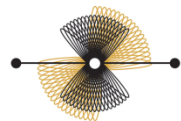
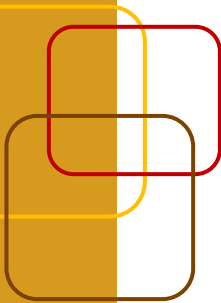


Securing your Business with IP Communications

Your Business's Best Friend for
Protecting Voice and Data

By
Rachel Wentink
Director, Product Management

April, 2008



INTERACTIVE INTELLIGENCE[®]
Deliberately Innovative

Copyright © 2008 Interactive Intelligence, Inc. All rights reserved.

Brand and product names referred to in this document are the trademarks or registered trademarks of their respective companies.

Interactive Intelligence, Inc.
7601 Interactive Way
Indianapolis, Indiana 46278
Phone and Fax | 317.872.3000
www.inin.com

Publish date 4/08, version 1

Introduction

It's a wonder IT directors ever get any sleep. The possibility of malicious attacks to a business's network and communications system, they'll tell you, is a constant threat. And if a security breach ever does occur, losing confidential data and the faith of customers can become their worst nightmare.

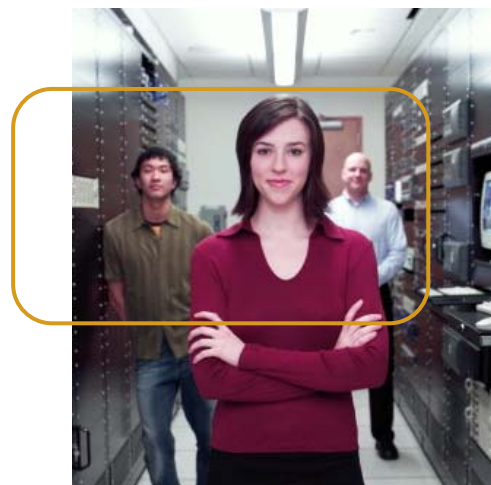
The security news for businesses utilizing Internet Protocol (IP) communications and voice over IP (VoIP), however, is good. Newer standards are constantly being deployed for IP technologies to make security more concrete, and as a whole, it's safe to say the IP security mechanisms now available are some of the most stringent ever.

Security at the levels a business needs

For organizations in which networked interactions and information need to stay private — financial institutions, healthcare providers, insurance companies, government agencies, retail organizations, contact centers, *et al* — it's critical to plan and implement the highest levels of security available to protect voice and data communications. A few examples: Regulatory guidelines for credit card processing require unified layers of data encryption and user authentication to protect customer privacy, as do healthcare industry guidelines to safeguard patient confidentiality • Remote workers necessitate a security plan for home office Internet connections and “personal” firewalls in conjunction with corporate security policies • Internally, encrypting voice payloads both at the station level and site level can prevent employees from “sniffing” a network to eavesdrop on VoIP calls from their PC or workstation. For the same reason, it's important to encrypt calls to interactive voice response (IVR) applications and automatic call distributors (ACDs) where confidential information is routinely exchanged.

It's unfortunate, but security attacks are a reality of business, and any organization that handles customer-related confidential information on an IP-based data network must make securing calls and information a priority. Thankfully for your business and the customers it serves, an IP communications platform lets you soundly align the security mechanisms of IP technologies with organizational processes and the human factor to build a stronger wall of protection.

Trust us.



Security for VoIP is rarely ever a straightforward issue, but for this particular discussion let's just say security can follow a proprietary path or a course that's open and standards-based.

In effect, those vendors who offer proprietary means of encryption in a VoIP solution rely on their programmers to outsmart an entire community of hackers. Programmers can ward off hacker activities to a degree, of course, but the law of averages says hackers eventually will win. By contrast, standards-based encryption is backed by a virtual community of developers around the world, and is considered the stronger security measure in that this entire global "community" can improve encryption for VoIP should hackers ever expose a vulnerability.

