstat”, used for intra-carrier calls in lieu of signing

Verstat is removed by egress IBCF/SBC if call is routed to another carrier

INVITE after tagging:

```
INVITE sip:+17325551212@carrier.net;user=phone SIP/2.0
...
... 
Attestation-Info: A
Origination-Id: 2FB71193-D137-4DA1-9B34-E35CEA35498F
P-Asserted-Identity: <tel:+17325550123;verstat=TN-Validation-Passed>
...
```
SHAKEN API for Signing and Verification

- Defined in ATIS-1000082 “Technical Report on SHAKEN APIs for a Centralized Signing and Signature Validation Server”
- Decomposes the STI-AS/VS functions
  - Particularly beneficial for call originations
- Supports centralized Signing/Verification resources along with distributed Authenticator/Verifier
- Authenticator can also be decomposed
  - Use Tagging to convey attestation and origid

- “Authenticator” determines the Attestation level and origid to be used for the call
- “Verifier” can perform syntax checking, canonicalization, etc. to screen pre-verification errors.
POST /stir/v1/signing HTTP/1.1
Host: stir.example.com
Accept: application/json
X-InstanceID: de305d54-75b4-431b-adb2-eb6b9e546014
X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
Content-Type: application/json
Content-Length: ...
{
   "signingRequest": {
      "attest": "A",
      "orig": {
         "tn": "12155551212"
      },
      "dest": {
         "tn": "12355551212"
      },
      "iat": "1443208345",
      "origid": "de305d54-75b4-431b-adb2-eb6b9e546014"
   }
}

HTTP/1.1 200 OK
X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
Content-Type: application/json
Content-Length: ...
{
   "signingResponse": {
      "identity": "eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbIsInR5cCI6IiIsInR5cCI6IiIi
      "orig": "eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbIsInR5cCI6IiIsInR5cCI6IiIi
   }
}
SHAKEN API for Verification

POST /stir/v1/verification HTTP/1.1
Host: stir.example.com
Accept: application/json
X-InstanceID: de305d54-75b4-431b-adb2-eb6b9e546014
X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
Content-Type: application/json
Content-Length: ...

{
    "verificationRequest": {
        "from": {
            "tn": "12155551212"
        },
        "to": {
            "tn": ["12355551212"]
        },
        "time": "1443208345",
        "identity": "eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUyLm5ldC9leGFtcGxlLmNlciJ9.eyJhdHRlc3QiOiJQOiJlbGwiZGVzdCJ9.eyJhdHRlc3QiOiJ1bmlrIl19",
    }
}

HTTP/1.1 200 OK
X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
Content-Type: application/json
Content-Length: ...

{
    "verificationResponse": {
        "verstat": "TN-Validation-Passed"
    }
}
Display: Trust & Intent
Trust – Reputation - Intent

**Trust** – Do we believe the calling number is correct?

**Reputation**

Every phone number has a Story...

- **Status** – Is it connected? Valid?
- **Ownership** – Who pays the bill?
- **Behavior** – What does the number do?
- **Connections** – How does it communicate?
- **Complaints** – What others say about this number?

**Reputation** is the aggregated view of this Story. Analytics Engines use past reputation to predict **intent**.

**Trust** combined with **intent** allow more accurate decisions whether call is to be blocked, flagged or allowed.
When to display a Positive Indicator: Trust & Intent

- **Today**: 0
- **SHAKEN Only**: 0
- **SHAKEN + Analytics**: ✔ Trust Identity of Number, ✔ Predict Intent of Caller
Display: Analytics Only

CVT Analytics (screens on intent)

CVT (Analytics)

Unscreened CPN

Neutral – display CPN

Likely SPAM/Robocalling

Customer Presentation
Display: SHAKEN + Analytics

SHAKEN CPN Validation
(detects non-spoofed CPNs)

Network (SHAKEN) Disposition

- TN-Validation-Passed; Attest=A

- SHAKEN not provided (baseline case)
  - TN-Validation-Passed; Attest=B/C
  - No-TN-Validation
  - TN-Validation-Failed

CVT Analytics
(screen on intent)

Customer Presentation

Valid CPN; not SPAM

Neutral

Likely SPAM/Robocalling
SHAKEN Display

Veriﬁed Calling Number

Unveriﬁed Calling Number

TRUST + INTENT
Positive Indicator displayed when Calling Number Verified And AT&T Call Protect Analytics determines no Fraud / Spam

Verified Calling Number

Verified Number: Full Attestation

Unveriﬁed Number: Partial/GW Attestation or no signature

Terminating Service Provider (AT&T)

Call Protect Analytics

Positive Indication

No Veriﬁcation Indication

Fraud/SPAM Indication