Technical Disclosure Commons

Defensive Publications Series

December 01, 2017

Robocall and fake caller-id detection

Junda Liu

Naveen Kalla

Shi Lu

Robocall and fake caller-id detection

ABSTRACT

Spam phone calls are a source of user unhappiness, and a tool for unscrupulous operators to prey on vulnerable individuals. Spam callers use increasingly sophisticated methods, e.g., disguising a call with a fake caller-id, such that a receiver of the call is given an impression that someone from their contact list is calling. Robocalls, wherein an automated program originates phone calls that targets individuals, e.g., for unsolicited sales or other purposes are a source of annoyance for phone users. One approach to eliminate such calls is to require authentication by a call originating party. However, spam or robocallers are unlikely to identify themselves as such.

Techniques described herein utilize signaling messages of a phone call to serve as a signature or fingerprint for the phone call. Legitimate phone calls have distinct signatures, while spam-calls, robocalls, and calls with fake caller-id have their own distinct pattern. This difference is leveraged to detect and thwart unwanted calls.

KEYWORDS

- Robocall
- fake caller-id
- caller-id spoofing
- call authentication
- VoIP
- SIP
- spam call

BACKGROUND

Spam calls, calls with spoofed caller-id, and robocalls are a source of user annoyance and displeasure with telephone calls. One approach to limit such unwanted calls is to enforce the originating party to send accurate information regarding itself. For example, in session initiation protocol (SIP), a header known as P-asserted-identity is provided. However, it is up to the sender to certify authenticity of the P-asserted-identity field.

Sophisticated spammers can, with some effort, successfully authenticate themselves using the P-asserted-identity field. It is in the interest of spammers, robocallers, and caller-id spoofers to not identify themselves as such. There are other mechanisms built into VoIP standards to allow calls only from authenticated callers and not from anonymous or fake callers. However, due to the complexity of the network and requirements for various legitimate but niche callers, e.g., businesses that do not want to reveal an internal extension number of its employees in outgoing calls, spammers find a way to masquerade as authentic, e.g., neither bulk-calling nor unsolicited, callers. Some current solutions perform a database look-up of caller-ids that are marked as suspicious. However, such approach is not real-time, and relies on massive crowd-sourced data collection with known inaccurate classifications. Further, a database lookup cannot prevent spoofed caller-id, e.g., when a fake caller appears as a caller from one’s contact list.

DESCRIPTION

A majority of robocalls today are VoIP calls, e.g., IMS-based, rather than PSTN-switched. The techniques described herein make advantageous use of the footprint of signaling messages of VoIP calls to characterize the call. Rather than relying on an originating party to authenticate itself, techniques of this disclosure identify spam-calls / robocalls / spoofed caller-id at the receiving end (if based on IMS call-flow), or at intermediate network nodes such as gateways (which can analyze signaling packets). The techniques include several mechanisms to fingerprint a call, as described below.

1. Fingerprinting SIP, SDP, RTP, RTCP packets. In current networks, the signaling needed to set up a call is separated from the media packets. Various protocols are used during call set-up and during media flow, such as:
    a. session initiation protocol (SIP), which is a signaling protocol used for call set-up;
    b. session description protocol (SDP), which is used to agree upon parameters, e.g., codec-type, used by both parties;
    c. real time protocol (RTP), which is used to transfer media packets, e.g., audio, after call establishment;
    d. RTP control protocol (RTCP), which is used to control parameters of the RTP during a call; etc.

   Each of these protocols have characteristics that reveal call origins, and thus can be used to establish or estimate the bona fides of a caller. For example, in SIP, there are hundreds of fields that each carrier fills in a different way. The way a carrier fills the SIP fields is used as a fingerprint for the carrier. Thus, per the techniques described herein, an incoming call with a suspicious SIP fingerprint is flagged as a call that may be spam, robocall, or have spoofed caller-id.

   Example (call authentication based on SIP analysis) A caller claims a false “From:” address in SIP, thereby effectively faking caller-id. The techniques described herein include performing an analysis of the network routing fields, e.g., at a gateway. If such analysis reveals a different provenance, it is established that the caller-id is fake.

