The Spoofing/Authentication Threat

An Analysis of the Spoofing/Authentication Threat in Voice Network Security

A Whitepaper From
SecureLogix Corporation

Introduction

Spoofing refers to the act of intentionally changing the source number and Automatic Number Identification (ANI) on an inbound call. This is the same concept as "Caller ID Spoofing," "Calling Number Spoofing," and similar terms. While some spoofing is legitimate, the vast majority of spoofing is used for malicious calls. Spoofing is illegal when used for fraudulent intent, but this does not deter most attackers. Spoofing makes all inbound voice call-based attacks more difficult to deal with, including robocalls in general, scams, vishing, Telephony Denial of Service (TDoS), and social engineering, including Account Takeover (ATO) in financial contact centers. The days of being able to trust the calling number and caller ID are long past.

The technical reason for this increase is that the Public Switched Telephone Network (PSTN) is no longer a closed network. It heavily uses Voice over Internet Protocol (VoIP) and increasingly connects to the Internet through the Session Initiation Protocol (SIP). It is trivial to introduce calls with any spoofed numbers into the network, via SIP, traditional telephony, and on a small scale with applications such as SpoofCard.

It has become more difficult to use email phishing and other forms of fraud. Better email filters, more educated users, chip cards, better online security, mobile authentication, etc., have made other forms of fraud more difficult, driving attackers to the weakest link, which is the PSTN and voice systems. In addition, the voice network still has an unfounded level of trust with many consumers. Users have been somewhat trained not to trust an email, but many still trust the PSTN and the calling number/caller ID, which again, is trivially spoofed.

Why Spoof?

Spoofing and the in ability to identify or authenticate the caller enables many inbound voice call-based attacks. Spoofing on its own is not an attack, but does make virtually all inbound call attacks more difficult to mitigate. Some attacks include:

- Voice SPAM—Telemarketing, surveys, debt collectors, etc. While some "legitimate" telemarketers use legitimate numbers, many do use spoofing. Spoofing is almost always used except when the telemarketer wants the consumer or victim to be able to call them back, in which case they must use a real number.

- Scams—IRS scams, tech support scams, other impersonation scams. These calls almost always use a spoofed calling number designed to impersonate a legitimate organization and trick the victim. This includes spoofing to numbers such as 1-800-TAX-1040, which causes "US Treasury" to come up as the caller ID. Attackers also spoof to random but official looking numbers from the D.C. area code. Attackers also spoof to numbers from legitimate technology companies such as Microsoft for tech support scams. Finally, attackers may spoof to well-known financial organizations to attempt to comment fraud.

- Phishing—Calls intended to gather information from the victim. This includes recent calls attempting to trick the victim into saying “yes” or something that can be recorded and used later.

- Bomb threats—Calls to schools or other locations designed to disrupt operations. By spoofing to a known number such as a local police department, it is more likely that a bomb threat call will be answered.

- SWATing—Calls to 911 to attempt to deploy law enforcement resources to another location. The attacker spoofs the number to the location that they want to resources to go to. A similar attack against 911 is to spoof a call to divert resources such as the Coast Guard to one location, to prevent them from monitoring illegal activity at another location.

- Voice mail attacks—Some voice mail systems use only the calling number for validation. If you call these voice mail systems with a spoofed calling number, you can get immediate access.

- Telephony Denial of Service (TDoS)—A flood of calls intended to disrupt operations, normally to a public-facing contact center. By spoofing the numbers for TDoS calls, it is much more difficult to differentiate them from legitimate calls.

