Security

Abstract

Contents

1 Introduction

Integration of voice services into an IS/IT data infrastructure raises several questions and concerns as how to guarantee the same level of security, availability, and quality of service as the classic circuit-switched telephony infrastructure.

This document provides an overview of the security mechanisms available to protect the MX-ONE™ solution from threats that are typical of the IS/IT infrastructure. The described measures are either enabled in the system by default, enabled during the installation/configuration phase of the systems, or need to be enabled manually by the system administrator.

The security measures available for the MX-ONE system are mainly based on the following open standard technologies:

SSL (or TLS)	The Secure Socket Layer (SSL) or Transport Layer Security (TLS) provides secure access to IP phones and web services and secure signaling between IP phones and MX-ONE Telephony Servers.
SSH	Secure Shell (SSH) provides secure console-based access to IP phones and the MX-ONE Telephony server
IPSec	IP Security (IPSec) is used to protect the signaling messages exchanged between LIMs (Telephony Servers).
SRTP	Secure Real-time Transport Protocol (SRTP) is used to protect the media streams of the voice communication

Additionally, other mechanisms to protect the MX-ONE solution are based on the following:

- Correct configuration of the corporate Local Area Network (LAN) infrastructure
- Authentication and authorization of all users of the system, including end-users and administrators
- Security mechanisms provided by the target operating systems (SuSe® Linux and Microsoft Windows®) as well as hardening measures

Beside the security functions described in this document, there are a number of general security aspects that need to be covered and taken care of by a system administrator. Every organization must have a clearly defined IT security policy in place, defining goals, assets, trust levels, processes, incident handling procedure, etc. The security mechanisms available in the MX-ONE system must be covered by and deployed according to this policy. An important security measure to be implemented is to preserve physical security. Only authorized personnel shall have access to server locations, since many data-exposure attacks can be mounted by having physical access to a host. Further, the IT data infrastructure must have a solid design, security mechanisms and protocols must be enabled and all components of the whole system must be correctly configured and maintained.

