The Telephony Denial of Service (TDoS) Threat

An Analysis of the TDoS Threat in Voice Network Security

A Whitepaper From
SecureLogix Corporation

Telephony Denial-of-Service (TDoS) and The Public Voice Network

TDoS is a form of Denial of Service (DoS) that affects enterprise, government, and other business voice systems. It is a significant threat to voice systems and by far the most common form of voice-based DoS. The reason for this 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).

Despite the deployments of VoIP and SIP, end-to-end SIP is very rare. While an attacker may use SIP, the victim organization is likely to use a combination of Time Division Multiplexed (TDM) and SIP trunking. This means that end-to-end Internet Protocol (IP)-based DoS techniques that rely on IP-level protocol issues are not effective. For example, SIP INVITE floods, REGISTER storms, and malformed or "fuzzed" packet attacks sent across the PSTN are just not practical. The PSTN contains many service providers who may translate calls between SIP and TDM; an IP-level attack will not continue through a TDM connection. Also, even within SIP networks, devices such as Session Border Controllers (SBCs) terminate and regenerate SIP messages, making it difficult to transmit packet-level attacks.

The primary attack unit is not an IP packet, but rather a malicious call. These calls usually originate with SIP, but arrive at the victim site as a call, whether on SIP, TDM, or whatever mix of systems. SIP trunks, consumer/cable SIP offerings, Internet-based SIP services, softphones, and compromised smart phones all combine to make call origination with spoofed/anonymous calling numbers cheap and easy.

Types of TDoS Attacks

The TDoS threat is evolving. Attacks have evolved to the point where, as with any Distributed Denial of Service (DDoS) attack, automation is almost always used. Most automated attacks are fairly low volume and simple. The attackers do not need to generate many calls, because their victims are not entire organizations or sites. The attacker has the advantage, because it is easy to generate the attack, the target usually has a small number of critical lines, and the victim has very limited capability to deal with the attack. The following table provides a TDoS threat taxonomy for different types of attacks:

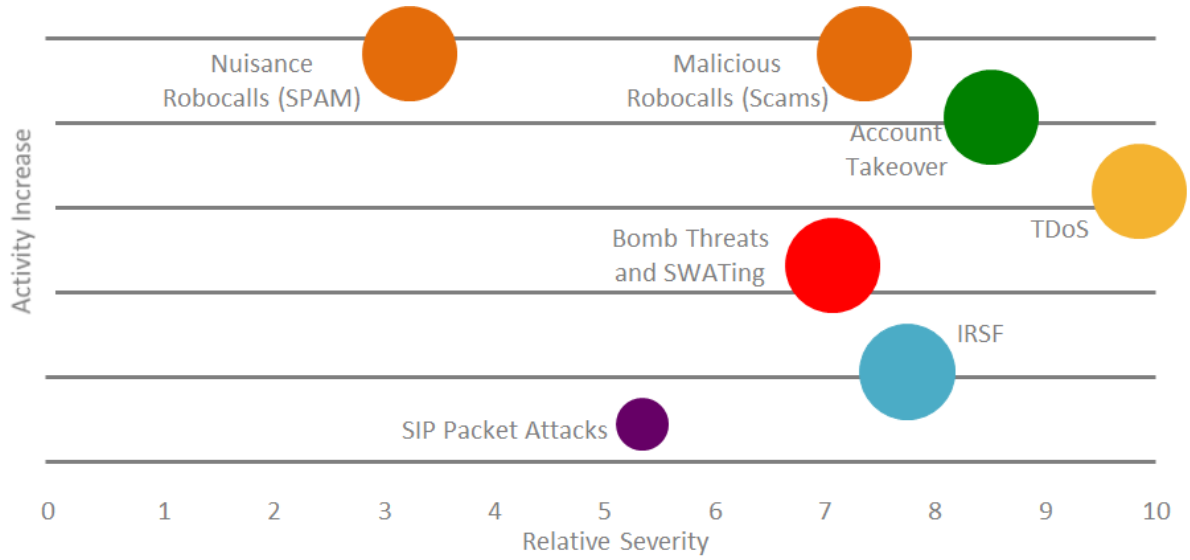
TDoS Category	Target	Frequency	Small Site Severity	Large Site Severity
Manually generated TDoS	Small Site	Uncommon (used in the past)	High	Low
Social network TDoS	Large Site	Uncommon	Moderate	Low
Simple automated TDoS	Small Site	Common	High	Low
Complex automated TDoS	Small or Large Site	Uncommon (but coming)	High	High
Distributed complex automated TDoS	Large Site	Uncommon (but coming)	High	High