Among open standards, the Session Initiation Protocol — or SIP — is highly accepted worldwide for its rigorous message encryption and user authentication in a VoIP environment. (SIP is also often recognized for paving a migration path to VoIP.) For security, the measures in SIP stem from the same intrusion concerns that have led to firewalls, intrusion detection systems, virtual private networks (VPNs), and the use of network DeMilitarized Zones (DMZs) to safeguard communications systems in their entirety.

The IETF and RFCs

SIP has become the most dependable tool for IP communications security because it's the most strictly regulated, compliments of the Internet Engineering Task Force (IETF). In conjunction with new and updated IP technologies, IETF member organizations continually introduce and amend SIP security specifications established in industry-wide Request for Comment (RFC) records. The SIP RFC itself is the largest in the IETF library, although several RFCs are available for security, such as RFC 1918 to describe the IP address space needed to build private networks.

TLS and SRTP for encryption

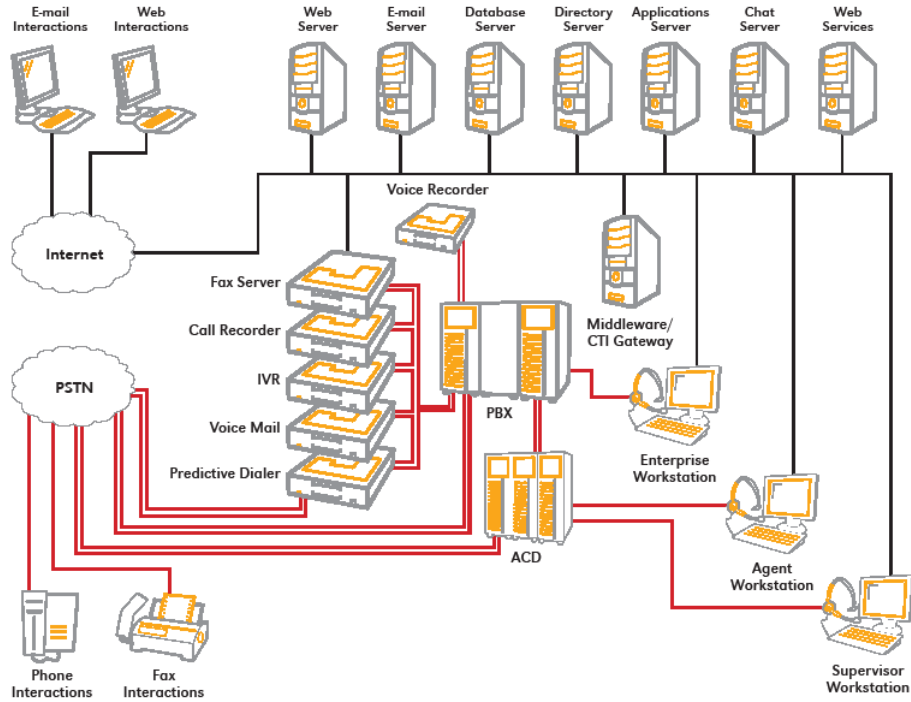
Two security standards to note for their encryption capability are Transport Layer Security (TLS) and the Secure Real-time Transport Protocol (SRTP). TLS, specified by the IETF in RFC 2246, is based on the Secure Sockets Layer (SSL) standard and extends two distinct layers of security for an IP-based network: the TLS Record Protocol, which ensures a private network connection via symmetric encryption, and the TLS Handshake Protocol, which provides authentication between an IP application server and a client using digital certificates. Organizations can additionally use the TLS Handshake Protocol for negotiating encryption algorithm cryptographic keys prior to establishing data communications. Because TLS overall is independent of applications-layer protocols at higher levels, such as the HyperText Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP), it essentially provides an extra level of protection for data transmissions.

Also for data security, SRTP (RFC 3711) is a profile of the Real-time Transport Protocol (RTP) and provides a framework for confidentiality, message authentication and replay protection to RTP traffic on a data network. SRTP's greatest benefit is that it defines a set of default cryptographic transforms and allows new transforms to be introduced as needed, making it a strong safeguard (with appropriate key management) for unicast and multicast RTP applications in environments built on a combination of wired and wireless networks.