2 MX-ONE Architecture

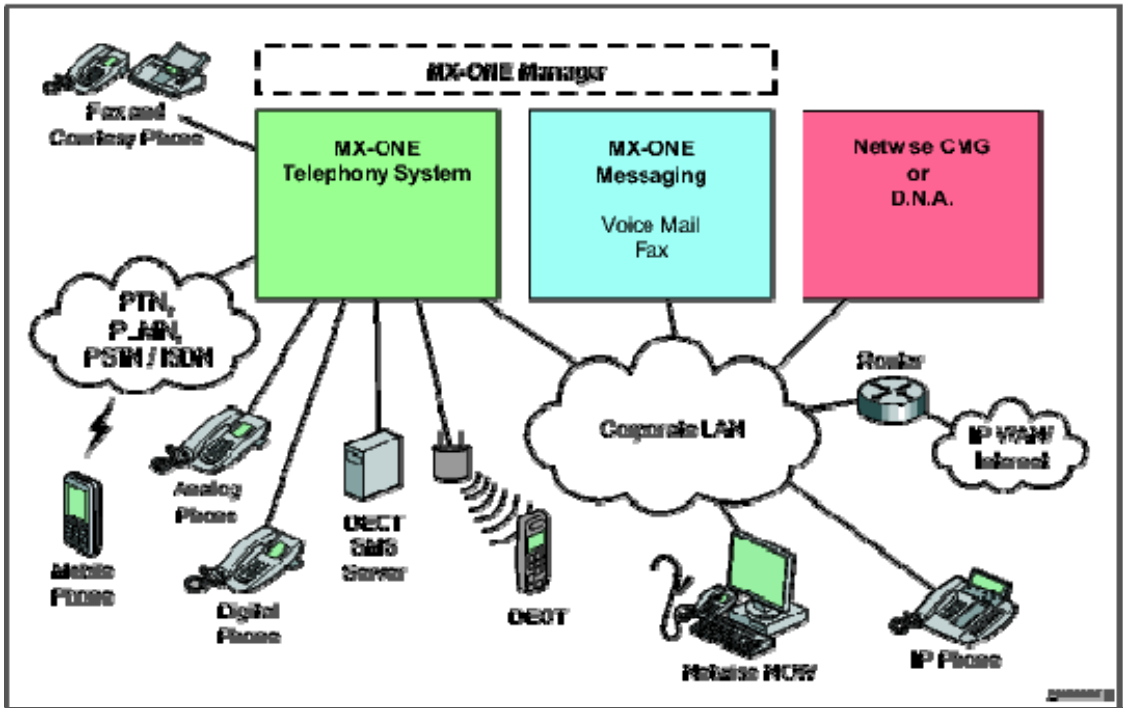

Figure 1 MX-ONE Architecture

The MX-ONE system comprises a number of components that communicate within an existing IT infrastructure, see Figure 1. The following sections illustrate the mechanisms that are available to protect MX-ONE from the architectural point of view.

2.1 LAN Configuration

The MX-ONE components communicate using the corporate LAN infrastructure, usually based on IEEE 802.3 (Ethernet). This is typically an open environment, and communication can be easily intercepted, eavesdropped, and hijacked if a number of configuration measures are not taken when setting up the network.

It is recommended that the LAN connecting the system nodes is fully switched, to avoid eavesdropping attacks that are extremely easy to perform in an Ethernet infrastructure only equipped with hubs. An eavesdropping attack is more difficult to carry out on a switched infrastructure, as Address Resolution Protocol (ARP) messages need to be intercepted and answered. However, ARP attacks have become quite frequent and software tools able to carry them out are widely available.

To make eavesdropping attacks more difficult to carry out, traffic on the LAN should be grouped together depending on the node functions and on their trust level. This can be achieved by the means of Virtual LANs (IEEE 802.1Q and port-based VLANs) that allow separating the communication for example for server-to-server signaling, server-to-client signaling, voice traffic, and so on, providing additional isolation and

making the system more robust against virus-based and network flooding attacks. In particular, if Voice over Internet Protocol (VoIP) traffic is grouped into a single VLAN, and the nodes on such VLAN are strongly protected, a worm-based attack causing network overload originated on a node located on another VLAN might only marginally affect the VoIP LAN. As a completion, the use of VLAN should be integrated with the use of different traffic priorities. Additionally, if the voice traffic must cross IP core networks, it is recommended to make use of Layer 3 techniques (such as DiffServ) to also provide traffic isolation when crossing Layer 3 devices.

The communication between the Telephony Server and the Media Gateway (valid for both Media Gateway LIMs and Media Gateway Classic LIMs) must occur on the corporate LAN, if full support of the available redundancy functions is needed. If support of the redundancy functions is not needed, it is possible to use a dedicated LAN segment to connect the Telephony Server to the Media Gateway. A possible setup is the following:

1. One VLAN grouping the VoIP Servers (Telephony Server, Media Gateways)
2. One or several VLANs grouping the IP phones
3. One or several VLANs for data traffic

If traffic priorities are implemented in the network, the VLAN grouping the VoIP servers shall have the highest priority and the VLAN used for data services shall have the lowest priority. Usually, each VLAN is associated to an IP subnet. Hosts or devices belonging to different VLANs can communicate only through a Layer 3 router. This means that broadcast traffic is blocked across VLANs. Additionally, some routers are enhanced with Intrusion Detection/Prevention Systems (IDS/IPS), able to block more advanced types of attacks.

All MX-ONE components (Telephony Servers, Media Gateway, IPLU boards, IP telephones) support the use and configuration of VLANs and DiffServ.

2.2 Voice over IP Traffic

Attention to the security aspects of an IP telephony infrastructure is increasingly growing by corporate Chief Information Officers (CIOs), IT administrators, and end-users. Voice over IP traffic (both signaling and media) must be protected from a number of attacks, such as media streams eavesdropping, toll-fraud attacks, signaling modification, and so on. For this reason, it is necessary to protect both the VoIP signaling messages as well as the media streams.