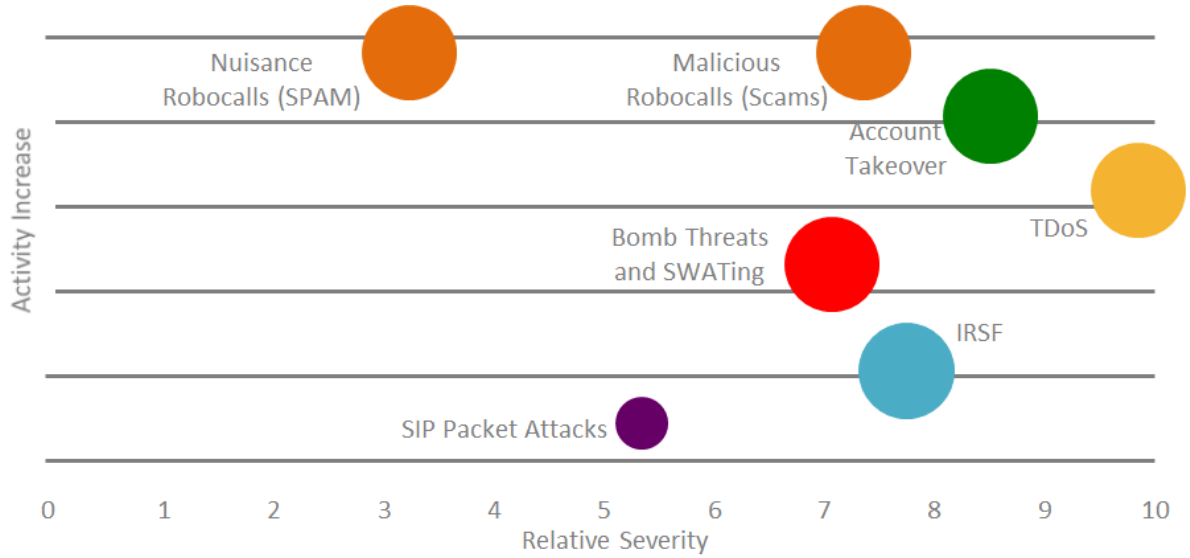
- Account Takeover (ATO)—This is a form of financial fraud where the attacker makes calls into a financial contact center and attempts to take over legitimate users accounts for the purpose of extracting funds. Spoofing is one way to increase the level of trust; spoofing the calling number to that of a known customer may reduce the complexity for the attacker.

The Current Spoofing Threat

Spoofing has all but enabled the robocall issue. Estimates place the number of robocalls in the billions per month. YouMail reports a peak of 2.61 billion robocalls in September 2016. A 2015 Harris Poll estimates that 27 million U.S. consumers lost approximately $7.4 billion to phone scams. The Federal Trade Commission (FTC), which tracks consumer complaints, collects on average more than 250,000 robocall/scam call complaints every two weeks, about 50,000-60,000 unique numbers each period, of which about 35,000 are new, mostly spoofed numbers.

The following chart provides an illustration summarizing the current threats we see in real-world enterprise voice networks and how they relate to one another in likelihood and relative severity/impact.

For every one of these attacks, with the exception of International Revenue Share Fraud (IRSF), which is an outbound calling attack, spoofing plays a significant role in making the attack more effective and in some cases is what makes the attack possible.



Expect attackers to come up with more scams over time. Attackers also use spoofing and spear vishing techniques to target specific users, similar to the "whaling" attacks occurring over email. We are already seeing this to some degree with bomb threats, where the attacker uses robocalls to find a source number from which the victim will answer a call (to defeat whitelists) and then uses text-to-speech software to interact with the victim.

How to Spoof

There are multiple ways to spoof the calling number. The easiest way for low volume generation is to use services and apps such as SpoofCard. This service has been available for many years and is a cheap and easy way to generate individual spoofed calls. It is also easy to use tools such as the Asterisk IP PBX, the sipp call generator, and other freeware tools to automatically generate calls. These tools make it possible to generate millions of calls, each with individual, random, or carefully selected calling numbers. There are a number of ways to do this, but as an example, Asterisk can be used to generate the calls. It is simple to create individual files, placed in the proper directory, with the destination number, message to play, and calling number to spoof. The application generating these calls can randomly select numbers from a list, always set the calling number to one number, select random numbers in a specific area code (such as 202), and employ sophisticated strategies such as always picking numbers that are legitimate and assigned. This is becoming more important as the service providers are starting to look at blocking calls from invalid or unassigned numbers.