An All-in-One Application Approach to Security

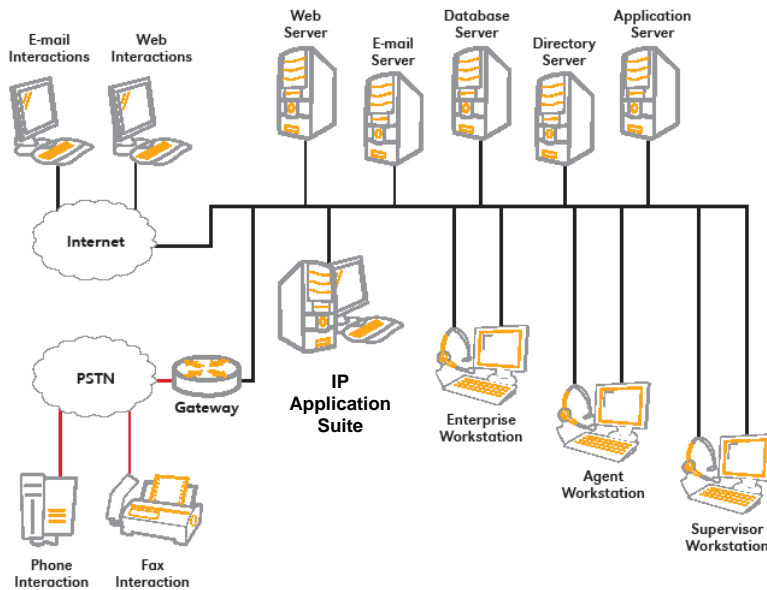
Traditional multi-point communication systems

Multiple systems and third-party integrations create more points of entry for potential security breaches.



All-in-one platform solution for IP communications

Single platform and pre-integrated application suite eliminates multiple access points.



An All-in-One Application Approach to Security

Inherent security with a single platform and application suite

Go back and look at the two architecture graphics for a minute, specifically the all-in-one platform solution at the bottom. Unlike multi-point hardware systems and their integrated third-party products, an all-in-one application suite channels voice, messaging and data functions down to one platform consisting of a few servers and far fewer moving parts. Inherently, then, security gets channeled down to the same server-based platform, where fewer access points exist for potential attacks. Moreover with all-in-one application suites in a VoIP configuration, servers are connected to and administered on a single SIP-supported data network (LAN or WAN), allowing an organization to reinforce security at the network level via SIP's built-in mechanisms for VPN, virtual LANs (VLANs), access lists, authentication, and the TLS and SRTP standards.

Don't buy in to "SIP-enabled" or "proprietary extensions"

A word of caution about what some vendors classify as IP platforms and all-in-one solutions: Be wary of any platform consisting of proprietary "SIP-enabled" hardware components and third-party applications. Here's why.

From its inception, SIP has been developed to make interoperability easier than with older protocols infamous for system compatibility problems, such as the Integrated Services Digital Network (ISDN) that has been utilized for years to support PBX phone equipment. Because the objective of SIP and VoIP is to direct calls to application servers on a data network the same way as emails, web chats and other converged media, SIP has dictated that IP

technologies themselves be software-oriented given the media adaptability involved. Therefore, the best platform for IP communications, and for SIP's available security measures, is one developed on an open, all-software architecture that pre-integrates the SIP standard throughout.

For the same reason, be wary of any vendor who offers "proprietary extensions" to SIP RFCs. SIP RFCs are standards that any vendor can choose to implement, and proprietary extensions mean that a vendor has chosen their own way to implement a standard. The problem with proprietary extensions is that they confine system behavior and guarantee vendor lock-in, much as in the old mainframe days. Likewise, they limit interoperability and, by default, limit your choices of interoperable SIP hardware and software for IP communications.

Security from the network to the desktop

Proprietary systems and most third-party integration packages simply aren't designed for SIP and its network security mechanisms. However, a platform that fully applies the SIP standard for VoIP can accommodate security standards between the network and application servers as *well* as the gateway and telephone devices at the desktop level.

WHY INTEROPERABILITY MATTERS

Interoperability in the IP world refers to the ability of equipment from various vendors to work together using a common set of protocols... theoretically to "talk to one another."

