How to Shut Down Robocallers

The STIR/SHAKEN protocol will stop scammers from exploiting a caller ID loophole

By JIM McEACHERN & ERIC BURGER

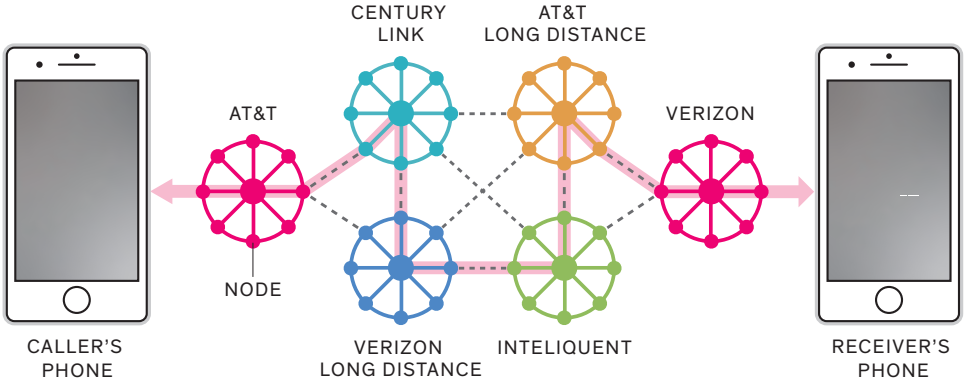
Have you ever received a phone call from your own number? If so, you've experienced one of the favorite techniques of phone scammers. • Scammers can "spoof" numbers, making it seem as though the phone call in question is coming from a local number–which can include your own–thereby obscuring the call's true origin. If you answer the call, you'll most likely be treated to the sound of a robotic voice trying to trick you into parting with some money. • One of us (McEachern) is a principal technologist for the standards organization Alliance for Telecommunications Industry Solutions (ATIS), and the other (Burger) was until recently the chief technology officer for the U.S. Federal Communications Commission. But you don't need us to tell you that robocalls are a pandemic. According to a report by the caller ID company Hiya, there were 85 billion robocalls globally in 2018. ➔

PHOTOGRAPH BY Dan Saelinger


2:52
Spam Risk
Remind Me
Message
Decline
Accept

Call for Directions

CALLING A FRIEND isn't as simple as transmitting data from point A to point B. Along the way, the call is routed through telephone infrastructure that may be operated by two, three, or more phone companies, or carriers. These routes are part of the reason it's so time consuming to identify the points where scammers place their calls.



RoboKiller, one company that has created an anti-spam-call app, estimates that Americans received 5.3 billion robocalls in April 2019 alone, or nearly 4,000 every second. And not only are scam calls annoying, they're costly. In 2018, phone scams tricked Americans out of an estimated US $429 million. Sadly, these numbers are on an upward trend.

Spoofing phone numbers is just one way phone scammers trick their victims. Scammers are also very good at reading people, gaining their confidence, and playing to their fears. But spoofing numbers is an often-effective opening gambit. The first thing a spoofer has to do is get someone to pick up the phone in the first place, and people are more likely to answer a call if they think it's from a local number. So, preventing the abuse of call spoofing, along with making it much harder for anyone to place huge numbers of robocalls, are two of the most important challenges to reining in robocallers and scammers.

The telecommunications industry has been developing a network-based system that would meet both of these challenges. It goes by an unwieldy name: "Secure Telephone Identity Revisited/Signature-based Handling of Asserted information using toKENs." Let's just call it STIR/SHAKEN, which is a lot easier to remember. STIR/SHAKEN is a technique for providing more reliable call-display information by closing a loophole that scammers exploit in telephony infrastructure.

Today, when you make a call, your phone company, or carrier, knows whether or not you're spoofing your number to make it appear that the call is coming from a different number. But what the company doesn't know is if you're *allowed* to spoof that number, nor does it have a way to securely send that information to the carrier delivering the call to the person you're calling (there are legitimate reasons why callers might spoof their numbers; more on that in a moment).

