



White Paper

# **Mitel 3300 IP Communications Platform (ICP) Secure Voice Communications**

White Paper



# White Paper

August 2006

**Copyright**

Copyright © 2006 Mitel Networks Corporation. This document is unpublished and the following notice is affixed to protect Mitel Networks Corporation in the event of inadvertent publication: All rights reserved. No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Mitel Networks Corporation. Trademarked Product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

## Table of Contents

<b>Overview .....</b>	<b>4</b>
The Challenge of Security and Why it's Important.....	5
<b>Security Threats and Challenges .....</b>	<b>5</b>
Security for IP Telephony Systems.....	6
PSTN and Legacy Devices.....	7
Figure 1– Legacy Interfaces .....	7
The Signaling Path .....	8
Figure 2 – The Signaling Path .....	8
The Media Path .....	9
Figure 2 – The Media Path .....	9
The Management Path .....	10
Figure 3 – Management Path .....	10
<b>Mitel: Secure Communications Solutions .....</b>	<b>11</b>
Mitel 3300 ICP: Open Platform, Choice, Investment Protection .....	11
Mitel Leverages the Underlying Security of Your IP Network .....	12
Mitel Secures Voice In a “Hostile” IP World.....	12
Encrypted Media Path and Signaling Path .....	13
Mitel Authentication: Known Devices and Users Only!.....	14
Core Platform and Desktop OS: Low Susceptibility to Attack.....	14
Hardened Against Denial of Service Attacks .....	15
Prevent Toll Fraud/Resource Misuse .....	15
Secure Management Interfaces.....	16
Secure Applications .....	16
SIP Security .....	17
Mitel Diligence .....	17
<b>Conclusion.....</b>	<b>17</b>
For More Information on Mitel Security.....	18
<b>About Mitel.....</b>	<b>18</b>

## Overview

The purpose of this document is to review the security threats to a voice communications system and discuss the comprehensive defenses available as part of Mitel® 3300 IP Communications Platform (ICP) portfolio of solutions.

When designing any communications system it is important to realize that no security technology alone can protect an organization against all security threats. An organization's own internal policies and procedures need to be carefully examined to ensure that best security practices are not only being implemented but are also being properly enforced. In addition, the type of network infrastructure utilized to carry your real time IP communications also varies with regard to its security vulnerability. Wireless IP infrastructure and public Internet connections pose a greater security risk than an internal wired network and appropriate consideration must be given to this. Appropriate security measures can be applied within each communication layer to suit the nature of the threat imposed, yet maintain the level of openness and compatibility required for the application. You must also consider that you are as much subject to attack from within by employees and trading partners as attack from external sources.

Appropriate levels of security need to be examined and deployed based on: the nature and value of the resources being secured, the business impact that exists should any resources be compromised, the estimated level of threat / vulnerability, and cost effectiveness of potential security solutions. Put differently, any security solution must be realistically deployable in terms of its usability and cost versus the consequences of a security breach. As a result security requirements will vary by industry sector and each customer's individual requirements.

## The Challenge of Security and Why it's Important

Of all forms of business communications, voice is probably the one that is taken for granted the most. It is almost unimaginable that you would ever pick up the telephone and that it would not work. Even when the power goes out, it is expected that the phone will keep on working. While there are many economical and application-oriented advantages for migrating to an IP-based telephony network, there are also new security challenges that must be addressed to ensure the same high degree of privacy and reliability we have come to expect from our voice communication networks is just as applicable in an IP environment.

An IP Telephony system is not based entirely on IP networking infrastructure. Just like a circuit-switched PBX system, an IP Telephony system must still provide connectivity to the public switched telephone network for external communications. This requires IP Telephony systems to protect against all the same security threats as their circuit-switched predecessors, while at the same time protecting against the additional security threats posed in the IP world. Fortunately, these threats can be minimized to an extent, to make deployment of an IP Telephony solution as secure as many of the older voice systems they seek to replace.

