Enterprise Voice Network Security Solutions

A Corporate Whitepaper by
SecureLogix Corporation

Contents

Introduction

Traditional data and voice network security procedures and technologies do not effectively address the primary vulnerabilities plaguing voice networks: voice fraud, including toll fraud and social engineering attacks; threatening calls, such as bomb threats; voice service abuse, such as theft of long-distance service and unauthorized ISP calls; and unauthorized modems and non-secure authorized modems that produce an unmonitored "back door" into the data network. Most of these threats exist whether the voice network is TDM, Voice-over-IP (VoIP), or hybrid. Additionally, the migration to VoIP introduces an additional set of vulnerabilities alongside these existing ones.

The vast majority of enterprises maintain a presence on the Internet in order to conduct business and provide Internet access for work-related activities. To secure the connection from the Internet and protect internal networks, enterprises deploy a variety of security measures, including firewalls, VPNs, intrusion detection/prevention, anti-virus, and content monitoring. When properly deployed and configured, these products help to protect the internal IP network from attacks originating from the enterprise's Internet connection. However, none of these Internet-related security technologies protects the internal IP data network from attacks through back-door connections from the voice network created by unauthorized or non-secure modems and poorly configured voice systems. Nor do they protect against malicious activity targeting the voice network itself, such as voice fraud, harassing and threatening calls, and toll service theft or abuse,

The best solution to all of these voice network threats lies in applying security concepts from the IP network to the voice network—specifically, the deployment of expandable, inline security devices on the enterprise voice network. This solution supports transparent voice security, providing unified visibility and security while simplifying the transition to VoIP for voice managers.

These inline security devices support multiple security applications such as a voice firewall, voice intrusion prevention system (IPS), call monitoring and alerting, and call content recording. This approach provides the voice network with the same security protections that have been present on IP data networks for years. Additionally, these security devices support usage and utilization reporting applications that provide a significant Return on Investment (ROI).

1. Voice Network Security Threats

TDM and VoIP networks alike are plagued by an often-unrecognized battery of threats to the security of voice communications, the data network, and proprietary and customer information. These threats are described below.

Toll Fraud

Toll fraud poses one of the largest threats to enterprises voice systems today. While accurate cost estimates for toll fraud are difficult to pin down because many companies are reluctant to publicly admit they have been targeted, experts worldwide estimate the costs to run in the billions of dollars annually. According to the most recent figures available from the Communications Fraud Control Association (CFCA) *Telecom Fraud Survey*, annual global telecom fraud losses amount to an estimated $54.4–$60 billion (USD). Experts also say that toll fraud is an easy and profitable crime, since it is often undetected until large amounts of money have been lost, and the perpetrators are hard to identify, minimizing their sense of risk. These factors increase the likelihood of such attacks.

Classic toll fraud, sometimes referred to as dial-through fraud or time theft, occurs when a hacker breaches a vulnerable voice system and then sells the number/codes to as many people as possible. For example, some companies enable services like Direct Inward Services Access (DISA), where a code/password allows off-premises

employees to call in and get dial tone to call out. DISA is a useful service for travelers, who can call in and use the company's long distance facilities, rather than using their cell phone, a hotel phone, or calling card. When hackers obtain these codes, they can exploit them in toll fraud.

In recent years, the frequency and severity of toll fraud attacks has been increasing, often at the hands sophisticated international crime operations and terrorist funding organizations. One example reported in the Wall Street Journal in June of 2009 was a large-scale toll fraud operation based out of the Philippines and Italy that broke into more than 2,500 PBX phone systems in the USA and Canada and stole at least $55 Million in Long Distance service. Leaders of this toll fraud ring allegedly have ties to al Qaeda, and profits from the scheme allegedly went to fund terrorist organizations and operations, including individuals responsible for the 2008 terrorist attacks in Mumbai, India. The perpetrators stole long distance services by hacking PBXs and poorly secured phone stations owned by U.S. and Canadian corporate and government entities, including the U.S. Federal Emergency Management Agency (FEMA). Compromised PBXs and phone stations were reprogrammed to provide remote long distance service access to at least 10 call centers in Italy operated by a group of Pakistani nationals. These call centers resold access to these stolen long distance services to the public via phone cards.

