Breaking the Deception Code:

Anti-Spoofing Strategies and the Pursuit of 'Impossible Call' Identification"

Howard Lang, P.E.
Expert Member of Technical Staff
AT&T Laboratories
hl1539@att.com

SIPNOC 2024

September 18, 2024

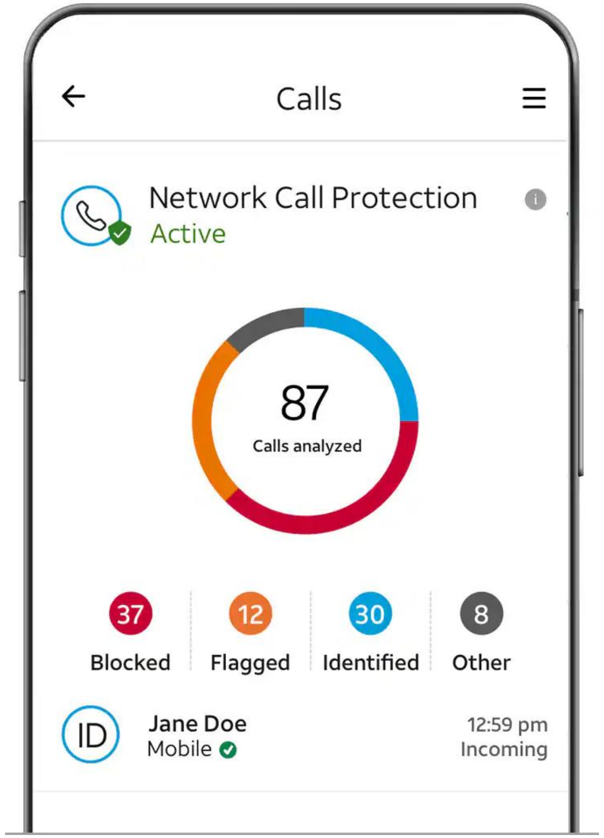
History

AT&T Launched ActiveArmor SM in December 2016

AT&T ActiveArmor SM provides Robocall Protection built into the AT&T Network

Incoming calls evaluated for SPAM / FRAUD activity upon arrival

An optional Free App (iOS / Android) provides enhanced security protection, and individualized customization options



AT&T

What do we know…

Most phone numbers have a History…

Status – Is it connected?

Ownership – Who pays the bill?

Behavior – What does the number do?

Connections – How does it communicate?

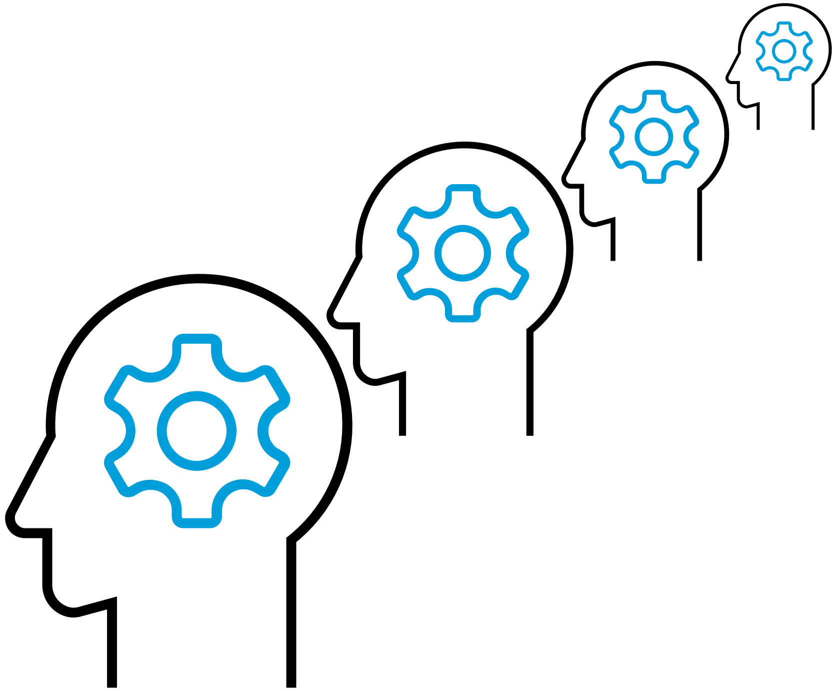
Complaints – What others say about this number?

Network – Where is the call originating and terminating?

Verified – Is call verified by STIR/SHAKEN or other method?

Call Routing – How did call traverse the network?