## Security Threats and Challenges

Security threats to an IP Telephony network are posed by the level of reliability and resiliency of the system design itself, the underlining IP network infrastructure, public network interfaces, employee mistakes, deliberate attacks from outside hackers and disgruntled or mischievous employees. Just like with any communication application, an IP Telephony system must be designed to meet a level of reliability and privacy appropriate to the needs of the individual organization.

Key security issues for IP Telephony networks can be summarized along the as follows:

*Confidentiality:* The need to protect transmissions, whether for voice-streaming or data services, to prevent eavesdropping or interception of conversations, call control signaling or passwords.

*Integrity:* The need to ensure that information is not modified by unauthorized users and to unequivocally prove a user or application is actually authorized to perform the task / function they are requesting, be it a voice call or a configuration change.

*Availability:* The need to ensure the operation of the communication system is not adversely affected by a directed Denial of Service (DoS) attack, an inadvertent network storm or a malicious computer worm or virus.

## Security for IP Telephony Systems

Security for any IP Telephony system must take into account the various different types of communication interfaces that comprise the overall system. Different security techniques and options can then be applied to provide the level of security needed for each situation.

IP Telephony systems utilize four main types of network communications as follows:

1. Legacy telephony and PSTN integration functions provide media and signaling gateway functions to traditional analog or digital telephony devices and systems as well as the PSTN.
2. The signaling path is used to set up and or control calls. An attack on signaling can be used to initiate a DoS attack, to modify call routing, to hijack calls, to impersonate another extension, etc.
3. The media path is used to carry the actual voice communications. This path can be subjected to eavesdropping or nuisance activities affecting call quality for example. Compromising the confidentiality or quality of this path can affect business confidence and integrity.
4. The administration and management functions allow access to system and personal configuration options, which in turn can be changed to affect the operation of an individual user or indeed complete system operation. Other management interfaces and protocols can be involved for application interfaces, call accounting, alarm and maintenance functions, centralized directory services, software downloads and upgrades.

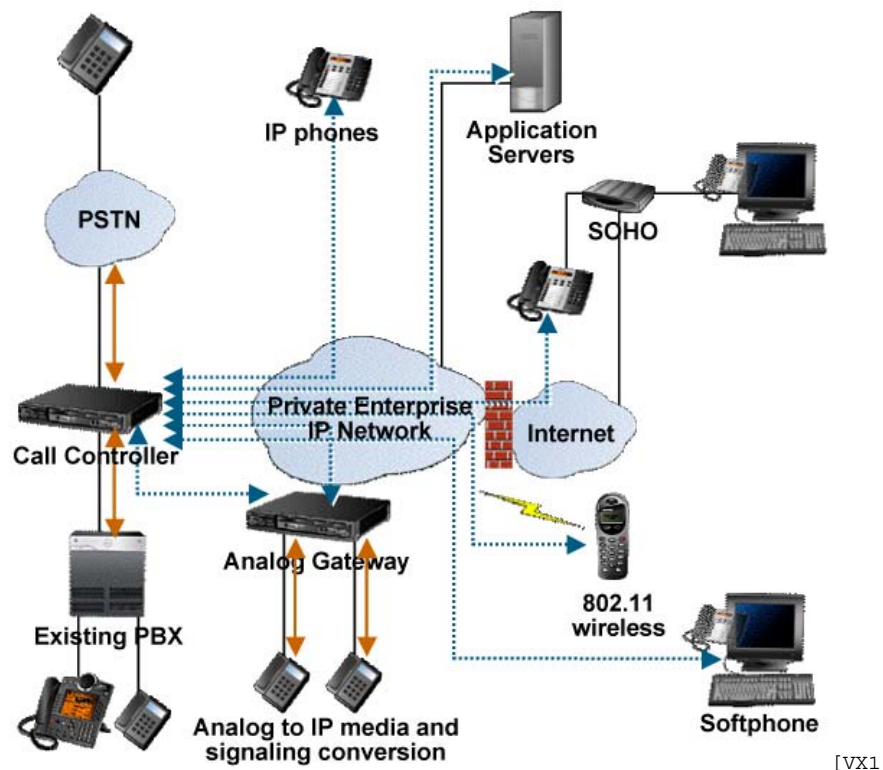
The integrity of each of these communication paths must be secured in order for the system to function properly and reliably. Confidentiality, authentication, and impersonation are important considerations for many of these communication path functions as well.

