TESTIMONY OF HENNING SCHULZRINNE
Levi Professor of Computer Science and Electrical Engineering
Columbia University

SENATE AGING COMMITTEE

"Ringing Off the Hook: Examining the Proliferation of Unwanted Calls"

June 10, 2015

Chairman Collins, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to appear before you today. My name is Henning Schulzrinne, and I am the Levi Professor of Computer Science and Electrical Engineering at Columbia University in New York. I was the Chief Technologist at the FCC from 2012 to 2014 and currently serve as a consultant to the FCC. I am testifying in my private capacity and my views do not necessarily reflect those of the Federal Communications Commission. I am pleased to join you to discuss technological issues and potential solutions surrounding robocalls and spoofing.

Robocalls & Spoofing – Causes and Technical Approaches

Types of Illegal Robocalls

There are many types of robocalls, some overlapping:

- *Consumer fraud*, with the caller offering non-existing or fraudulent services or goods, such as bogus computer tech support, extended warranties, fraudulent charities or cruises. For the tech support case, the caller may install keystroke logging software to obtain personal information or install ransomware. Callers may also resell credit card data provided by the victim.
- *Extortion,* where the caller threatens the called party with deportation, arrest or prosecution if they do not wire money to settle a fictitious tax debt (*e.g.*, "IRS scam"[1]).

[1] http://www.consumer.ftc.gov/blog/scammers-continuing-pose-irs-agents; http://www.irs.gov/uac/Newsroom/IRS-Repeats-Warning-about-Phone-Scams ("Based on the

- "*Swatting*", where false 911 calls claim a crime is in progress.[2]
- *Telephony denial-of-service attacks* where a large volume of calls overwhelms small call centers, such as public safety answering points (911 call centers), medical facilities, nursing homes or hotels, blocking all other incoming calls.
- *CNAM fraud* where the caller collects a fraction of the dip fees from CNAM database operators when the terminating carrier queries for the caller name. (Terminating carriers typically pay a small fee, such as $0.005, for each number lookup to the CNAM database.)
- *Premium rate fraud* where the caller leaves a message ("you have won a prize") to entice the called party to return the call to an international number incurring high toll charges.

Spoofing Caller ID and Caller Name Facilitates Robocalls and Other Fraud

Caller ID spoofing is used for several purposes:

- By changing the originating number, robocallers can evade filters and black lists (i.e., a set of consumer-chosen phone numbers from which the consumer does not want to receive calls), including such on-line lookup services as http://800notes.com/. This also facilitates telephony denial-of-service.
- Falsified caller ID information can also facilitate impersonation (*e.g.*, when calling a bank or utility[3]) or to gain access to voicemail.
- Caller ID spoofing can also be used to easily obtain the caller name for a particular number, even if the caller decided to suppress the information for privacy reasons.

The Nature of VoIP Services Facilitates Robocalling and Spoofing

The widespread availability of commercial VoIP services has facilitated both robocalls and number spoofing. VoIP services are cheap to set up and have low per-minute costs. Calls placed to the U.S. cost the same whether they originate within the United States or in another country since the originator only has to pay for local Internet access and the VoIP gateway fee. (VoIP calls travel to the country of destination via the Internet and are then handed off to gateway service providers that interconnect with the traditional phone system.)

All it takes to generate false caller ID information is a configuration of a suitable open-source or commercial call generation platform or VoIP private bank exchange (PBX), which is a private telephone network used within an enterprise. Such platforms are now widely available and can be installed in any commercial cloud-hosting service. These cloud services are often available with no more than a credit card, possibly stolen or acquired anonymously for cash at a local convenience store. Calls are typically routed through multiple VoIP call handling services before they end up at a VoIP gateway that translates them to traditional, circuit-switched calls. It is quite common that the same PBX originates calls from many different phone numbers, e.g., if it serves as a virtual PBX for a number of local branches of a chain restaurant or resells services to small businesses.

90,000 complaints that TIGTA has received through its telephone hotline, to date, TIGTA has identified approximately 1,100 victims who have lost an estimated $5 million from these scams.")