The use of VoIP for business voice services can add additional risks. With some VoIP architectures, the IP PBX is decomposed into several systems that communicate over the data network. For example, you may have an IP PBX that communicates with a separate media gateway, sometimes integrated with a network edge router. If the media gateway does not have the proper Access Control Lists (ACLs) and security, it is possible to directly connect to it via a VoIP protocol such as H.323 and make calls with no control from the IP PBX nor entries in the IP PBX call accounting database.

Social Engineering Attacks

Phone-based, social engineering attacks place corporations and their customers at risk for information/identity theft and financial damages. Most people are familiar with Internet- and email-based "Phishing" schemes, whereby criminals attempt to acquire personal information such as usernames, passwords and credit card account information by fraudulently representing themselves as trusted entities. Many corporations, especially financial, insurance, retail and healthcare organizations fall victim to these types of social engineering/identity theft attacks conducted over corporate phone lines. Some industry leaders believe this avenue of attack is on the rise particularly because the large investment in and ubiquitous deployment of sophisticated security solutions on the IP data network has driven perpetrators to the unprotected voice network.

Voice Service Abuse

Voice service abuse—the use of corporate voice network resources by an internal caller for non-business purposes—is a costly and widespread concern for most organizations. In addition to hard costs for abuse of toll services such as long-distance calling, unauthorized/restricted phone service usage consumes bandwidth, which affects telecom trunking infrastructure needs and associated costs to maintain acceptable Average Peak Utilization ("APU") service levels. Voice service abuse can be perpetrated in a number of costly ways.

Most PBXs have some basic features to help address toll service abuse, such as class restrictions and authorization codes. Class restrictions are applied to phones/extensions and dictate what services can be used, such as specific trunk groups for long distance. While useful, this is not very granular. Authorization codes require users to enter a code before they use certain services, like long-distance calling. Authorizations codes are useful and can be fairly granular, but they require a lot of maintenance, depend on use of strong codes, and most critically, require users to protect the codes. These codes can be easily shared, lost, or sold, which defeats the purpose. Another issue with

these features is that they work differently for all PBXs, even systems from the same vendor. These features are also very difficult to manage if an enterprise has 100s or 1000s of remote systems.

Virtually all PBXs generate call records for each call. These calls records are often saved in a database, from which reports can be generated. One way to identify toll service abuse is to frequently generate reports and check for any unusual activity. Unfortunately, this approach is manual, time-consuming, useful only if it is done at least weekly, and does not prevent or mitigate service abuse in real time. It also does not provide information about call types, since PBXs do not report the type of call, leaving this important indicator of abuse hidden.

Harassing and Threatening Calls

Harassing and threatening calls sap productivity and can create financial risk for an organization. Examples of these types of calls include bomb threats, harassing personal calls, disgruntled customers calling corporate executives, and fringe elements threatening corporate executives or other prominent members of the organization. Bomb threats alone cost organizations large sums of money for each occurrence.

Modems

Although not new, modem-based vulnerabilities are still a real problem, due in part to the IP-based security protections that most organizations have applied to their IP networks. Unauthorized modem connections represent a significant security risk to any organization. Unauthorized modem connections can occur from two sources: misuse/unauthorized access of legitimate modems, such as PBX maintenance port modems, and employee-installed personal-use modems. Authorized modems have a legitimate business purpose, but still pose a risk to the data network if they are improperly secured or unlawfully accessed by an unauthorized person. An even greater threat arises from employee-installed modems, a hidden threat that exists in most enterprises. Employee-installed modems, used for unmonitored Internet access or deliberate data transfer by a disgruntled employee, bypass the data firewall and create unsecured phone line access points into corporate data networks, opening the back door for hackers, viruses, data leakage, and other threats. Since traditional data firewalls cannot see traffic on the phone network, and PBX systems cannot distinguish call types, this threat is invisible to traditional network monitoring equipment and practices.

Many industry groups and regulatory agencies recommend and/or require aggressive measures to address corporate modem vulnerabilities. For example, the Department of Homeland Security issued guidelines in *Recommended Practice for Securing Control Modems, January 2008,*

Organizations attempt to mitigate the modem problem in a number of ways. Although these solutions provide some benefit, they address only part of the problem and/or are prohibitively manpower-intensive.

For example, written modem use policies and procedures are important for any enterprise. Unfortunately, such policies typically lack necessary visibility for effective enforcement in the absence of real-time voice network monitoring.