The upshot is that when you see the number of an incoming call, you have no way of knowing if the number displayed on your caller ID is legitimate or spoofed. STIR/SHAKEN will give phone companies a secure method of communicating a caller's number to a recipient when a call is placed. This capability is vital to establishing the caller's reputation so that scammers and other bad actors can be reliably identified and blocked before you waste any time on the bogus call. And should an illegitimate robocall still get through, STIR/SHAKEN simplifies the process of tracing a call back to its source. Hopefully, simpler tracing will make it feasible for law enforcement agencies to prosecute scammers for illegal robocalling. The technology will also securely provide information to call-blocking apps, allowing the apps to more accurately identify spam calls and inform you with a notice such as "Spam likely" or "Unverified number" before you answer a call.

If it all works out, robocalls could become as manageable as email spam. You'll be less likely to be tricked into answering a scam call, and you'll receive far fewer in the first place.

SPOOFING NUMBERS ISN'T NEW—it's been possible for half a century. Telephone switching equipment known as private branch exchanges (PBXs), which many businesses use, preassign the number that will be displayed on the recipient's phone when it receives a call from the business. There are legitimate reasons for businesses to spoof numbers. For example, they may want to display a toll-free number for calls from the marketing, sales, or service departments. Women's shelters are another example of the need to disguise numbers, as they often replace the shelter's actual number with a national number to avoid tipping off a domestic abuser.

The problem is not spoofing itself. The problem is that in the last decade or so, three things have changed to create the mess we see today.

First, phone calls are a lot cheaper. In many countries nowadays, unlimited nationwide calling is standard in basic phone plans. Second, the Internet has reduced the costs of running a scam to almost nothing. The PBX of choice for fraudsters is an Internet-enabled IP-PBX to further lower the price per call. With the Internet, scammers don't even have to be in the same country to place

ILLUSTRATION BY Mark Montgomery

robocalls, and they can use live agents in countries with low-cost labor. Third, anyone can place hundreds of calls per minute with the small investment of an inexpensive PC, a hundred-dollar Voice over Internet Protocol (VoIP) expansion card, free open-source software, and a few days of assembly.

Put it all together and you have the recipe for a potentially lucrative business with very low risk. These scammers are fundamentally playing a numbers game: While most people won't answer their calls, a small percentage will, and some of those people can be conned into sending money or revealing their bank account information. Robocall scams are so cheap that even one success among hundreds or thousands of calls can still make scammers money. The Internet can cheaply connect a U.S.-based IP-PBX making hundreds of calls per minute with call agents in another country to talk to any victims who fall for the spoofed call. Meanwhile, the carrier has no way of knowing that this is an illegal robocall operation until unsuspecting victims complain. Only after receiving complaints is the carrier aware that it should trace back the calls and identify the illegal caller.

Before STIR/SHAKEN, individual phone companies did not have all the information needed to identify and stop a scam, because it often takes two or three companies to complete a call. The last company in the chain, which completes the scammer's connection to your phone, doesn't know if the number has been illegally spoofed, so it can't advise you to use caution or ignore the call. The scam emerges only when you answer the call and discover that it isn't really the tax collector on the other end of the line.

DESPITE THE JAMES BOND theme, the STIR and SHAKEN technologies don't by themselves constitute a license to kill robocalls. Instead, the goal is simply to communicate, securely and in real time, information between the phone companies on each end of a phone call.