[2] http://www.wzzm13.com/story/news/local/coopersville/2015/01/20/family-of-boy-convicted-in-school-swatting-it-ruined-our-life/22070055/, http://www.ktul.com/story/27859162/western-oklahoma-police-chief-shot-while-investigating-bomb-threat

[3] This is sometimes call "vishing," an analogy to "phishing."

While robocalls probably differ statistically from legitimate calls, the variation among legitimate calls is sufficiently large that it is hard to filter out "bad" calls reliably. The amount of information is far more limited than the type of information available for credit card payments, where the credit card processor knows about the payment history for its customers, gets information about the nature of the transaction and knows the location of the merchant. If a telemarketer spoofs a random phone number, the downstream VoIP provider or large carrier has no way of knowing what kind of calls are typical for that number since the number is most likely not a customer. Also, by the time robocalls reach one of the larger providers, they are typically part of a large aggregate of calls, including legitimate, human-dialed consumer and business calls, legitimate automated call services and illegal robocalls. Thus, it is often difficult to reliably distinguish "good" from "bad" calls, without blocking an unacceptably large fraction of good calls. Carriers could still track complaints for specific originating numbers and refuse to do business with entities that generate an exceptionally large number of robocalls complaints relative to their call volume, but spoofing makes such tracking harder.

Preventing Spoofing is Helpful, but Not Sufficient, to Reduce Illegal Robocalls

Preventing illegal robocalls from reaching consumers requires two fundamental operations: (1) identifying unwanted calls reliably; and/or (2) allowing consumers to block or redirect ("filter") such calls. Some of the technology solutions that facilitate both identification and filtering is described below. If robocallers spoof their caller ID, they can easily bypass call filters. It is true that currently, many illegal robocalls do not spoof their caller ID (presumably so that the called party can return calls when the robocaller could only reach voicemail), but illegal telemarketers may increase spoofing as call filtering becomes more effective.

Spoofing CNAM

Fraudsters may use the current CNAM (caller name) system to their advantage even if they do not spoof the phone number itself. In the current system, the carrier delivering the call to the consumer (*i.e.*, typically the local phone or cable company) queries one or more industry databases to map the caller ID information to a name. The call setup request currently only contains the number, not the name. CNAM is decentralized - many database services operate number mapping services - and some of these services appear to apply little scrutiny to the textual information that is added for a specific number. For example, these services do not always check whether the business name is a trademark of another company or corresponds to the name filed with the Secretary of State or Department of Commerce in the state the business is located. Thus, a tax debt extortion scam might associate a name like "Internal Revenue" with their number if they want to look more convincing to their victims. (In general, there does not appear to be a comprehensive list of CNAM database services; they are not registered with the FCC, for example.)

Technology Solutions to Reducing Robocalls

In my opinion, there are at least eight technical solutions that, individually and in combination, can reduce robocalls:

1. Filters based on simultaneous ringing
2. Smartphone apps
3. Number signing and validation
4. Improved caller name validation

5. Consumer filters
6. Carrier filters
7. Do Not Originate
8. Honey Pots

I will describe each in turn, summarizing their operations, effectiveness, privacy, applicability, and trade-offs.

Filters Based on Simultaneous Ringing

Operation: A consumer configures their phone service to simultaneously ring all of their calls to a third-party service provider, such as Nomorobo.[4] The service provider sees the incoming call; if the number is in the user's white list, the service provider takes no further action and the subscriber picks up the call. If the call is on a black list, it picks up the call and then hangs up. For unknown callers, the service may challenge the caller to enter some numeric code as a CAPTCHA, forcing the caller to prove that it is human rather than a robot.

Effectiveness: Like many of the other filtering approaches discussed below, this approach relies on crowd sourcing (*i.e.*, users indicating whether a call was unwanted or not). Thus, this type of system becomes less effective as more robocallers spoof their caller ID.

Privacy: By its nature, the third party has access to every inbound call reaching the user.

Applicability: The system requires the cooperation of the carrier and only works for certain types of modern VoIP-based landline systems landlines,[5] such as those provided by cable companies, but not cellular services. Older landline systems may not support simultaneous ringing or carriers may choose not to enable the feature.