The diagrams on the following pages provide additional illustration of these communication paths and their involvement in a typical Voice-over-IP deployment.

## PSTN and Legacy Devices

In any discussion involving the security and integrity of IP systems, it is incumbent to realize that legacy devices and PSTN connectivity are an integral part of the equation. That is because IP Telephony systems must typically support analog devices as well as connectivity to the public switched telephone network. This is of particular significance as in many cases; interfacing with an existing PBX system is required to enable a more gradual migration to IP.

### Analog LS, ISDN, Q.SIG, DPNSS



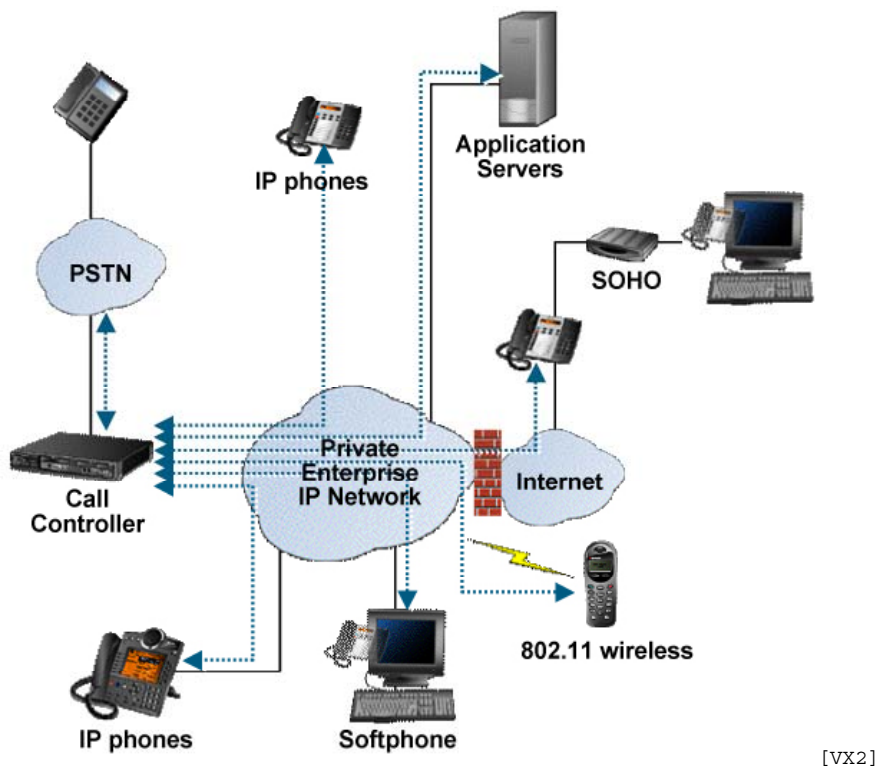
### Figure 1– Legacy Interfaces

When you connect any communications system to the PSTN, toll fraud security becomes a costly risk that must be considered. The system architecture used for legacy device support can also be different depending on the IP Telephony system design. Some systems convert everything to IP prior to switching calls, while others may switch TDM to TDM traffic directly and avoid the need to connect those calls over the IP infrastructure at all. Direct TDM switched calls do not have IP security issues, but could still be subjected to eavesdropping via wiretap.

## The Signaling Path

The call controller is involved with all the signaling control associated with setting up calls within the network as illustrated in Figure 1. IP Telephony devices and applications are reliant on the call controller for; call establishment, tear down, transfer, etc. The controller must authenticate the device prior to providing it with service. The call controller determines if a device is authorized to make a given call based on the device's privilege or class of service. The signaling between call controller and IP Telephony device can be vendor proprietary or standards-based such as H.323 or SIP. Multiple protocols can be supported from the same call controller.