By leveraging SIP, an open IP platform can easily support an organization's voice and data applications, end-user devices, existing business systems and other equipment within the same IP infrastructure. That not only reduces implementation and operations costs, it positions a business for easier interoperability in the event of an acquisition or merger.

Unfortunately proprietary IP solutions tend to work only with other products from the same vendor, severely limiting true solution interoperability.

The Human Factor

Employees can pose significant risks when they ignore a company's security processes or deliberately circumvent them for personal gain. Though hiring laws and costs often keep businesses from conducting background checks to limit potential worker security risks up-front, a business *can* leverage the system and user security controls in most IP communications application suites to monitor employees. They can also make sure every user abides by established corporate policies with regard to those controls. Among other security measures at the employee level, a business can:

- Assign user access rights to specific system functions, such as database access to customer account records, CRM records, etc.
- Assign user license keys, by user or station, to designate system administration users, departmental users (Finance, Tech Support, etc.), remote users, and other user types.
- Listen to live calls, record calls and "screen record" desktop activity (a common monitoring practice in contact centers), and designate strict user rights for accessing and playing back recording files.
- Establish company guidelines and user permissions to make external calls, long-distance calls, X number of calls at a time, etc., with permissions granted by individual, workgroup, or role (class of service).
- Set access levels for all users, such as system access for 900 calls.
- Routinely track and report on calls, emails, web chats and other media.

Preventing Fraud and Malicious Attacks

The best way to establish security controls against fraud and malicious system attacks is by jointly maintaining class of service, supporting standard firewalls and handling Denial of Service (DoS) attacks. Here are some best practices to consider.

Class of Service

Toll fraud prevention

IP communications make it possible to prevent toll fraud by disabling voice the aspects of an IP application suite's PBX/IP PBX and ACD functions and establishing remote access points on a per-user basis. One method of remote access is with the Follow-me/Find-me feature in most IP systems, by which users can forward their corporate extension to a mobile device or home office phone. Another way is via a company directory that allows external access to the corporate system.

Malicious Attacks

Phone configuration on the network

One of the most prominent benefits of VoIP and SIP is the new breed of low-cost SIP phones, which demand their own security precautions when deploying them over an IP network. Because a SIP phone is essentially a small computer, each individual device utilizes a specific file for configuration. Also if using a Trivial File Transfer Protocol (TFTP) server to specify the extensions an organization can upload for SIP phones, the TFTP server can be in a read/write mode yet not allow configuration (.cfg) files to be overwritten or modified. Some IP systems even include an auto-provisioning server that can be configured behind the firewall to prevent rogue phones from being registered.

Malicious Attacks (continued)

Spooing the server

A potential vulnerability with VoIP is that hackers can send Reset messages to SIP phones using a device established to impersonate a call server. Security measures such as public key/private key certification can help by assuring a SIP phone that it's indeed connecting to the IP application server it expects to connect to, not a device inserted into the environment for malicious purposes.

Access list support

In most IP system configurations for VoIP, organizations can configure their network to support Medium Access Control (MAC) access lists to prevent man-in-the-middle attacks and rogue device connections. Simplifying the MAC process, system administrators can even create an access list for specific MAC addresses via the switches on a network.

List IP addresses to deny communications

Many IP application servers support the ability to list forbidden IP addresses, and can be configured to understand IP addresses that aren't allowed to communicate directly with the server. In such configurations, the universal control for the Network Layer actually serves as the firewall to protect against unwarranted IP address connections.

Protection against malfunctioning devices

Though they've gotten more reliable, devices such as SIP phones and gateways can sometimes fail or malfunction within an IP communications configuration. When they do, a Denial of Service (DoS) prevention algorithm can safeguard against excessive signaling from devices that are malfunctioning or operating in a disruptive manner.

Firewall support

For VoIP, a security best practice is to *not* open your network to the Internet. To keep your network closed, application servers for IP communications typically run behind the firewall just as any other business application server does on the network. Also depending on the

specific IP platform, it's sometimes possible to separate and control each type of communication media via a firewall using different TCP/IP ports for web, application, and data communications, with access controlled via the firewall. For SIP session routing, for instance, the firewall can be made "SIP-aware" to handle SIP-based calls on a WAN.

