Network Protection vs. On-Device Protection

Contrasting and Comparing the Two Ecosystems

Disclaimer:

The following focuses on consumer inbound voice call traffic to a **modern mobile smartphone handset.** Solutions will differ for other endpoints, e.g. IoT devices, traditional landline phones, etc.

Introduction:

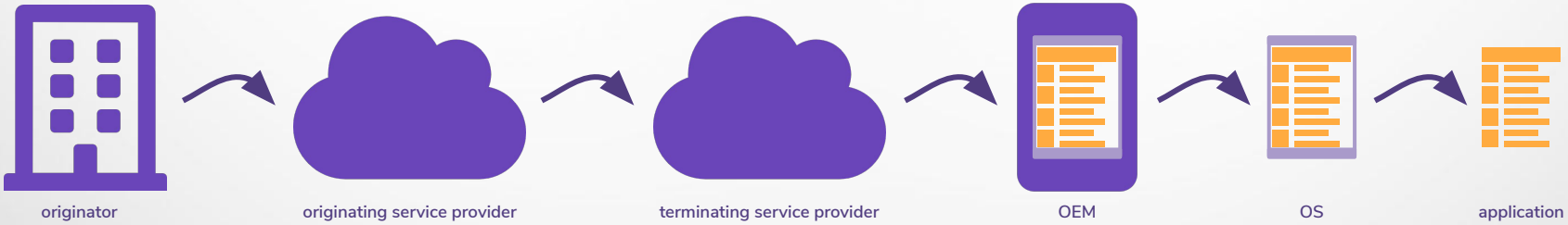
Jonathan Nelson, Director of Product Management,Hiya
Hiya has 100M+ users across call originator, carrier, OEM, and application deployments. Major solutions: AT&T Call Protect, Samsung Smart Call

Overview

Problem: There are more than two ecosystems

Consumers have several choices for voice call spam protection

Solutions are available in many cases across entire infrastructure of a call



Solutions at various points all have advantages and limitations*

* ”Software can do anything”: some limitations highlighted in this presentation could be addressed through creative programming solutions. This overview assumes standard implementation based on existing product trends today.

On-Device App Solutions

Examples: Hiya, Truecaller, Trapcall, etc.

Call analytics offered through 3rd-party mobile application. Runs within standard capabilities and limitations of OS. The capabilities of Android and iOS are extremely different.

The 3rd-party app **does not know the phone is ringing**.

Applications can register a list of phone numbers and a requested identification string or block state.

The OS checks registered lists for incoming call traffic

Block events happen automatically

The 3rd-party application can either request permission to call activity, or register as a Dialer.

With call activity, app can see call activity and draw an overlay on top of user's dialer.

If registered as a Dialer (more difficult), app controls entire incoming call UI directly.

On-Device App Solutions: iOS

Lists in blocks of 2 million numbers registered through CallKit. Can register with identity or with flag to block. Blocked calls are suppressed entirely. Lists must be updated by application when possible.

+ Call blocking prior to phone ring
+ Forced privacy protection of users
+ OS is aware of address book entries

- Static lists only; no real-time intelligence
- List updates hampered by OS app policies
- Consumer unaware of blocked call
- Each 2MM block individually OK'd by user
- No intelligence contributed to detection
- Limited UI, controlled by Apple

On-Device App Solutions: Android

Multiple integration tiers are available depending on engineering effort. Majority of clients surface either via on-screen overlay, or if a Dialer app will be full-screen experience.

+ Real-time lookup, with some r/t signals
+ Rich call UI support
+ “Innovation-rich” environment
+ Access to address book (with permission)
+ Access to user number (with permission)

- Call ID & blocking delayed by lookup
- No true call blocking
- Network signal access limited
- Explicit permissions requests for TN, add. book
- Vulnerable to OS policy changes

Integrated OS Solutions

Examples: iOS call blocking, Google Pixel Dialer, Call Screener

Call analytics or review by the mobile operating system. Generally an extension of manual block features that have been available for a while. Can be processed in advance of call indicators.

+ Best SIP signal intelligence on device
+ True call blocking capability
+ Rich call UI support
+ Easy local data access

- Closed market
- (Android) OEMs can choose to disregard

Integrated OEM Solutions

Examples: Samsung Smart Call, AT&T Call Protect

Call analytics integrated by hardware manufacturer. Lookup is triggered to third-party analytics upon receipt of phone call event. Integrates to native dialer. In mobile world, limited to Android only.

- \+ Rich call UI support
- \+ Lowest barrier to entry of all opt-in solutions
- \+ Direct address book access under ToS
- \+ Direct user TN access under ToS
- \- Call ID & blocking delayed by lookup
- \- SIP intelligence filtered by OS

Terminating Service Provider Solutions

Examples: AT&T Call Protect, T-Mobile Scam ID

Performs analytics and call disposition at the network level, before engaging with consumer hardware at all. Must send necessary details to device for display to consumer.

+ Immediate deployment to users (no device sw)
+ Immediate updates e.g. enable auto-block
+ Works for private callers
+ Minimum service latency
+ Operating system agnostic
+ Full SIP signal intelligence capabilities
+ Genuine call blocking capability

- No address book
- Limited to single text field
- OEM may favor local service, or address book
- Consumer unaware of blocked call

Clients in a Supporting Role

Examples: AT&T Call Protect

A TSP solution can be supported/enhanced with device-side software. This can be either a standalone application, or integration with OEM for richest out-of-box experience

+ All the benefits of network-level solution
+ Adds richer on-device experience
+ OEM partnership means no software install
+ Creates opportunity for user feedback
+ Adds visibility into blocked calls

- Double-point solution adds complexity

Originating Service Provider

The OSP can help by both declining known fraud calls from being created in the first place, and/or to pass along suspicions downstream.

