SHAKEN AND Stirred

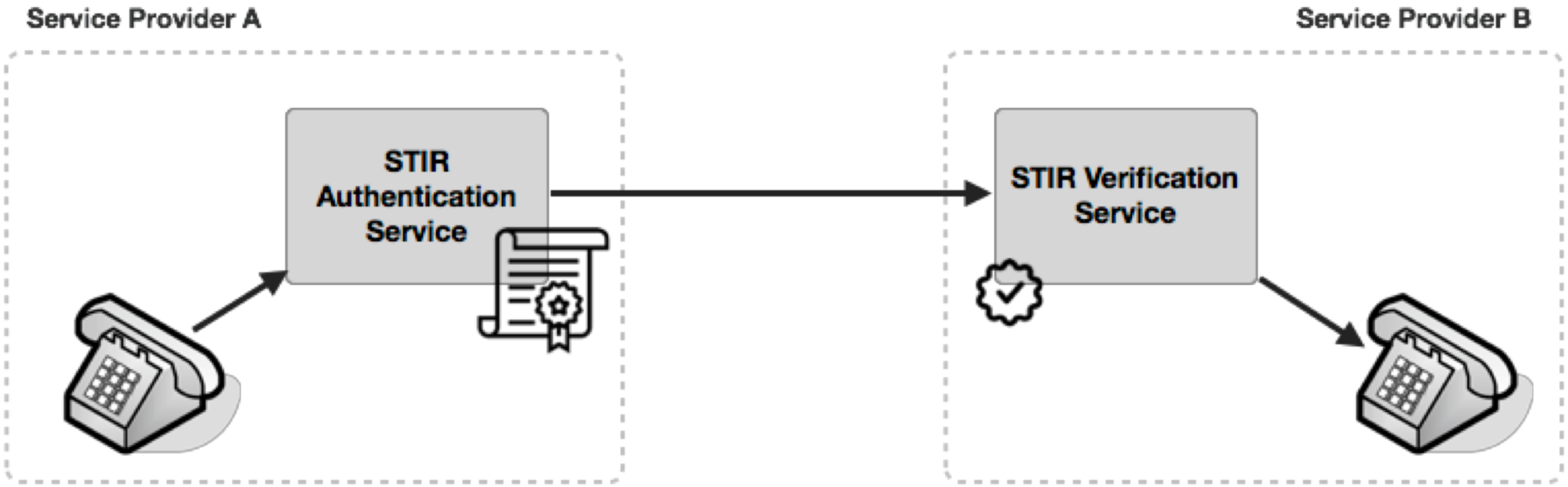
Advanced Mixology

Chris Wendt - Director, IP Communication Services

COMCAST

SHAKEN/STIR Goals

- Set of tools for core authentication/verification of calling identity (telephone number)



- The core specifications define
  - the base protocols
  - PKI - certificate management

SHAKEN/STIR Goals

- **Primary Goal** (near term):
    - Make sure we have a set of tools/levers/knobs to provide end-to-end security for the many scenarios and use-cases that can/could/will occur in the telephone network
    - Deploying these tools across the entire telephone network is not an easy task, so doing as much as we can upfront to have a comprehensive set of tools is critical
    - Provide “full attestation” and end-to-end call authentication to as many calls as possible
- **Secondary Goal** (longer term):
    - Use validation of identity as a value-add to the telephone network
    - Provide consumers and enterprises a better more informative, more customizable experience they can trust and make better, more efficient communications choices

Adding tools to the toolbox

- Beyond the core A to B subscriber call scenarios
  - **Diversion/Call retargeting** - Call Forwarding, etc.
  - **Enterprise/Call Center/“legitimate” robocalling services**
  - **Calling Name integrity** - info beyond telephone number
- Expand the core definitions and capabilities so that Authentication and Verification service implementations can support protocols for proper verification as routing and SIP application network equipment (TAS/PBX/SBC) support is enhanced to handle more advanced call scenarios

Diversion/Call Retargeting Overview

- Diversion, or call forwarding types of scenarios, are both important call features as well as potential ways of getting around STIR/SHAKEN if not handled properly
- Calls are initiated by SP-A, initially terminated at SP-B/PBX-B, then forwarded to SP-C/PBX-C.
- Core SHAKEN covers signing call from A to B, but not B to C.
- draft-ietf-stir-passport-divert defines the protocol solution, we are finalizing the SHAKEN profile of divert as we speak.
- This provides the proper standard framework for protecting against using the many forms of retargeting as an attack vector
- May require evolution in the industry to follow this framework to ensure validated calls
- 8XX calls are a special case of this with geographic routing number retargeting

