Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 15, Issue 4

Advanced Analytics to Combat Robocalling

By: Paul Florack

The Federal Trade Commission (FTC) received 4.5 million robocall complaints in 2017, up from 3.4 million the prior year. This significant increase helps to explain why the robocall epidemic is squarely in the crosshairs of wireless and wireline operators, regulators and legislators, technology vendors, and, of course, consumers.

The FTC and Federal Communications Commission (FCC) have been working with the telecommunications industry to encourage solutions to stop robocalls for several years. Illegal spoofed robocalls, where the caller name and telephone number is faked in order to deceive the call recipient, have drawn particular attention. Key to the industry's response has been the development of call authentication technology known as STIR (Secure Telephony Identity Revisited) and SHAKEN (Secure Handling of Asserted information using toKENs).

STIR was originally created four years ago by the IETF (Internet Engineering Task Force).

ATIS (The Alliance for Telecommunications Industry Solutions) and the SIP Forum joined and created a task force, the IP-NNI, to deal with number portability, among other concerns. SHAKEN was a direct result of their interface as a task force. STIR/SHAKEN is now an FCC call authentication framework, overseen by both the chairman and the wireline competition bureau, that provides verified information about the origin of calls by enabling service providers to sign and authenticate information in the SIP header related to the origin of calling numbers.

STIR/SHAKEN employs the same type of public/private key structure that has been used on the Internet for a decade to prevent the spoofing of website addresses. The schema filters out spoofing by requiring a public/private key handshake in order to successfully authenticate a call. This practice is currently limited to domestic SIP-to-SIP calls, which are uninterrupted along the network path.

Nonetheless STIR/SHAKEN will undoubtedly provide a key foundational layer in attacking bad actor robocalls. However, it is also certain that a layered approach to the bad actor robocall threat will continue to be required. Based on our own analysis of more than 1 billion network events every day and our broadview across the public switched telephone network as a signaling, IPX and routing hub for over 500 providers, we believe there are a handful of key components for carriers and other stakeholders to consider as part of an effective multilayered approach:

Call authentication does not address call intent

If those whose work has been focused on detecting and addressing nuisance and illegal robocalls know one thing, it is that bad actors change tactics quickly. STIR/SHAKEN authenticates that a call has not been spoofed, but it does not determine caller intent. While call authentication is an important component of rooting out bad numbers, bad actors may still make these calls by registering numbers which, while registered to the callers, are authentically theirs.

For example, relying solely on STIR/SHAKEN, a call originator with an authenticated number could claim to be an IRS representative when in fact it is a bad actor attempting to steal the call recipient's personal information or money. So while the call originator isn't spoofing the number and won't be able to use the same unauthentic spoofed number over an extended period of time, the originator can still be effective by changing tactics. It is entirely possible that bad actors will register blocks of numbers, make fraudulent calls, burn through the numbers quickly, drop them, get a new set of numbers and start the process again.

Questions remain with STIR/SHAKEN

There are indeed numerous questions related to STIR/SHAKEN implementation. Examples include: How secure is the computer storing the private key? How are certificate recipients validated? What happens after call validation? How is the public educated about initiating a traceback? Where will post-call reporting take place? How are tracebacks enforced? Can a private key be intercepted and misused? How are keys revoked? What happens when a number is ported? What's the time-to-live (TTL) for a certificate, and can it be extended via a hack? How are third parties making legitimate calls on behalf of an enterprise authorized to spoof their caller name and number? What must operators buy and deploy? When will it be available? How much will it cost? How, if at all, do we recover the costs of implementing a strategy? What will our liability be if we block a good call or authenticate a bad call?

STIR/SHAKEN is indisputably an essential foundational layer to combat spoofing and other robocall tactics, which is why large carriers are rightly investing in deploying the STIR/SHAKEN authentication standard in their networks as they move towards initial operational capability in 2018–2019. However, we are unlikely to see an all-IP network for several years, which means that carriers should maintain both a short- and long-term focus and expect that bad actors will focus on all available paths leading up to widespread network implementation.

Layered analytics are key

A better understanding of the intent of a call is the work of the real-time analytics layer (i.e., the analytics server). Further, depending on the provider, the analytics server is available for all types of carriers across all networks, whether VoIP or TDM, via ENUM, SIP, AIN, or RESTful API, or all of the above. This layer is already in play today with the major carriers on many devices.

Advanced machine learning methods for blocking robocalls using real-time AI in combination with big data gleaned from the network addresses the constantly changing identities of robocallers. This methodology makes it possible to create an algorithm which can detect call patterns without requiring crowdsourced reporting.

Machine learning is a method used to devise complex models and algorithms that lend themselves to predictive analytics. The analytical models allow data scientists to produce reliable and repeatable decisions while also uncovering hidden insights through learning from historical relationships and trends in the data.

As an additional input to this model, crowdsourced feedback allows the analytics provider to layer in context. By supplementing the unstructured data provided by the machine learning methods,

crowdsourced data allows the analytics layer to provide information at a more granular level, such as whether a telephone number is being used to claim to offer free cruises, or is a legitimate call from a bank with a fraud alert related to a credit card.

Today, it is possible to detect caller ID spoofing and other malicious and nuisance robocalling behavior based on real-time network data analytics. STIR/SHAKEN will eventually remove some of the burden borne by analytics servers today, but will not render this crucial component unnecessary.

Enforcement and follow-through is required

The FCC continues its exploration of methods to pursue bad actors, including blocking and tracebacks, and seeks the industry's help in its latest public notice to refresh the record on advanced methods to target and eliminate unlawful robocalls. Carriers and other industry experts involved in solving the robocall problem will be providing more detail about their approaches. Naturally, STIR/SHAKEN will play a significant role with respect to blocking and traceback efforts.

In addition, analytics providers will be explaining the complex role they play in overlaying context for robocalls that do not involve spoofing, and will be providing the FCC with further insights regarding additional steps that can be taken to address this ongoing problem. The industry will be looking to the FCC for guidance and support as we seek to further differentiate good calls from bad. Further, we will seek ways to support the FCC by onboarding data from vetted outbound callers and facilitating traceback efforts.

For now, it is encouraging to see this problem coming into greater relief as the industry works together to reestablish trust in calling.