A MITEL
TECHNICAL PAPER

MiVoice Business

MiVoice Business Secure Voice Communications Technical Paper

September 2024

Mitel
Powering connections

Contents

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's MiVoice Business portfolio of solutions.

When designing any real time 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 the best security practices are not only being implemented but are also being properly enforced. In addition, the type of network infrastructure utilized to carry real time communications is also a variable to be considered with regards to security. For example, Wireless (Wi-Fi) infrastructure and public Internet connections generically pose a greater security risk than an internal private wired network and consideration must be given to the network infrastructure. Security measures can be applied within each communication layer to suit the nature of the threat imposed and yet maintain the level of openness and compatibility required for the application(s). A customer must also consider the reality that they 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. Or worded 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 by each customer's individual requirements.

The Challenge of Security and Why It Is Important

Of all forms of business communications, voice is the one that is taken for granted the most. It is almost unimaginable that someone 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 to an IP-based communications network, there are also security challenges that must be addressed to ensure the same high degree of privacy and availability that users have come to expect historically from voice communication networks.

While all Unified Communications (UC) systems are reliant upon the underlying network, their security and availability are not based entirely on the IP infrastructure. Current UC systems must still provide connectivity to legacy telephony devices and the public switched telephone network (PSTN) for external communications. This means that a modern UC system must still protect against the same security threats as its circuit-switched predecessors, while at the same time also protecting against the additional security threats posed within the IP world. Fortunately, these threats can be minimized to an extent, to make deployment of a UC solution as secure as many of the older proprietary voice systems.

Security Threats and Challenges

Security threats to a UC solution are posed by the level of reliability and resiliency of the system design itself, the underlying network infrastructure, public network interfaces, employee mistakes, deliberate attacks from outside hackers and disgruntled or mischievous employees. Just as with any communication application, a UC 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 and UC can be summarized 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 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 Unified Communication Systems

Security for any Unified Communications (UC) system must consider the 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.

UC solutions utilize several types of network communications:

1. Legacy telephony and PSTN integration functions provide media and signaling gateway functions to traditional analog and digital telephony devices and systems. Devices used for this function include Analog Terminal Adapters (ATAs), Analog Gateways and Digital Gateways.
2. The signaling path is used to set up and control calls. An attack on signaling can be used to initiate a Denial of Service (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 (or video) 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. Non-voice media types such as chat, collaboration, SMS/MMS, presence engine and email integrations with the UC solution and other UC capabilities.
5. Application Programming Interfaces (APIs) that are used for integrating with backend systems.
6. The administration and management functions that allow access to system and personal configuration options, which in turn can be changed to affect the operation of an individual user or 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 for the system to function properly and reliably. Confidentiality, authentication, and impersonation are important considerations for 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.

Legacy Interfaces - Devices and Trunks

In any discussion involving the security and integrity of IP systems, it is incumbent to include legacy device and trunk support. That is because IP Telephony systems must often support analog devices as well as connectivity to the public switched telephone network, which may still sometimes include TDM circuits such as analog POTS lines or T1/E1 PRI circuits. This can also be a factor when attempting to interface the IP Telephone system to legacy PBXs, as these connections may also be TDM as well in some instances.