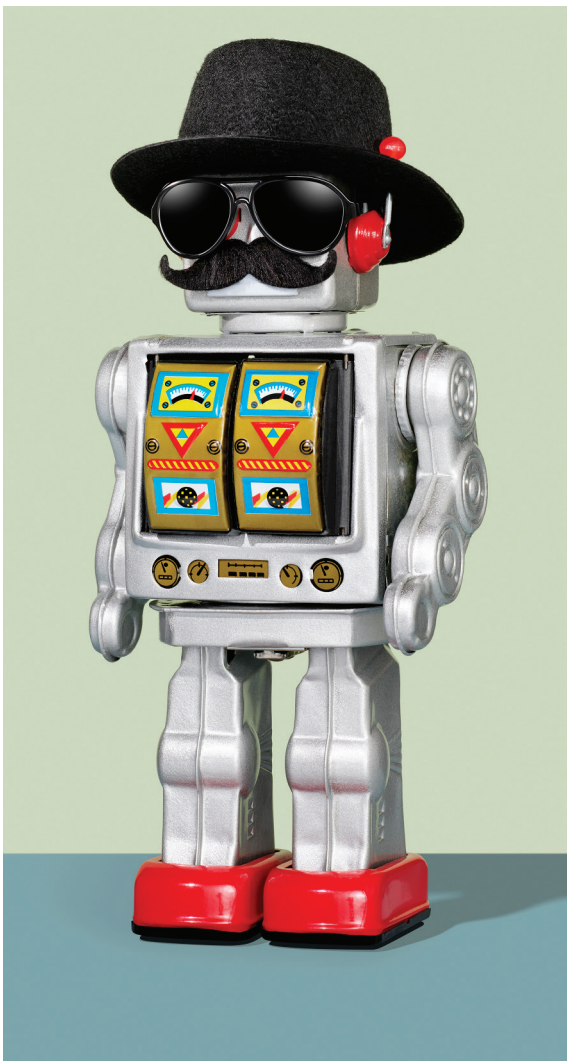
The Internet Engineering Task Force (IETF), which works on issues related to secure telephone identity, began work on STIR in 2013. The IETF designed the STIR protocol to be very flexible. The basic mechanism is a certificate issued to authenticated callers. However, STIR requires individuals to be proactive about authenticating themselves and managing their personal key, which confirms their identity. STIR's downside is that very few people have the expertise to do either. The good news is that STIR's flexibility allows phone companies to implement it in their network with minimal hassle.

In 2015, ATIS also began studying mechanisms to reduce unwanted robocalls. A joint task force between ATIS and the SIP Forum, an industry association, built upon the IETF's work on STIR.

As it turned out, STIR's extreme flexibility was a problem. Indeed, the protocol's flexibility made it easy for each phone company to implement it in its network. However, as a general rule, the more flexible a protocol is, the more likely it is that different implementations won't play well together. So when two different service providers implement the protocol on each of their networks, a caller ID sent from one to the other might not make it through intact. The task force's goal was to create a precisely defined subset (known as a profile) of STIR, called SHAKEN. Because the task force specified the SHAKEN profile of the STIR protocol, you might see it referred to as "STIR/SHAKEN."

SHAKEN starts with the information that the originating phone company—the carrier—knows about the call. For example, mobile phones and residential landlines transmit their phone numbers whenever they originate a call. For businesses, where legitimate spoofing is commonplace, the carrier also assigns to the call a unique key, called an "orig-id," or origination identifier, in order to identify the business placing the call. In all cases, the carrier creates a digital signature using the available information and transmits it with the call. The caller ID information is included within this digital signature. The phone company completing the call verifies the digital signature to confirm the information hasn't been modified, and then identifies the originating carrier. This last step allows spoofed calls to be linked to their source for call-blocking apps and law enforcement.

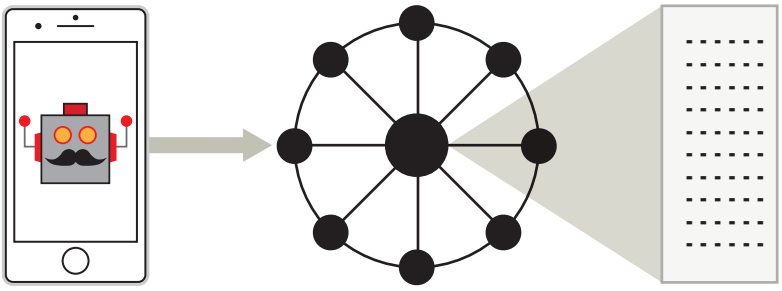
SHAKEN's contribution is to take what the originating phone company knows about the caller, courtesy of the digital signature, and classify that knowledge succinctly. So one of the biggest challenges the task force faced early on during SHAKEN's development was deciding which information was actually important. Including too little information in the classification would mean that important details would be