The following security measures are supported in the MX-ONE Telephony System:

- Secure Real-time Transport Protocol (SRTP) to protect media streams
- TLS to protect signaling messages
- Support for a number of flexible security policies, in order to support environment with different security requirements

TLS guarantees the signaling privacy when the SRTP keys are interchanged between the parties.

The main principle for the security policy is that it directs if an extension is allowed to register to the system or not. Once the extension is registered, the calls to any other party is allowed from a security perspective.

2.2.1 Media Encryption

2.2.1.1 General

Support for SRTP is given in the IP phones (DBC 42x 02 and DBC 44x 01) and in the Media Gateway Classic (IPLU/1 boards). SRTP support is not implemented in the Media Gateway version 1 (BFJ 901 03), in the Operator Assistant media device, or in Softphones like the ECC.

2.2.1.2 Function

SRTP makes use of the Advanced Encryption Standard (AES) with a 128 bits key to protect the media streams. The encryption keys are exchanged according to the ITU-T H.235.8 specification or to RFC 4568 for SIP. For a two-party phone call, four keys will be needed to be exchanged between the two parties. Each party originating a media stream will generate two keys, a Master Key and a Master Salt and send them to the other party during the call control phase. These values are generated using high-entropy pseudo-random number generators in the IP telephones and in the Telephony Servers. The actual keys used by SRTP (one encryption key for each direction, one integrity key for each direction) are being calculated using the procedures defined by the SRTP specification. The signaling messages carrying the encryption keys are encrypted by TLS before being sent.

2.2.1.3 H.323 Trunks

Media encryption using the SRTP protocol is supported for calls over H.323 trunks. Unlike SRTP for extensions, here the H.323 signaling messages that carry the encryption keys are not encrypted by TLS before being sent.

2.2.1.4 Gateway Calls

SRTP is available only in the Media Gateway Classic (IPLU/1 boards). SRTP support is not implemented in the Media Gateway. This effects the GW calls made on a H.323 Trunk. Only GW calls via the IPLU board are media encrypted. In scenarios where some calls may be through the IPLU and others through the Media Gateway, media encryption is automatically disabled, for example, for Conference Calls.

Whenever there is a change in the Non-GW and GW conditions of the calls, the media encryption of the new call depends upon whether the new call is over IPLU or Media Gateway. Whenever pause and rerouting is executed the media encryption capabilities are re-negotiated.

2.2.1.5 Non-Gateway Calls

For non-GW calls media encryption depends on the H.323 endpoints. The H.323 trunk is transparent in non-GW scenarios. An H.323 trunk does not decide on the media encryption of the non-GW calls. However due to pause and rerouting if the call

condition changes to gateway then again the trunk decides about the media encryption.

2.2.1.6 Trunk Calls towards ASB501

ASB501 does not support media encryption. So if a trunk call is made between an MX-ONE and an ASB501, media encryption is disabled in the MX-ONE during the H245 negotiation. Hence calls towards an ASB501 are plain RTP calls.

2.2.2 Signaling Encryption

To enable support for TLS in Ericsson IP phones, see the Installation Instructions for DBC 425, DBC 422, and DBC 420.

2.2.2.1 TLS Signalling

The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications.

By use of asymmetric key encryption, parameters for the data transfer are negotiated in a safe way. Each transferred data packet is encrypted. By adding a modified message digest with each message (each data packet) the receiving application can verify the data integrity.

TLS consists of two protocols (layers), the handshake layer and the record layer.

The Handshake layer allows the server and client to authenticate each other and to negotiate for an encryption algorithm and keys before the application transmits or receives its first byte of data. The Handshake layer performs this operation using the certificates and asymmetric keys.

The Record layer provides connection security. Each record is encrypted using the symmetric key established in the handshake. The symmetric key is a secret key shared by the two parties.

2.2.2.2 Terminal Signaling Encryption and Decryption

Logon procedure

When the user presses the logon button the phone prompts the user to enter a password.