Analog Devices, Analog and Digital Trunks

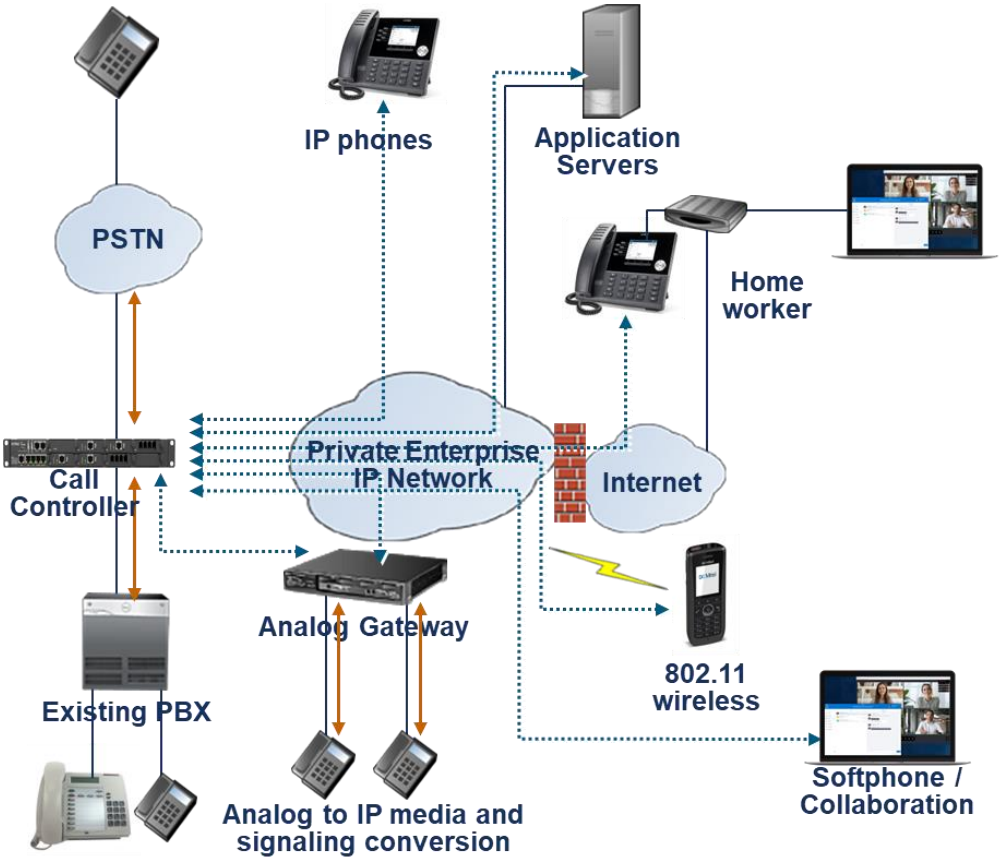

Figure 1 – Legacy Interfaces

When connecting any communications system to the PSTN, toll fraud security must be considered. Programming of the system to restrict call type and call barring to ensure only permitted calls is also a must, with use of features such as Account Codes to ensure identity and authorization of people making calls on legacy devices.

The system architecture used for legacy device support can also vary depending on the 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. Direct TDM switched calls do not have IP security issues but could still be subjected to eavesdropping via a physical wiretap. Consequently, physical security is a primary defense, including access to wiring frames, when it comes to legacy telephony to stop intrusion of calls.

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 2. IP Telephony devices and applications rely on the call controller for call establishment, tear down, and transfer. 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 programmed privilege level. The signaling between the call controller and IP Telephony device can be vendor proprietary or standards-based with SIP. Multiple protocols can be supported from the same call controller.