PHOTOGRAPH BY Dan Saelinger

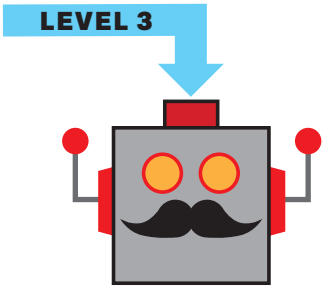
How STIR/SHAKEN Tracks Down a Scammer

When a carrier rolls out STIR/SHAKEN, the only change its customers will notice is a message on their caller ID screens warning of a potential scam call. But there's a lot more going on behind the scenes when a scammer places a robocall. Here's how STIR/SHAKEN keeps everyone involved informed about whether a call is worth answering.

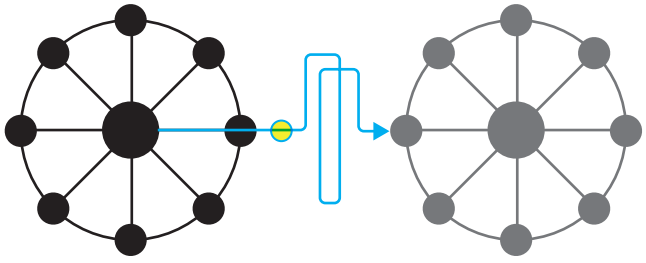


1. A scammer starts up the robocalling equipment and begins placing calls.

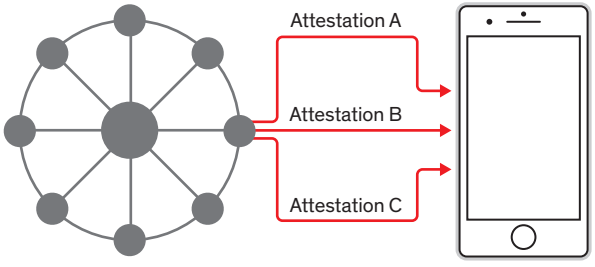
2. The scammer's own carrier logs each robocall's entry point—the device used and its physical location—into the telephone network.



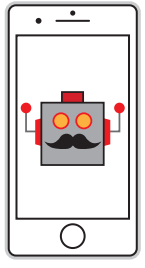
3. The carrier also assigns an "attestation level" (A, B, or C) to the call based on what the carrier knows about the caller.



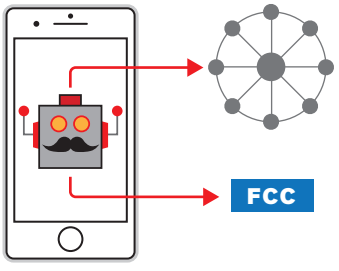
4. The carrier encrypts this information and sends it through the network, alongside the call itself, to the call receiver's carrier.



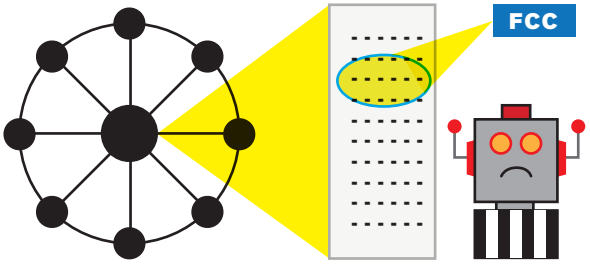
5. Using the assigned attestation level, and taking into account previous complaints about calls from the same network entry point, the carrier determines the caller's reputation as a likely scammer.



6a. The call recipient avoids picking up a phone call from a probable scammer.



