# In the News

no jitter

## Exploring Telephony Denial of Service

*Brute force attack against voice systems is a real, and growing, problem.*

*By Gary Audin*

November 11, 2016

In a denial-of-service (DoS) attack, the goal is to make a resource unavailable to its intended users, usually in a temporary interruption or suspension of services. DoS attacks are well known in data systems and networks, but can also happen to a telecom system or network.

I first learned about telephony DoS, or TDoS, attacks in the recent GCN article, "DHS working to protect emergency call centers against denial-of-service attacks." Although the article focuses on emergency call centers, the problem applies to call centers in general.

To learn more, I contacted Michael Boukadakis, founder and CEO of ENACOMM, which creates intelligent self-service applications. He is spearheading ENACOMM's transition to multimodal voice and data applications, and has decades of experience driving national IVR and call center solutions. What follows is an edited version of our conversation.

**Explain a classic TDoS attack.**
**Boukadakis:** Criminals use low-cost VoIP tools to mount a massive telephone calling campaign, simultaneously bombarding an organization's phone and IVR systems with electronically generated calls. These brute force attacks cripple the organization's voice services and stop the organization from conducting business. These calls also serve to circumvent traditional security or fraud measures during the attack.

**Has a DoS attack ever occurred with legacy TDM systems?**
**Boukadakis:** Yes. TDoS attacks occur regardless of the technology in use by the victim. VoIP and TDM voice systems are equally vulnerable. Multiple auto-dialers have been used with TDM systems to mount attacks. There are cases of fax attacks. VoIP is a much more efficient attack tool, however.

**How is a TDoS on an IP system different?**
**Boukadakis:** An IP-based DoS attack not only can disrupt the telephone channels, but has the potential to affect the data channels/circuits by consuming network bandwidth.

**How does someone produce a TDoS attack?**
**Boukadakis:** Low-level attacks can be mounted by individuals all calling the same number simultaneously, as has been done by some social activists, but would not be as effective as software-generated VoIP attacks.

**What is the rationale or reasons behind creating this kind of attack?**
**Boukadakis:** Political and social terrorism (terrorist groups or social activists) disrupt business and cause financial harm by launching a TDoS attack. Anecdotal reports indicate some competitors will use TDoS attacks against other call centers.

Fraud is another motivator. [These attackers] simultaneously flood a call center or customer service staff with bogus calls.

(Continued on reverse)

They then launch social engineering attacks against contact center agents. Fraudsters have been able to take advantage of the chaos to steal corporate or customer account information that they will later use to defraud the organization or the customer.

**What industries suffer the most from TDoS attacks?**
**Boukadakis:** All call centers suffer, along with government agencies (especially 911 centers), banks, corporations, and other targets of social activists.

**How does an IT organization prepare for these attacks?**
**Boukadakis:** Perhaps the most important part of preparation is to ensure that, during an attack, all unwanted traffic is diverted, while true customers are allowed to connect without interruption.

The best way to prepare is to seek the guidance of third-party firms that are well versed in identifying and stopping these types of attacks. These firms, such as ENACOMM, work in conjunction with telcos to implement proven, proprietary methods and the solution that will best fit the needs of each specific customer.

There is additional best practices information [from APCO International in the PSC Online article], “Telephony Denial of Services (TDOS) to Public Safety Communications Phone Service.”

**Does any particular pattern occur that makes these attacks detectable?**
**Boukadakis:** There is not one pattern as criminals continue to develop new and innovative tactics every day. In general, these attacks are recognized due to the massive increase in call volume and the virtual shut-down of the telephony systems, blocking all or most legitimate inbound and outbound calling.

In addition, VoIP calls, which can be identified, will soar in volume. Spoofed ANI numbers may be detected and other patterns, which are proprietary to ENACOMM’s systems, will be recognized. Attacks may also be more likely during presumed call center or IVR maintenance periods, or may emanate from foreign countries in unusual volumes.

**What do you think will happen with TDoS in the near term?**
**Boukadakis:** As with the massive Dyn distributed DoS by Internet of Things devices attack this month, TDoS attacks will continue to grow both in the number of occurrences as well as in severity. Anyone or any organization that uses telephones is a potential victim.

The FBI, U.S. Department of Homeland Security, and other federal and state agencies have issued public warnings citing increased levels of TDoS attacks against public and private organizations. As early as 2013, more than 200 documented attacks had been reported. Overall, we suspect that many, if not most, attacks are not publicly reported -- which means that the TDoS problem is much worse.