IP application servers typically run behind the firewall just as other business application servers do on your network.

Hardening Your Network

When deploying VoIP, place SIP phones in a voice-based virtual LAN (VLAN). This measure improves security and also ensures that VoIP traffic gets handled more efficiently by protecting phones from broadcast traffic. Note that a voice VLAN approach requires all voice endpoints, including the IP application server, media servers, etc., to be placed in the voice VLAN. System clients, however, should remain in a Data VLAN or the Default VLAN.

Securing Open Ports

Transport protocols, services and the number of enabled ports are another vulnerability issue for external IP system attacks, which are most likely to occur when open ports are utilized for too many purposes and make the job harder for the firewall. To ease the firewall's workload, simply open fewer ports if possible. Likewise because the protocol for communication is proprietary using IP, hackers find it harder to access information being passed, especially when an IP solution includes a TCP/IP port to handle proprietary messages between the application server and desktop clients.

Virus Protection

With an IP system acting as a PBX/IP PBX as well as an ACD in a VoIP environment, most IP vendors now pre-validate popular virus protection software to run on their application servers. A best practice for maximum protection against any virus is to follow all vendor recommendations.

Denial of Service Attacks

DoS attacks usually occur through open ports and, due to their constantly-changing nature, are extremely difficult to defend against. A few configuration measures can help protect an IP application server should a DoS attack occur.

- Structure communications between services in a proprietary encrypted protocol. This way, all network messages received on open ports are simply ignored or disregarded.
- Add a configurable access control list both in your IP platform and SIP Proxy. Doing so allows a system administrator to grant or deny access by specific IP addresses, or range of IP addresses, when configuring a SIP connection.
- Guard SIP phones against DoS attacks by configuring your IP system to cut off whenever too many requests come from a particular device.

Securing Web Chat

As web chat continues to establish its place in business and IP communications, securing a web server independently of an IP application server will minimize most security risks. That means securing passwords, implementing a firewall, and shutting down unnecessary network services on the web server itself. And when initially configuring a web server, protect against known risks by following these security guidelines from Microsoft:

- Run your web server outside the firewall.
- Do not run your web server as a member of the domain, or maintain domain passwords on the server.
- Employ chat encryption measures to protect senders/receivers who are exchanging private information.
- Stop all unnecessary services and scripts on your web server.
- Immediately install security patches each time they become available.

In addition when recording web chats, encrypting chat recording files is recommended whenever confidential data is routinely exchanged with customers.

Preventing Fraud and Malicious Attacks

Database Controls

Database security is imperative in any organization, but most notably in automated self-service IVR and online applications that allow callers to access confidential data. Controls in this case again come down to various security mechanisms working in unison.

- If your IP platform utilizes Windows NT, leverage the NT Registry to administer user information, system information and database resources for the purpose of logging report data and user/workgroup contact directories.
- If a database itself is not encrypted, employ the Advanced Encryption Standard (AES) to secure all connections between a database and an IP applications server.
- Establish an administrative ID and password for authorized users to connect to Open Database Connectivity (ODBC) drivers for ODBC-compliant databases.
- Protect online transactions using Soap Tools to communicate to web services on a Secure Sockets Layer (SSL). In an IP configuration, this security measure can provide the transport layer technology for authentication and data encryption between a web server and web browser.

Protection Monitoring Systems

Protection monitoring systems can be invaluable for an IP communications system. The keys here are to incorporate monitoring tools such as intrusion prevention software to automatically detect, classify and respond to complex threats, and to effectively leverage other PM offerings

Intrusion prevention software can automatically detect, classify and respond to complex threats.

to protect applications and systems as well as end users. At deeper security levels, the ability to detect and prevent suspicious malware activity such as Trojans, key loggers, silent backdoors and root kits (based on a behavioral heuristic approach) also is critical, as is the ability to protect against memory-based attacks.

Safe Connections to Other Applications on the Network

Security becomes more secure when an IP platform connects to other applications via TCP/IP communications on the network, and when the system incorporates the user ID and passwords of an ODBC connector for user connections to ODBC-compliant databases. For email in an IP system configuration, for example, the IP application server can connect to an organization's email server via TCP/IP, and still utilize an administrative ID and password to send and receive email from the email server.

