



Enterprise IP PBX Security

System Evaluation Across Multiple Levels

Introduction

Security is a vital consideration when evaluating an enterprise IP telecommunications solution. Typically referred to as an IP PBX, though now encompassing much more than simply an IP version of a TDM-based PBX, these systems leverage the data network to reduce total cost of ownership and increase productivity for both end-users and systems administrators alike.

In addition to delivering business benefits, a voice-over-IP system may also become a new target for unauthorized or malicious users and must be secured against these threats. As many organizations understand, if threats and vulnerabilities are not adequately addressed, the results could be devastating with respect to lost productivity, resources and reputation.

Fortunately, a high level of telecommunications security can be achieved without additional cost by deploying a voice-over-IP system which has been designed with robust security capabilities, has undergone rigorous security testing and is deployed on top of a network already protected by common and standard network security practices.

Security considerations for voice-over-IP systems fall into three areas:

- 1) resilience of the system against threats and vulnerabilities,
- 2) security features to enable effective access control, and
- 3) the ability of the system to enhance overall security for the organization.

To aid in the evaluation process, government entities such as the National Security Agency and the National Institute of Standards and Technology develop security guidelines and establish the most rigorous security testing programs to provide the highest levels of assurance that an enterprise telecommunications system is secure and reliable.

Sphere understands the importance of securing voice-over-IP enterprise telecommunications systems as our customers demand mission critical reliability in such environments as police/fire departments, hospitals and military installations.

This white paper outlines the security capabilities available in the Spherica11 system, rigorous independent security testing completed and best practices accumulated over years of voice-over-IP enterprise telecommunications experience.

Rigorous Security Testing

Recently, Sphere Communications submitted its system for the most rigorous independent security testing available which is conducted by the U.S. Department of Defense in conjunction with the National Security Agency (NSA).

Known as Information Assurance, this highly rigorous series of security testing evaluates the capabilities and the resilience of Sphere's enterprise IP telecommunications solution which consists of its Spherically software and VG3 media gateways.

The testing process follows standards defined in the National Security Telecommunications and Information Systems Security Policy¹ and is based on:

- International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement²;
- National Institute of Standards and Technology³ (NIST) Federal Information Processing Standard⁴ (FIPS) validation program;
- National Security Agency⁵ (NSA) and NIST National Information Assurance Partnership⁶ (NIAP) evaluation and validation program; and
- Department of Defense policy and guidance for the protection of voice signaling and bearer traffic.

The DoD Information Assurance test requirements are divided into two phases, a functional security phase and a vulnerability assessment phase. The functional security phase uses the NSA/NIST PBX Telecommunications Switch Protection Profile test methodology to determine whether the switch under test meets the required security features. These features include the granularity of administrative control, the protection of audit data and account activities.

The second phase of testing consists of a comprehensive vulnerability assessment following NIAP guidelines on Network Security Testing. The objective is to determine the resilience of a voice solution to common types of attacks such as denial of service, malformed packets, LAND-type attacks, etc. Several types of network security testing techniques employed include Network Mapping, Vulnerability Scanning, Penetration Testing, Security Test & Evaluation, Password Cracking, Log Reviews, File Integrity Checkers, Virus Detectors and War Dialing.

Sphere Communications has completed this highest level of independent security testing and is the only product of its kind to do so. Additionally, the DoD's Joint Interoperability Test Command⁷ (JITC) has determined that this system meets critical interoperability requirements and achieves 99.999% reliability as defined in its Generic Switching Center Requirements⁸ (GSCR).

¹ NSTISSP #11 is national security policy governing the acquisition of information assurance (IA) and IA enabled information technology products (www.nstissc.gov/Assets/pdf/NSTISSP_11_revised_fst.pdf).

² ICC is an alignment of the existing European, US and Canadian information technology security criteria; ITSEC, TCSEC and CTCPEC respectively (www.commoncriteriaportal.org).

³ NIST is a federal technology agency that develops measurement, standards and technology (www.nist.gov).

⁴ FIPS are issued by NIST for federal government requirements including computer security and interoperability (www.itl.nist.gov/fipspubs).

⁵ NSA protects U.S. information systems including all classified and sensitive information that is stored or sent through U.S. government equipment (www.nsa.gov).

⁶ NIAP develops security requirements and evaluation measures for IT systems under the Computer Security Act of 1987 (<http://niap.nist.gov>).

⁷ JITC evaluates and certifies all information technology systems for the Department of Defense (<http://jitic.fhu.disa.mil>).