It is possible to use manual calling to attack an individual, but this type of attack does not scale. There have also been some social-network-originated attacks, leveraging Facebook and Twitter to organize individuals into a TDoS calling campaign. As mentioned, the vast majority of TDoS attacks use automation to generate the attack calls, with most to date being simple, using a single origination point and limited calling number spoofing. However, we are starting to see more complex attacks using sophisticated calling number spoofing and distributed origination. One recent attack used Twitter to deliver a link to malware, which caused many smartphones to continuously dial 911. This is a real-world example of a complex distributed TDoS attack, in this case a hybrid because it used social networking to deliver the malware.

The Current TDoS Threat

TDoS can affect any government, enterprise, or small business, but most commonly impacts organizations with critical, public-facing contact centers. This includes 911, financial services, government, health care, and critical infrastructure. With TDoS, the objective is to make a significant number of calls and to keep those calls active for as long as possible, to overwhelm or at least “clog” all or a portion of the victim’s voice system. This can include trunk circuits, emergency phones, attendants/agents, an Interactive Voice Response (IVR) system, specific phone numbers, or some other choke point.

The chart below provides an illustration summarizing the current threats we see in real-world enterprise voice networks and how they relate to one another in activity increase and relative severity/impact. As you can see from this illustration, TDoS attacks have high severity in relation to other voice network threats.



A common TDoS attack targets public health and safety infrastructure. Over 1,000 of these attacks have been reported to the Department of Homeland Security (DHS). This type of attack involves calling a victim who may have taken out a "payday" loan in the past and threatening that if they do not pay, their place of business will experience a TDoS attack. Again, the attacker targets an enterprise with a critical set of phones. At its peak, this attack was generating some $200,000 for the attackers every few weeks. according to figures from AT&T and Verizon.

Some financial organizations have been affected by larger scale TDoS attacks and very aggressive call pumping, which overwhelmed smaller parts of their contact centers. In another example, the Anonymous hacking group threatened and executed a TDoS attack against the FBI call centers and some local law enforcement offices. This attack illustrates that a well-known and capable hacking group such as Anonymous considers TDoS an effective attack technique.

TDoS has targeted public safety, in the form of 911 and emergency responders. An isolated attack against 911 itself can be very disruptive. If coordinated with a physical terrorist attack, the TDoS attack would be particularly disruptive, resulting in a large number of victims not getting through to the emergency service. This would in turn make the physical attack more damaging, because victims would not receive prompt attention. DHS has issued multiple warnings about TDoS attacks to educate government and commercial entities of the approach and methods used and to provide recommended steps for organizations that suffer such attacks, or are concerned that they may suffer such an attack.

An example of a real-world distributed TDoS attack that affected 911 occurred in Q4 of 2016. An individual leveraged a click-to-dial vulnerability on smartphones. The attacker built a simple piece of code, really just a loop,

which used the click-to-dial feature to continuously dial 911. This software ran until the user rebooted the smartphone. This malware was downloaded and delivered by a malicious website, which the attacker tricked victims into accessing by including an obfuscated link to several thousand of his followers on Twitter. His followers, who trusted him, clicked the obfuscated link, which went to the malicious website and downloaded simple software that exploited the vulnerability. Again, the malware caused each affected smartphone to continuously call 911, mostly in Phoenix and the surrounding area, where most of the attacker's Twitter followers resided. The malware needed to exploit the click-to-dial vulnerability was very simple and easily downloaded. We expect fixes to be made available for iOS and Android. Fortunately the attacker only had a relatively small number of followers on Twitter. Imagine if this attack was delivered via a major celebrity's Twitter account, which could have 10s of millions of followers.

TDoS can also target critical infrastructure, which commonly uses voice modems for control. Attackers can use SIP-based scanners such as Warvox to quickly identify these modems. A TDoS attack is used to repeatedly call the modems, both at the remote and controlling site, thereby preventing legitimate calls and disrupting operations. The remote sites are particularly easy to disrupt, since they typically have a single line available. Control sites are particularly lucrative to attack, since when they are disrupted, they are unable to control remote sites.