+ Reduces overall unwanted traffic for network
+ Earliest possible signal for fraud calls

- Recipient has no control, visibility
- Logical for fraudulent activity only

What about the Originators?

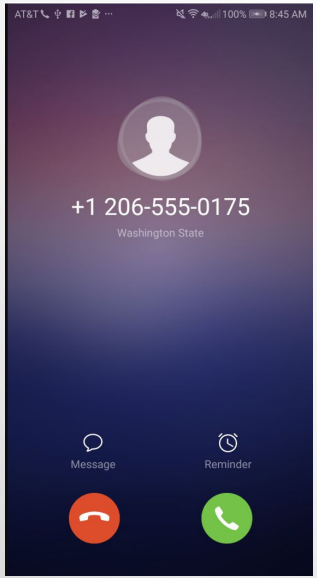
Examples: Delegated Certificates, Hiya Connect

The call originators can play a role in solutions as well. High-value targets can support confirming their own traffic, to stop the fraudulent calls.

+ Originators take control over number activity
+ Can be paired with identity validation
+ Out-of-band solutions can work now

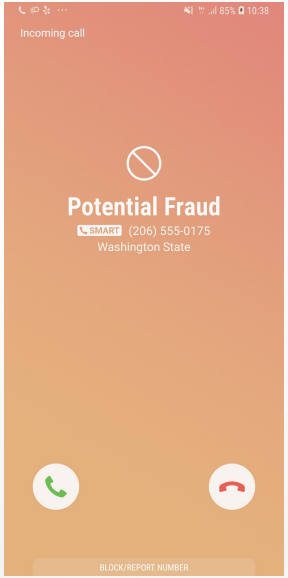
- Only works one originator at a time
- Limited to impersonation spoofing

Side-by-Side Comparison

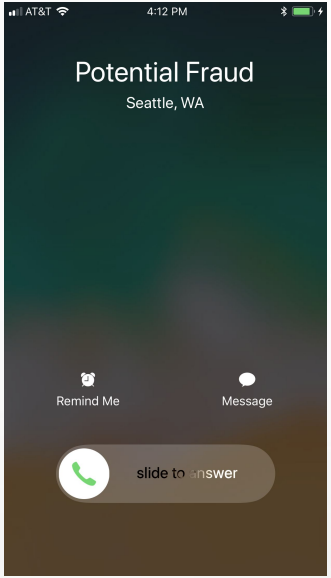


Nothing

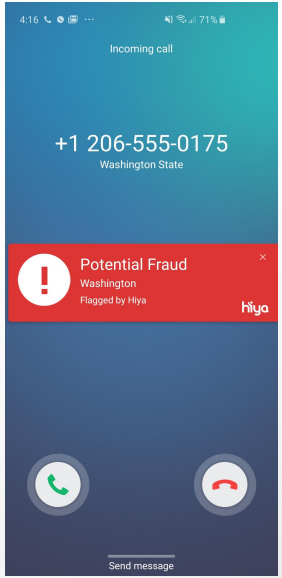
Network-Level



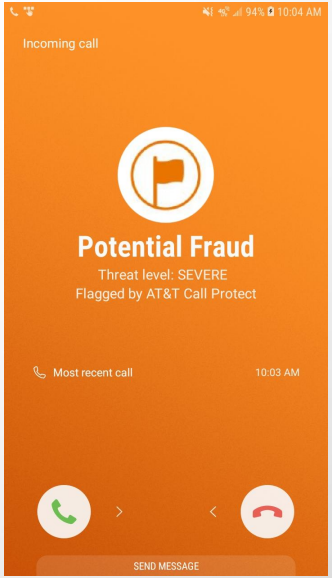
OEM Integration



App (iOS)



App
(Android Overlay)



App*
(Android Dialer)

*Image is OEM integration, but experience is similar

On the Horizon

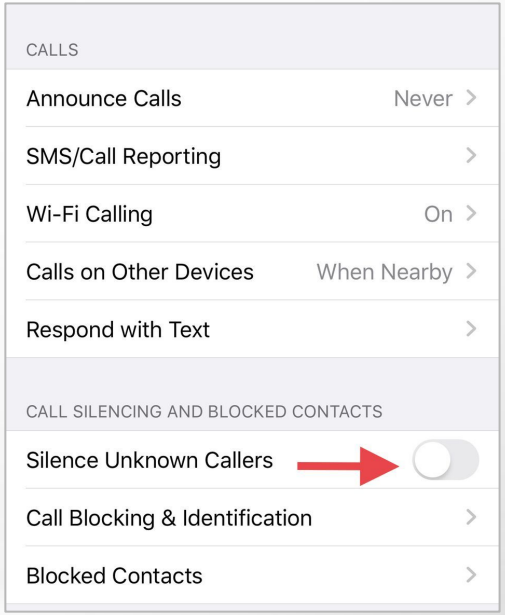
Ensure OS, OEMs are motivated to expose STIR/SHAKEN signals to app ecosystem

OS platforms may consider service integration options for user

Network solutions improve on-device experience through eCNAM/RCD

Decent call blocking of fraud behavior shifts focus to identification, not protection

In a race before call industry becomes the “voicemail industry”



“Screw it, just block everybody.” -iOS 13

hiya