Many organizations attempt to mitigate some of the modem threat through war-dialing projects, conducted internally or through a third party at significant cost. War-dialing expenses typically include long distance calling charges, consultant or staff labor costs, and software license fees. Unfortunately, in spite of its substantial cost, war-dialing has proven to be a severely limited means of identifying rogue modems in the enterprise, because illicit modems are often either in use (the war dialer gets a busy signal), not set up to auto-answer, or disconnected when not in use. Plus, enforcement based on this limited information is dependent on manual, desk-to-desk inspection and removal of the identified unauthorized modems. And new unauthorized modems can be easily

installed by any employee mere moments after search and removal. War-dialing provides no ability to alert/block/prevent modem threats in real time. As a case in point, one government security administrator found approximately 70 modems when he scanned his phone numbers—but found approximately 700 modems when he used a real-time voice firewall designed to detect all modem calls.

Most enterprises providing remote access to users have set up IP-based VPNs and/or managed Remote Access Servers (RAS). These systems can be centrally managed and enforce good security, effectively removing the need for an individual to set up a personal RAS. Despite the availability of a VPN or RAS, however, some users still set up personal remote access. The reasons for this breach of security vary, but include a simple lack of awareness of the RAS, a real or perceived instability of the RAS, and a desire to work outside the monitoring of the VPN or RAS.

Other solutions such as dialback modems, secure modems, or modem proxies attempt to protect authorized modems, but management of a large number of these point products is very difficult and expensive. Further, these measures only address security issues related to known and authorized modems, which represent only a small subset of the total number of modems inside the typical enterprise.

Many PBXs have security features that can be used to mitigate some of the modem threat, such as preventing inbound calls to authorized modems designated for only outbound calls. But in large, geographically dispersed organizations with hundreds of systems, the lack of centralized visibility and management of these features makes them difficult and time-consuming to implement and maintain.

3. Effective Security Solutions for the Voice Network

As described above, several traditional voice technologies partially address some of the threats plaguing voice networks, but none address them entirely and in an easy-to-use, centrally managed, remotely upgradeable system that is scalable to meet the needs of geographically distributed enterprises. The solution to protecting the IP data network from attacks through the voice network and protecting the voice network from unauthorized access and fraud attempts is to apply security technologies patterned after those on the IP network in a robust, integrated, centrally managed, unified solution set. The solution deploys expandable inline security devices on the voice trunks, enabling secure, optimized and efficiently managed enterprise voice environments, irrespective of the network's underlying mix of vendor systems and voice media. Security applications deployed on a single hardware platform may include a voice firewall, voice IPS, and call monitoring, as required to meet an enterprise's security and voice implementation needs.

In addition to hardening the security perimeter, this solution enables collection of key voice network usage data that demonstrates a tangible and significant ROI. This data can be used by applications to detect toll fraud, long-distance abuse, as well as poor bandwidth and telecom resource utilization. The data can also be used by other applications such as billing.

Lastly, this solution supports a seamless transition for securing VoIP, allowing voice managers to both secure their entire voice service and adapt as their voice network migrates to VoIP.

Figure 1 illustrates an inline voice security system deployed on all voice circuits entering an enterprise. These expandable, centrally managed devices can be augmented with security applications appropriate to the needs of the individual enterprise.

