



A White Paper

Simple, Secure VoIP Now!

**KoolSpan, Inc.
+1 (240) 880-4400
www.koolspan.com**

COMMUNICATIONS COMPLEXITY

The ability to blend telecom technology required at work, home and travel is more of an art than a science. The critical goal is enabling the end user, regardless of location, to make calls and retrieve messages as seamlessly as if they are in the office.

However, giving the end user this flexibility is not without vulnerabilities. Opening the door to a colleague also opens the door to strangers. Enabling telecom access from external end points may lead to those end points misusing the system as well. At the same time, internal end points may also be a source of system misuse.

Most Internet Private Branch eXchanges [iPBXs] intrinsically allow remote usage. Enabling the end user to reach these functions over the Internet is one way to provide services to the remote worker. Unfortunately, enabling end user connectivity via the Internet will also enable hackers and phreakers (phone hackers) to detect the iPBX's presence and services, and may result in security breaches. As Voice over Internet Protocol [VoIP] often requires modifications to otherwise hardened firewalls, these exposure issues are further exacerbated.

For many companies, the fear of security compromises has led to a 'shut it out, shut it down' policy. These companies configure their firewalls to block ports and User Data Program [UDP] traffic that are required for voice. Further complicating VoIP communications, the use of Network Address Translation [NAT] equipment hides the end points making peer-to-peer communication impossible.

VoIP Advantages

Although it has many challenges, VoIP still promises significant cost and operational advantages. Beyond obvious efficiencies of reduced calling charges and deployment of a combined data and telecom infrastructure, users also enjoy new capabilities including greater call clarity and portability enhanced by presence and video services. These benefits are driving market-wide enthusiasm for VoIP services and analysts predictions rapid adoption across the next several years.

The VoIP promise also drives a significant effort industry-wide to address deployment challenges. The trick, however, is to solve these complex problems simply as each layer of complexity serves to erode the VoIP advantage. The following section discusses VoIP and the changing network landscape and provides best practices to a successful deployment.

The iPBX, the Internet and your LAN

The evolution of the Private Branch eXchange [PBX] is the iPBX where the "i" equals the Internet. Every "PBX" manufacturer has adopted and adapted to the use of the Internet in some way. Use of the Internet naturally introduces exposure to Internet-based elements that may exploit the iPBX—now deployed on the corporate network.

With the iPBX converged on the internal network the opportunity for traditional IT headaches to affect the voice network quickly becomes a reality. Voice has become simply another application running on a server. Server attacks on the iPBX and specific VoIP application attacks are possible. While hardening servers is a good strategy, today's hardened system maybe tomorrow's vulnerability.

As the concept of wires and circuits gives way to sockets and sessions, the iPBX is simply another application server. However, unlike other application servers, each iPBX vendor has implemented very different operational and security models. In some cases, this variation exists within a single vendor's own product line offerings. For large corporations with a mix of vendor solutions across multiple locations, familiarity with one iPBX platform does not provide a comprehensive view to security risks and policies organization wide.

VoIP sessions create connections between an iPBX and IP phones. Most IP phones are intelligent end points that could be attacked, much like the rising trend of attacks on cell phones. Worms and viruses are engineered to attack IP phones, iPBX and the network to which everything is connected, leaving an enterprise vulnerable to attack.

Security strategies should address the iPBX along with other application servers and the IP phones as equivalent nodes requiring security on the corporate network.

iPBX Interconnection & SIP Trunking

Legacy PBXs took advantage of technology that brought "big pipes" (known as Integrated Services Digital Network - Primary Rate Interface [ISDN - PRI]) directly into the PBX. These pipes are dedicated voice circuits that have nothing to do with the Internet. Today, major carriers and the vendor community recognize that this technology is costly to implement and could be replaced with the concept of SIP Trunking. SIP Trunking involves multiple concurrent sessions that the iPBX establishes with the carrier over Internet-based facilities. This removes the boundaries of specific circuit counts or limits and permits more concurrent sessions. While the iPBX may connect directly over Internet to the network service provider (a.k.a. carrier), most companies still opt for a dedicated facility. As the iPBX connects to the Internet, the value of the voice network expands according to Metcalfe's law (which approximates a network's value to be equal to the square of its number of users). Metcalfe's math may also serve as a corollary to the security threat represented by the Internet.

VoIP sessions are designed to rely on routers to move voice packets. Using the Internet, which was designed to leverage redundancy and to find the best possible route for packet traffic, is an asset to VoIP. Within the VoIP architecture, phone numbers are associated with IP addresses and routed across the Internet to the nearest point. Configuring a VoIP network with both dedicated and Internet known addresses allows for additional redundancy.