Existing Countermeasures

The current state of the art in spoofing detection is very limited. The most common countermeasures are described below.

Managed Blacklists

Most of the vendors providing these managed blacklists use a similar process, that being to maintain an active blacklist and block arriving calls on that list. The vendors update these lists as a function of the traffic they monitor and based upon comments from their users. These solutions work pretty well when they are available, but are not widely available to some POTS landline users, less popular mobile devices, and businesses and enterprises.

The biggest challenge with blacklist approaches is that they do not work for new calls that are not on the list nor calls that use randomly spoofed calling numbers. The robocallers know about the blacklists and if they really want to deliver a call, they either know what numbers are on the blacklist or can easily probe to find out.

Do-Not-Originate

Service providers are starting to work on defenses such as Do-Not-Originate (DNO), where they block a call coming into their networks that has an invalid number and/or which has never been assigned. Since a relatively small percentage of the North American Numbering Plan (NANP) has been assigned, a poorly designed random calling number generator is likely to generate unassigned numbers. The service providers could start to block these. Some service providers have started to do this for individual numbers, again such as 1-800-TAX-1040 (which never makes outbound calls).

The Robocall Strike Force has been looking at the robocall and spoofing issues. The FCC very recently, in late March, provided the following request for spoofing solutions. See the following links for more information.

https://www.fcc.gov/news-events/events/2016/10/second-meeting-industry-led-robocall-strike-force

https://www.fcc.gov/document/robocall-blocking-nprm-and-noi

STIR/SHAKEN

The industry, including the Internet Engineering Task Force (IETF), Alliance for Telecommunications Industry Solutions (ATIS), SIP Forum, and service providers, are working on the Secure Telephony Identity Revisited (STIR) Request for Comment (RFC) and Signature-based Handling of Asserted information using toKENs (SHAKEN). These efforts are an attempt to authenticate the calling number that is presented to the destination user. STIR has been around for a while, with SHAKEN being a more recent definition of how it will be implemented in practice. It is possible that due to the impact of spoofing, that these standards will be adopted more aggressively. However, even if they are, they will take some number of years to be deployed and there will be large gaps in their coverage, such as calls that traverse the legacy network. See the following link for more information:

http://www.sipforum.org/content/view/443/171/

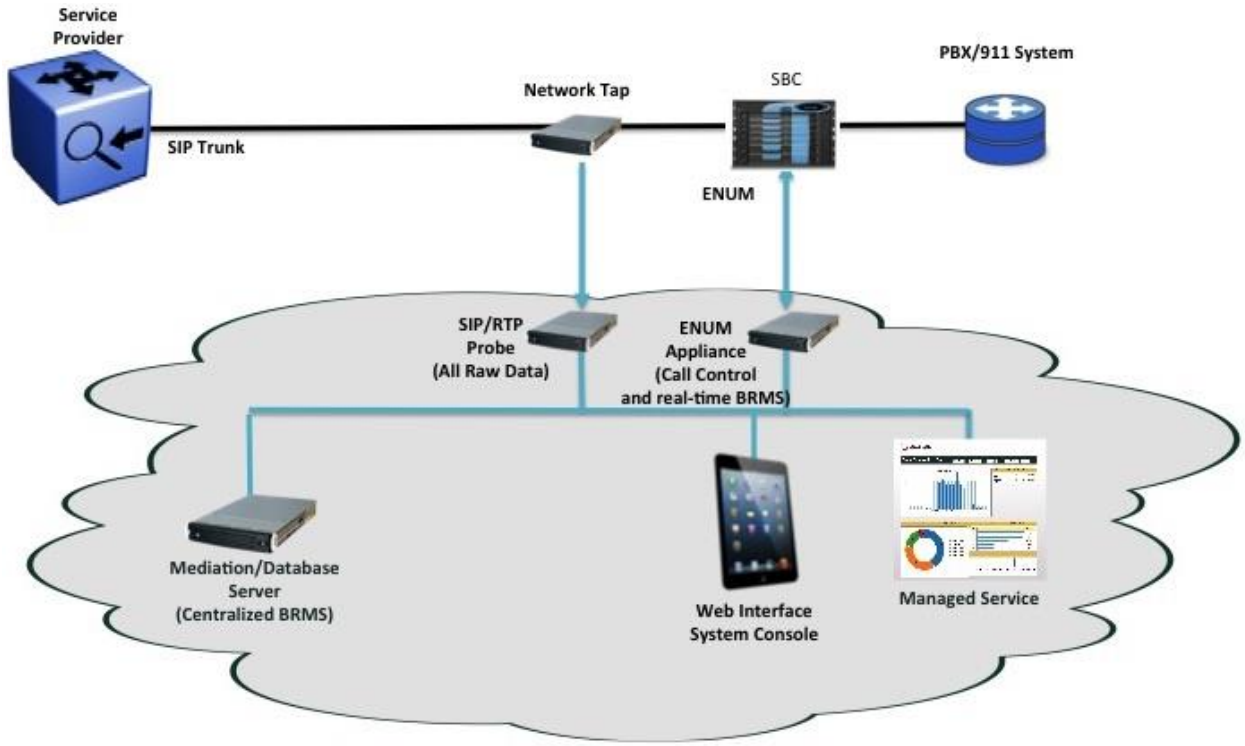
Proprietary Authentication

There are a number of methods to authenticate a caller. One very common method is Knowledge-Based Authentication (KBA), which is the familiar method used in say financial contact centers to identify and authenticate a caller by asking them questions that only the caller should know the answers to. KBA is becoming less and less effective, is expensive for contact centers to implement, and is frustrating to consumers. There are also well-known approaches such as voice biometrics which, for example, use active and passive speech analysis to authenticate the caller. These approaches work reasonably well, but are expensive and sensitive to noise, call quality, and other factors.

There are also a growing number of approaches that authenticate by determining something that the consumer has, such as a mobile phone. This includes use of mobile apps, which authenticate the user through some means and then use some out-of-band method to authenticate the consumer when they call a contact center. There are a number of other approaches that determine that a caller has indeed made a call from a specific landline or mobile device to the financial contact center. These approaches work well for specific use cases, such as mobile or specific service providers. None of these approaches work for every caller and every type of device.

Solutions

SecureLogix offers solutions to mitigate spoofing. Our enterprise-focused solutions address the various forms of spoofing. In addition, we are working with service providers and with the Department of Homeland Security (DHS) to enhance our solutions to address more sophisticated calling-number spoofing. We are also working with financial contact centers to orchestrate the authentication process, by integrating and selectively querying various authentication services. We are also working with service providers on additional authentication capability. Our solutions can be deployed in SIP and TDM networks, support large and small sites, and have very flexible polices that are used to detect and mitigate robocalls. Our solutions integrate with common network infrastructures such as Cisco routers and SBCs through network interfaces, also allowing for a cloud-based deployment. A high-level architectural diagram of our high-capacity SIP solution is shown below.



Our solutions allow new business rules and policies to be built without impacting the underlying software. All of the call attributes and, in the case of VoIP, SIP signaling attributes are available to feed new business rules. The solutions offer call control options and support for semi-static and dynamic white and black lists. A set of network queries, including source phone number checks, number type checks, and queries to call authentication services are also available. This allows any combination of business rules for different signatures, vertical requirements (such as health care, emergency services, or financial services), or specific customers to be built without changing software.

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 (210) 402-9669 • www.securelogix.com