Trade-offs: This approach has the advantage that it works today, without modifying existing systems. However, since caller ID information is provided after the first ring, all robocalls still ring once at the subscriber. Spoofed calls may fool the system.

Smartphone Apps

Operation: A user installs an app on their smartphone. The app[6] monitors incoming calls and terminates blacklisted calls, redirects a call to voicemail or flags a call as a likely robocall.

Effectiveness: The effectiveness is similar to other filtering approaches. Since users have a choice between multiple apps, apps can compete on their effectiveness, including preventing the blocking of wanted calls. They may offer different degrees of filtering (*e.g.*, to allow a user to avoid all charity calls). Reviews on the Google Play Store for apps of this type are mixed and they do not appear to work in all cases. Apps typically require payment for access to the blacklist.

Privacy: Apps may differ in what information they convey to the app vendor. If the app queries the backend service for each call, that service now has a complete incoming call log. There are approaches ("Bloom filters") where the app itself would store some number of blacklisted numbers and thus avoid querying the service.

---

[4] See https://www.nomorobo.com/.

[5] For example, Nomorobo stated that its system is operational with AT&T UVerse, Comcast Xfinity voice, Optimum, Time Warner Cable, Verizon Digital Voice or Vonage, but not for many traditional TDM landline services. See https://www.nomorobo.com/signup.

[6] Examples: PrivacyStar, TrueCaller.

Applicability: Due to choices made by the designers of smartphone operating systems, apps only work for Android, not Apple IOS.

Trade-offs: Apps are available today but only for Android.

Number Signing and Validation

Operation: The originating service provider cryptographically signs the call signaling request, indicating that the caller is authorized to use the caller ID contained in the call setup message. Any carrier along the way can validate the signature and detect spoofed caller ID. A carrier may then either block the call or rewrite the caller ID to indicate that the original one was spoofed. For example, it may replace the caller ID with a number drawn from the "666" area code, allowing the called party to filter the call if desired. The Internet Engineering Task Force (IETF)[7] STIR working group[8] is working on standardizing the components needed: signaling message formats and how cryptographic keys ("certificates") are distributed to originating carriers. The certificates would likely be assigned by one of the administrative entities managing the U.S. numbering plan, such as the Number Portability Administrator (NPAC).

Effectiveness: The mechanism prevents spoofing and facilitates locating illegal robocallers, but does not by itself reduce robocalls. Number signing is most effective if all or almost all originating carriers sign and most terminating carriers validate.

Privacy: The mechanism does not reduce caller or called party privacy. The caller can still place anonymous calls (*i.e.,* calls that suppress caller ID information at the subscriber).

Applicability: Number signing is only applicable to VoIP systems, not legacy systems. However, almost all robocalls originate on VoIP systems, and gateway providers that bridge between VoIP and legacy systems can perform validation.

Trade-offs: Call handling software at both the originating and terminating carrier needs to be modified. A system for handing out certificates to carriers needs to be established.

Improved Caller Name Validation

Operation: Instead of looking up caller ID information in a CNAM database and mapping numbers to caller names, the call signaling information in VoIP can carry caller name information "in-band" and possibly additional identifying information, such as whether the caller is a registered charity or financial institution.

Effectiveness: This approach does not reduce telemarketing robocalls by itself, but rather makes it more difficult for robocallers to impersonate financial institutions, charities, and government agencies. It also eliminates the current CNAM dip fee scams.

The effectiveness depends on whether the originating carrier validates the caller name information provided by their customers. Just like "green" certificates for sensitive web sites, it may be sufficient if security-sensitive callers validate their caller name information so that called parties can know whether an entity claiming to be a government agency indeed is one. For consumers and small businesses, standard identity validation techniques may be sufficient to ensure that consumers provide their actual name. These identity

---

[7] "The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. " See http://www.ietf.org/about.

[8] Secure Telephony Identity Revisited (https://datatracker.ietf.org/wg/stir/charter/)

validation techniques are sometimes called dynamic knowledge-based authentication (KBA) or "out-of-wallet questions"[9].

Privacy: This requires no additional disclosure of information from the caller to the called party. It is also likely to increase consumer privacy since the current system allows any party to map telephone numbers to names using CNAM lookup services, even for unlisted numbers.