…and more…



Innovative Bad Guys constantly trying new attacks, and new calls arrive, so **History evolves**

Reputation is evaluated freshly upon arrival of each call to maintain high accuracy

Calling Party TN **Reputation** is the aggregated view of this Story.
Analytics use this Reputation to determine if call is to be considered unwanted

AT&T

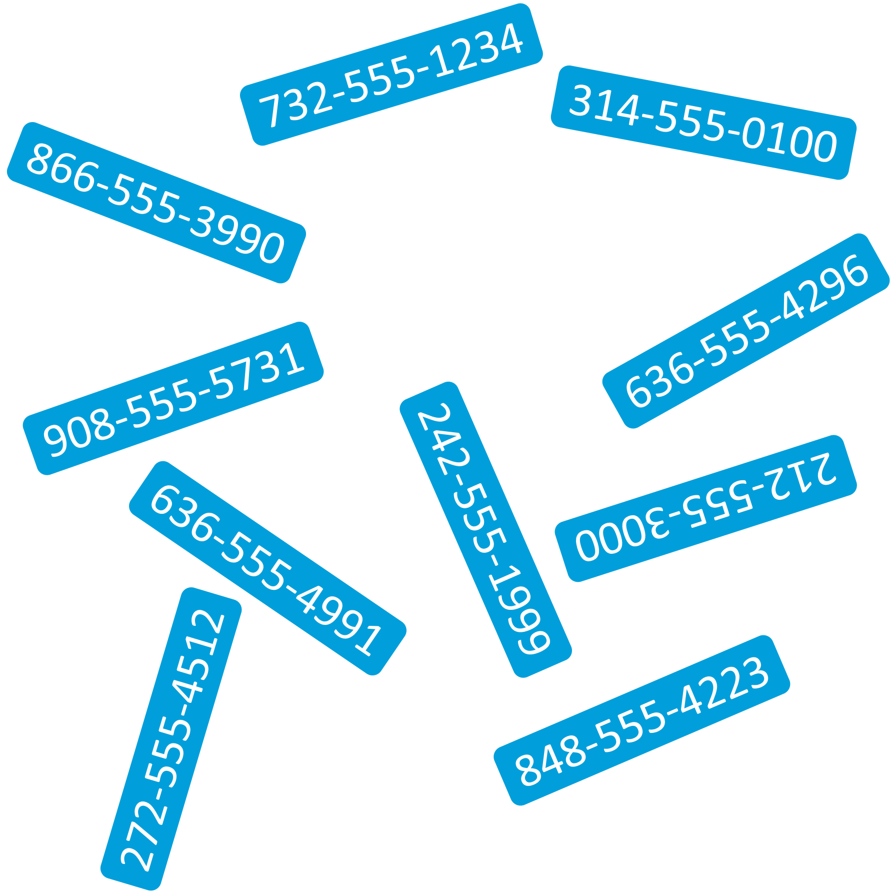
We don’t always have a History….

Number Rotation Robocall Attacks

Number Rotation Robocall trend: **Spread attacks across many numbers**, with few (perhaps 1) bad call per number