SIP, Proprietary

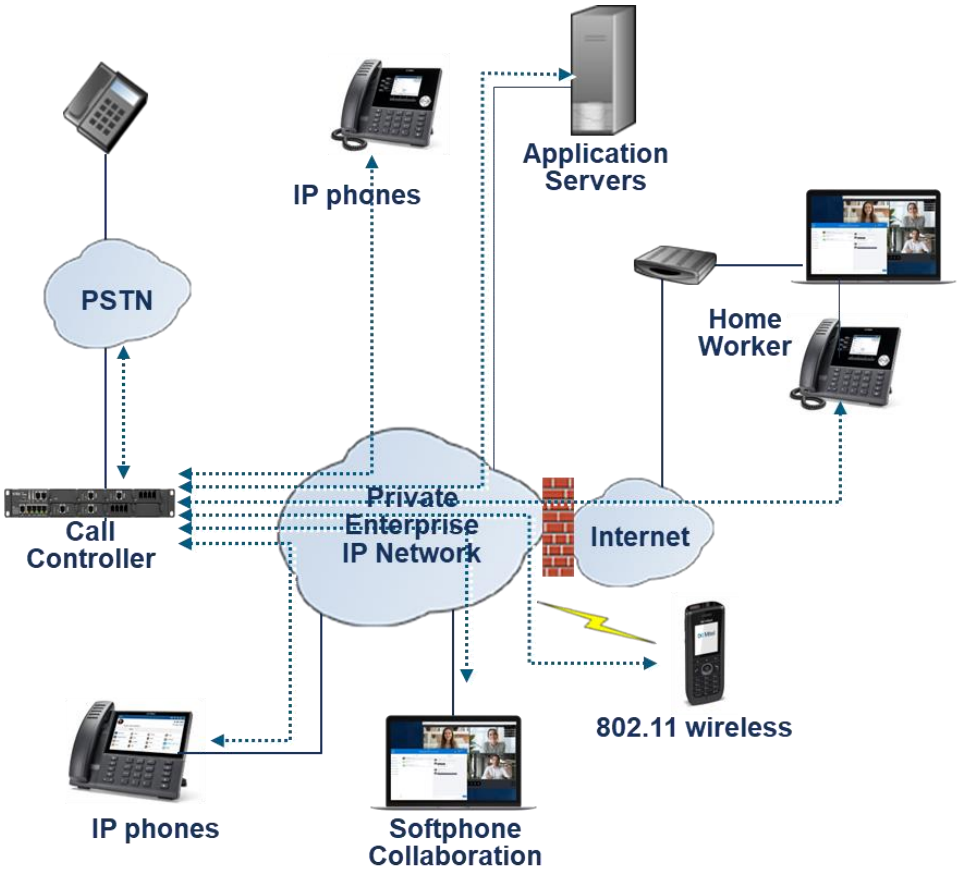

Figure 2 – The Signaling Path

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.

Strong authentication mechanisms and strong encryption of the signaling are the key elements to signaling security. Mitel by default utilizes Transport Layer Security (TLS) 1.2 or better for signaling encryption. While not as critical as it once was due to the increased availability of bandwidth, ensuring that the signaling packets have the correct priority on the network (e.g. 802.1p and DSCP [Differentiated Services Code Points]) in case of congestion remains a relevant concern.

The Media Path

With MiVoice Business, voice media packets are sent directly between the communicating devices as shown in Figure 3. The call controller provides the devices with the details needed to establish a direct media path between one another. For calls between IP Telephony devices and the legacy PSTN, a media conversion between IP and digital/analog must take place. In this case, the local IP Telephony device is directed to send its media packets to the media gateway which may be integrated within the call controller as shown or it can be a separate device (such as an ATA). The conversion step is not applicable to SIP trunks where the calls are already IP and are routed via Session Border Controller (SBC) instead.