6b. If the recipient answers a scam robocall, they can report the robocaller to their carrier and the authorities.



7. The recipient's carrier, and the authorities, can trace the call back to its origin using the entry point logged by the first carrier, allowing for prosecution.

ILLUSTRATION BY Mark Montgomery

lost, such as the distinctions among individual businesses in a single building. Too much information would create clutter and make it more difficult to zero in on the data that's important. For example, you don't need to know whether a caller is using a landline or a mobile phone to determine whether they're illegally spoofing a number.

The solution was a three-level system to categorize the essential information about the caller into levels of "attestation" for the call. These attestation levels characterize a caller's right to use a particular number. Full attestation, also known as "A-attestation," has several requirements but provides the highest level of confidence by the originating carrier. The call originates on the carrier's own network, as opposed to originating from another carrier or a VoIP provider. The carrier has also directly authenticated the caller and verified the caller's right to use the number. This way, SHAKEN still allows for legitimate number spoofing, but only if the carrier knows the customer has the right to spoof that number.

Partial attestation, or "B-attestation," indicates that the originating carrier cannot verify enough information about the caller for the carrier to vouch that the caller is using its assigned number. The call still originates on the carrier's network. The carrier still authenticates the caller but does not verify the customer's right to use the number that's being displayed. It's possible that the customer is using the number legitimately, but the carrier hasn't verified it. There are valid reasons why a customer might be using a number that hasn't been verified. A business might have swapped carriers but kept its original toll-free number, for example.

Gateway attestation, or "C-attestation," indicates the lowest level of confidence. The call starts on some other carrier's network that hasn't implemented SHAKEN. Because the carrier doesn't know the customer or whether it has the right to use the number that is associated with the call, the carrier merely identifies the call's entry point into its network. Gateway attestation may not carry a lot of confidence about the caller's identification, but it can still be useful in tracing calls to quickly identify the source of problems.

Identifying a call as spam can happen only once a call is placed. This limitation highlights a key difference between phone calls and email, and helps explain why we've had spam filters for years while SHAKEN is only now emerging to help identify illegitimate voice calls. Spam filters scan email before delivery to compare the content against known scams. These filters are not perfect, but they're good enough to hold email spam down to tolerable, if still slightly annoying, levels.

That's not possible with a telephone call—it's not really feasible to disclose the content of a call before it's connected. SHAKEN does the next best thing, by making it possible to easily track calls from the point where they physically enter the network (more on that shortly) and then establish a caller's reputation. Reputation is determined in large part by the level of attestation callers receive from carriers. Reputation is also determined by connecting callers to their orig-id, so that over time less-reputable callers may be identified by the number of complaints made about that caller. If the carrier knows a call is originating on its own network and the caller has the right to use the number—and the carrier has not received complaints about that caller—then, generally speaking, the carrier can be more confident the caller is not a scammer. By being able to identify less-reputable calls as they are placed, SHAKEN makes it possible to confidently label a call as spam before it is answered.

ONE CRITICISM OF SHAKEN is that it cannot indicate whether a call is a scam based on whether or not the number is legitimate. A call with "full attestation" can potentially still be a scam. Fraudsters can often gain access to fully verified numbers for short windows of time, and then vanish by the time anyone realizes they're using those phone numbers. That's why SHAKEN has also been designed to simplify the call traceback process.

Traceback is exactly what it sounds like: It's a process that begins with the person receiving the call, tracing the call back through carriers to the person or organization that made the call. In the United States, the United States Telecom Association currently leads an industry traceback initiative to identify the origin of illegal calls. Traceback is largely a process of scanning call-detail records to correlate a call coming into carrier A with a call going out from carrier B, and then repeating the process for as many carriers as necessary to reach the person or business that placed the call. The process is now semiautomated, but it's still a complicated, multistep process.

SHAKEN simplifies traceback, turning it into a one-step process no matter how many carriers have been involved in the call. The same digital signature that authenticates a call's orig-id and attestation level identifies exactly where a problem call entered the network. This

What Carriers Know

Phone companies don't always know everything about a call. STIR/SHAKEN uses levels of attestation so that carriers can classify what they do know about each call.