2. Verifying carrier-ID as determined by fingerprint analysis against claimed carrier-ID. An incoming call is served by an originating carrier, and the name of the carrier (and radio-access technology) is declared in appropriate packet headers. However, as described above, fingerprint analysis of the signaling packets can reveal that the declared carrier name is false. Differences between the declared carrier and carrier determined using fingerprint analysis indicates that the call is spam, robocall, or has a spoofed caller-id.

3. Detecting that the caller-id is fake. If a database look-up shows that the claimed caller-id is a real number that belongs to a certain carrier, and a fingerprint analysis of the signaling packets reveals a different carrier, it is determined that the caller-id is false. A caller-id field that is of certain formats, e.g., unsigned format, is a flag that the caller-id is false or that the call is a robocall.

4. Detecting fake calls based on caller patterns. A sudden change in the pattern of a caller on a contact list is also an indication of spoofed caller-id. For example, if a call is received via VoIP with information that it is from a person on a contact list, and it is known that the person normally calls through PSTN, such information is used as an indicator that the VoIP caller is fake.

5. Detecting spam based on general properties. Spam and robocalls are likely generated directly by a computer using VoIP, and typically originate from a small cluster of locations. While such properties do not definitively establish a call as spam, they serve as an

indicator. Such indicator is combined with other indications of spam, to establish the true nature of a call.

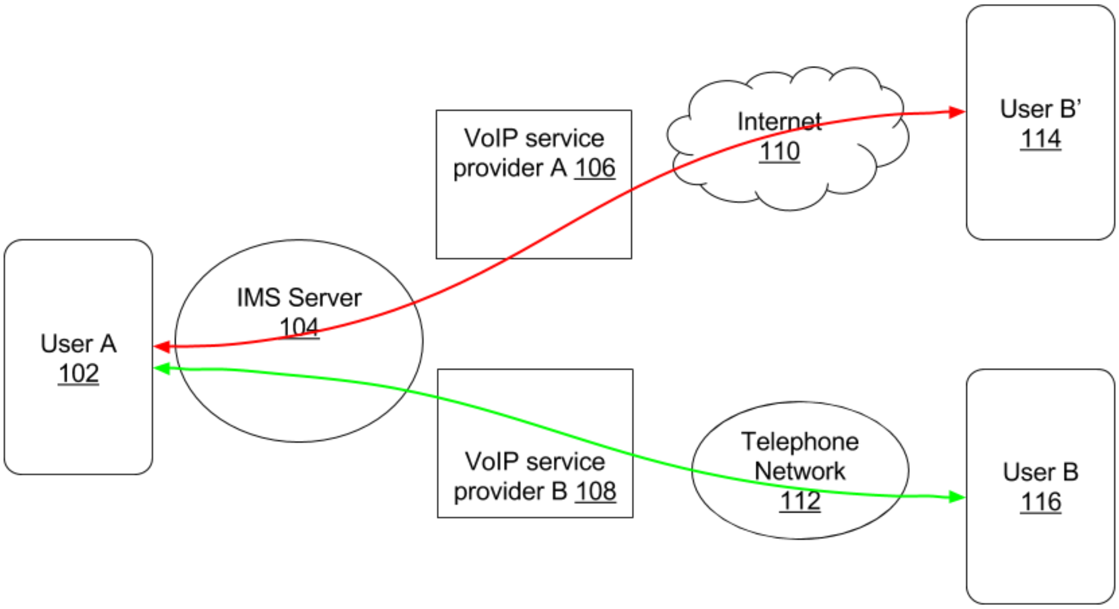

Fig. 1

6. Detecting a spoofed call based on routing pattern. Fig. 1 shows detection of a spoofed call based on routing patterns. As illustrated in Fig. 1, user A (102) receives a call from user B' (114) who pretends to be another user B (116). The spoofed call is routed to user A via the internet (110) through a VoIP service provider A (106) and IMS network (104), as illustrated by the red arrow. However, it is known that the actual route to user B is via telephone network (112), VoIP service provider B (108) and IMS network (104), as illustrated by the green arrow. The call from user B' cannot take the same route as that from the real user B. Based on the different routing patterns, it is determined that the call is not from user B. The detection can be performed on the device of user A, by the IMS server, and/or by the VoIP service provider.

The techniques described herein can be implemented as part of a smartphone operating system to detect spam calls, robocalls, and calls with fake caller-id information.

CONCLUSION

Techniques of this disclosure detect spam-callers, robocalls, or spoofed caller-ids based on fingerprint analysis of packet headers and call properties.