Real-Time Protocol (RTP) Packets

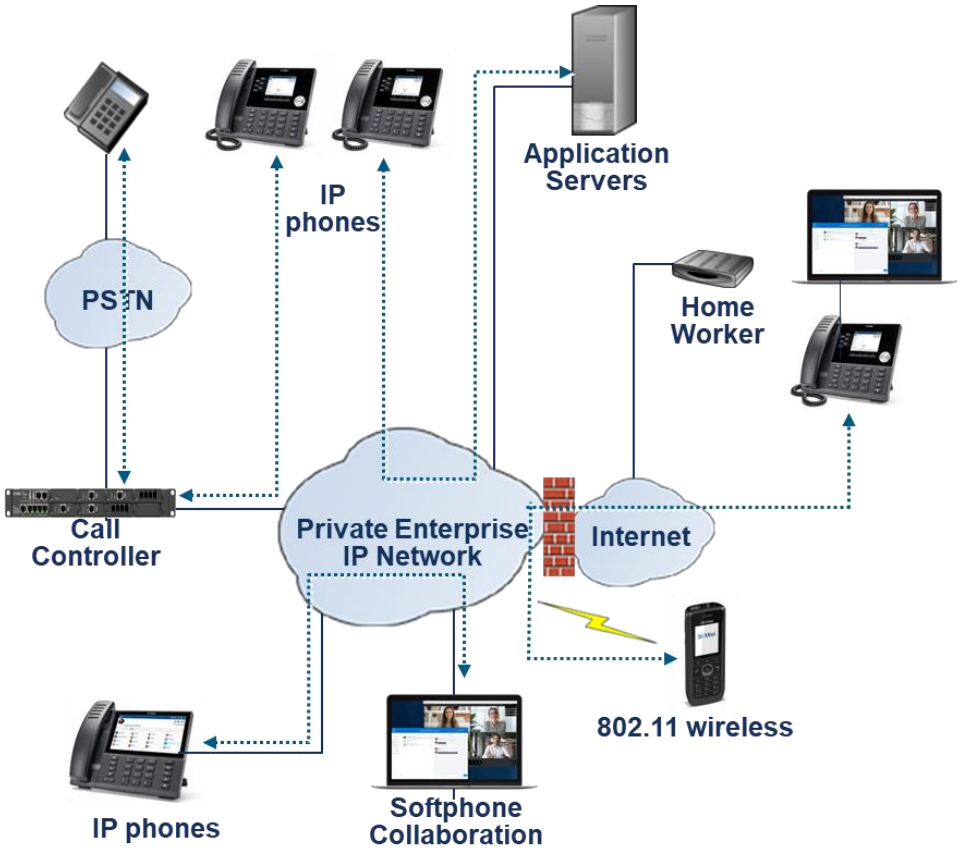

Figure 3 – The Media Path

Eavesdropping and transport disruption are the primary threats to voice media packets. Since IP voice traffic is typically routed directly between devices on the same LAN (Local Area Network), simply monitoring the Ethernet port of the call controller would not provide access to much of the actual phone traffic occurring on the local network. However, attempts to eavesdrop on the Ethernet port of a given phone through physical access to wiring, remote monitoring probes or packet rerouting could be a potential threat. Attempts to disrupt 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.

As with all the scenarios, limiting physical access is a big part of the security requirements. Ensuring that a potential intruder does not have access to the LAN equipment physically or remotely to activate features such as port or VLAN (Virtual Local Area Network) mirroring. Once a call is set up, the media should be encrypted

using Secure Real Time Protocol (SRTP). MiVoice Business uses SRTP with 128-bit AES bulk encryption cipher for the streaming media. For end-to-end encrypted communications both endpoints must support SRTP, and support for SRTP should be confirmed when using any non-Mitel voice device.

Non-Voice Media

Non-voice media types are a part of the MiVoice Business solution's ecosystem, including such applications as MiCollab and MiContact Center Business (MiCC-B).

MiCollab for example provides unified messaging (multiple integration choices), instant messaging and a presence engine as well as collaboration and administration tools. Each of these features needs to be authenticated and authorized. Administration configuration of the users should be such that the minimum feature set required for that user is applied. External users are connected through a MiVoice Border Gateway, typically deployed in a customer's DMZ (De-Militarized Zone), for additional security.

MiContact Center Business is the reporting engine for Automatic Call Distribution (ACD) on MiVoice Business and integrates by collecting call records and API events. MiCC-B also supports the routing of non-voice media such as web chat, SMS and Email. In fact, just about anything, including messaging from Internet of Things (IoT) devices, can be queued and routed through MiContact Center Business using the Open Media feature and REST APIs. MiCC-B also utilizes the Mitel Border Gateway as a secure proxy for the Ignite web client for remote agents which is used to interact with these non-voice media interactions. It is therefore imperative that these connections are also secured.

The Management Path

The management path is used for system administration and configuration, data provisioning and 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 person has been calling lately.

Figure 4 depicts some of the management interfaces that may be involved in 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 also have management related network connections to central directory servers, enterprise management systems, alarm systems, call accounting systems, or other application servers. Remote access for system service is also a consideration. In short, many management interface options are potentially available and must be considered when thinking about system security. With a new MiVoice Business, interfaces are disabled by default; however, an administrator should never assume that that an unused interface is disabled and should verify and reconfirm periodically as well as after an upgrade.

