How STIR/SHAKEN Contributes to an Identity Assurance Framework

Kevin Riley, CTO & EVP of Advanced R&D
Agenda

- Motivation
- Definitions and Foundational Concepts
- Solution Components and Requirements
- Building and Identity Assurance Framework
- Call to Action
Motivation and Scoping the Solution
RoboCalling Statistics

Q1 2019 saw 15.3 billion robocalls, the highest volume ever

Making this about 15.5 robocalls per person per month

In 2018, the FCC demanded CSPs to implement a Call Authentication solution and their message was “Resistance is Futile”
Fraud By the Numbers

$29.2 billion in Toll Fraud Loss in 2017

2017 Top 5 Fraud Types

1. International Revenue Share Fraud – $6.10B
2. Interconnect Bypass (e.g. SIM Box) – $4.27B
3. Arbitrage – $3.26B
4. Theft / Stolen Goods – $3.02B
5. Premium Rate Service – $2.29B

Source: 2017 CFCA Global Fraud Loss Survey
Defining Identity Assurance

To assure identity and one must validate legitimate use of service
- Consider multiple inputs, no one piece of data can assure identity
- Policy must be invoked in real-time and adapted constantly, bad actors are moving targets

What constitutes compromised identity?
- Spoofed credentials
  - Masking identity with alternate, legitimate ID
- Stolen services
  - Bad actor takes over legitimate endpoint and uses in place

Challenges
- Mobility and multiple access modalities per user
- Legitimate actors can have common traits with Bad actors
- There is no single method to assure identity

Primary Use Cases
- Fraud
- Robocalling
Three Key Inputs

Identity
Who is the originator?

Reputation
Is this someone I want to talk to?

Trust Context
Where did the call originate and where will it terminate?
Determining Identity

Known Subscribers

Do Not Originate List (DNO)
- Numbers that never originate calls (e.g. IRS call center +1-267-941-1000)

Un-Assigned Numbers
- Unassigned NPA/NXXs (LERG 6 has most assignments)
- Unassigned extensions (per carrier lists)

Invalid E.164 Calling Numbers
- Screening functions in call processing

STIR/SHAKEN Attestation
- Signing of phone calls to attest identity of call originator
- Initially only phone companies will sign but eventually enterprises may participate
- Bad actors will eventually figure out how to sign calls
Determining Reputation

Reputation is the Internet’s FICO score
– Multiple companies will be inventing their proprietary algorithms that they do not disclose

Reputation is fundamentally tied to your identity
– Get the identity of the caller wrong and reputation score is worthless

Assessing Reputation pulls from multiple Data Sources
– Proprietary algorithms
– Analytics/ML/AI
  • High volume calling parties
  • Unique signaling aspects
– 3rd Party Proprietary Reputation Data
  • Carrier and/or crowd sourced generated lists
  • Possibly distributed ledger technology

Context matters
– Location where call enters a network and where it is destined to terminate
– A known subscriber number on an internal interface is always verifiable
– A known subscriber number entering from a wholesale interface might be spoofed
– “Trust Context”
Architecting a Framework for Identity Assurance
What Does STIR/SHAKEN Provide?

The Goal
Mitigate unwanted robocalls and bad actors who use caller ID spoofing to increase the chances of speaking to a subscriber.

The Method
Service providers attest to the authenticity of a call originating in their network; this attestation is passed in-band with the call such that the terminating Service provider receives the attestation.
1. **STI-PA**: STI Policy Administrator
2. **STI-CA**: STI Certificate Authority
3. **SKS**: Secure Key Store
4. **SP-KMS**: Service Provider-Key Management Server
5. **STI-CR**: STI-Certificate Repository
6. **STI-AS**: STI-Authentication Service
7. **STI-VS**: STI-Verification Service

**STI** = Secure Telephone Identity
Where STIR/SHAKEN Come Up Short?

Intent and Reputation
A calling number is effectively “vouched for” as owned by the service provider but the user behind the number is not verified.
Analytics is Compulsory To Mitigate Identity Abuse

**Fraud**
- Track the behavior of individual subscribers and the activity of called numbers in the network
- Abnormal calls beyond selected variances are alerted

