

## Mitel 3300 IP Communications Platform Security Frequently Asked Questions (FAQ)

The purpose of this document is to answer frequently asked questions regarding security in a Mitel® 3300 IP Communications Platform (ICP) environment. Security of IP Telephony communications is very important for you and your business. Mitel recognizes your requirements with measures to protect business communications from security threats today, and ongoing diligence to ensure the security of future communications. Security threats to 3300 ICP implementations are similar to that of any other IP application service. As with other IP applications, Mitel's voice-over-IP (VOIP) applications can also take advantage of the existing security options available within an IP networking infrastructure.

### **General Security:**

#### **Q. What are the key security issues for a 3300 ICP deployment?**

**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 configuration change.

**Availability:** The need to ensure the operation of the communication system is not adversely affected by a directed denial of service attack, an inadvertent network storm or a malicious computer worm or virus

#### **Q. How does a 3300 ICP solution defend against hacking attacks?**

Hacking is a general term to describe attacks on a system. Specifically, these attacks can take many forms such as eavesdropping, toll fraud, and denial of service attacks. Mitel's goal is to develop solutions that inherently defend against attacks and to also share best practices that help users avoid malicious attacks.

### **Encryption:**

#### **Q. Do Mitel solutions support encrypted call control?**

Yes. Encrypted call control is currently enabled by default on the 3300 ICP and available across Mitel's entire portfolio of IP phones. All call control signalling is encrypted using 128-bit AES encryption.

#### **Q. Do Mitel solutions support encrypted voice?**

Yes, all voice streams are encrypted by default using the industry standard of Secure RTP (SRTP) with 128-bit AES encryption.

#### **Q. Is encryption supported by softphones?**

Yes, the Mitel Your Assistant™ Softphone supports encryption today on the local area network (LAN) with both encrypted call control and encrypted voice using the same 128-bit AES encryption as our regular desktop sets.

## **Confidentiality**

### **Q. How does a Mitel voice solution ensure the confidentiality of call control and signaling?**

In a 3300 ICP implementation, call-signaling traffic is sent across the network using Mitel's proprietary MiNet protocol secured by 128-bit AES encryption.

### **Q. A malicious user could attempt to use IT network tools to intercept data packets. How does a Mitel voice solution prevent these types of eavesdropping?**

Voice traffic is sent across the network using standard Secure Real-time Transport Protocol (SRTP) using 128-bit AES encryption. IP sets will only send and receive voice traffic when instructed to do so by the 3300 ICP through commands sent in the encrypted MiNet call control stream. A set that is instructed to establish a voice connection also receives (over the encrypted call control connection) a unique session encryption key that is used for the encryption of that one call. A random SRTP stream sent to an IP set will be ignored.

## **Integrity**

### **Q. How can an unauthorized set be prevented from connecting to the system?**

After registration, the 3300 ICP has knowledge of the relationship between MAC Address, IP address, extension numbers and PIN Registration Number. This relationship of MAC/IP/Ext/PIN must be valid in order for the 3300 ICP to allow communications to proceed.

### **Q. How does Mitel prevent modification, alterations or corruption of the voice stream?**

Through the use of the encrypted Secure RTP mentioned previously, Mitel is able to ensure that the voice stream is not modified or altered during transmission across the network.

### **Q. How do you prevent modification, alterations or corruption of the call signaling?**

Call-signaling traffic is sent across the network using an encrypted version of Mitel's proprietary MiNet protocol. Secure MiNet traffic is only accepted from devices that have first been authenticated with the 3300 ICP. Each device (i.e. IP phone) sends a unique identifier in the encrypted MiNet call control stream. The 3300 ICP processes the MiNet requests if the unique identifier has been approved and associated with a valid extension in the system. Authorization of the unique identifier is typically done by the system administrator using the 3300 ICP web manager (ESM). The IP phone sends its MAC address as a unique identifier. Note that this identifier is sent in the encrypted MiNet call control stream and not as a Layer 2 transmission, which could be easily spoofed.

### **Q. How can unauthorized free calls be avoided?**

Mitel implements Class of Service, Class of Restriction and Interconnect Restrict controls that can be used to define the available features, dialing restrictions and interconnectivity of devices and trunks in predefined situations.

### **Q. On start-up, Mitel IP phone sets download their software via TFTP. What prevents an attacker from substituting their own malicious software load and manipulating the behavior of the phone?**

In a 3300 ICP deployment all set software loads are encrypted and tamper-proof to ensure that set will only open the correct load. Upon download and decryption, the sets perform an integrity check to ensure that the software load was not modified.