Examples – HTTPS, FTP, SNMP, SSH

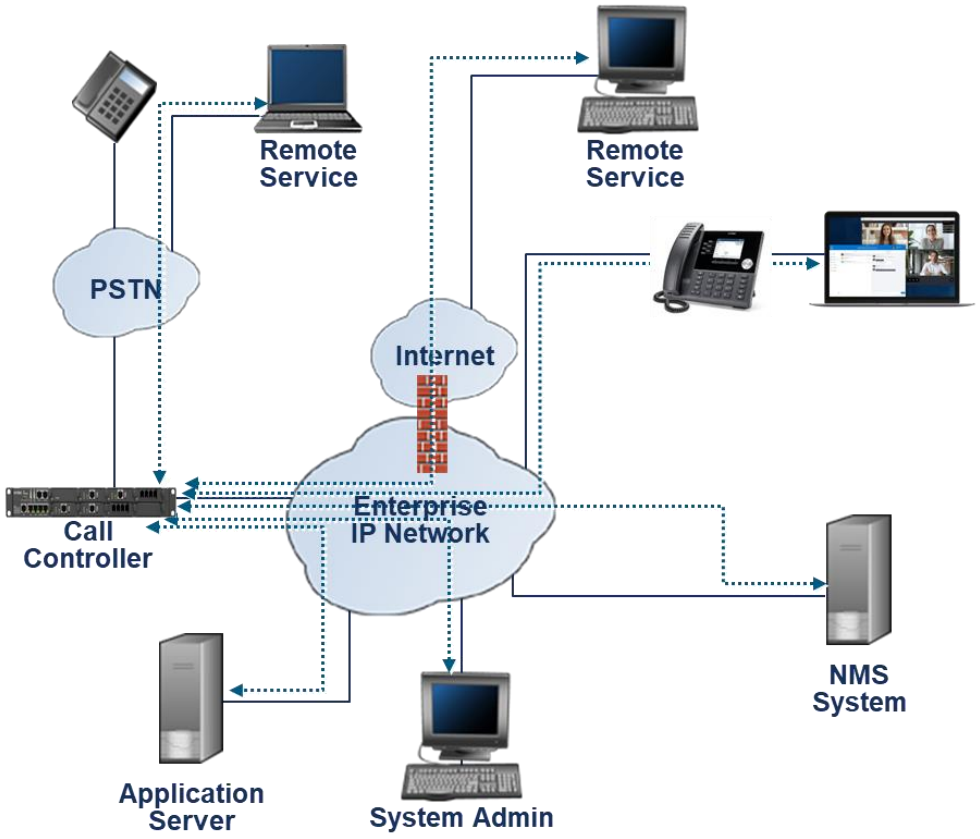

Figure 4 – Management Path

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

Mitel MiVoice Business: Open Platform, Choice, Investment Protection

Mitel's MiVoice Business system provides enterprises with a highly scalable, feature-rich communications system designed to support businesses from 30 to 100,000 users. MiVoice Business provides enterprise IP-PBX capability plus a range of embedded applications including unified messaging, auto-attendant, call center (ACD) and wireless gateway capabilities.

At the user level the MiVoice Business supports a range of desktop devices including entry-level to executive-level IP phones, wireless handsets (Wi-Fi or IP DECT [Digital Enhanced Cordless Telecommunications]), soft

phones for smart devices and full-duplex IP audio conference units. MiVoice Business also supports a powerful suite of applications including multimedia collaboration, Customer Relationship Management (CRM) integration and Unified Messaging (UM). Industry standard Application Programming Interfaces (APIs) are supported for extensive third-party applications through the Mitel Solutions Alliance (MSA) network (https://www.mitel.com/developer).

Mitel's MiVoice Business system can be configured and integrated into any corporate LAN/WAN infrastructure regardless of the network equipment manufacturer. Mitel Unified Communications (UC) solutions have been designed to be network vendor neutral and can provide IP Telephony and application access to thousands of users within a single building or across any number of locations. Mitel UC solutions can also be seamlessly networked with other Mitel systems and seamlessly interoperate with traditional PBX telephone systems, protecting existing investments while allowing organizations to add advanced communications to work groups, departments, and new locations and facilities at their own pace.

Mitel Leverages the Underlying Security of Your IP Network

The openness of the Mitel platforms provides a business the opportunity to implement and deploy the private IP network infrastructure that best meets their 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 / Intrusion Prevention 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. A Mitel communications solution leverages these advanced defenses to help customers secure voice on their network.

Mitel Secures Voice in a "Hostile" IP World

Mitel considers the defenses discussed above as only one layer of the 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 MiVoice Business family of products. The following sections describe the specific capabilities available for your secure MiVoice Business deployment.

Physical Security

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 an attacker without physical access. When MiVoice Business is hosted either in a private data center or within a public cloud infrastructure such as AWS (Amazon Web Services) or Microsoft Azure, the application servers and call control are already located within secure datacenters, so physical access is already covered.

Physical security may be adequate protection for confidentiality within the local private 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 the next level of an advanced level of defense.

Encrypted Media Path and Signaling Path

Very early on, Mitel recognized the importance of encryption and implemented both media path and signaling control encryption as an integral part of both its on-premises and Teleworker deployment models. Mitel's Teleworker solution, provided by the Mitel Border Gateway, allows devices to connect Over-the-Top (OTT) via the public Internet. Encryption is especially relevant to the Teleworker deployment model, which takes advantage of the potentially "hostile" public Internet to provide remote users with transparent access to communications.

As mentioned, Mitel considers even the host IP infrastructure to be a potentially hostile environment. Therefore, Mitel supports both media and signaling encryption for its complete IP telephony endpoint portfolio with MiVoice Business. 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) or better, and the signaling path uses TLS 1.2 or better encryption. It is worth noting that Mitel has chosen to protect its customers' investment by making encryption backwards compatible to support both currently shipping IP endpoints as well as legacy Mitel IP endpoints that customers may have previously deployed.