### SIP, H.323, Proprietary



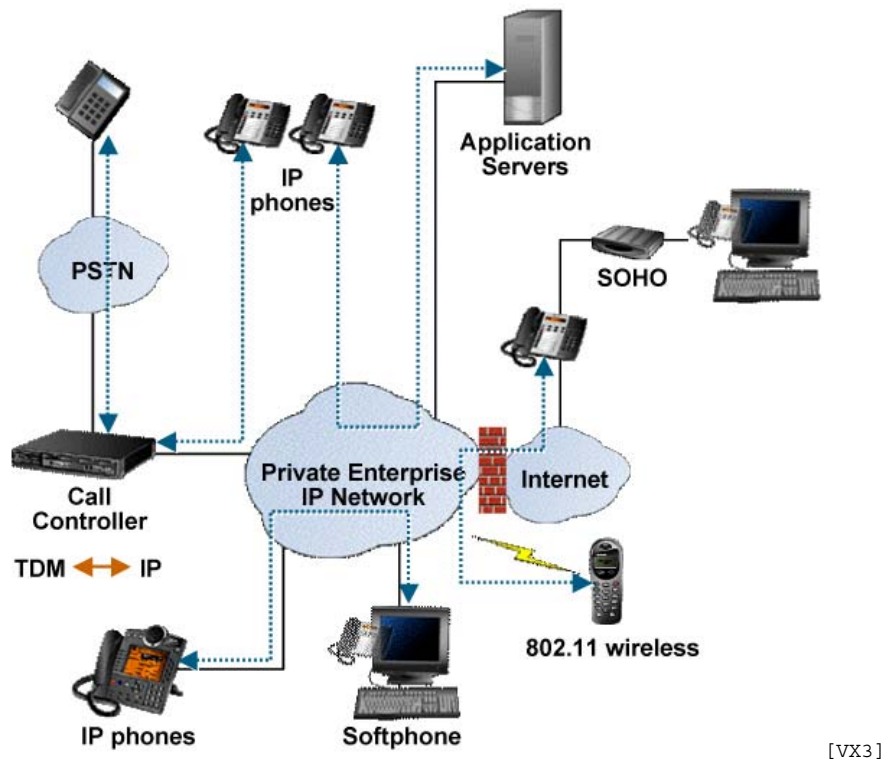
### Figure 2 – The Signaling Path

Threats to the signaling path include impersonation to steal phone service or disrupt a valid user's phone service. Eavesdropping on the signaling path can be used to learn account codes that can be used to override toll call restrictions.

## The Media Path

Media packets are sent directly between the communicating devices as shown in Figure 2. The call controller simply provides the devices with the details needed to establish a direct media path between one another. For calls between IP Telephony devices and the PSTN, a media conversion between IP and TDM/analog must take place. In this case the local IP Telephony device is directed to send its media packets to a media gateway device which can be integrated within the call controller as shown or it can be a separate device.

## Real-Time Protocol (RTP) Packets



**Figure 2 – The Media Path**

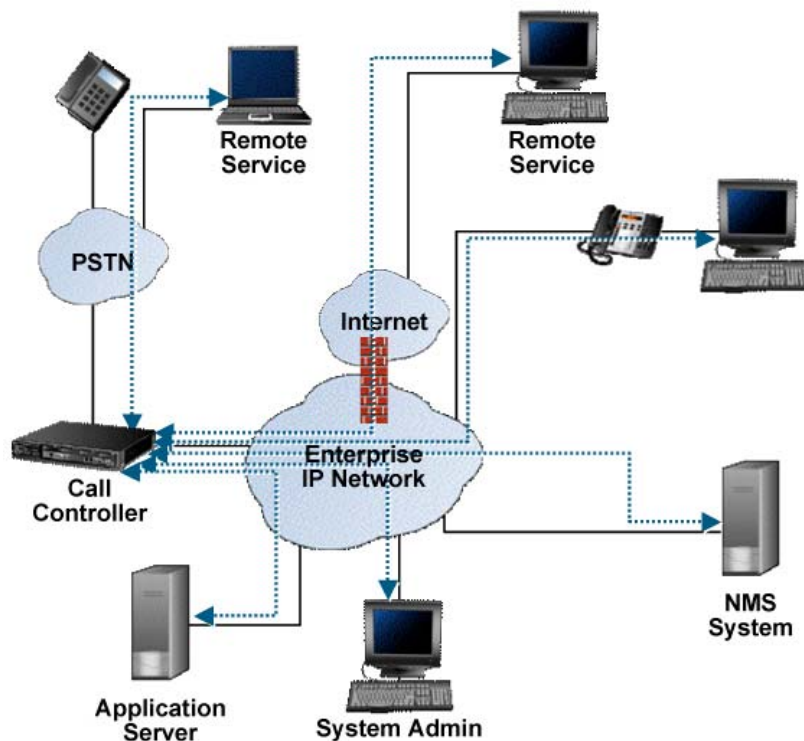
Eavesdropping and transport disruption are the primary threats to voice media packets. The fact that they route directly between communication devices means that monitoring the Ethernet port of the call controller would not provide access to all the phone conversations. Attempts to eavesdrop on the Ethernet port of a given phone through physical access to wiring, remote monitoring probes or packet rerouting would be a potential threat. Attempts to disrupt media packet flows through packet-flooding type