Identify repetitive calling patterns to anomalous places and flag or block them

**Telephony Denial of Service**
- Detect calling anomalies metrics such as Call Rate Exceeded, Long/short durations, etc.
- Automatically alert and blocks rogue calling patterns

Siphon out unwanted, disruptive calls from your RTC network

**Nuisance Calling**
- Use third party databases to identify Robo calls
- Complimentary analytics for STIR-SHAKEN
  - Capture and score potential spoofed calls

Multi-tiered approach to stop excessive nuisance calls affecting your customers
Digital Fingerprinting UC with Machine Learning

Machine Learning

Model & Classify

Digital Fingerprint

Device, User & Session Characteristics
The Foundational Pillars of an Identity Assurance Architecture

- Transactional Policy
- Real-Time Attestation
- Inferred Behavioral Knowledge
- 3rd Party Integrations

Identity Assurance

OSS and Infrastructure KPIs

Learned Policy

Imported Policy
The Taxonomy of Identity Assurance Components

**Producer & Consumers**
- Any network component that:
  1. Sources data contributing to identity assertion
  2. Needs to assert or verify identity

**Call Adaptation Service**
- Call signalling aids used to influence calls without opening the internals of existing network components

**Policy Service**
- Overall responsibility for “what to do with the call”, determines if the call should be routed, dropped etc

**Assertion Service**
- Tasked with [asserting, verifying, scoring] if a call is using a valid and legitimate identity

**3rd Party Services**
- Any 3rd Party component we may interact with to resolve the fate of a call

Identity Service
Services loosely coupled via APIs

Producer & Consumers
Any network component that:
1. Sources data contributing to identity assertion
2. Needs to assert or verify identity

Call Adaptation Service
Call signalling aids used to influence calls without opening the internals of existing network components

Policy Service
Overall responsibility for “what to do with the call”, determines if the call should be routed, dropped etc

Assertion Service
Tasked with [asserting, verifying, scoring] if a call is using a valid and legitimate identify

3rd Party Services
Any 3rd Party component we may interact with to resolve the fate of a call

Identity Service
Flexible Cloud, Hybrid and Premise Deployment Options

Boundary between premise and cloud is flexible

**Producer & Consumers**
Any network component that:
1. Sources data contributing to identity assertion
2. Needs to assert or verify identity

**Call Adaptation Service**
Call signalling aids used to influence calls without opening the internals of existing network components

**Policy Service**
Overall responsibility for “what to do with the call”, determines if the call should be routed, dropped etc

**Assertion Service**
Tasked with [asserting, verifying, scoring] if a call is using a valid and legitimate identify

**3rd Party Services**
Any 3rd Party component we may interact with to resolve the fate of a call

**On Premise**

**Cloud**
Delivering Increasing Levels of Identity Assurance in Phases

- **SIP Robo**
  - STIR/SHAKEN
  - White/Black-List static policy

- **SIP Fraud**
  - Behavioral Analytics
  - Inferred Policy

- **Beyond SIP**
  - SS7/Diameter
  - REST-based

- **Advanced Policy**
  - Post call setup modification
  - Third party, out of network interrogation and modify ML/AI-based modelling
Componentry of a Comprehensive Identity Assurance Solution

**Identity Assurance Hub**
- Combines multiple identity and reputation inputs using a rule profile
- Assigns a reputation score and brokers call treatment policy

**Cloud Identity DB**
- 3rd Party Identity Service
- 3rd Party Robo DB (Identity)
- Carrier Identity DB / Opt-in status

**SBC/GW**
- Policy/Routing

**Trust Context**
- Operational Measurements
- Signaling

**Analytics**
- CDRs
Call to Action
Call To Action

Federal agencies and consumers have spoken
  – CSPs must mitigate identity abuse

There is no single technology or standard to assure identity in your network

STIR/SHAKEN implementations need to continue and expand

Analytics must be woven into your identity assurance strategy
  – Static policy cannot keep pace with evolving threat vectors
  – Behavioral analytics and ML to baseline your network to then identify out bad actors

Think beyond your network
  – Architect to onboard third-party databases and services
  – Embracing SaaS services and federated data accelerates deployment velocity and capabilities
Thank You

Kevin Riley
kriley@rbbn.com