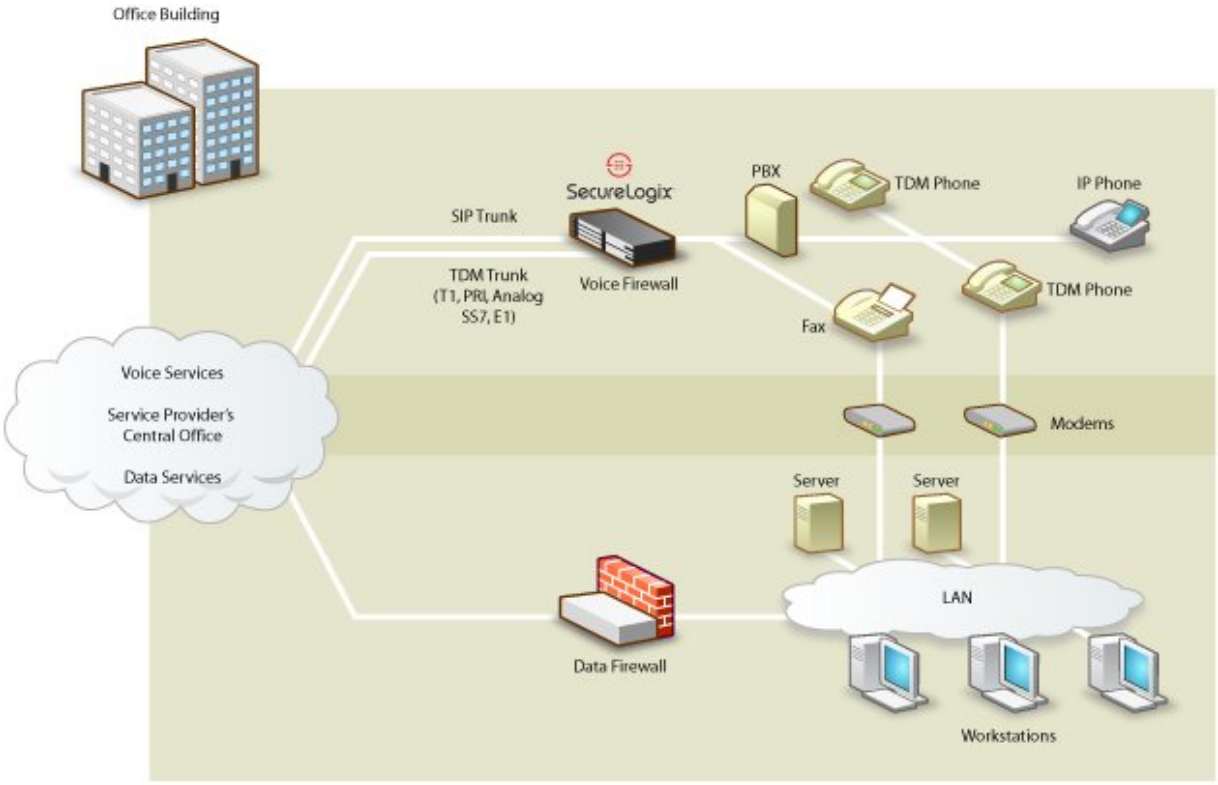

Figure 1 – Security System for the Voice Network

In a fashion similar to data network perimeter security and management devices, ETM Platform Appliances sit at the edge of the enterprise voice network, the optimal position to provide visibility and control over all inbound and outbound voice network access and usage. The edge-network intelligence of the platform appliance also allows it to host a large array of voice security and management applications, all of which can be uploaded from a remote location. As with any security device, secure, centralized, remote management and the ability to perform remote upgrades are essential requirements.

As with network-based Internet security, the needs of the enterprise determine the order for deploying applications on the expandable security device. A firewall is usually the first application deployed, followed by other applications that include intrusion detection and content monitoring. The following subsections describe these applications.

Voice Firewall

As on the Internet connection, a firewall is the first application to deploy on the voice network. A voice firewall is an application driven by a security policy defining whether to allow or deny certain calls and notification actions to be taken. The voice firewall transparently passes allowed calls through to their destination, but cleanly terminates disallowed calls. In either case, an email, SNMP, or console notification can be generated. Functioning on the voice network, the voice firewall must be highly reliable and add no noticeable latency.

As shown in **Figure 2**, a call to an unauthorized modem is identified as unauthorized activity and the firewall denies the call and sends an alert to designated administrators, all in accordance with the security policy. Regardless of whether an external attacker or an internal user tries to access the unauthorized modem, the firewall denies the call. Likewise, if a user tries to dial an ISP prohibited by the policy, the firewall blocks the call.

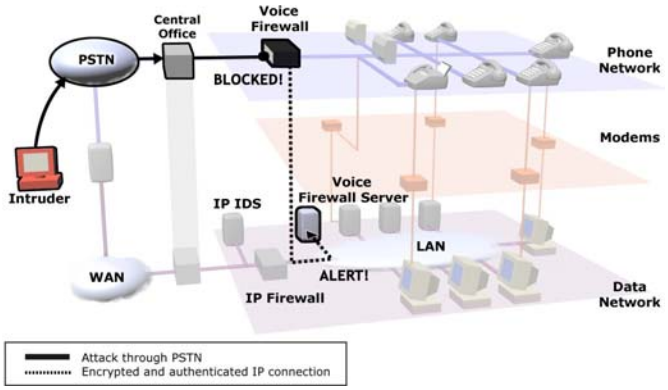

Figure 2 – Voice Firewall Blocking an Intrusion Attempt

A policy is merely a list of rules defining criteria by which calls are allowed, denied, and/or alerted. Rules are evaluated in sequence against each call. If the call matches a rule, the firewall executes the actions the rule prescribes. A default rule allows all calls that do not match a previous rule. For example, consider the following rules addressing modem use, described below and illustrated as Rules 1 through 4 in Figure 4:

Rule 1: Allow inbound modem calls to a group of phone numbers for the RAS. Log all matching calls.