⁸ GSCR defines interconnection requirements for the Defense Switched Network, a worldwide private line telephone network (<http://jitic.fhu.disa.mil/tssi/certdocs.html>).

Spherically Security Architecture

Sphere Communications has designed its system from the ground up to be highly secure, reliable and resilient to potential threats and vulnerabilities.

Its carrier-grade architecture, which separates call control from the underlying network infrastructure, enables the system to be designed and protected as any other mission critical application on the network. This alleviates the additional challenge of ensuring the security, reliability and resilience of proprietary voice switching equipment as well as alleviates these same challenges found in solutions that embed call control intelligence in the operating systems of switches and routers in the existing network infrastructure.

To address threats and vulnerabilities to the enterprise telecommunications system, security controls are applied at four levels in the Sphere solution. These are: user-level security, application-level security, administrative-level security and network-level security.

User-Level Security

User-level security provides access control while enabling the use of resources available on the system. The Sphere system provides a complete suite of user-level security features to control dialing, endpoint access, feature configuration and monitoring rights. Significant granularity of control is provided down to the type of information users can and cannot see consistent with both security and individual privacy concerns. For instance, with the Spherically system a manager with the proper user rights may monitor a subordinate's use of the system, while the capability is provided to ensure this feature operates in a one-way manner so that the subordinate is not inadvertently granted the rights to monitor the manager's use of the system.

Additionally, user-level security features of the Spherically software protect against unauthorized, malicious and fraudulent access and therefore mitigate risks such as unnecessary toll charges, toll fraud and over consumption of bandwidth.

Specific features include:

- Feature Restriction – The Spherically System Administrator develops profiles on a feature-by-feature basis which are then separately applied to users and lines. For example, the Sphere system limits the use of certain features given to a user, such as call waiting or video conferencing.
- Monitoring Control – User-by-user configuration is provided to control which users have the rights to monitor calls, obtain caller ID or to view the presence⁹ state of other users.
- Line and User Rights – The process of matching users to lines enables the Spherically System Administrator to restrict which devices a user controls and accesses.
- Class of Service Profiles – The Spherically System Administrator develops Class of Service profiles which groups users, lines and systems with specific access controls such as restricting and enabling telephone numbers users can or cannot dial. For example, an organization may restrict the use of 900 numbers (common in the US). This feature enables mandatory access control policies to be developed and applied across the enterprise.
- Personal Identification Numbers – With the proper rights granted under a user profile or class of service profile, authorized users may override restrictions assigned to a station by applying a Personal Identification Number (PIN) on a call-by-call basis. This discretionary

⁹ Presence - a productivity capability that displays availability of other users such as "on the phone", "in a meeting", etc.

access control enables authorized users to achieve real-time flexibility in pre-defined work processes. For example, traveling employees may utilize a shared office or cubicle and be able to make long distance phone calls over an otherwise restricted line.

- Desktop Authentication – Whether utilizing the Spherical Desktop on an office PC integrated with an IP or legacy phone, or utilizing the Spherical Desktop with headset/microphone in a softphone configuration, a network login is required which leverages the existing security system to authenticate the user and provide access to a particular endpoint. Because this access control capability is part of the underlying network it can be further enhanced through two-factor authentication solutions widely available and in use today.
- Call Routing and Blocking – Calls coming into the Sphere system can be routed based on numerous call characteristics including time of day. For instance, calls may first go to an internal extension (e.g. office assistant) prior to transferring into a conference room phone. This ability to limit inbound access from the PSTN ensures a high level of control for the Spherical System Administrator.
- Multilevel Precedence and Preemption – This feature, designed for use in military and government environments, enables senior ranking authorized users to preempt subordinate users as designated by their class profile. Applied in non-military environments this feature enables security officers for example to immediately preempt existing calls in a crisis situation.
- Call Detail Reporting – Multiple means of capturing call details and usage are available both in real time and via audit trail records, which are used for ad hoc review and regular reporting to identify security concerns as well as to support common call accounting and reporting applications alerting of system misuse.
- Emergency Dialing – Spherical System Administrators establish emergency numbers such as 911 that take precedence over non-emergency calls. This feature includes the ability for the system to automatically drop other non-emergency calls if necessary should the system be at capacity at any given moment. Additionally, station identification data can be sent to Public Safety Answering Points¹⁰ (PSAP) for use by emergency services personnel. This capability directly contributes to physical security for individuals and can enhance business continuity and disaster recovery procedures for the organization.