Just as protecting live interactions and their resulting data is critical to a business, it's become far more vital to protect the identity of customers. Within an IP communications environment, a primary best practice for customer privacy is using authentication to validate all users involved in voice interactions and data transactions. Two other layers of security help ensure the confidentiality of customers as well: encryption for calls and voice messaging, and administrative password settings on back-end business systems. Again, however, the best safeguards result when an organization's security plan incorporates all available aspects of protection, including the following tools.

User Authentication

Three viable options come into play for user authentication. For companies utilizing Microsoft Windows NT in their communications system framework, NT authentication can safely validate each logged-in user against a domain that's equally valid for that company's IP system. A second option is for organizations to deploy their own method of user authentication, for example by incorporating a Dynamic Link Library (DLL) to support customized user authentication methods. Or a third option is to leverage the user name/password authentication available in many IP application suites, such as that required to retrieve voice messages.

Digest Authentication

Using digest authentication assures that passwords are never sent across the network without being encrypted. If you're researching an IP communications platform, be sure it can encrypt all passwords and data that travel between the IP application server and the systems' desktop clients for individual users.

Keystroke and Other Input Logging

Keystroke and input logging measures are just good common sense. If an IP application server is locked, only the system administrator should be able to access the keypad to access the server. In accordance with your company's network security policies, each desktop machine in an IP system should also be password protected to lock the computer or workstation within X seconds after an employee leaves his or her desk; or simply have the policy state that employees automatically lock their PC whenever away from the desk.

Administrative Rights

Multi-point communications systems don't just include multiple components; they typically require separate administrative interfaces for each one. With the unified nature of an all-in-one IP system, however, administrators get a single interface to provision users and manage the system's pre-integrated communications applications. Or translated, administrative rights funnel into a central environment easily secured on a granular basis by one system administrator (and often a backup administrator), or by small IT teams that oversee specific functions such as configuring SIP lines, maintaining auto attendant and dial plan functions, etc.

Administrative Audit Trails

Administrative change logs and associated reports are an air-tight way to audit system changes for security purposes, especially in that they allow administrators to verify who made a specific change at any given time.

Encryption

Encryption standards to secure voice messaging traffic

Encryption via the Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) standards has become a best practice for protecting calls that travel over an IP communications network. Organizations can incorporate virtual private networks (VPN), virtual LANs (VLANs), access lists and authentication to further protect voice traffic in an IP infrastructure.



On the data side of a call — imagine a customer using an automated IVR self-service menu to make a banking transaction — organizations can configure IVR applications to make callers enter a secured account number or PIN to access their information. In automated processes such as screen pop, where sensitive customer info flows from a database to a user's client via an IP application server, businesses can safely encrypt data traffic using the symmetric Advanced Encryption Standard (AES). AES allows all data destined for a host to be seamlessly encrypted on the IP application server and then decrypted only by the host client receiving the message, meaning the entire message is encrypted from end-point to end-point.

Another valuable layer of voice messaging security for an IP system is the Internet Protocol security (IPsec) protocol, a framework of open standards that leverage cryptographic security services to protect communications traveling over IP networks. Comprehensively, IPsec supports network-level peer authentication, data origin authentication, data integrity, encryption for data confidentiality, and replay protection. Among communications vendors, Microsoft is a true IPsec believer, having implemented IPsec in much of its Windows product lineup via standards developed by the Internet Engineering Task Force (IETF) IPsec working group.

Encrypted voice payload

In organizations using an IP communications system, a common security concern is an employee's ability to "sniff" a network and eavesdrop on a VoIP call from their PC or workstation. To securely encrypt voice payloads and prevent sniffing, organizations should consider supporting SRTP configuration both at the station level and site level, and at other potential points of a voice flow process such as IVR applications and ACD workgroups.

Voice Recording Encryption

Good security procedures include protecting data while it is in transit, and also while it is “at rest”, stored on servers. In turn, protecting confidentiality has created the dual need to encrypt voice message data during transit over an IP network, and then to encrypt the recording prior to storage as a recording file. In security terms, that means safeguarding recordings at the device level as well as the logical level.