This architecture looks for the network edge to be self empowered. However, many carriers and enterprises have been concerned with this ability and have deployed devices to control how sessions are managed at the edge. These “session controllers” are designed to be aggregation points for VoIP traffic and to guard the “borders” of the network. As both carriers and enterprises have deployed these devices on their networks with the goal of protecting their own facilities, there are interesting questions of authority and control as these devices themselves rely on interoperability with third-parties. To assure proper inter-organization communications trust and testing are required. While the session controller addresses real concerns, the problem with aggregation points is that they become possible points of failure, particularly since many are designed to stay in the path of the media.

VoIP’s Many Challenges

VoIP deployment challenges include:

- *NAT Traversal* – SIP, the VoIP protocol, is incompatible with NAT. To complete calls, a corporation must implement additional hardware or compromise its firewall.
- *Infrastructure Exposure* – A networked voice system is susceptible to network attacks. As VoIP is deployed on the corporate network, the corporate LAN becomes exposed.
- *Bandwidth* – Encryption compounds problems with bandwidth-dependent call quality
- *Complexity Creep* – VoIP’s benefits are at risk of being overrun by complexity as organizations implement layers of additional systems to fortify the system.
- *Security* – Conversations are exposed to eavesdropping and the corporate network to a new set of attacks if not protected.
- *Evolving Standards* – A laborious process, success of these efforts relies on their timely completion and the preservation of the simplicity on which the Internet relies.

KOOLSPAN: A SIMPLE SOLUTION TO VOIP’S COMPLEX PROBLEMS

KoolSpan delivers a very powerful, yet simple approach to a secure robust voice network—enable all VoIP devices on the network to securely interoperate with each other as true LAN-peers without a proxy or any other interference.

KoolSpan provides its users these immediate benefits:

- *Strong Security* – Mutual authentication and 256-bit AES encryption with per packet keying, based entirely on Smart Cards, not servers.
- *Extended Infrastructure* – All connections are secure Layer 2 UDP links, enabling for the rapid and easy rollout of the VoIP network with all functionality to any endpoint.

- *NAT Traversal a Non-Issue* – All callers are always local to the iPBX from anywhere; without a proxy, and with a Layer 2 link, all VoIP devices are true-LAN peers.
- *Equipment Independence* – All VoIP equipment is supported with modification. Ideal for environments comprised of a mix of vendor equipment, KoolSpan establishes the highest common denominator in security and functionality.
- *VoIP ROI: Expansion without Replication* – Reduce iPBX deployments for multiple sites as the VoIP LAN is easily extended to branch offices and remote workers, enabling IP Phones and softphones to operate without an iPBX extender.
- *SIP Trunking Simplified* – Easily interconnect with carriers and branch offices with snap-in-line equipment that operates automatically and without ongoing management.
- *Beyond Voice* – Leverage the same security architecture for non-voice applications and other Internet, LAN and WAN communications.

KoolSpan uniquely addresses the interconnection and security issues of voice networks. By design, KoolSpan is very VoIP friendly. Based entirely on UDP (as is VoIP), KoolSpan operates inside and outside the firewall at the network layer (OSI: Layer 2). As a result, KoolSpan operates without any modification to VoIP protocols or equipment and all VoIP features including broadcast are available at every secured endpoint. It automatically provides mutual authentication and per packet 256-bit Advanced Encryption Standard [AES] protection without impacting the communications in between.

The KoolSpan solution is based entirely on Smart Cards, not servers. Implemented on both sides of the communications link, Smart Cards are embedded in KoolSpan Locks and Keys respectively. Locks are paired with Keys for secure user connectivity, or with other Locks for secure inter-network connectivity. Whether it's Locks connecting with Keys or with other Locks, the resulting links enable the extension of a highly secure VoIP network where all equipment on the network, regardless of location and without modification, operates as if it were on the same LAN. There is no proxy or other complexity and a voice network can be extended without infrastructure replication. Broadcast services such as paging and reverse 911 remain available to all end points on the network.

In short, the iPBX at headquarters, remote workers with a soft phone, and physical IP phones at a branch office all recognize each other as true-LAN peers. All traffic is highly secured, NAT issues are sidestepped and no modifications were made to the VoIP equipment itself.