Rule 2: Allow inbound modem calls from allowed numbers, during a specified time, limited to a specified duration, to a list of authorized modems used for remote maintenance (i.e., a PBX maintenance port). Log all matching calls. The firewall could also require that users be authenticated before the modem connection is allowed.

Rule 3: Allow outbound modem calls, from allowed numbers, during a specific time range, limited to a set duration, to a list of authorized numbers. Log all matching calls. This rule would be valuable for Supervisory Control and Data Access (SCADA) or remote offices where periodic data upload/control is needed. Again, authentication could be required.

Rule 4: Terminate any modem call not explicitly authorized by a previous rule. Email security personnel and log all matching calls. This prevents illegitimate use and ensures that users with legitimate modem needs adhere to the corporate process for requesting a modem and getting it added to the list of authorized modems in the policy.

Although Rules 1-4 focus on modems, the ability to determine the type of the call allows additional policies to be developed, including rules that manage standard voice calls, fax usage, and Secure Telephone Unit (STU) and Secure Telephone Equipment (STE) usage.

The voice firewall can provide additional factors of authentication, such as allowing only calls from a known source number or at a designated time. In some cases, this is not practical, because a remote user such as a salesperson may be calling from an unknown location. In this case, the firewall can provide for additional authentication not tied to the source number, such as a username and Personal Identification Number (PIN) before allowing a connection to a protected sensitive resource.

The U.S. Department of Energy conducted a demonstration at several SCADA sites in April 2004. The security analysis summary states that the combination of voice firewall technology and authentication for remote access to modems adds a needed level of protection to remote modems that access infrastructure resources. The analysis also stated that with the inclusion of security best practices, the combination was highly capable of preventing unauthorized access to unprotected remote modems/controls systems, reducing vulnerability from an integrity compromise of 100% to 15%; and more significantly, reducing exposure time from 24 hours per day to just the few minutes an access token is valid.

Voice Intrusion Detection/Prevention

A voice IPS monitors traffic for abusive call patterns, including voice fraud and password guessing. Voice fraud patterns include excessive long-distance or international calls during non-business hours or an excessive number of access attempts to the PBX maintenance port. Password guessing patterns are seen as a pattern of short-duration calls when an attacker attempts to access an authorized modem, but the system terminates the attacker's connection after a short period of time due to several unsuccessful password attempts.

Thresholds for various types of calling patterns can be set, and actions dictated for calls that exceed the set threshold. The voice IPS can terminate calls when an abusive pattern is detected and send alerts to designated systems and personnel. Future matching calls can also be prevented for the duration of a user-defined time period.

Figure 3 illustrates an IPS monitoring voice calls for abusive patterns. An alert is sent to designated recipients when abusive patterns are detected.

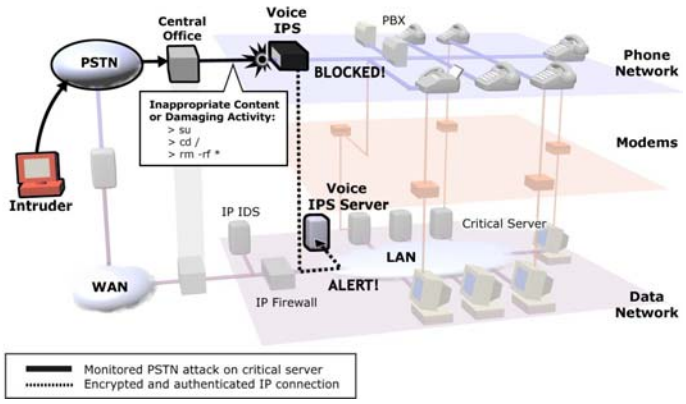

Figure 3 – Voice Intrusion Detection/Prevention

Content Monitoring

Enterprise security or operational processes may define a need to record and analyze the content of specific voice, fax, and modem calls. The recommended solution records audio content specified by a call recording policy and stores the recordings on the appliances for remote download, playback and analysis. Recordings can optionally be securely transmitted to an analysis site for review, analysis, and storage. This recording capability is useful for conducting investigations such as Communications Security (COMSEC) monitoring.