A–ATTESTATION	B–ATTESTATION	C–ATTESTATION
Originates on carrier's own network	Originates on carrier's own network	Originates on some other network
Carrier has confirmed who the caller is	Carrier has confirmed who the caller is	Carrier has NOT confirmed who the caller is
Carrier has verified caller's right to use the phone number	Carrier has NOT verified caller's right to use the phone number	Carrier has NOT verified caller's right to use the phone number

method simplifies the process of tracing illegal calls, and will enable authorities to investigate many more complaints in the same amount of time. In the United States, for example, enforcement is handled by the Federal Trade Commission (FTC), the FCC, the FBI, and state and local law enforcement. The agencies should have an easier time coordinating their efforts with a simpler traceback tool.

It's also possible that a less-legitimate carrier could be tempted to solicit illegal robocalls. After all, the carrier would still be paid for the service by the caller. Simpler tracebacks make it easier to spot a pattern if, for instance, one carrier is hosting a lot of illegal robocalls. While mainstream carriers have no interest in hosting robocalls, SHAKEN removes the small temptation that fly-by-night carriers might have to make money by soliciting these callers.

SHAKEN's digital signatures also provide hard evidence of the source of illegal calls, making successful prosecution easier. In June, the FTC announced that the agency had filed 145 cases to date against illegal robocall operations. Of course, those 145 cases predate SHAKEN. It's not a large number, although the FCC, for its part, did go up against some big players, including one man, Adrian Abramovich, who made over 100 million robocalls and was fined US $120 million. SHAKEN won't stop robocalls directly, but it will be an important tool in identifying, locating, and prosecuting illegal robocallers and those who support them at a far greater rate. Given time, SHAKEN should have a huge impact on how many robocalls scammers can get away with, and how many new actors attempt to start their own scams.

That said, scammers are nothing if not resourceful. They will find a new weakness to exploit, just as they've exploited a loophole for call spoofing. When weaknesses are discovered—and it is a question of *when*, not if—SHAKEN must be adjusted quickly to patch the vulnerability.

SHAKEN is being deployed in the United States and Canada independently because the current specifications consider only how the protocol operates within a single country. It's our hope to extend it internationally. That's important because, as we've mentioned, scammers often place robocalls internationally using the Internet. The task force that developed SHAKEN has already begun working on expanding the protocol so that carriers in one country can verify calls that have been digitally signed in another country. As robocalls are brought under control in the United States and Canada, illegal robocallers are likely to attack citizens and businesses in other countries.

AS YOU READ THIS, calls are already being signed and verified across live networks by major carriers in the United States, with Canada following in 2020. So you can now relax, knowing you'll never be bothered by a robocall again, right?

Unfortunately, SHAKEN can't completely stop robocalls on its own. It's a tool that can be used by call-blocking apps to reduce the number of unwanted calls. It will also help differentiate between legitimate calls and illegal calls, so users will be less likely to be taken in by scams. In addition, SHAKEN makes it much faster and easier to find and sanction illegal callers.

And it bears repeating that when SHAKEN begins to reduce illegal calls, scammers won't just give up. The industry will need to be vigilant to understand robocallers' latest tricks for avoiding SHAKEN and will need to regularly adjust the way the protocol is used to close the gap.

STIR/SHAKEN will make a difference. Not overnight, but over time the number of illegal robocalls scammers place, and the calls' effectiveness, will decrease. The user experience will be like that of email spam. At one time, experts predicted that email would become useless because no one would be able to find the real email among all the spam. But the industry deployed a variety of anti-spam measures, and eventually the situation improved. Email spam didn't go away (you still have a spam folder, after all), but it has minimal impact. SHAKEN will provide the first step for a similar assault on unwanted robocalling. ■

↗ POST YOUR COMMENTS at https://spectrum.ieee.org/robocalls1219