attacks are also possible. Perhaps the most significant eavesdropping threat would be associated with media packets that must traverse the Internet or wireless connections.

## The Management Path

Typically the management path is used for system administration and configuration, data provisioning or synchronization, accounting, application interfaces, alarm and maintenance functions. Management interfaces can be monitored to gain someone's password or be used in a DoS attack. A management interface for call detail records could be monitored to obtain call accounting information that could include account codes or information such as who a particular person has been calling lately.

### Examples – Telnet, http, FTP, SNMP, XML, TAPI, Proprietary



### Figure 3 – Management Path

Figure 3 depicts some of the management interfaces that may be involved with regard to a typical IP Telephony system. End users can have login access to the system to set some of their own personal parameters such as speed dials, feature keys, and forwarding functions. The system may have management related network connections to central directory servers, enterprise management systems, alarm systems, call accounting systems, or other application servers. System administrators require access

to higher-level system functions or external Network Management System (NMS) applications. Remote access for system service is also a consideration and could be based on PSTN dialup or other means such as the Internet. In short, many management interface options are potentially available and must be considered with regard to system security. Any interfaces that are not required should also be disabled.

## **Mitel: Secure Communications Solutions**

Mitel® solutions are the foundation for scalable enterprise networks that offer compelling benefits at both the user and infrastructure level. To be productive and effective, enterprise users need to access, manage and control an increasingly complex array of communications and productivity tools. They need to communicate and collaborate effortlessly with customers, colleagues and partners, whether at their desk or away from the office. All of these functions must be available with the confidence that communications will be secure.

Mitel addresses your need for secure communications with a comprehensive portfolio of security solutions to protect your business communications from security threats today, and ongoing diligence to ensure the security of future communications.

## **Mitel 3300 ICP: Open Platform, Choice, Investment Protection**

Mitel 3300 IP Communications Platform (ICP) provides enterprises with a highly scalable, feature-rich communications system designed to support businesses from 30 to 60,000 users. The 3300 ICP provides enterprise IP-PBX capability plus a range of embedded applications including standard unified messaging, auto-attendant, ACD and wireless gateway.

At the user level the 3300 ICP supports the industry's largest range of desktop devices including entry-level IP phones, web-enabled IP devices, wireless handsets (WiFi or IP-DECT) and full-duplex IP audio conference units. The 3300 ICP also supports a powerful suite of applications including multimedia collaboration, customer relationship management and unified messaging. Industry standard Application Programming Interfaces (APIs) are supported for extensive third-party applications through Mitel Solutions Network (MiSN).

The 3300 ICP offers can be configured and integrated into any corporate LAN/WAN infrastructure – regardless of manufacturer – to provide IP Telephony and application access to thousands of users in a single building or campus setting. The 3300 ICP can also be seamlessly networked via IP or TDM with other 3300 ICPs and seamlessly interoperates with traditional PBX telephone systems, protecting existing investments while allowing organizations to add IP-based communications to work groups, departments, and new locations/facilities at a pace that make sense for them.

