Agenda – All About RRAPTOR

• ZipDX Background / History
• RRAPTOR Strategy & Objectives
• What Does It Do?
• How Does It Work?
• Action-packed Live Demo
• What Are We Learning?
• How Can We Best Leverage It?
  • Providers, Brands, Enforcers
ZipDX & Robocalls Through the Ages

• 2013: Federal Trade Commission Robocall Challenge
  • Our contest entry proposes Traceback (we did not win)

• 2018: ZipDX develops the “Secure Traceback Portal” adopted by USTelecom’s ITG

• 2019-2020: Thousands of calls traced back using our platform

• 2021: Robocall Mitigation Database Explorer (https://portal.legalcallsonly.org/rmd)
  • On-line searchable history of the RMD
  • Evaluation, scoring and ranking of Robocall Mitigation Plans

• 2022: STIR/SHAKEN Toolkit Introduced
  • IDENTITY Header Decoder (https://portal.legalcallsonly.org/shaken)
  • SHAKEN test numbers display signature details (http://portal/legalcallsonly.org/identity)

• Subscribe to our Blog at https://legalcallsonly.org/subscribe/
Strategy & Objectives

- Call Authentication can validate Caller-ID and deter malicious spoofing
  - Call recipients can (perhaps) know to be trusting or skeptical before they answer
- But STIR/SHAKEN also identifies the PROVIDER that put the call on the network
- We’ve always said the best place to stop illegal calls is at the source
- The signer of the call is closest to the source and best positioned to act

- We can usually identify a call as likely illegal only after answer with the audio available
- Increasingly, illegal robocall signaling includes the Identity header
- Given the audio & the signer we know which providers contribute most to the problem
- We can deliver actionable, real-time data to those providers
- The Provider and Enforcement communities can know providers’ reputations
- This is effective even when less than 100% of calls are signed
What's In A Signature?

Identity: eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ1c2VyIiwiaWF0IjoxNjYwMDcwNTA4LCJmdmVzdCI6WyJ0b3QiOiJ0b3QiLCJpYXQiOjE2NDgxNjE2NTB9.eyJ0eXBlIjoiTW9kZWwifQ

Organization (from Certificate Subject):
- COMMON NAME: SHAKEN 939H
- VALID FROM: 2022-06-16 18:28:03
- VALID TO: 2022-06-16 18:28:03

Details:
- TO: 17262085771
- FROM: 18333813053
- TIME: 2022-08-09 18:36:13 UTC
- ATTEST: B

SHAKEN Signature Verification: PASS
STIR/SHAKEN Tackles Robocalls Today

• Virtually ALL Originating Providers are required to sign calls
  • 47 CFR § 64.6301(a)(2)
  • Exception still for small facilities-based providers, but they originate few robocalls

• ALL Providers must take measures to prevent origination of illegal calls
  • 47 CFR § 64.1200(n)(3)
  • One measure: vetting customer RMD entries
  • Another: ensuring all calls are properly signed by the originator

• There are still gaps due to TDM networks
  • But the vast majority of robocalls travel via SIP

• We’re already equipped to stop most illegal robocalls
What do you think?

Poll #1
What Are We Learning?

• RRAPTOR currently receives almost 10,000 calls per workday

• We recognize about one-third of those as SUSPECT
  • Others are short or silent or hang up before answer; also legit calls to old or wrong numbers

• About two-thirds of suspect calls are signed

• A third of THOSE calls are signed by three major intermediate providers

• Many calls do not carry the signature of the ORIGINATING provider
  • Providers are improperly relying on the signature of their downstream intermediate

• Some providers are signing carelessly
  • Improper format for FROM and/or TO numbers; expired and missing certificates
Two Ways To Stop Illegal Calls

**IDEAL: STOP AT THE SOURCE**
- Illegal calls never get on the network
- Responsible providers refuse to accept calls from nefarious originators
- Calls that sneak past are quickly identified and the caller shut down

**OR: MITIGATE DOWNSTREAM**
- Originating providers that continue to facilitate illegal calls quickly earn a bad reputation
- Analytics tools recognize calls from those providers
- Calls are labeled and/or routed appropriately

• Legal calls are properly labeled and delivered based on the positive reputation of the originating provider
What Does RRAPTOR Do?

• RRAPTOR is a surveillance network for robocalls

• It operates automatically and passively, on the theory that robocallers placing a large volume of calls will end up calling our numbers

• SCALABILITY is a key objective – robocalling is a huge problem; we want to automate whatever we can to get our arms around the problem

• URGENCY is critical – RRAPTOR can immediately alert a provider when it sees their signature on a nefarious call

• RRAPTOR is OBJECTIVE – it just presents what the data says

• Our first priority is to get PROVIDERS to be part of the solution; we want to give them actionable data

• All RRAPTOR information is owned by ZipDX; none of it is bound by any confidentiality agreements

• RRAPTOR is NOT PERFECT
  • We’re focused on the highest volume callers / signers
  • Once we address those, we’ll move onto the next batch
  • We might miss some suspect calls; limit false positives
  • Most robocalls go via SIP (cheapest), but not all

• RRAPTOR does not address ALL nefarious calling
  • Does not address Denial of Service, Social Engineering, etc.
  • Robotexts are a future feature

• Our focus is not evidence-gathering for a court case
  • We are a tool for understanding behaviors and trends

• We are not lawyers & not focused on regulatory nuances
  • We’re trying to convince providers to use their discretion to behave the way they SHOULD, not just the way they MUST

• Not all providers are as altruistic as we would like
  • Strategic enforcement will always be a critical element
How Does RRAPTOR Work?