### **Q. What intrusion detection utilities are provided or recommended in a Mitel IP telephony environment?**

Mitel wants its customers to have maximum choice in their technology decisions and therefore is agnostic in

relation to intrusion detection systems. Your Mitel Systems Engineer can provide information with regard to the specific ports and protocols utilized by the platform if desired. This information is also available in the Mitel 3300 ICP Engineering Guidelines.

## **Authentication**

### **Q. How can users or classes of users be restricted from dialing external or long distance numbers?**

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

Mitel's implementation of CoR affords great flexibility. Up to 64 different Classes of Restriction can be specified. An extension user attempting to dial barred numbers will result in them receiving a 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 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 SMDR, relating to billing and/or call management. System Account Codes can be added and automatically dialled by the system when outgoing calls are made on network services that have such a requirement

### **Q. 802.1X is a standard that addresses how to keep a user from gaining access to voice or system management by plugging an unauthorized PC into a corporate network. How does Mitel address 802.1X with respect to softphones and desktops?**

Mitel's 5212, 5224, 5235, 5330, 5340 and Navigator IP desktop phones all include support for 802.1X in their firmware. With 802.1X enabled, the phones use EAP-MD5 to respond to EAP challenges from a network switch. The user programs into the set a user name and password which is sent in the EAP response and can then be passed from the network switch to an authentication service such as a RADIUS server.

Mitel's softphone is called Your Assistant. It appears as just another application on a Windows PC and simply takes advantage of 802.1X software configured in the Windows operating system. For instance, if Your Assistant Softphone was on a Windows XP laptop, that laptop would have to use the included 802.1X supplicant to connect to the network before Your Assistant Softphone could even start to work.

### **Q. How are Mitel phones authenticated when installed or deployed?**

Each set has a unique identifier that is sent in the encrypted call control stream and is mapped in the ICP to an extension which has a Class of Service and Class of Restriction that determines the features the set is allowed to use and the dialing level permitted.

### **Q. Do Mitel phones need to authenticate to place each call?**

The phones do not need to authenticate to the 3300 ICP for each call as the MiNet call control connection is always up between the ICP and sets (different from, for instance, a SIP environment). However, Mitel has the additional support for account codes that would require a phone user to enter a valid code before any call is made.

For each call that is made the phone's capabilities e.g.(CoS, CoR and Interconnect Restrict) are consulted. For example if a change in the set's CoR was made the new call barring rules would be applied on the next

call made.

**Q. Can a H.323 or SIP client (such as NetMeeting or Windows Messenger) place an unauthorized external call?**

Mitel's solution is not based on H.323. Neither NetMeeting or other similar H.323-based clients may place external calls. As of 3300 ICP Release 7.0 UR2, SIP trunks are supported and are subject to the same restrictions as standard trunks. Support for SIP endpoints is planned for an upcoming release and, again, all SIP endpoints will be subject to the same restrictions as standard sets.

**Availability**

**Q. How is a 3300 ICP solution protected against virus attacks and/or worms?**

The 3300 ICP uses an embedded operating system, VxWorks, that provides a very small base "common" functionality and is therefore not affected by the viruses and worms typically found on networks and the Internet. So called "general purpose" operating systems such as Microsoft Windows, Linux and UNIX all include as part of their base functionality such services as a web server, file/print services, etc. Because these are common to all installations of the operating system, they are an easy target for authors of viruses, worms, trojans, etc. In comparison, VxWorks provides only a very small common base and relies on each vendor to add whatever functionality they need. What this means is that Mitel's implementation of VxWorks will be very different from another vendor's implementation of VxWorks. In practice, this makes it extremely difficult for an attacker to write a virus targeted at generic VxWorks implementations. While it would be theoretically possible for an attacker to write a virus targeted at Mitel's specific VxWorks implementation, the reality is that it would be extremely difficult for such a virus to propagate, as the means to introduce it into a network would be severely limited.

A similar statement could be made with regard to the embedded operating system used in Mitel desktops (MQX). Here the risk is even lower because the limited memory available in a desktop limits how sophisticated a program can be run inside of the desktop.

**Q. How is the Mitel solution protected against denial of service (DOS) attacks?**

The comments made above in relation to viruses apply to 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, many DoS attacks are against the TCP/IP networking layer itself and so attack any IP-connected device. With each release of the 3300 ICP and Mitel's IP desktops, Mitel continues to harden the systems against DoS attacks. Hardening is a continuous process and high priority at Mitel to ensure our customers are protected against attackers who unfortunately are constantly coming out with new DoS attacks.