As time passes, it becomes increasingly easy to generate a large scale, high-volume TDoS attack. For example, there are increasing numbers of inexpensive SIP access service providers, who are likely to turn a blind eye to TDoS attack traffic. Consider all the "robocall" traffic, which represents billions of calls, normally directed at many different victims. What if this infrastructure was trivially modified to send all those calls to one site? A TDoS attack could use multiple SIP access providers and cycle through new ones as others get shut down.

As previously described, a sophisticated attacker would coordinate a TDoS attack with a physical attack or a simultaneous attack against Internet resources such as a web site. This would naturally drive more traffic to voice systems. Consider a worst-case scenario where a physical attack causes many individuals to call 911. At the same time, a TDoS attack overwhelms the already-overloaded 911 systems. This would result in many individuals not being able to be serviced in a timely manner, making the effect of a physical attack more severe.

More complex TDoS attacks are starting to occur, where the attacker spoofs the calling number for each call. Perhaps the numbers are randomly generated and mostly invalid, but consider that it will take but a few days of effort to enhance the attack to where the numbers are randomly picked from a list of legitimate numbers, such as the easily obtained Federal Trade Commission's (FTC's) Do Not Call List (DNCL). Again, the attacker has the advantage and can quickly progress to complex TDoS, which is very difficult to mitigate, even by state-of-the-art defenses. Couple this with use of multiple origination points or a botnet for a distributed TDoS attack and you have the potential for very disruptive attacks.

Another factor to consider is that government and enterprise voice networks are aggressively transitioning to centralized SIP call control and access. Rather than having 100s or 1,000s of PBXs at each site, along with dedicated trunking, the call control along with trunking is being consolidated and centralized into data centers. These data centers are often in organizations' private clouds, but can also be in public clouds and managed by various service providers. Part of this centralization is the right sizing of trunking and call control, which means that much less overall capacity is available. While this architecture offers redundancy through multiple data centers and service providers, it still creates an enormous choke point where a distributed TDoS attack could overwhelm the voice system of an entire enterprise or even multiple enterprises. Even a targeted distributed TDoS attack has the potential to "bleed over" across the organization.

Generating a TDoS Attack

There are several ways to generate TDoS attacks. Aside from the smartphone-originated attack described above, it is simple to use free software, 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 hundreds, possibly thousands, of concurrent calls. In the near future, distributed TDoS will be possible, where a voice-aware botnet can be used to generate tens of thousands of simultaneous calls.

A brief summary of how SIP is used to generate TDoS attacks is as follows:

- Select the phone numbers at the victim. Since the numbers are generally public facing (often 1-800 numbers or 911), they are very easy to source from the victim's website. For a large contact center, it is also possible to locate some portion of the contact center that has limited resources and/or is a choke point.
- Install and configure the Asterisk or other open source/free IP PBX software. These systems require nothing more than a capable Linux server. There are many resources on the Internet that describe how to set them up.
- Set up a call generator, which uses the underlying Asterisk software to make the calls. During this process, the attacker can set victim numbers, chose how to spoof the calling number, decide what audio to play, choose the call rate, etc.
- Execute the attack during the time when it will be the most disruptive. This may be during the busiest part of the year (a national or local emergency, tax season, any holiday, peak shopping time, etc.) and/or the busiest time of the day. The attack may also be synchronized with a traditional DDoS attack against the victim's website, driving more traffic to the voice systems.

The ability to spoof the calling number and make anonymous calls, and the difficulty in tracing the attack back to the source, makes it very difficult to mitigate TDoS attacks. Even service providers have difficulty mitigating attacks.

Existing Countermeasures

The current state of the art in TDoS defense and mitigation ranges from virtually no capability, to static black and white lists, to the ability to deal with simple automated and manual/social-network-originated TDoS attacks.

Legacy Systems

Many potential victim sites still use legacy TDM trunking and a variety of legacy and VoIP PBXs. Consider the wide variety of systems in use throughout major corporations as a result of multiple acquisitions/mergers as well as government agencies that are attempting to upgrade their voice environment on limited budget, so transition is usually accomplished in a phased approach. Even modern IP PBXs from vendors such as Cisco and Microsoft provide only minimal protection.

Session Border Controllers (SBCs)

Organizations using SIP trunking use SBCs for SIP security. SBCs offer basic blacklisting and whitelisting capability, but such capability in an SBC was not designed to address TDoS and only allows limited ability to mitigate some variations of simple automated TDoS. SBCs do not have capability to identify and/or mitigate more complex forms of TDoS. SecureLogix is very familiar with the TDoS capabilities of the major SBC vendors, because we partner with and integrate with several of them for TDoS defense solutions.