## **Mitel Leverages the Underlying Security of Your IP Network**

The openness of the Mitel platform gives you the opportunity to implement and deploy the private IP network infrastructure that best meets your needs and provides the security defenses that best protect your organization.

Today there is extensive array of security solutions available for private IP networks from a host of security and infrastructure vendors:

- Firewalls
- Traffic policing solutions
- Intrusion Detection Systems
- VPN
- Access Control Servers
- Trust and Identity Management Systems

To maximize the security of your overall communications solution, these solutions can be deployed to achieve an appropriate level of security to protect the private IP network infrastructure itself. For example, VPN technology must be used to secure private IP communications that must traverse an unsecured public network. Authentication and encryption must be applied to secure 802.11 wireless connections. The entire private IP network must be secured from the Internet via firewall technologies. These are simply standard security practices for any private IP network and are needed to provide an underlying layer of security. Your Mitel communications solution leverages all of these advanced defenses to help you secure voice on your network.

## **Mitel Secures Voice in a “Hostile” IP World**

Mitel considers the defenses discussed above as only one layer of your overall effort to secure your communications solution. In fact, Mitel looks upon the underlying network, no matter how secure, as a hostile environment which can host attacks on your Mitel voice solution. It is this conservative and rigorous approach that has led Mitel to offer the extensive suite of security defenses for its 3300 ICP family of products. The following sections describe the specific capabilities available for your secure Mitel 3300 ICP deployment.

## Encrypted Media Path and Signaling Path

When deploying an IP Telephony solution, the first line of defense is to secure physical access to wiring closets, LAN switches, application servers and the call controller. This makes eavesdropping more difficult to accomplish for a perpetrator without physical access.

Physical security may be adequate protection for confidentiality within the local private “wired” network for many organizations. However, some organizations wish to deploy a more sophisticated level of defense to prevent unscrupulous persons from trying to access enterprise conversations or communications signaling. Even the most well maintained telephony environment hosted on a highly secure IP infrastructure still poses some risk. Encryption of the Media and Signaling paths provide an advanced level of defense.

Very early on Mitel recognized the importance of encryption and implemented both media path and signaling control encryption as an integral part of its Teleworker Solution, first released in 2003. Encryption is especially relevant to the teleworker application which takes advantage of the potentially “hostile” public Internet to provide remote users with transparent access to communications.

As mentioned, Mitel considers that even the host IP infrastructure is a potentially hostile environment. Therefore, Mitel supports both media and signaling encryption for its complete IP desktop telephone portfolio on its 3300 ICP. Unlike many competing products, encryption is *enabled by default* and is not an option that must be configured as an extra step. The media path encryption is accomplished with Secure RTP (SRTP) using 128-bit Advanced Encryption Standard (AES) and the signaling path also used 128-bit AES encryption. It is worth noting that Mitel has chosen to protect its customers’ investment by making encryption backwards compatible to support both currently shipping desktops as well as all existing Mitel IP desktops that customers may have previously deployed.

In addition to implementing encryption for Mitel IP desktops, Mitel provides encryption of the media path between multiple ICPs using SSL which is important for customers wishing to scale their applications by configuring ICPs into clusters or deploy systems as part of a centrally managed but distributed architecture.

## **Mitel Authentication: Known Devices and Users Only!**

IP Telephony devices and applications are reliant on the call controller for call establishment, tear down, transfer, etc. The controller must authenticate the device prior to providing it with service. The call controller determines if a device is authorized to make a given call based on the device's privilege or class of service.

As discussed securing access to the internal physical network is a basic first line of defense. However, for internal personnel or intruders with access to wired Ethernet switch ports or devices, physical level authentication cannot be completely relied upon to take the place of effective and secure authentication at the application and user level. To address this requirement, Mitel's voice solution implements set authentication that requires a unique association of MAC address, IP and user entered PIN registration number. For further protection, desktop software downloads are encrypted and digitally signed to ensure that sets cannot be spoofed.

