

Mitel 3300 Integrated Communications Platform Security Frequently Asked Questions (FAQ)

The purpose of this document is to answer frequently asked questions regarding security in a Mitel® 3300 Integrated 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 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 available as an add-on option for the 3300 ICP and provides support for Mitel's popular 5220 and 5215 IP Phones. With Mitel's next major software release for 3300 ICP (Release 6.0) encryption will be integrated directly into the 3300 ICP and an even broader range of desktops will be supported.

Q. Can you provide some detail on Mitel's encryption process?

Encrypted IP-voice streams are currently supported by Mitel Teleworker Solution. Fully integrated support for encryption will be provided the next major software release for the 3300 ICP (Release 6.0). Mitel uses Secure RTP for encryption. The precise encryption algorithm used today is CAST5-128. The 6.0 release will utilize AES.

Q. Is encryption supported by softphones?

Yes, Mitel Your Assistant Softphone supports encryption today through the use of VPNs. The softphone will support encryption natively in mid-2005.

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. Encrypted call control is currently available as an add-on option for the 3300 ICP. With Mitel's next major software release for 3300 ICP (Release 6.0) encryption will be integrated directly into the 3300 ICP.

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 Real-time Transport Protocol (RTP). IP sets will only send and receive voice traffic when instructed to do so by the 3300 ICP through commands sent in the MiNet call control stream. A random RTP stream sent to an IP set will be ignored. Encrypted IP-voice streams are currently supported by our Teleworker Solution. Fully integrated support for encryption will be provided the next major software release for the 3300 ICP (Release 6.0).

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. 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? For example a malicious user could attempt to use inactive handsets as listening devices.

Call-signaling traffic is sent across the network using Mitel's proprietary MiNet protocol. 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 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 MiNet call control stream and not as a Layer 2 transmission which could be easily spoofed.

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

Mitel offers several defenses to protect call signaling. First SSL is used to protect the integrity of the call stream. Second sets can only connect if authorized by the administrator. Finally Encryption can be utilized as previously discussed.

Q. How can unauthorized free calls be avoided?

Mitel implements Class of Service controls that can be used to define what users/devices can use set system resources 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 digitally signed to ensure that set will only open the correct load.

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 utilised by the platform if desired.

Authentication

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

Mitel implements Class of Restriction (CoR) is 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 Classes of Restriction 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 use of account codes provide additional control options. Verified Account Codes allow the users to utilise 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. 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 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. In this instance, the 802.1x functionality is completely separate from our application. Mitel desktop 802.1x support is planned for the next major release of the 3300 ICP software (Release 6.0).

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. How are Mitel phones authenticated when installed or deployed?

Each set has a unique identifier that is sent in the call control stream and is mapped in the ICP to an extension which has some Class of Service that determines what the set is allowed to do.

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

The phones do not need to authenticate 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 does have support for account codes that would require a phone user to enter a valid code before any call is 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 or SIP and so neither NetMeeting or Windows Messenger may place external calls.

Availability

Q. How is a 300 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 attackers are constantly coming out with new DoS attacks.

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. Up to fifty simultaneous system log-ins, five concurrent system admin users, five concurrent group admin users and ten concurrent desktop tool users are permitted.

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. This site will continue to be updated with relevant information about Mitel's security solutions. In addition, if you have 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

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.