This solution also facilitates compliance with regulations, such as those impacting the medical community that may require patient privacy be ensured by either encrypting or monitoring faxes. Allowed modem sessions and fax

transmissions are recorded based on policy and then stored on the appliance or transmitted to the analysis site for reconstruction, review, analysis, and storage.

User Interface

The user interfaces for the recommended applications should seamlessly unify security and visibility for any mixture of TDM and VoIP traffic.

Figure 4 illustrates the user interface at a unified performance manager, which provides access to the policies for the voice firewall, voice IPS and recording technologies.

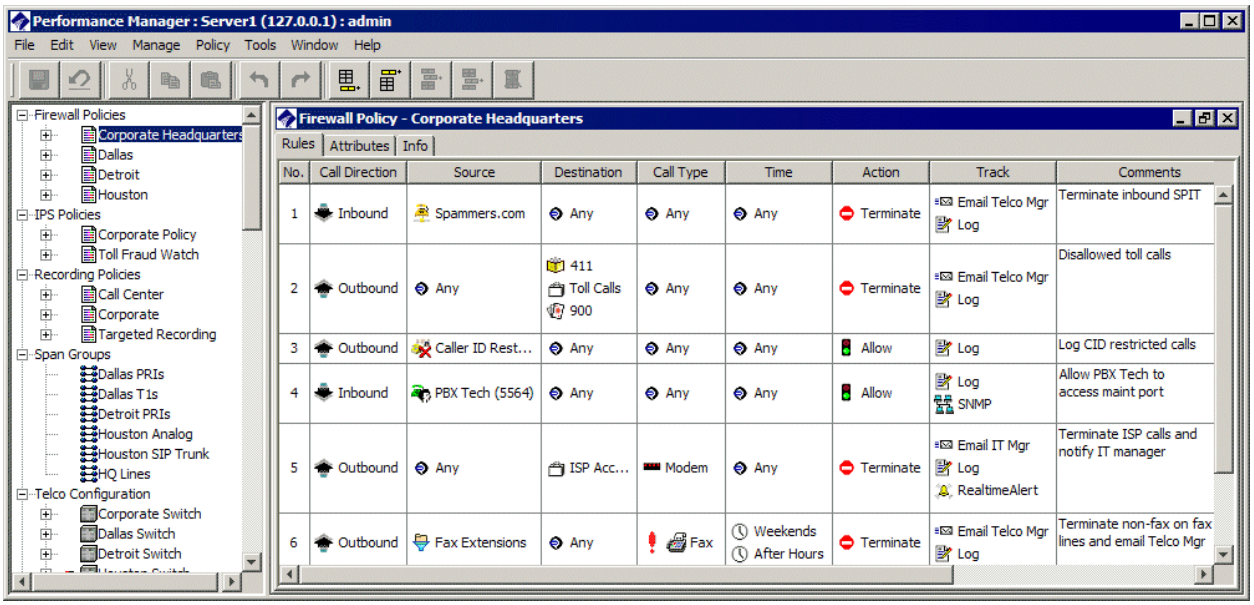

Figure 4 – Unified Performance Manager and Unified Voice Firewall Policy

Figure 5 illustrates a call monitor, which provides a real-time display of voice activity across monitored TDM and VoIP circuits.