Less reliance on calling history

More reliance about specific call received



732-555-1234

314-555-0100

866-555-3990

636-555-4296

908-555-5731

242-555-1999

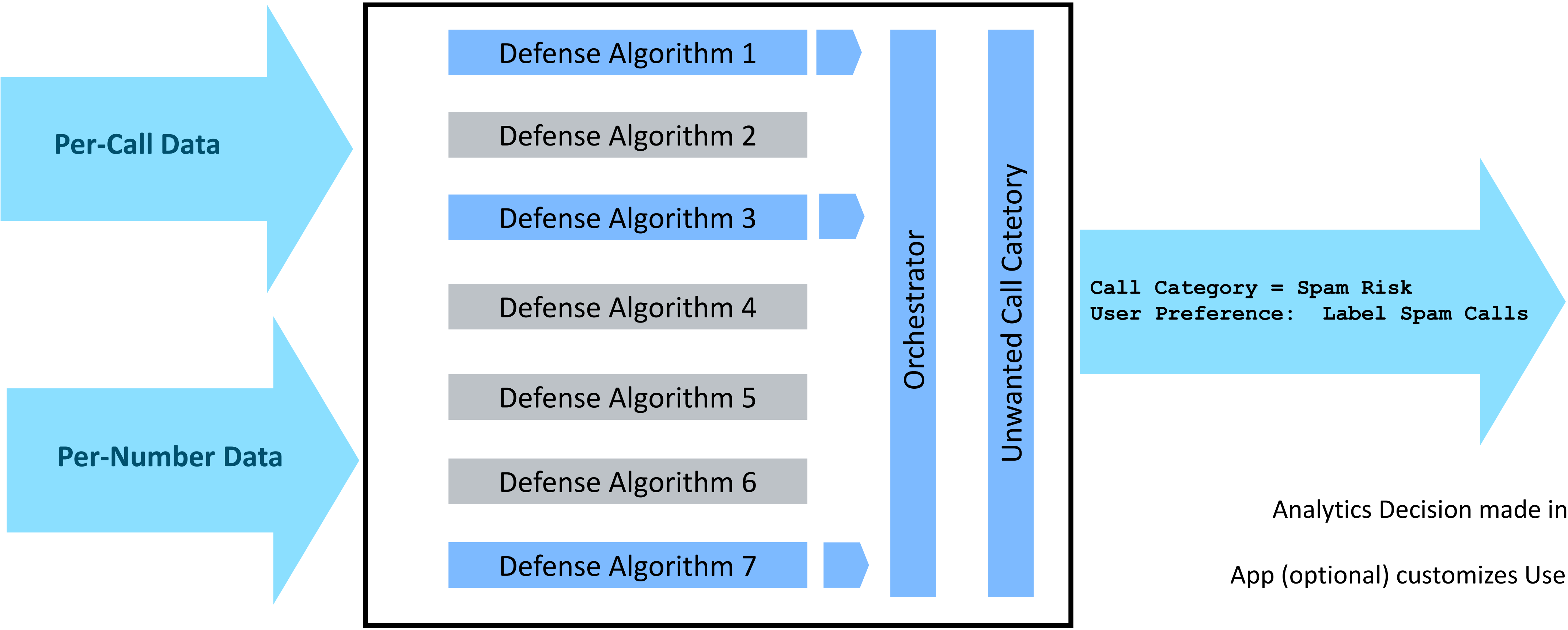
212-555-3000

636-555-4991

272-555-4512

848-555-4223

Incoming Call Analysis Overview



Per-Call Data

Per-Number Data

Defense Algorithm 1

Defense Algorithm 2

Defense Algorithm 3

Defense Algorithm 4

Defense Algorithm 5

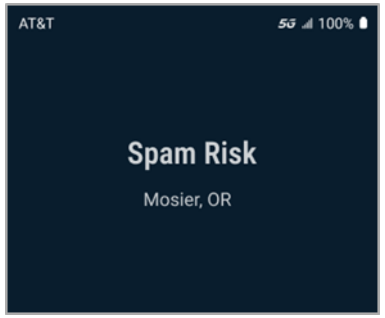
Defense Algorithm 6

Defense Algorithm 7

Orchestrator

Unwanted Call Catetory

```
Call Category = Spam Risk
User Preference:  Label Spam Calls
```



AT&T

5G 100%

Spam Risk

Mosier, OR

Analytics Decision made in Network

App (optional) customizes User Preferences

Defense Algorithms updated as new threat profiles detected

Robocall Attacks Trends

Robocall Attacks intend to target victims with precision to cause significant harm.

A common strategy in these attacks is to build trust with the victim:

- Voice cloning without authorization, for example, of someone the victim is familiar with (Illegal)
- Information about victim obtained from alternate sources
- Spoofing of originating number, to appear to be from trustworthy source

Spoofed Calls

A technique where the originating caller presents an alternate originating number to increase Trust