As a component of a comprehensive security policy, effectively implementing these and other user-level security features on the enterprise telecommunications system requires two major steps. The first step is to establish the requirements necessary for users to perform their jobs effectively in support of business processes. Next, the Spherical System Administrator maps these requirements into profiles to be applied across users, lines and calling patterns on the system.

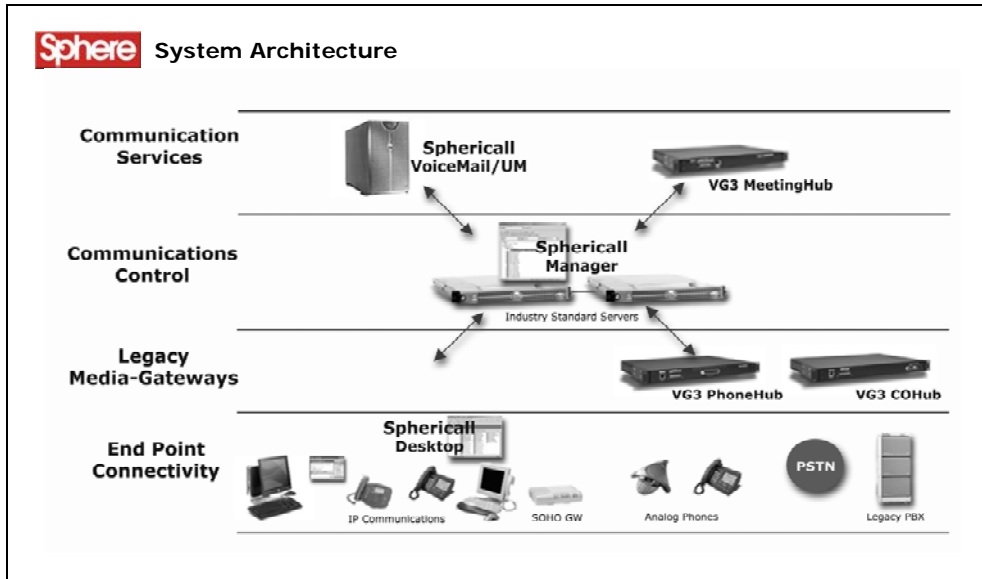
Application-Level Security

Application-level security ensures the resilience of the Spherical Manager software which runs on industry standard servers. This ensures that call processes are highly available to perform the necessary functions for system operation.

The Sphere system architecture defines a network of Spherical Manager servers that make up the core enterprise telecommunications system. Multiple servers are typically decentralized across multiple sites, the system architecture is centralized with a primary administration server updating subordinate administrators throughout the system. Should one of the Sphere servers fail, the entire Sphere system continues to operate transparently to every end user anywhere on the system. This centralized system architecture which is inherently easier to protect, delivers greater security as well as greater resilience for the telecommunications system.

¹⁰ A Public Safety Answering Point (PSAP) is a facility equipped and staffed to receive 911 calls.

Sphere leverages industry standard servers to host the Spherical Manager application. Security controls aimed at addressing vulnerabilities of network servers are applied using the same tools and procedures that already exist in the organization for protecting other network servers hosting mission critical applications.



Sphere Communications' Spherical Manager and Spherical Desktop software applications run in a Windows environment and leverage the security features of the Windows operating system. As with any Windows operating system, certain care must be taken to mitigate known security risks. For example, Sphere does not require the IIS service and strongly recommends that it is disabled on servers running Spherical.

In addition, Sphere recommends best practices specifically designed to ensure integrity of the Spherical telecommunications system. These include:

- Application services running within the Spherical Manager are set to automatic recovery which enables an instantaneous restarting of individual system services transparent to end users which ensures compliance with its fault tolerant system design;
- All unnecessary services or applications such as Web hosting, internet services (e.g. IIS) or web browsing applications are not permitted on the Sphere servers;
- Standard procedures of implementing virus protection updates, back up and maintenance on an ongoing basis are recommended;
- Sphere servers should be distributed with respect to power and physical location to ensure disaster tolerance;
- Sphere servers should be physically secure such as located in locked cabinets within a secure data center to ensure compliance with an organization's operations security policy.

A complete list of best practices and procedures when implementing the Spherical system are found in Sphere documentation.

Administrative-Level Security

Administrative-level security is primarily concerned with access control surrounding the Spherical Manager application which allows the Sphere system to be configured and changed by the Spherical System Administrator.