An Inbound call to a monitored pool number is received by RRAPTOR. It sends a SIP INVITE to the monitored pool number with the following details:

SIP: 4086669812@rraptor.zipdx.com

RRAPTOR answers the call after 10-20 seconds, during which it plays "Hello" and begins recording the call. The system then extracts details such as the called and calling numbers, the identity header, and validates the signers and attestations. The audio is transcribed, and keywords and phrases are analyzed.

The system checks if the signing provider has reached the notification threshold. If yes, an alert is sent via email. The database stores all the details and analysis results.

NOTE: RRAPTOR detects ringless voicemail and can also capture TEXTS (without S/S) sent to our monitoring pool.

Legal Calls Only

A ZipDX Initiative
Let’s RRAP!

- RRAPTOR displays its data in real time
- Slice the data by KEYWORDs in the messages
- OR by the PROVIDER associated with the signatures
- See summaries: called numbers, ANIs, attestations, invalids
- Examine specific time windows
  - I like TODAY and PAST 7 DAYS best – what’s happening now?!?
- DRILL DOWN to read the transcripts & hear the audio
- See signature details, DNC stats, etc.
Signature Defects from the Real World

- Mis-formatted FROM and TO numbers
  - Missing leading 1 (should be 1NPANXXYYYY)
  - Spurious prefix digits (112175551212 or 300012175551212)
- Wrong Time Zone (US ET vs. UTC)
- Time in the future (inaccurate clock)
- Expired Certificate
- Signature verification via Public Key does not match (forgery?)

These and other errors will result in Vertstat TN-Validation-Fail for terminating providers and analytics engines.
Is RRAPTOR A Honeypot?

Definitions from the Internet:

• a person or thing that acts as a lure or decoy in a trap, scam, or scheme
• something that is attractive or rewarding and that entices a specific group of people
• a computer system established as bait to lure malicious hackers into engaging with it, thereby revealing the identity or technique of the perpetrator

• RRAPTOR does not lure or entice
  • We are doing nothing to solicit or encourage these calls
  • We do not publish our numbers, nor do we sign up at any website and we certainly do not give consent to call
  • Many of our numbers are on the national Do-Not-Call list

• We just answer calls that are already being made

• Presumably our numbers are on stale lists, perhaps bought or stolen by today’s robocallers
  • Or maybe they are being called at random
Marrying RRAPTOR with Traceback

• Until now, Traceback has been our best method for identifying robocall sources
• The traceback process is semi-automated and reasonably fast, but limited in scope
• Daily, RRAPTOR associates signers with dozens of campaigns and thousands of calls

• Traceback can fill gaps in RRAPTOR’s surveillance

• Why are certain calls unsigned, or carrying an intermediate provider signature?
  • Originators are failing to sign as required
  • Calls are originating via exempt providers
  • Calls are transiting via TDM
  • Intermediate providers are dropping Identity headers
Ending Whack-a-Mole

• Illegal robocalls persist because a cottage industry of providers choose to accept payment to facilitate these calls

• Stakeholders complain that if calls are rejected at one spot they just crop up somewhere else

• With tools like RRAPTOR, SHAKEN establishes provider reputations

• Those that persist in facilitating these calls will find it impossible to send their traffic onward

• Everybody that wants to contribute to solving this problem needs to step up to a higher level of engagement – the status quo is not sufficient
Reputation is Everything

• RRAPTOR’s goal is to establish provider reputations based on the calls they do (or do not) facilitate, and to help them maintain an excellent reputation

• Providers that have been part of the problem can become part of the solution

• A provider’s participation in problematic robocalling will be on display for all to see

• Downstream providers can opt to increase scrutiny when considering traffic from problematic upstreams

• Analytics providers can use signer reputation to inform call treatment
RRAPTOR Subscriptions for Service Providers

- $2,500/month or $20K annually
- Web Portal shows:
  - Statistical summaries for all providers and/or all categories, incl. total calls, A/B/C attestations, unique called and calling numbers, numbers on Federal DNC (who is signing suspect calls?)
  - Drill-down with individual call dates/times, called and calling #’s, audio recording, transcript, signature decoding, days on DNC (full detail only for Subscriber’s signed calls)
  - Filter by date window, category, state area code
  - Defective signatures
- Email alerts (configurable for weekly, daily, immediate)
- Comments (visible to all or restricted)
What do you think?

Poll #2
Provider Priorities based on Today’s Rules

Everybody needs to follow the rules we already have:

- Originating Providers must sign (or have their downstream sign) with the OP’s Certificate
- Providers must assign attestation level according to their knowledge of the SUBSCRIBER (Caller)

Intermediate providers need to ensure their upstreams are following the rules:

- Reference the RMD; look at certifications and RMPs
- Call sources must adhere to their obligations: verify that calls that should be signed ARE signed

Originating providers are responsible for the calls they put on the network:

- They need to know ALL the rules
- They need to confirm that their subscribers are following ALL the rules
Can ZipDX Help?

• Our SHAKEN test tool lets you verify your calls are being properly signed
  • http://portal/legalcallsonly.org/identity

• Use the Robocall Mitigation Database Explorer as part of your KYC process for new and renewing customers
  • https://portal.legalcallsonly.org/rmd

• RRAPTOR will show you:
  • Full details for suspect calls you are signing
  • Defects in your signatures
  • Data on suspect calls signed by other providers (perhaps your current or future customers)

• Email support@zipdx.com to activate a free RRAPTOR trial