Security for the SIP-Based Contact Center

- **Steven Taylor**
- **Editor-in-Chief, Webtorials**

As SIP explodes beyond connecting VoIP calls to a plethora of communication modes, now, more than ever, hyper-connected Contact Centers must quickly adopt and implement the highest measures of security to ensure an entirely new level of protection.

SIP is rapidly expanding far beyond a being mechanism for simply connecting VoIP calls. In fact, there is a veritable explosion of additional modes of SIP-enabled communications that users are rapidly adopting in an IP-based world. Not surprisingly, many of these additional modes include capabilities that are a part of the hyper-connected contact center. Rather than the contact center being based on traditional telephony, the contact center is now a conglomeration of media supporting a wide range of activities.

Our recent report, "**2015 Unified Communications, SIP, and SBC Plans and Priorities**," demonstrates that the number of SIP based applications has mushroomed over the past couple of years. High-growth areas related to the contact center include:

- Web conferencing - 131%
- Collaborative workspaces - 101%
- Desktop sharing - 99%
- APIs to integrate other applications - 98%
- Instant messaging - 89%
- Presence - 86%
- Desktop video conferencing - 50%

Challenges

This hyper-connectivity presents a range of challenges, especially from a security perspective. The most basic security threat is a Distributed Denial-of-Service (DDOS) attack. Since VoIP calls must involve a call setup, DDoS attacks for VoIP calls are easily mounted, just as they are for any other IP-based communications; a rogue process sends out a flood of connection requests; when the host system responds, the process never responds, wasting precious bandwidth and processing resources over the network. And, unlike the simplicity of TCP-SYN attacks, DDOS attacks have now evolved to include UDP flood attacks, GET flood attacks, and other variations. Additionally, as the Internet of Things (IoT) evolves, there are many new devices that can initiate such attacks on a network.

As the trend to support these different applications grows within the contact center, so does the need for additional SIP trunks and the need to secure the applications that run over them. The need for contact center security solutions can be seen on several levels. So far, we've only addressed availability of the infrastructure - making sure that communications (calls) can be established. From a systems perspective, the databases that provide information in order for the contact center personnel to be able to work effectively must be also protected. Virtually all web sites endure a constant barrage of SQL-injection attacks. Further, contact center personnel are highly trained professionals, and their time must be protected so that they can work efficiently.

The Imperative of Hyper-Security Measures

The security question is greatly exacerbated by the rapid change in network architecture for the contact center. Several years ago, the "call center" was housed in a central location, often accommodating hundreds or even thousands of individual agents. Relative to how we operate and do business today, building a "digital moat" around this castle was rather straight-forward. Those days are long gone.

The infrastructure of the contact center may span across several data centers, including both main and branch offices. And this same infrastructure may be comprised of a hybrid of dedicated and virtual systems and a mix of premises-based and cloud-based systems. In addition to infrastructure changes, the distributed contact center, whereby agents work virtually anywhere - including a home office - are becoming the norm rather than the exception. All of these components bring with them their own set of security concerns.

Solution

But is there a light at the end of this tunnel? Fortunately, the answer is "yes."

In our report, we explored the integral link between SIP and the Session Border Controller (SBC), which supports a wide range of functions for SIP-based communications. The respondents to the survey ranked "Security for SIP Sessions" as the most important job of an SBC.

However, other desired SBC features that are relevant to the contact center include:

- Voice transcoding: VoIP-to-VoIP – because incoming calls may enter using a wide variety of packet-voice algorithms. Furthermore, all major carriers have already announced the intent to discontinue traditional voice (PCM), resulting in even an even more urgent need for supporting a range of voice algorithms.
- Support for integrating mobile devices - because contact centers must support "callers" on any device from a phone to a tablet to a computer. (Hopefully fax support won't continue to be needed!)
- Call Admission Control - to help ensure bandwidth is available for the calls.
- Video conferencing transcoding - which will increasingly need to support formats such as WebRTC.
- Voice transcoding: PCM-to-VoIP - because some degree of traditional voice will be around for a while.

- Presence - to determine agent availability.
- Collaboration (desktop sharing) transcoding/translation - for customized support.
- Voice over Wi-Fi support and VoLTE - because phones will continue to evolve.
- Instant messaging translation - especially for SMS services.

The SBC has become an integral component for enabling IP-based communications across a network, regardless of the deployment model (appliance vs. virtualized, cloud-based vs. premises based, etc.). It's mission-critical that contact centers take advantage of the value SBCs bring to their network, ensuring the highest standards of authentication, encryption, transcoding, and DDoS protection.

To discuss this TechNote with your professional colleagues, check out the on-line version at Webtorials.

This **TechNote** is brought to you in part due to the generous support of:

Sonus

About the Author

With over thirty years' experience as President and Principal Analyst at Distributed Networking Associates, Inc. Steven Taylor has spent his career as an analyst, journalist, teacher, and evangelist for emerging technologies. This experience allows him to temper the often starry-eyed prognostications about the "Next Big Thing" with a heavy dose of realism and *deja vu*, Over a decade ago, he also founded the Webtorials project where he pioneered the use of the Internet to supplement (and replace) traditional technology trade publications and training. The Webtorials community also provides an excellent database of thought leaders who act as a sounding-board for reality checks on current trends.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
Steven Taylor

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of *Steven Taylor* and *Jim Metzler*