Spoofed calls may be Legitimate or Not Legitimate

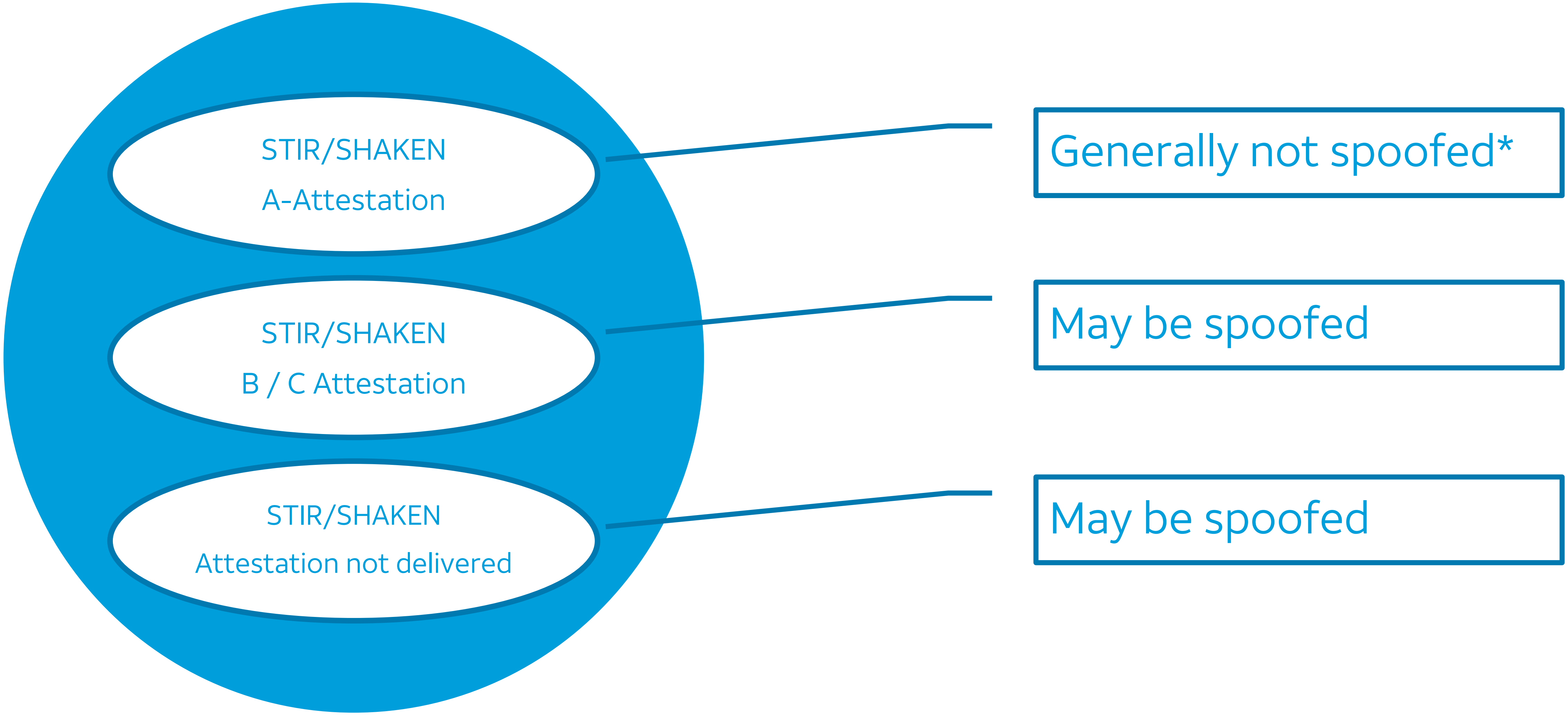
- Legitimate: Customer Care of Enterprise contacts customer, and displays main company number rather than individual number of customer care representative
- Not Legitimate: Bad Guy spoofs alternate number without authorization with intent to harm victim

Challenge:

There may be a mix of legitimate calls and not legitimate calls from the same originating number

How to distinguish??

What do we know about the Incoming Call?



STIR/SHAKEN
A-Attestation

Generally not spoofed*

STIR/SHAKEN
B / C Attestation

May be spoofed

STIR/SHAKEN
Attestation not delivered

May be spoofed

*In analysis, must pay attention to both Attestation Level and who signed the call

Identifying “Impossible Calls”

Is the call plausible?

For incoming calls that are not STIR-SHAKEN A-Attested, is the call plausible?

- What do we know about the carrier that owns the number?
- Is a Subscriber associated with the number?
- Is the calling number able to initiate an outbound call (i.e. Do Not Originate)?
- Is the calling number fully registered?
- Does the call enter the network align with expectations?

Information about the incoming call must be evaluated on a per-Call (not per TN) basis, since legitimate and not legitimate spoofed calls may share the same originating number.

This additional information can augment STIR-SHAKEN Attestation, to indicate if the incoming call is plausible.

STIR-SHAKEN and Not Legitimate Spoofing

Unverified Call

~~Trust~~

Unknown Identity

SHAKEN Only

~~Intent~~

Unknown Intent

Impossible Call Check

~~Not fully verified~~

~~Impossible Call~~

Not Legitimate Spoofed

SHAKEN + Analytics

- ✓ Trust Identity of Number
- ✓ Predict Intent of Caller

Intra-Carrier vs Inter-Carrier Spoof Detection

Intra-Carrier

- For calls that originate and terminate on the same carrier, more is known about the call.
- Carriers can more readily determine if the call origination legitimately was initiated on their own network.
- Originating calls, using a Carrier’s number, but arriving from an alternate source, are likely not legitimate (Spoofed).

Inter-Carrier

- Cooperation / Standards needed to share additional information about the originating calls, which also satisfies legal / privacy concerns

AT&T

AT&T