Shaken 101: Mitigating Illegal Robocalling and Caller ID Scams Webinar

Panelists:
Dr. Eric Burger  
Chief Technology Officer  
FCC

Jim McEachern  
Principal Technologist  
ATIS

Moderator:
Brent Struthers  
STI-GA Director  
ATIS

January 30, 2019
Brent Struthers
STI-GA Director
ATIS
Eric Burger

Chief Technology Officer

FCC

eric.burger@fcc.gov
Jim McEachern
Principal Technologist
ATIS
Outline

• Problem Statement
• SHAKEN vs. STIR
• SHAKEN Protocol
  • Functional elements
  • Attestation levels
  • origid
Caller ID

Originating service provider inserts Caller ID in network signalling

Service Provider

So what’s the problem?
Originating service provider inserts Caller ID in network signalling

Enterprise inserts Caller ID at PBX

Origining service provider generally doesn’t validate Caller ID for enterprise
Caller ID Spoofing: The Problem

Open source IP-PBX inserts Caller ID

Call appears to originate locally

Call center agent could be anywhere…

Service Provider
Caller ID Spoofing: The Problem

Call center agent could be anywhere...

Routing through multiple service providers further complicates things
Verified…

202-555-0123
Just because a call is “verified” doesn’t mean it’s “good”.
Key Insight Behind SHAKEN

• The **originating carrier always knows something** about the call origination.

• Sometimes the carrier knows/controls **the number** in Caller ID:
  – Mobile phone authenticates with the network
  – Landlines are hard-wired to the switch

• Sometimes the carrier knows **the customer**, but allows the PBX to insert Caller ID:
  – Enterprise PBX could display receptionist number for all outgoing calls
  – Call center could display toll free number, or local callback number

• Sometimes the carrier only knows the **entry point** into their network.

• **The problem**: today there isn’t a secure mechanism for the originating carrier to communicate this information to the terminating carrier.

• **SHAKEN** was designed to provide a secure mechanism for this. (Nothing more…)
Outline

• Problem Statement
• SHAKEN vs. STIR
• SHAKEN Protocol
  • Functional elements
  • Attestation levels
  • origid
SHAKEN vs. STIR

STIR:
- Protocol for creating a digital signature with calling party info
- Allows signature to be created/verified in various locations
SHAKEN vs. STIR

SHAKEN:
• Specifies how STIR can be deployed in service provider networks
• Focused on “deployability”
The essence of SHAKEN is:

1. Originating service provider creates digital signature based on what it knows about the call origination:
   A. The customer and their right to use the number, or
   B. The customer (but not the number), or
   C. The point it enters their network

2. Assign “origid” to uniquely identify the call origination
Outline

• Problem Statement
• SHAKEN vs. STIR

• SHAKEN Protocol
  • Functional elements
  • Attestation levels
  • origid
Phase 1: SHAKEN – Published January 2017

Mechanism to sign calling party information, including attestation claims and origid, to generate PASSporT token.

On-the-wire encoding of PASSporT token in SIP Identity header.

Mechanism to verify signature and validate PASSporT claims.

ATIS-1000074: Signature based Handling of Asserted information using ToKENs (i.e., SHAKEN)
SHAKEN Attestation Claims – Full Attestation

A. Full attestation: The signing provider shall satisfy all of the following conditions:
   – Is responsible for the origination of the call onto the IP based service provider voice network.
   – Has a direct authenticated relationship with the customer and can identify the customer.
   – Has established a verified association with the telephone number used for the call.
   – NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). … but they are not asserting that the call is actually from the number that appears as the calling party (i.e., SHAKEN allows “legitimate” spoofing).
   – NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number”… but it will impact “reputation”
SHAKEN Attestation Claims – Partial Attestation

B. Partial attestation: The signing provider shall satisfy all of the following conditions:

– Is responsible for the origination of the call onto its IP-based voice network.
– Has a direct authenticated relationship with the customer and can identify the customer.
– Has NOT established a verified association with the telephone number being used for the call.

– **NOTE**: When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature … allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. Also … for forensic analysis or legal action where appropriate.
C. **Gateway attestation**: The signing provider shall satisfy all of the following conditions:

- Is the entry point of the call into its VoIP network.
- Has no relationship with the initiator of the call (e.g., international gateways).
- **NOTE**: The token will provide a unique origination identifier of the node in the “origid” claim. (The signer is not asserting anything other than “this is the point where the call entered my network”.)
Origination Identifier – (“origid”)

• **origid**: unique origination identifier (“origid”) is a globally unique opaque identifier corresponding to the service provider-initiated calls themselves, customers, classes of devices, or other groupings that a service provider might want to use for determining reputation or trace back identification of customers or gateways.

• For Full Attestation, in general, a single identifier will be used for all direct service provider-initiated calls on its VoIP network, but a service provider may also choose to have a pool of identifiers to differentiate geographic regions or classes of customers.

• For Partial Attestation, a single identifier per customer is required in order to differentiate calls both for trace back and reputation segmentation so that one customer’s reputation doesn’t affect other customers or the service provider’s call reputation.

• Best practices will likely develop as trace back and illegitimate call identification practices evolve.

From ATIS-1000074
SHAKEN Functions

Authentication

STI - AS

SIP Proxy

STI - CR

STI - VS

SIP Proxy

Verification
SHAKEN Example: Full/Partial Attestation

Service Provider (IMS)

Service Provider (IMS)

STI - AS

STI - VS

SHAKEN Attestation
SHAKEN Example: GW Attestation
SHAKEN Example: Origination Identifier (origid)
SHAKEN Example: Origination Identifier (origid)
SHAKEN Example: Origination Identifier (origid)
SHAKEN Example: origid But No Analytics

- Both calls are verified with the same level of attestation.
- origid still allows quick traceback once problems reported.

Note: no Analytics function
Future Webinars

• Future webinars will address:
  – SHAKEN Governance
  – ATIS/Neustar SHAKEN Testbed
  – Display Framework: Alternatives and Tradeoffs
Questions
Thank you for attending the Shaken 101: *Mitigating Illegal Robocalling and Caller ID Scams* Webinar

All registered attendees will receive a follow up email containing links to a recording and the slides from this presentation.

For information on the SHAKEN Governance Authority, visit http://www.atis.org/sti-ga/