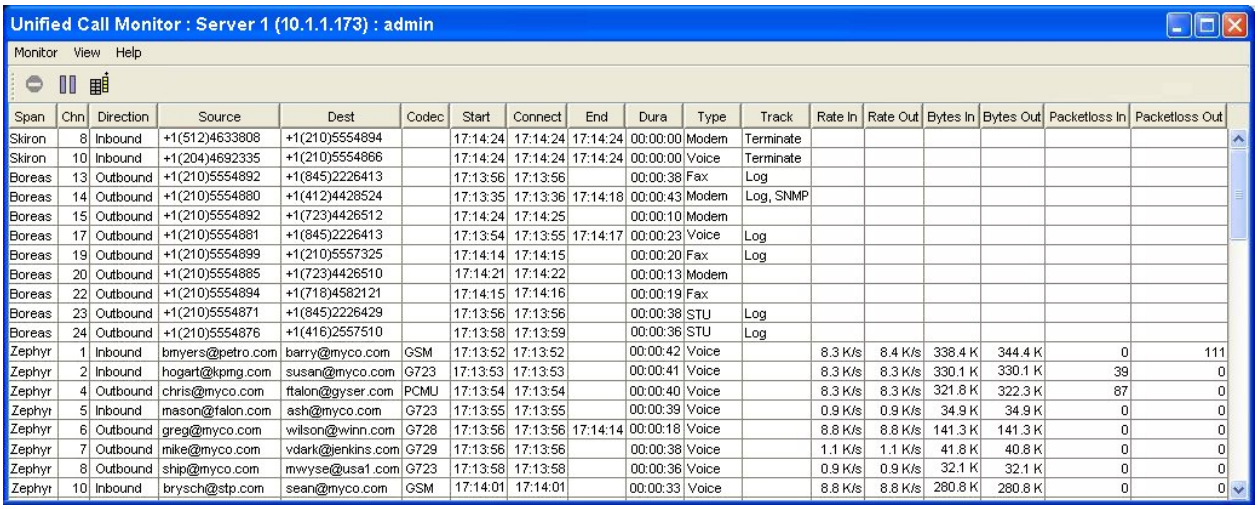

Figure 5 – Real-Time Unified Call Monitor

4. Hybrid TDM/VoIP Security Solutions

The voice network is slowly transitioning from TDM to VoIP. Although VoIP represents about 1% to 2% of current enterprise voice, it is gradually replacing traditional voice system implementations. Most new purchases support or include VoIP, and many enterprises are engaged in VoIP evaluations, pilots, or in rare cases, large-scale implementations. Typically, migration to VoIP will be a long-term process, and it is understood that most enterprises deploying VoIP will continue to be a hybrid mix of legacy services and IP services for a long time.

While VoIP introduces new security vulnerabilities and makes some types of attacks easier, the primary voice threats remain the same for VoIP as for TDM. In this hybrid environment, voice managers need unified visibility and security control across both the TDM and VoIP networks. A single telecom security hardware platform can be as hybrid as the enterprise network it secures, supporting security applications for both legacy and VoIP services, addressing the unique, real-time performance requirements of VoIP, while securing the threats introduced by unsecured legacy phone lines and PBX systems and those unique to VoIP.

Joint or separate security and usage policies can be developed for a hybrid environment. The voice firewall policy can contain TDM-specific rules, VoIP-specific rules, and rules that apply to both networks, as illustrated in Figure 4. Real-time call activity visibility can be provided for both networks, as illustrated Figure 5. Additionally, reports can be generated that use data collected from both networks, as illustrated in Figure 6. In short, the proposed solution provides a unified approach independent of the underlying transport type, with a user interface that insulates the voice manager from the details of the underlying hardware, transport, and protocols.

5. Return on Investment

The 2004 CSI/FBI Survey states that most organizations conduct some form of economic evaluation of their security expenditures, with 55% using ROI and 28% using Internal Rate of Return (IRR). [1]

Additionally, large corporate customers that attended the 2003 VoiceCon conference, where discussions focused on the business of planning, securing, and cost-justifying VoIP, said that ROI is a real issue with the expansion of their VoIP plans. [2]

A major advantage of this vice security solution is that its monitoring of call traffic into and out of an enterprise captures enterprise-wide data useful for managing trunk utilization, departmental bill-back, fax utilization, toll fraud, etc. **Figures 6, 7, and 8** illustrate sample reports that help this security solution provide a significant and tangible ROI.