For organizations wishing to implement an even increased level of defense, Mitel provides 802.1X authentication for desktops. Mitel's implementation offers support for the Extensible Authentication Protocol (EAP) using EAP-MD5 challenge authentication to a RADIUS Server. Users authenticate through the phone interface by entering a username and password. This support is provided on Mitel's dual mode 5212, 5215, 5220, 5224, 5235, 5330, 5340 and Navigator IP Phones.

## **Core Platform and Desktop Operating System (OS): Low Susceptibility to Attack**

Many system attacks today are targeted at "general purpose" operating systems such as Microsoft Windows, Linux and UNIX. These operating systems all include as part of their base functionality such services as a web server, file/print services, etc. Because these utilities are common to all installations of the OS, they are an easy and attractive target for authors of viruses, worms, trojans, etc. Malicious programs target vulnerabilities found within common services running on a server or in the case of viruses, target desktop applications once they are opened. Application services listen on their associated ports for client connections and if vulnerabilities are found a worm can exploit them.

Unlike many solutions that utilize versions of “general purpose” operating systems to implement voice solutions, the Mitel 3300 ICP uses an embedded OS called VxWorks. VxWorks is far less susceptible to attack by viruses or worms that target traditional applications and their OS services because it provides a very small base “common” functionality. It is therefore not affected by the viruses and worms typically found on networks and the Internet. In practice, this makes it extremely difficult for an attacker to write a virus targeted at generic VxWorks implementations.

## **Hardened Against Denial of Service Attacks**

The industry term for deliberate attacks on system availability is known as Denial of Service (DoS) attacks. DoS attacks are aimed at the interruption of the operation of IP network switches, telephone sets, application servers, or any other internal components of an IP system. These attacks attempt to “break” the components in such a way that their performance is either degraded or rendered unusable. For example, an attack could be launched against the IP Telephony call controller, the “heart” of the system, in an effort to bring down the entire voice network. If successful, all voice communications both internal and external to the organization would be affected.

Mitel’s core platform OS strategy takes into account DoS threats as well. Given that the 3300 ICP and Mitel’s desktops do not use general-purpose operating systems, they are not vulnerable to the entire class of DoS attacks against the components of those operating systems. However, it should be noted that other DoS attacks are targeted at the TCP/IP networking layer itself and so will attack any IP-connected device. With each release of the 3300 ICP and Mitel’s IP desktops, Mitel continues to harden the systems in order to mitigate DoS attacks. Hardening is a continuous process and always a priority at Mitel to ensure our customers are protected as much as possible against DoS attackers.

## **Prevent Toll Fraud/Resource Misuse**

Mitel implements Class of Restriction (CoR) to bar the dialling of certain external telephone numbers or ranges of numbers (Call Barring). This is achieved by associating in software each extension with a CoR and providing specific barring plans with each CoR.

Mitel’s implementation of CoR affords great flexibility. Up to 64 different CoR can be specified. An extension user attempting to dial barred numbers will result in them receiving Number Unobtainable Tone. Alternatively, the extension user could be routed to an answer point, such as the switchboard, for the offering of advice. An extension may have a different CoR for use with Day Service, Night 1 and Night 2 services, respectively. This would allow users to dial external digit sequences during certain time periods that could be restricted at other times. Anyone wishing to impersonate a device in an attempt to bypass these restrictions would require an in-depth understanding of

Mitel's proprietary signalling mechanisms (protection of these signalling mechanisms is discussed in the preceding sections of this document).

The utilization of account codes provide additional control options. Verified Account Codes allow the users to utilize features that are not normally available at an extension. These Account Codes can be used to change the Class of Service (features) and Class of Restriction (barring) parameters of the extension. Non-Verified Account Codes allow the extension user to enter codes in Mitel's call reporting utility, the Station Message Detail Recording (SMDR), relating to billing and/or call management. System Account Codes can be added and automatically dialed by the system when outgoing calls are made on network services that have such a requirement.

## **Secure Management Interfaces**

The 3300 ICP provides three embedded management tools for administration and configuration. Each of these tools is designed for a particular user type: desktop user, group administrator, and system administrator. The browser interface to these management tools is based on secure HTTPS to protect both login password information and content from being monitored. The 3300 ICP is also designed to withstand a DoS attack directed at this interface. Performance of the management interface could be degraded by a DoS attack; however this will not affect voice operation which is of a much higher system priority.