**General Network Questions**

**Q. Mitel phones generally include a second Ethernet port that is often used to support a user's PC. How is that port secured?**

The PC port on a Mitel desktop is purely a simple Ethernet switch that provides basic Layer 2 connectivity to whatever device is plugged into the PC port. It simply passes all traffic through to the switch to which the IP set is connected. Any security/authentication must be handled by the network switch and or network authentication services.

**Q. What security is available for wireless phones?**

Mitel currently provides two types of wireless devices: wireless handsets from SpectraLink and the WLAN Stand which allows a Mitel desk phone to connect to a wireless network. All currently provide support for WPA/WPA2 (in Personal mode) encryption as well as legacy support for WEP. For the most recent information on SpectraLink products, please visit [www.spectralink.com](http://www.spectralink.com).

**Q. Is it possible for incoming connections on the TDM side of the 3300 ICP to somehow gain access to data network on the IP side of the system, i.e. is there a potential for someone calling in on a PSTN trunk line to gain access to the corporate data network? Or vice versa?**

No. While the 3300 ICP provides a gateway between TDM and IP, all TDM connections are terminated on the TDM side of the 3300 ICP and all IP connections are terminated on the IP side. A connection over a (TDM) trunk line to an IP phone would be terminated within the 3300 ICP and a new IP connection made from the 3300 ICP to the IP phone. Likewise in a call from an IP phone to a trunk line or other TDM set, the IP connection would be terminated within the 3300 ICP and a new TDM connection made over the appropriate trunk to the appropriate set. Note that in this IP-to-TDM translation process there is no noticeable impact for the users, i.e. all the caller hears is the recipient answering the phone. The actual conversion process occurs transparently within the 3300 ICP.

### **Teleworker / Remote Worker Support**

**Q. How does Mitel address the issue of secure traversal of firewalls?**

The Mitel Teleworker Solution is a server that sits on the edge of a corporate network, either directly on the edge or in a DMZ, and allows Mitel phones to be securely located anywhere across the Internet. The Teleworker solution maintains an encrypted call control link to the remote phone and dynamically opens and closes firewall pinholes when a secure voice connection is made. The Teleworker Solution can work with the 5212, 5224, 5235 and Navigator IP desktop phones and provides the full features and functionality of a phone on the corporate LAN.

**Q. Can remote phones be located behind firewalls/gateways that perform Network Address Translation (NAT)?**

Yes, remote phones can be located on any type of broadband connection and can be behind one or multiple layers of NAT.

**Q. How secure is the Teleworker Solution?**

The Mitel Teleworker Solution uses SSL-encrypted MiNet call control and 128-bit AES-encrypted Secure RTP.

**Q. Can a remote user plug a PC into the second Ethernet port on the back of the teleworker set and connect into the corporate network?**

No. As mentioned previously, the second Ethernet port merely provides any device plugged into it with connectivity to the local Ethernet network. It does not provide any mechanism for a device to connect across the secure connection established between the remote set and the Teleworker server located at the corporate office. Any such data connections would require the use of a separate data VPN system

### **Management**

**Q. How does Mitel prevent an unauthorized access to the web management interface of the 3300 ICP?**

Mitel implements SSL to defend against "sniffing" of user names and passwords. Access to the management interface requires a user name and password. Further safeguarding is afforded by providing multiple levels of access control.

**Q. How do you prevent modification, alterations or corruption of the management commands?**

All web interfaces implement SSL and are password protected to ensure secure access.

**Q. Are multiple levels of administrative access supported?**

Mitel supports three levels of embedded administration tools. One level is for system administration, one is for group administration, and one is for end users to directly control their desktop device. All are web based and secured via SSL.

**Q. Are there limits on the number of simultaneous users of the embedded administration tool?**

Yes. There can be a total of up to fifty simultaneous system users, of which five may be concurrent system admin users and five may be concurrent group admin users. All session will timeout after 20 minutes of inactivity.

**Additional Information, Support, Services**

**Q. Where can I find more information such as guidelines and best practices for implementing effective security in a Mitel IP-telephony environment?**

Mitel provides information on its public web site at [www.mitel.com/security](http://www.mitel.com/security). This site will continue to be updated with relevant information about Mitel's security solutions. In addition, if you have an account, you can access security documentation and engineering guidelines using the Mitel OnLine web site.

**Q. Does the Mitel offer security patches for Mitel IP telephony solutions?**

Yes. Generally distribution of security patches is available using a software download. Customers are notified by critical e-mail to technical contacts. Additionally, security advisories are issued publicly on [www.mitel.com/security](http://www.mitel.com/security)

**Q. Where can I obtain access to pre- or post-sales, on-site, professional security assessment/planning services?**

Mitel's resellers and professional services organization offer network assessment/planning services. Please contact your sales representative for more information.