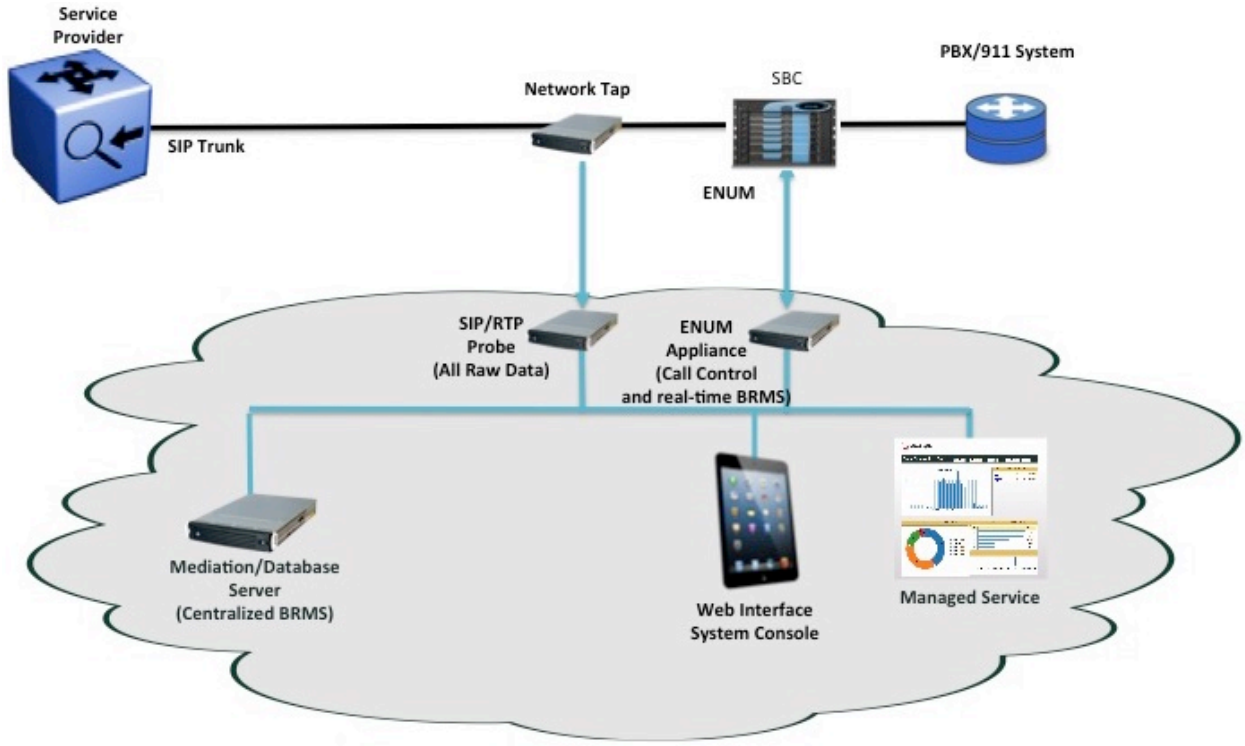
Service Providers

Service providers' capability to mitigate TDoS varies greatly. Service providers generally lack the ability to respond quickly, especially for attacks moving through many different providers. If a service provider does detect a large number of calls coming from a specific peering partner or mobile provider targeting specific victim numbers, then all traffic from that source can be blocked. This "burn the bridge" approach may work for isolated and unsophisticated attacks, but for large service-provider peering partners that carry a large amount of traffic, this is not practical because many legitimate calls will also be blocked. Plus, this mitigation is not as effective when the attack becomes more sophisticated.

Again, SecureLogix is very familiar with selected service provider solutions because we work closely with several of them. For example, SecureLogix is the recommended solution for both Verizon and AT&T when one of their customers is a victim of a TDoS attack.

Solutions

SecureLogix offers solutions to mitigate TDoS attacks. Our solutions address forms of TDoS seen in recent attacks and we are working with the Department of Homeland Security (DHS) to improve our solutions to address more complex attacks expected to be common in the future. 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 TDoS. Our solutions integrate with common network infrastructures such as Cisco routers and SBCs through network interfaces, also allowing 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, to include 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