



Practicing Safe SIP

Decision makers are attracted to the many appealing benefits Internet telephony services, such as VoIP/SIP Trunking and Unified Communications as a Service (UCaaS), can provide. Advantages of these IP communications options include increased productivity, Quality of Service (QoS) assurance and virtual PBX hosting. However, before proceeding with a purchase commitment, these C-level managers often ask if IP communication services are safe. Of main concern is the fear that the interconnectedness of the web results in vulnerabilities that could expose company networks, communications and information databases. Although increased exposure is a consequence of utilizing the Internet, IP voice communications solutions can be integrated with confidence, when access is secured through the implementation of Safe SIP practices.

Recognizing the Risks

The transition from TDM to IP communications exposes weak infrastructures. There are more end points; the multitude of end points in turn attracts interest from more hackers. In addressing this increased exposure, IT departments and value added resellers (VARs), need to make every effort to prevent or minimize the potential for disruption or piracy by evaluating security environments, settings and access codes.

Dan York, in his book "Seven Deadliest Unified Communications Attacks," describes the types of attacks that a company could be susceptible to if unaware and unprepared. He explains how the Unified Communications (UC) ecosystem, which consists of IP based equipment (phones, PBXs, routers, etc.), commonly used applications (email, search, database access, etc.) and the integration of voice, video and data in order to provide true presence collaboration, are all exposed to the same security access issues that data has always faced. Therefore, IT managers must be ever vigilant and apply similar procedures for insecure endpoints as those they have implemented for access to business networks and applications.

The end of geography encapsulates the expansion of worldwide interconnectedness, which for the purposes of IT departments can be thought of as the expansion of potential victimization from anywhere. A business can implement procedures that create a very secure environment only to have it compromised by exposure to a partner's unprotected or vulnerable IT network. Control channel vulnerability can lead to toll and international calling fraud, phishing, as well as denial-of-service attacks.

York notes that despite such threats from without, threats from within a company are in fact the most prevalent, most costly and most difficult to prevent. Man-in-the-middle style attacks are a larger threat than all others, because the easiest place from which to eavesdrop or alter

information is from within the enterprise or business itself. After all, the sophistication required to access voice and data packets in the clutter of the Internet highway or private IP networks such as Broadvox is considerably more expensive and difficult than the more commonplace ability of employees and other persons with accessibility from within to eavesdrop, pilfer, modify or appropriate confidential data.

So why don't we read more headlines about employees stealing company secrets and selling them to competitors for a profit, or about the slipping of documents to a colleague in order to help them game the system? - Because incidents of internal abuse are underreported, in an effort to avoid the costly repercussions of a loss of trust in management (from clients, employees, business partners and investors). Internal breaches do occur, and the cost of lost business continued to be the most expensive consequence of a security breach in 2009. On average, the resulting abnormal churn rate was 3.6 percent, according to the Ponemon Institute report entitled, *2009 annual Study: Cost of a Data Breach*.

The Need for Protection

Even innocuous intentions can lead to breaches. When employees do not follow password procedures (or when they compromise secure office computers by visiting unapproved or questionable websites, social networking or entertainment sites) company end-points are exposed to the wild wild web.

Recent events at Gawker Media Inc., a blog publishing website, emphasize the need for such protection. Gawker Media was compromised when hackers accessed over a million usernames and passwords in December and subsequently shared this data free online. Most account holders are notorious for re-using passwords, or popular usernames and default passwords. When extrapolated over many service provider databases, these passwords and usernames become exploitable and can facilitate breaches.

The 2009 Ponemon study demonstrated that both the direct and indirect costs of a security breach are on the rise. Combined, these costs average \$204 per exposed record, totaling an average company loss of \$6.6 million per breach.

Today, the threat of a breach has expanded beyond the world of data - and into the realm of voice communications. Techniques employed to hack for data can be used to disrupt or alter conversations, rich media, telepresence and other collaborative applications.

Prophylactic Procedures

In order to avoid the loss of trust and reputation that a breach incurs, it is important for IT departments to apply the same high standards for voice security as they do for data. Armed with the knowledge of where potential breaches can occur, Internet telephony services can be easily safeguarded to ensure security and limited access. Furthermore, end users can achieve safe interoperability between VoIP/SIP Trunking services and their individual networks.

The first step in practicing safe SIP involves managing administrative access. After properly segmenting access, insisting upon the use of strong passwords that include capitalization, characters and numbers is paramount. These first two steps will address unintended access or the nefarious actions of most disgruntled employees. Additional steps include assuring laptops and servers are properly disposed; backing up databases with strong encryption; and insisting on regularly recurring password changes. In addition, maintaining patch updates when weaknesses and viruses are discovered is essential. Employing automated patch management software will provide for a consistent defense. Supplementary or managed security solutions such as those offered by Sipera, or Session Border Controllers with VoIP security features from AudioCodes, Ingate, Dialogic and other Internet security platform providers, are product offerings available to further assist IT department safety initiatives. Finally, securing broadband connectivity through your SIP Trunking provider minimizes exposure to the public Internet and maximizes QoS.

By simply practicing Safe SIP, businesses can assure that the coupling of secure IP telephony services with their protected business network and ecosystem will be safe from breaches, attacks and viruses. At Broadvox, our SIP engineers assist customers and VARs by explaining the need for these safety measures and by supporting the actual implementation or configuration of required changes. When the potential security concerns and subsequent voice quality issues are understood, clients experience satisfying results – whether they utilize Broadvox broadband or select our Bring Your Own Broadband (BYOB) option. Minimizing security breaches is simply good business for our customers, partners and us.

[For More Information on SIP Trunking visit us at www.broadvox.com](http://www.broadvox.com)