Applicability: The in-band mechanism is only applicable to VoIP calls, but improved validation applies to both the existing CNAM databases and VoIP delivery.

Trade-offs: Transitioning to this mechanism may require additional standardization efforts, the cooperation of a large number of carriers and changes in the validation of customer information. Current CNAM displays are often limited to 15 characters, making it difficult to render more detailed information.

Third-Party API-based Filters

Operation: Third-party API filters are a variation of the earlier filtering mechanisms. Here, the carrier serving a subscriber queries a third-party service chosen by the subscriber among competing offerings, using a standardized protocol. The third party service then recommends that the call is blocked, redirected to another party, forwarded to voicemail, or completed normally, possibly with additional information that could be included in the caller ID display. In addition, the mechanism may allow subscribers to label the most recent call as unwanted (*e.g.*, using a vertical service code or "star-code"), similar to the *57 malicious caller identification code that most phone service providers offer.

Effectiveness: The effectiveness is similar to other filtering solutions discussed earlier.

Privacy: In general, the privacy implications are similar to other filtering solutions. However, as long as subscribers do not need personal white or black lists, the carrier could query the service without revealing the destination of the call so that the third party offering the filtering service does not get to keep a call log.

Applicability: This mechanism works for all types of systems, including VoIP, legacy circuit-switched and cellular, although it is probably easier to implement for VoIP and cellular systems.

Trade-offs: Third-party filters require the least amount of consumer effort since they do not need to install any apps. Since they work for legacy systems, they could be available to all consumers.

Do Not Originate (DNO)

Operation: Gateway vendors check incoming calls against a Do-Not-Originate (DNO) list of numbers where the holder of the number has declared that such calls do not use VoIP gateways or do not use that specific provider. The DNO list may also include telephone numbers that have not yet been assigned by numbering authorities to telecommunication carriers, as such unassigned numbers are commonly used by telemarketers that spoof caller ID.[10]

---

[9] See http://en.wikipedia.org/wiki/Knowledge-based_authentication.

[10] For example, it is currently possible to spoof numbers from area codes that are not in use and will most likely never be assigned, such as 311 and 911.

Effectiveness: This mechanism prevents only the impersonation of institutions that avail themselves of the mechanism. Organizations that would be the targets of spoofing, such as financial institutions, insurance companies and government agencies, would likely register in a DNO list. Thus, since it requires active participation by spoofing targets, the mechanism is likely to reduce, but not prevent all illegal robocalls.

Privacy: There are no consumer privacy implications, and the list of numbers does not need to be confidential since the entities on the list are likely to include well-known "800" and other numbers.

Applicability: This is only applicable to VoIP gateway providers who cooperate.

Trade-offs: This mechanism does not require changes in protocols, but does require a mechanism for entities wanting to add themselves to the DNOL to do so without having to contact every VoIP gateway service provider.

(Telephony) Honeypots

Operation: M³AAWG defines a telephony honeypot as follows: "A telephony honeypot is a telephone service endpoint to which calls can be directed. It may appear to callers to be a normal telephone number (*e.g.*, a typical 10-digit residential or business phone number) but is specifically designed and deployed to collect information on unwanted calls. It might automatically process calls or employ humans, is computer monitored and might be recorded."[11]

Effectiveness: Honeypots can be used for enforcement purposes and to populate filter black lists.

Privacy: There appear to be no consumer privacy implications.

Applicability: Honeypots can be used for all kinds of telephone numbers, including mobile.

Trade-offs: Honeypots themselves do not prevent robocalls but can be an important part of making other mechanisms more effective.

Summary

A set of technical approaches, deployed incrementally, can help to make illegal robocalling unprofitable by reducing the number of households scammers can reach. Validated caller ID, a better caller name system, and user-chosen call handling can return control over their phone to consumers. Some of the systems proposed require standardization and development work, but all can be integrated into commercially-deployed VoIP systems, both landline and mobile.

---

11 https://www.maawg.org/sites/maawg/files/news/M3AAWG_Telephony_Honeypots_BP-2014-08.pdf; M³AAWG is the Messaging, Malware and Mobile Anti-Abuse Working Group.