Remote Worker Connectivity

Remote workers simply need a KoolSpan Key to transform their laptop and softphone

into a peered extension of the corporate telephony network. Calls are placed and received as if the user were on the corporate LAN, complete with internal extension dialing. Simply plug in the KoolSpan Key, a USB token which houses a Smart Card, enter a security PIN and a secure Layer 2 connection is established between the Key and the network Lock. The Lock does not act as a proxy or attempt to manage the media, but instead simply and efficiently establishes secure links. As a result, the soft phone registers with the iPBX as a true LAN-peer and all network services including DHCP services are provided by the telephony network. NAT issues are simply avoided and the media flows securely but without manipulation. The Key and Lock deliver this same secure connection whether the user is inside or outside the LAN, providing protection to sensitive conversations, which may be conducted entirely within the firewall.

Of significant importance, the user experience is intuitive and unchanging regardless of location. The result is a reduction in complexity and training, with a corresponding increase in telecom security. After all, security is only as good as it is easy to use.

Highlighting the advantages of KoolSpan for remote workers:

- Reduces operational expense
- Strong security with authentication and encryption across the Internet
- Universal equipment and application compatibility
- Easy, intuitive and consistent operation
- Avoids Internet Service Provider challenges

Connecting the Branch Office

The branch office is supported by connecting multiple KoolSpan Locks. A Parent Lock on a logical network segment with the iPBX and Children Locks at any number of remote locations. The result is a single secured telephony LAN. So regardless of the iPBX configuration distant end points can be easily enabled without replication of the iPBX infrastructure. As KoolSpan combines AES (a non-expanding encryption algorithm) and UDP (a stateless protocol which is used by VoIP), protected connections are delivered without discernable impact on bandwidth.

The benefit of this branch office connectivity is that there is a clear reduction in the complexity at each point on the network and particularly at the remote offices where corporate resources are often more limited. With secured Layer 2 connections part of the network-wide foundation, all features of the iPBX are available across the entire network which further enables, in some cases, for less expensive or intelligent physical IP phones to be used.

The Internet is often a good choice when connecting remote branch offices. While it cannot be relied on for *all* voice traffic, it's a solution that currently supports millions of users regularly and has the distinct advantage of being ubiquitous. Private circuits are sometime also a good option, but should be implemented with the same security

concerns that are involved in Internet based architecture.

Summarizing KoolSpan unique benefits for branch offices deployments:

- Reduce branch office complexity, 'home' phones to remote iPBXs
- Enable all network features without configuration in the field
- Bypass of NAT traversal issues
- Accelerate VoIP ROI
- Roll-out VoIP without increasing infrastructure complexity
- Enable strong security for voice and any other applications

PBX Interconnection & SIP Trunking

VoIP reflect the original phone network, in that each carrier has built their respective network based on their requirements. The result is that VoIP has developed as a series of isolated islands that now need to be interconnected or bridged. While the various peering methodologies are beyond the scope of this paper, the momentum behind this market signals a clear shift from a traditional circuit switched network to SIP trunking architecture. The benefits of trunking include reduce cost and new possibilities for rich media services such as improved voice compression and collaborative conferencing.

The elegance of KoolSpan is that whether you are connecting two iPBXs directly together, or enabling your carrier to reach your network by providing a child Lock at the carrier's end, you are delivering secured sessions directly between the iPBXs and carrier switches without a device adding complexity to the network or getting in the middle of the media.

This reduces the reliance on any one carrier's strategy and enables self management including the possibility of relying on the open Internet when appropriate, or rolling out your own communication tools. This includes features such as paging, reverse 911 and video calls.

The advantages of KoolSpan for Interconnecting Trunks include

- Ideal for immediate, secure field communication
- All applications, services and devices bridged automatically with no modifications
- Independent interaction from carrier's solution
- Fully duplex communications/discovery
- Preconfigured, no setup or ongoing maintenance

Simplicity is the Best Practice

KoolSpan simplifies the issues associated with deploying VoIP networks by making all elements of the network part of a single logical network. This approach allows the iPBX and all VoIP phones to operate with their full feature set and without a cascading set of intermediary equipment.

KoolSpan's automatic operation delivers secure connections inside and outside the firewall. This constant, unchanging operation, reduces network complexity, deployment costs, equipment expense and ongoing management overhead. The solution can be implemented in a variety of architectures ranging from small office connectivity to large enterprise topologies with multiple branch offices and volumes of nomadic workers. Keeping with its simplicity Koolspan is not VoIP-specific and can be leveraged by any other application across any network.

Simple and highly secure, KoolSpan enables the practice of keeping access easy to implement and administer.

For more information please contact info@koolspan.com

About the author

Carl Ford has been working on Voice over IP solutions since 1998 and is at the heart of the VoIP industry as Vice President of Content and Community at pulver.com. He can be reached at carl@pulvermedia.com.