In addition to implementing encryption for Mitel IP endpoints, Mitel provides encryption of the signaling path between multiple call controllers using TLS, which is important for customers wishing to scale their applications by configuring MiVoice Business systems into clusters or deploy systems as part of a centrally managed but physically distributed architecture. Media streaming between IP endpoints registered to different MiVoice Business call controllers can occur directly between the IP endpoints using the above mentioned same Secure RTP (SRTP) with 128-bit Advanced Encryption Standard (AES) or better.

Mitel Authentication: Known Devices and Users Only!

Mitel 6900-series IP phones, when connected to the MiVoice Business, use a stimulus-based, encrypted, proprietary protocol (MiNet) and behave similarly to a thin client in that the "brains" are in the call control server and the phones are responding to user input or call control instructions. The web server for the 6900-series phones is disabled by default.

The IP endpoints and applications are reliant on the call controller for call establishment, tear down, transfer,

etc. However, before that can happen 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 it is known.

Securing access to the internal physical network is the first line of defense. However, for internal personnel or intruders with access to wired Ethernet switch ports or devices, physical level authentication cannot solely be relied on to replace effective and secure authentication at the application and user level. To address this requirement, Mitel's voice solution also 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 increased level of defense at the network level, Mitel provides 802.1X authentication for desktop devices. Mitel's implementation offers support for the Extensible Authentication Protocol (EAP) using EAP-MD5, EAP-PEAP or EAP-TLS, depending on the phone model and vintage, challenge authentication to a RADIUS Server. Users authenticate through the phone interface by entering a username and password.

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 MiVoice Business uses an operating system, Mitel Standard Linux (MSL), where Mitel has removed unneeded functionality and hardened it to support real time communications. By keeping only the code that is required for the solution it has a much-reduced attack footprint available to an attacker. In addition, non-Mitel applications are not permitted to be installed on the Mitel servers. Consequently, MSL 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 of "common" functionality.

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 "brains" 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 also considers DoS threats. Given that the MiVoice Business 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 MiVoice Business 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 dialing of certain external telephone numbers or ranges of numbers (Call Barring). This is achieved by associating in software each extension and user with a CoR and providing specific barring plans with each CoR. Before being able to talk with the call control to make a call or use a feature the IP set must have first been authenticated successfully previously.

Mitel's implementation of CoR affords great flexibility. Each and every time a user makes a call the CoR of the user / device is verified and a telephone extension user attempting to dial a number that is not permitted by their level of access will result in them receiving Number Unobtainable Tone. Alternatively, the telephone 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, and the permitted numbers can be allowed or barred based upon the time and day the call is taking place on. This allows users to dial external digit sequences during certain time periods, but the same digits can be restricted at other times if desired. Anyone wishing to impersonate a device in an attempt to bypass these restrictions would require an in-depth understanding of Mitel's proprietary signaling mechanisms and also break the TLS encrypted authentication and signaling (protection of these signaling mechanisms is discussed in the preceding sections of this document).

The utilization of account codes provides 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 MiVoice Business 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 using TLS to protect both login password information and content from being monitored. The MiVoice Business 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 Mitel Performance Analytics application to provide secure remote administration.

Secure Applications

Mitel addresses the need for security across its broad portfolio of applications. For instance, the Mitel MiCollab Client application provides a softphone (available for PC, MAC, IOS and Android) with encrypted call path and call signaling using the same encryption methodologies as the desk sets (SRTP for media and TLS signaling) as well as secure, encrypted, instant messaging that can be restricted to inside a customer's network. Mitel's wireless offerings also include secure IP-DECT solutions and encryption for 802.11 wireless telephony (desk of handheld), including support for Wi Fi Protected Access (WPA) 2 and 3.

Mitel has directed its concern for secure communications to its growing portfolio of SIP desktops. Mitel SIP desktops support Secure RTP. They also provide support for firewall traversal and support for TLS encrypted SIP (SIP-TLS). 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 under the guidance of the Chief Information Security Officer (CISO) team. 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.

Conclusion

The advantages of converged 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
- Toll fraud protection

Mitel provides a secure "best in class" IP Telephony and Unified Communications 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 with standard security techniques and practices available, ensures a secure and realistically deployable solution.