As noted above, the Spherical Manager runs within an isolated Windows environment and provides two levels of security for access.

First, access control to the server is achieved through standard network level security of user name/password granted to an authorized user by the Network Administrator. As noted above this level of security can be further enhanced through widely available two-factor authentication solutions. In addition, standard security practices apply for timely changing of passwords, uniqueness of password, limited users, etc., as for all network application servers in the enterprise.

The second level of access control is provided by restricting access to the Spherical Manager itself. In order for an authorized user to modify the Sphere system, the user must specifically be granted access rights from a current Spherical System Administrator. This second level of security enables a high level of access control to ensure protection of the enterprise telecommunications system.

Network-Level Security

An important element of the Sphere system architecture is that call control intelligence is purposely separated from the underlying network. This enables an enterprise telecommunications system to be deployed as a truly open system in the same manner as other mission critical applications on the network such as ERP, CRM, databases, email, etc.

With the Sphere system, voice traffic appears as normal data and exists within the overall data security procedures implemented on the network. The Sphere system utilizes standard RTP data streams for voice and therefore once a call is established, only the call media streams traverse the network. As a result, the Sphere system leverages all of the benefits of an open system and requires no additional investment in equipment, training or services to maintain a highly secure enterprise telecommunications system.

Existing network security practices such as the implementation of firewalls, intrusion detection and prevention systems and anti-virus software provides security for the telecommunications system in the same way that other data, systems and applications on the network are secured. Network-level security for the Spherical system is further enhanced through the following best practices:

- Virtual separation of the voice traffic via VLANs to subnets that are not directly connected to the outside world.
- Restriction of TCP and UDP availability to only necessary ports. The Sphere system does not use common ports used by other applications as these are typically the most likely targets of security breaches or attacks.
- Implementation of Quality of Service mechanisms to give priority to voice traffic and ensure overriding potentially unauthorized traffic that may be maliciously introduced on the network such as during a DoS attack.
- Provide access to off-network devices such as remote softphones via VPN or other secure tunneling methods.

Conclusions

By choosing a properly designed voice-over-IP telecommunications system that offers robust security capabilities and by deploying the system as a mission critical application in an environment of security best practices, IT decision makers will find that no additional cost is required to ensure security, reliability and resilience.

As a result, careful consideration should be given to each system under evaluation to assess given security capabilities and to understand whether additional policies, practices and infrastructure may be required to adequately address threats and vulnerabilities.

Though some consideration is given to proprietary security schemes (i.e. security by obscurity), the reality is that an unknown security capability results in an unknown level of risk incurred by the organization. Instead, IT decision makers should consider open systems that have been subjected to the highest levels of rigorous and independent testing as these enable an organization to confidently deliver a highly secure, reliable and resilient enterprise IP telecommunications solution.

Additionally, careful consideration should be given to how well the system enhances the organization's overall security policy. Systems designed with best practices in mind developed through years of voice-over-IP telecommunications experience are well positioned to integrate effectively with an organization's various security guidelines and procedures ranging from individual privacy, physical security and disaster recovery.

By choosing such a system, IT decision makers will find themselves well positioned to achieve significant business results through an enterprise IP telecommunications solution.

Kurt Jacobs
Director of Strategic Alliances
Sphere Communications Inc.
kjacobs@spherecom.com

Andy Mercker
Director of Marketing, CISSP¹¹
Sphere Communications Inc.
amercker@spherecom.com

About Sphere Communications

Sphere Communications is the first to deliver IP PBX technology as a business application for Service Oriented Architectures. A software company, Sphere has the most robust IP-based software communications technology available in the marketplace. Developed around hundreds of enterprise installations, the Spherical platform hosts an extremely rich PBX feature set and is proven in deployments that scale to more than 20,000 users. Sphere provides application developers with a Communications Web Services SDK, enabling communications to be integrated with a wide range of business applications. Founded in 1994, Sphere Communications is headquartered in Lincolnshire, Illinois and provides its products to a variety of enterprise customer networks. For more information please see the Sphere Communications web site at www.spherecom.com or contact us at 1-888-774-3732.



Sphere Communications Inc.
300 Tri-State International, Suite 150
Lincolnshire, Illinois 60069
USA

www.spherecom.com
Telephone: 847-793-9600
Facsimile: 847-793-9690

P/N 0904-WP-SCE

¹¹ Certified Information Systems Security Professional (www.isc2.org).