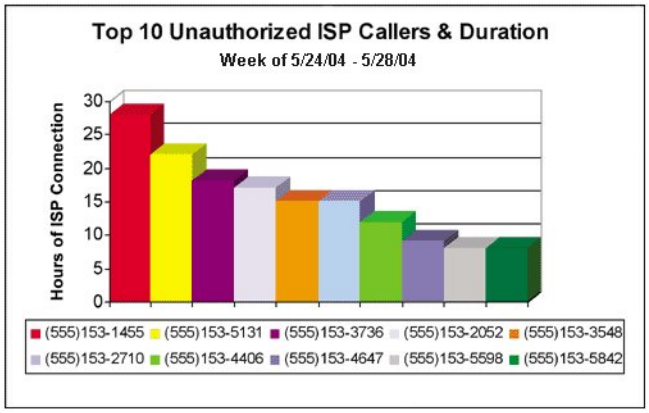

Figure 6 – Top 10 Unauthorized ISP Callers Report Sample

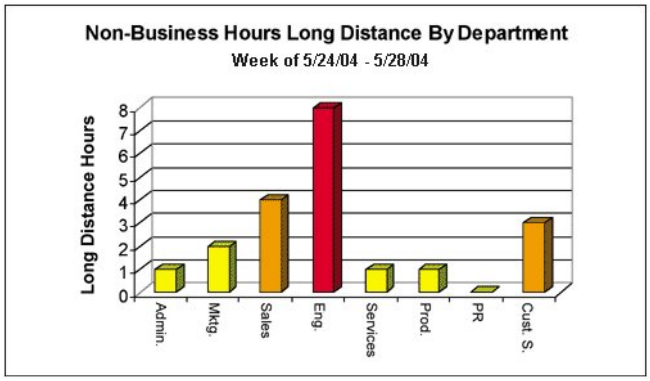

Figure 7 – Non-Business Hours Long Distance Report Sample

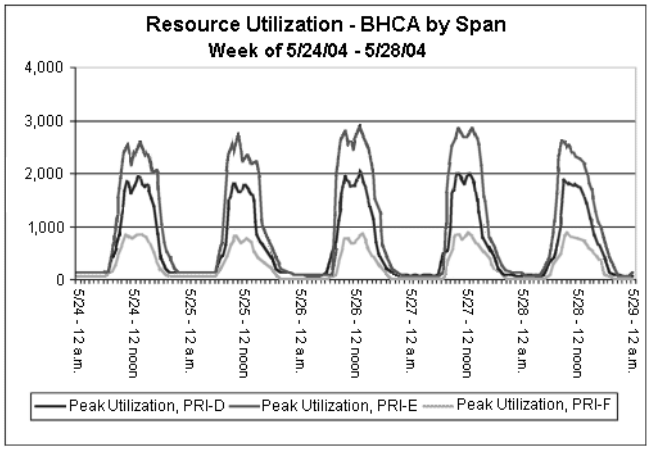

Figure 8 – Resource Utilization Report Sample

6. Summary

Both the voice network and the data network face significant threats through the unsecured telecom environment. Concepts from the data network can be applied to the voice network to address these threats. Specifically, deployment of expandable inline telecom security devices allows the use of various security applications to prevent attacks against or through the voice network. These applications include a voice firewall, voice IPS, and content monitoring, deployed as needed to meet an enterprise's security needs.

While some of these applications are currently available from several sources, most vendors do not provide them as an integrated robust solution set, and many lack the necessary scalability, reliability, and management capabilities.

The patented technology in the ETM System from SecureLogix provides all of these features in an integrated solution set that is capable of controlling security across a mixture of both TDM and VoIP networks, is agnostic to the underlying transport type, has a robust management infrastructure, is scalable to any size of organization, and provides a user interface that insulates voice managers from the myriad details of the underlying hardware, transport, and protocols. Investment in the robust solution presented in this document to meet the long-standing and emerging threats to the traditional voice, VoIP, and data networks provides significant security benefits coupled with a strong ROI.

Acronyms

COMSEC – Communications Security

DTMF – Dual Tone Multi-Frequency

IPS – Intrusion Prevention System

IP – Internet Protocol

IRR – Internal Rate of Return

ISP – Internet Service Provider

PBX – Public Branch eXchange

PIN – Personal Identification Number

RAS – Remote Access Servers

ROI – Return on Investment

SCADA – Supervisory Control and Data Access

STE – Secure Telephone Equipment

STU – Secure Telephone Unit

TDM – Time Division Multiplex

VPN – Virtual Private Network

VoIP – Voice over Internet Protocol

References

[1] Computer Security Institute, *2004 CSI/FBI Computer Crime and Security Survey.* 2004, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[2] Hochmuth, Phil, *Costs, security vex VoIP users.* Network World, February 2003. http://www.nwfusion.com/news/2003/0224voicecon.html

[3] Recommended Practice for Securing Control System Modems, January 2008, accessed 21 July 2009. http://csrp.inl.gov/documents/SecuringModems.pdf

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 • PH: 210.402.9669 • FX: 210.402.6996 • TF: 800.817.4837
www.securelogix.com