Mitel also offers the optional Mitel Management Access Point to provide secure remote admin for VPN or dial-up access.

## **Secure Applications**

Mitel addresses your need for security across its broad portfolio of applications as well. For instance, the award-winning Mitel Your Assistant™ application provides a softphone with encrypted call path and call signaling as well as secure instant messaging to keep your instant messaging (IM) traffic encrypted and inside your network.

Mitel's wireless solutions include secure IP-DECT solution (EMEA only) and encryption for 802.11 wireless telephony, include support for encryption using Wi-Fi Protected Access (WPA) and authentication using WPA and WPA2.

Mitel solutions can take advantage of XML to develop powerful applications. Mitel's XML implementation supports encryption of all traffic using standard SSL and strong certificate-based authentication is required for the application program interface (API) usage.

## SIP Security

Mitel has directed its concern for secure communications to its growing portfolio of SIP desktops. Mitel SIP desktops support Secure RTP and satisfy the challenging PROTON test suite for CERT advisory CA-2003-06. They also provide support for firewall traversal and support for SSL-encrypted SIP. Mitel continually monitors evolving SIP security standards and will implement additional standards as they become ratified.

## Mitel Diligence

Mitel understands that the quest for security must be ongoing and relentless. To that end, Mitel has implemented a strategy to ensure that security is a focus of every facet of Mitel's product and service lifecycle. Mitel maintains a broad-based internal security team encompassing R&D, test, product management, product support and product verification. A well defined escalation process for managing reported security vulnerabilities has been instituted that includes triage by the product security team and escalation to the appropriate product groups. As needed security advisories are posted to [www.mitel.com/security](http://www.mitel.com/security).

Mitel is an active participant in relevant security industry bodies. Specifically, Mitel is a member of the VoIP Security Alliance (VOIPSA) and maintains connections with groups including CERT, US-CERT and NISCC (National Infrastructure Security Co-ordination Center).

## Conclusion

The advantages of converging voice and data communications are derived through the many application innovations and economies made possible by the openness and ubiquity of the IP communication fabric. These same fundamental qualities inherent in IP networks expose them to potential security risks. Mitel understands these risks and their consequences.

Specifically Mitel's voice solution provides the core defenses you require:

- Encrypted media path and signaling path, enabled by default
- Authentication
- Secure Management Interfaces
- Hardened against DoS attacks
- Proven PSTN protection

Mitel provides a secure "best in class" IP Telephony solution that is designed for and assumes deployment into a "hostile" IP environment and leverages the available defenses provided by the IP infrastructure of your choice.

This approach, when used in conjunction with standard security techniques and practices already available, ensures a secure and realistically deployable solution.

## For More Information on Mitel Security

Mitel provides security information on its public web site at [www.mitel.com/security](http://www.mitel.com/security).

**North America**  
(613) 592 2122  
1 800 648 3579

**Latin America**  
(613) 592 2122  
1 800 648 3579

**UK**  
Tel: +44 (0)1291 430000  
Fax: +44 (0)1291 430400

**France**  
Tel: +33 (0)1 61 37 00 90  
Fax: +33 (0)1 61 37 00 99

**Benelux**  
Tel: +31 (0)30 85 00 030  
Fax: +31 (0)30 85 00 031

**Italy**  
Tel: +39 02 2130231  
Fax: +39 02 21302333

**Germany, Switzerland, Austria**  
Tel: +49 (0)211 5206480  
Fax: +49 (0)211 52064899

**Portugal and Spain**  
Tel: +34 91 350 66 33  
Fax: +34 91 350 70 14

**Middle East**  
Tel: +971 4 3916721  
Fax: +971 4 3915288

**South Africa**  
Tel: +27 82 559 8688  
Fax: +27 11 784 6916

**Asia-Pacific**  
Tel: +852 2508 9780  
Fax: +852 2508 9232

[www.mitel.com](http://www.mitel.com)