Naturally voice message encryption begins at the device level, namely a phone, a desktop client or a handheld, and extends throughout an IP network. Encryption required at the logical level, however, is much broader, and can include applications (IVR, auto attendant, etc.), the premises at which a business is located, and ultimately the message exchange and associated information being recorded.

The perfect example of a message exchange is someone voicing a credit card number that lands in a recording file. And because a recording file is the perfect place from which to steal such a number, the ability to encrypt call audio — as well as encrypting recording files and all information about a call — is an absolute best practice to be considered. (Better still is the ability to record, monitor and encrypt calls *simultaneously*. Interactive Intelligence is one of very few vendors whose all-in-one platform allows organizations to do exactly that.)

Administrative security policies should also be implemented for recording files, first by way of authorization at the file management level, and then at the end-user level for all persons who need to access and play-back call recordings.

Reduce fraud by utilizing speech recognition

Talk about security right out of a science fiction movie. For speech-enabled IVR applications, or even prior to speaking to an agent through an ACD, speaker verification — a.k.a. voice authentication or a “voice print” application — validates a caller by identifying aspects of that person’s voice when they first call. Or think of speaker verification as a voice fingerprint that authenticates callers and allows them to access to secured data and conduct sensitive transactions. To establish their voice print, callers must record a password phrase, such as a favorite movie. Each time they call thereafter, the speaker verification mechanism OKs the caller by detecting their personal speech pattern and inflexion in the security phrase they recorded.

Physical Security

In a traditional Time Division Multiplex (TDM) voice communications system like a PBX, it’s alarming that someone like a telephony engineer can patch into virtually any live conversation, and do it at any time. All the person has to do is hack into the patch panel or directly into a telephony board corresponding to an end-user’s station. While encryption can prevent this type of attack in IP systems, however, other types of physical attacks can still be perpetrated on communications equipment within a building. To deter unauthorized access to an equipment room and prevent system intrusions, effective physical security remains the best initial wall of defense. Remember, security clearance devices and “Authorized Personnel Only” signs truly do serve a purpose.

Remote Access, the Remote and Mobile Workforce

One of the benefits of an IP communications platform is remote user capability for at-home users and mobile workers, most commonly with logins via any TCP/IP connection. A security downside, however, is that broadband access widens an organization's circle of required protection for digital assets and increases threat levels for network attacks and data leaks. For the remote and mobile workforce, a few security precautions can help:

- Establish and strictly enforce corporate policies requiring remote users to log in to any desktop client using a VPN connection. Configuring a VPN environment in conjunction with IPsec optimizes security for remote connections.
- Secure your network with a firewall that can scan all network traffic for threats. Also implement "personal" firewall devices at a remote user's home or remote office for high-speed connections.
- As much as possible, make sure a remote user's PC operating system and web browser meet corporate security standards. Make sure as well that all remote users can readily access new security patches and updates.
- Guard against malware on a laptop or USB device by maintaining security behind the network and between departments. Firewalls with LAN switching capabilities provide the best security for communications from external sources, and internally from zone to zone.
- Assign a remote access telephone number to authorized users based on a local or long-distance number, but deny remote access using an international number.
- Encrypt any sensitive data on a laptop to guard against unauthorized access in the event the laptop is stolen or lost.
- When possible, deploy Citrix or Terminal Services for remote access to business applications.



Take Action

Since 1994 Interactive Intelligence has offered a fully integrated, standards-based all-in-one software platform for multimedia business communications. In 2002, we architected our platform on the SIP communications standard to take advantage of VoIP and SIP's voice and data security mechanisms — one of the industry's first vendors to do so.

The result is more than 3,000 organizations worldwide now protecting voice interactions and critical customer information using our platform technology and pre-integrated IP contact center and IP PBX application suites.

Visit us at www.inin.com to learn more about our solutions... and how they can be your business's best friend for security.

Read more about our solutions' advanced security controls in the white paper "Security Considerations for an IP PBX and Contact Center Application Server"