Diversion/Call Retargeting Overview

- divert is a PASSporT extension that adds a new claim to the PASSporT object ‘div’
- The first leg of the call will follow base SHAKEN procedures and add a ‘shaken’ PASSporT
- Any additional legs of the call will add a new additional identity header with a ‘div’ PASSporT
- The ‘div’ claim represents the previous leg destination of the call and therefore provides a signed link between identity headers, so the full call path can be validated.

```
{
  "orig":{"tn":"12155551212"},
  “dest”:[{"tn":"12155551214"}],
  "iat":1443208345,
  “div”:{"tn":"121555551213"}
}
```

Enterprise/Call Center/“legitimate” robocalling services

- 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(s) chosen to originate call, likely on a call-by-call basis.
- Reasons for this can be many:
  - Redundant provider for failover
  - Intentional spoofing for application reasons:
    - Call centers
    - Calling services
    - Robocalling
    - 3rd Party Call Control

Problem Statement

- We want an efficient, secure, cost-effective 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 provisioning and querying centralized or cross provider databases
  - needing to pre-arrange/provision the potentially complicated relationships between TN providers and origination service providers
  - needing to expose more information than necessary between providers and customer

TN-PoP Solution

- STIR/SHAKEN is about validation of information passed from originating provider to the terminating provider
- Use the same fundamental technologies and same PKI of STIR/SHAKEN to authenticate the customer/number provider to the trunk provider
- Fully automated system that uses same mechanisms including ACME to provide “TN-POP” certificates from the number provider validated by Authority that the trunk customer can provide to the trunk provider and the telephone number/block can be validated.

Validation of trunk customer caller-id

Validation of trunk customer caller-id

Validation of trunk customer caller-id

Validation of trunk customer caller-id

Validation of trunk customer caller-id

COMCAST

TN-PoP Solution Status

- Solution specification pretty mature in SHAKEN
- Now that divert is almost out-the-door, TN-POP is next priority to complete
- Looking for more folks to provide input because this is a problem that impacts not just service providers but enterprise/call-center and other industry players.

Calling Name/Metadata Integrity

- Two Cases to support:
  - POCN - “Plain old Calling Name” ™
  - Rich Call Data - JCard, Logos, etc.
- draft-ietf-stir-passport-rcd-01
  - Proposes a new simple way to incorporate ‘rcd’ into PASSporT extensions
- This SHAKEN specific variant does assume a service provider specific case where the calling name is signed at the point of origination STI-AS. For 3rd party CNAM or terminating CNAM dips the default ‘rcd’ extension would apply.

POCN

- For POCN scenarios, the validation/verification of the calling name will utilize the ‘rcd’ claim with the ‘nam’ object set to however the calling name is represented in the INVITE. No plan to add any SIP mechanisms or standardize on one.
- Simply, using existing mechanisms for delivering calling name, the identity header will simply sign the exact string of the calling name and serve the ability to do a string compare with the ‘rcd’/‘nam’

Example POCN case

SIP INVITE

```
INVITE sip:+12155551213@biloxi.com SIP/2.0
Via: SIP/2.0/UDP
pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: “Bob” <sip:+12155551213@biloxi.com;
user=phone>
From: “Alice” <sip:+12155551212@atlanta.com;
user=phone>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Date: Sat, 13 Nov 2015 23:29:00 GMT
Identity: “sv5CTo05KqpSmtHt3dcEiO/1CWTS
  ZtnG3iV+1nmurLXV/HmtyNS7Ltrg9dlxkWzoeU
  7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI
  3d7SyN21yNDo2ER/Ovgtw0Lu5csIppPqOg1uX
  ndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs=“;
  info=<https://biloxi.example.org/
  biloxi.cer>;alg=ES256;ppt=“shaken”
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

PASSporT

```
Protected Header
{
   "alg":"ES256",
   "typ":"passport",
   “ppt”:”shaken”,
   "x5u":"https://biloxi.example.org
      /biloxi.cer”
}
Payload
{
   “attest”:”A”
   "dest":{“tn”:["12155551213"]}
   "iat":1443208345,
   "orig":{“tn”:"12155551212"},
   “origid”:”123e4567-e89b-12d3-a456
      -426655440000”,
   "rcd":{"nam":"Alice"}
}
```

Rich Call Data

- Name, Address, URI to logos, etc.
- RFC7095 jCard will be a standard case for ‘rcd’
- Either can be embedded directly or URI to jcard object
- Will provide a hash function and possibly encryption mechanism to protect the integrity and privacy of RCD

KEEP
CALM
AND
EAT YOUR
VEGETABLES

I WANT YOU
TO EAT YOUR
VEGETABLES

Vesper - open source STIR/SHAKEN implementation

https://github.com/Comcast/vesper