Why Robocall and Fraud Mitigation Needs to Be Webscale

July 2021

Michael Stovenour
Chief Field Architect – Core Products
Agenda

• My Background
• Introduction
• Definitions
  – Robocall and Fraud Mitigation
  – Webscale
• Three-Pronged Solution: Robocall and Fraud Mitigation
  – Decouple: Separate capabilities out of the network into their own domain
  – Adapt: Make the system highly configurable
  – Automate: Fundamentally change how software is developed, tested, and deployed
My Background

• Sonus / Ribbon 21 Years
• Director Verification Office Test Lab
  – Customer network reproduction and testing
  – Software deployment MOP development
• Professional Services Network Design
  – Designed networks worldwide; US, Europe, and Japan
• Systems Engineering Director / Tier 1 Accounts
• Chief Field Architect
  – Virtualization
  – Robocall Fraud and Nuisance Mitigation
Introduction

• Answer This Question:
  “How can I keep up with the rapidly changing regulatory and competitive landscape for robocall and fraud mitigation?”

• Decouple The Problem Set Into Two Domains
  – Core Platforms + connecting calls – no margin for error; has immediate and direct impact on customers experience
  – Ancillary Services – enhance customers’ experience but will not severely impact experience if interrupted

• Employ Webscale Techniques to Ancillary Services
  – Proven strategy for reacting quickly within a highly reliable communications network
  – Adapt
  – Automate
Fraud and Robocall Mitigation

• Robocall and Fraud
  – Closely related but not entirely the same
  – Some fraud is not through Robocalling
  – Some Robocalling is not fraud, but users still might consider it unwanted

• Not Simply STIR/SHAKEN
  – STI is an enabler but does not authenticate or determine intent

• Origination Robocall Mitigation
  – Prevention of clearly fraudulent ANI spoofing at origin
  – Behavioral analytics to detect unexpected robocalling customers

• Termination Robocall Mitigation
  – Blocks clearly fraudulent ANI spoofing
  – Provides called party notification and/or treatments
What is Webscale?

• Apply Techniques of Web Monsters to Development, Testing, and Deployment
  – Facebook, Amazon, Netflix, etc.
  – Continuous development without user interruption
  – Minimize operational costs while meeting dynamic service demand

• Pace of Innovation
  – Respond to fierce competition with rapid introduction of capabilities

• Scale
  – High volume, auto-scaling services

• Service Assurance

• Automation

• A Mindset Not a Technology
  – Technologies are enablers and there are many that can be employed
Webscale Enablers

• Enablers of rapid innovation and scale
• Containers
  – Docker, Portainer, OpenShift, each public cloud container service, etc.
  – Allows developers to develop and test with an exact production configuration
• Microservices
  – Loosely coupled, *reusable* components
  – Independent scaling vectors
• Automation
  – Kubernetes, Docker Swarm, Cloudify, Rancher, Amazon EKS, Google GKE, etc.
  – Lowers cost and increases velocity
  – DevOps
  – Continuous Integration
  – Continuous Deployment
Poll Question #1

How are you deploying a robocall & fraud mitigation solution?

- Tightly integrated to existing call processing
- Separate from existing call processing, but in my network
- Separate and hosted by 3rd party
Decouple
Core Call Processing System Challenges

• Core Call Processing Systems
  – Critical call path elements that directly define network quality
  – Changes are deliberately slow because of risk
  – Balance risk vs. delay in mitigation
  – Software upgrades must be carefully planned and executed

• Challenges With Fraud and Robocall Mitigation In Core Call Processing Systems
  – Requires significant time and effort to roll out new routing designs for each robocalling threat
  – Customer routing database design complexities introduce delay to threat response
  – Every network design and blocking technique can require a custom data ingestion and routing design
Deployment Challenges in Fraud and Robocall Mitigation

• Pace of Development
  – Even for just STI, we didn’t know what we didn’t know
  – Signing as a service, non-IMS networks, etc.

