

Article

SIP Security

As SIP trunking helps reduce communication costs for enterprises, by eliminating the need for PSTN gateways, unused ISDN cards and underutilised lines at remote offices, its use has become accepted and part of common voice technology. As this gradual uptake increases, SIP trunks are bridging the gap between PSTN and IP communications. The gap is becoming blurred and companies need to be educated to the security concerns and measures that can be used to ease these security concerns.

What are the main concerns?

Eavesdropping has always been an issue in voice networks and SIP is no different. Previously, voice networks have been closed reducing the possibilities for snooping. The use of the internet for voice has changed that. Unauthorised interception of the media stream can allow an attacker to listen to the call. **Solution:** Encrypt the media stream, like RTP or encrypt all traffic or use a closed IP network, such as VxDSL.

Availability. Loss of service through a Denial-of-Service (DoS) attacks can effect an any IP based services. These attacks send excessive amounts of traffic to parts of your or the service providers network to overwhelm routers and network equipment. **Solution:** Networks can be configured to reduce the effect of DoS attacks. Your ISP will normally be able to stop attacks

when they occur. You could also use a closed network, such as VxDSL.

Authentication is identity a system or user to a particular account. It's important that Digest authentication is used, rather than just clear text. Digest uses MD5 hashing function on a combination of username/password. This protects a user from their details being copied. Some providers only authenticate on IP address, which is a dangerous option and should be carefully monitored and controlled.

Theft covers both service theft, basically toll fraud, and data theft. Authentication helps to prevent toll fraud, which when combined with data security, such as firewalls drastically reduces the threat. One key element that users tend to forget, is securing their side of the network. Your service provider can have the best security, but that will not help if your system is wide open. Make sure your firewall is protecting your voice system, as well as data.

SPIT. Spam over Internet Telephony isn't high on the radar for either service providers or users, at the moment. This will change as more and more SIP systems connect, with the major role of your SIP provider changing from providing connectivity to controlling who connects to you. Vishing (the VoIP version of phishing) is the spoofing of a caller id, making the person receiving the call think the caller is someone else. The technique has been used to harvest personal details from users.

VoIP Threats

Threat	Example	Impact	Solution
Privacy	Calls Eavesdropping Call Recording Voicemail tampering	Identity theft Compromise secrets	Use encryption or private connection such as VxDSL
Availability	Denial of Service (DoS) attack Buffer overflow attacks Worms & viruses	Service outages Service quality	Configure network to prevent DoS and update.
Identification	Registration hijacking Caller ID spoofing Sound insertion	Disruption Identity theft	Protect authentication credentials
Theft	Server of service – toll fraud Data theft – Masquerading data as voice. Invading data network	Excessive phone bills Lost revenue Industrial espionage	Use authentication and monitor usage
SPIT	Unsolicited calling Voice mailbox stuffing Vishing (Voice phishing)	Productivity & system resource Identity theft	Use closed networks, such as Voiceflex

Further information

For further information or help, or to sign-up as a reseller, please contact sales@voiceflex.com.