• Drivers of Rapid Change
  – Regulatory
  – Competitive: Users are starting to publicly comment on competitive differences
  – Reduce fraud costs

• Pace Not Slowing Down
  – STI alone: DIV, RPH, 607/608, Out of Band
  – Verified Caller and RCD
  – Honeypots, fraud campaign fingerprinting, ML based scoring algorithms, threat federation, and new database sources

Go Fast To Keep Up With the Bad Guys
Decouple

• Scoring for Robocall and Fraud Mitigation
  – Rapid Innovation
  – Quickly adapt to robocalling changes
  – Low risk to network stability
  – Employ Webscale techniques

• Call Processing
  – Measured progress
  – High stability, slow to adapt
  – Implement rules-based call treatments once
    • Call Validation Treatment

Scoring Layer

High Innovation
Lower Risk
Webscale Innovation

Call Processing Layer

Measured Progress
High Stability

Called Party
Adapt: Make the System Highly Configurable
• Goal: Robocalling and fraud threat response with zero design overhead

• Eliminate where possible:
  – Vendor or internal R&D lead time
  – Network and routing design time
  – Software testing and rollout
  – Production risk to core platforms

• Move to:
  – Risk isolated service
  – Field adaptable data lookups and decision criteria
  – Rapid CI/CD development and deployment

• Responsive
  – Configurable in minutes for most evolving threats
  – Scoring systems software rollout every 30 days for new advanced techniques
Core Platforms – Embedded Flexibility

• Minimize Upgrades
  – Support rapid response to changing threats

• Generic Call Treatment Rules and Actions
  – Support multiple scores mapped rules in a hierarchy

• Generic Signaling Mapping
  – Mapping of SIP content to scoring service request
  – Mapping of scoring response to SIP content
• Scoring System Must Be Able To:
  – Add new data sources at any time
  – Add and adjust scoring algorithms at any time
  – Create multiple scores for the same call
  – Support open APIs – compose new things on the fly

• Service Chaining
  – Easily chain in REST services as threats change
  – Designed around “zero development” integration model

• Reputation Data Sources
  – Big Data / NoSQL cloud-scale database
  – Designed for large data sets and frequent data updates
  – Should easily add new data sources from as threats emerge
  – “Zero development” integration model for new data sources
Adaptable Scoring Models

- Global Data Sources
- Custom Request Attributes
- Custom Data Sources
  - Private Tenant Data
  - Federated Data
- Custom Scoring Models
  - Data source weighting
  - ML model training and inference in Identity Hub
- Tenant Specific Exceptions
Automate
Continuous Synthetic Testing

• Fundamental Enabler: Automated testing
• Testing should run 7 x 24 x 365
• Simulate actual service queries and responses
• Measure both service fidelity and response times
• Immediate call out for fidelity defects or SLA excursions
• Input to Blue / Green deployment fall back (next slide)
• Deploy *Software* – Test – Migrate
• Continuous Synthetic Testing
• Pre-testing with synthetic clients
• Controlled Migration
• Automated, unconditional rollback
• Human gates
  – Initial deployment testing
  – At x% of production
Blue / Green Deployment – Used for Configuration Changes

- Deploy Configuration – Test – Migrate
- Continuous Synthetic Testing
- Pre-testing with synthetic clients
- Controlled Migration
- Automated, unconditional rollback
- Human gates
  - Initial deployment testing
  - At x% of production

Managed Config Changes

- Production Clients → WF Prod → SG1v0 → KPI Monitoring & Alerting
- Test Clients → WF Test → SG1v1
- Controlled Migration
- Rollback Automation
Poll Question #2

Of externally hosted services you've deployed, what is your primary motivation?

- Reduced operational expense
- Better able to manage scale
- Speed of new feature deployment
- All the above
How To Get To The New Paradigm?
Deploying Webscale

• Build Out Private Webscale Infrastructure
  – Some Tier 1s are doing this for their 5G infrastructure, inclusive of operations
  – Highly focused on 5G and not ready to apply to existing voice network needs
  – Voice network operations infrastructure and process need to be adapted to Webscale infrastructure

• Outsource to hosted services provider, leveraging Webscale on public cloud
An Example of A Real Deployment

- Session Border Controller + Policy and Routing Server + Hosted Identity Assurance Services

- Upgraded call processing core up to minimum release to leverage:
  - Advanced API capabilities for Reputation Scoring and Secure Telephone Identity (STI)
  - Advanced call validation treatments and flexible signaling mapping

- Subscribed to Ribbon Identity Assurance services
  - Ribbon Identity Hub is cloud-hosted SaaS platform for STIR/SHAKEN and Reputation Scoring services
  - Dynamically reconfigure service as needed to adjust scoring and add new data sources
  - Leverage Ribbon CI/CD process
  - Adopt monthly deployment cadence to capture new rapidly changing scoring challenges
Robocall and Fraud Mitigation Summary

- Embrace a Webscale mentality to keep up and win
- De-risk by decoupling robocall & fraud mitigation from call processing infrastructure
- The bad guys innovate fast; ensure your solution is adaptable by design
- Increase scale, operational efficiency and resiliency by leveraging automation and blue/green deployment
- Yes, you can do this using a hosted services provider
Thank You