- In case the user does not enter the password the RRQ (for H.323) or Register (for SIP) is sent insecurely. If this registration is accepted or not depends on the Security Policy set in the Telephony Server.
- If the user enters the password the client (the IP extension) starts the TLS negotiation. After the session keys are established the client sends the encrypted RRQ or Register. The server decrypts it and checks whether the correct password is received.

2.2.3 TLS and SRTP Interaction

TLS ensures signaling encryption and SRTP ensures media encryption.

The TLS procedures are exchanged with the Telephony Server only. Hence once an extension is registered via TLS the signaling, will be encrypted until the extension is logged off. If both TLS and SRTP is used end-to-end, a security icon is shown on the telephone display.

Media encryption by SRTP depends on the Media Gateway and the IPLU of the Media Gateway Classic. The Media Gateway has no support for SRTP. For each call SRTP support is negotiated with the Telephony Server. Hence in case of extensions registered towards the Media Gateway media encryption is not possible, but still the signalling will be encrypted. Although an extension with both TLS and SRTP capabilities is logged on, the media may not be encrypted.

2.2.4 SIP

The MX-ONE system includes support for HTTP digest authentication for the SIP interface. Each time a SIP phone registers itself to the SIP Registrar, it will also be required to authenticate itself.

2.2.5 Certificate Management

The certificates are used to authenticate the communicating parties in the handshake procedure.

Each server has a private key and a public key. A message that is encrypted with the private key can only be decrypted with the public key. If a message is encrypted with the public key it can only be decrypted by the owner of the private key.

The keys can be generated by different algorithms. For example, for large keys generated with the RSA algorithm, no practical method has yet been found to retrieve the encrypted data without access to the private (secret) key.

In order for the telephone to be able to authenticate the server, the telephone has a certificate repository with a number of root and trusted certificates. These certificates cannot be changed or increased in number.

The X.509 certificate has to be stored in each Telephony Server. The respective signed certificate with the generated public key is sent by each party in the TLS communication.

For further information, see the installation instructions for INSTALLING AND CONFIGURING MX-ONE TELEPHONY SYSTEM.

2.2.6 Security Policies

Security policies have been defined to give flexibility in administration and to provide sufficient system security. The administrator must be judicious in choosing the

security policy for the system. A security license is needed for assigning security policies.

For the MX-ONE system three security policies, 1, 2, or 3, can be set for the system. When no policy is set the system is open for all types of terminals that are defined for the system.

1. In the ALL SECURE system policy only Secure Extensions are allowed to register in the system. Both TLS and SRTP must be supported by the extensions.
2. In the ALL SECURE + EXC EXT policy the All Secure policy is modified by giving a security exception to specified extension numbers. Users at these numbers are allowed to logon insecurely.
3. In the ALL SECURE + EXC TYPE policy the All Secure policy is modified by giving a security exception for the telephone type. This can be used, for example, to enable softphones to use the system.

For further information on security policies, see the operational directions for VOIP SECURITY and the command sec_policy.

2.3 Traffic among Servers

In a modern IS/IT infrastructure, servers are generally grouped together and located in server farms. These locations need to be physically protected and only authorized personnel should be allowed to access them. This means that traffic among servers is likely to never leave the physical locations where servers are stored. Layer-2 and Layer-3 network devices are also located in the same locations and contribute to guarantee the physical separation of server traffic from other kind of network traffic. As a further measure to protect server-to-server traffic, it is recommended to set up a specific VLAN just for grouping servers, Section 2.1 LAN Configuration.

If servers are located at remote locations, it is highly recommended to set up a Virtual Private Network (VPN) system, and firewalls to protect and monitor the communication among them.

2.3.1 IPSec

The LIMs composing the MX-ONE Telephony System communicate using a proprietary inter-LIM signaling protocol, used for management messages, control signals, and call control signals. This communication can be protected by the means of IPSec, which is a suite of protocols for securing IP communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.

The IPSec procedure can be divided into the following three steps:

1. IKE Phase 1
   Internet Key Exchange (IKE) authenticates IPSec peers, performs Deffie Helfman, and negotiates Security Association (SA) policy to set up a secure channel. It can be performed in one of the following modes:

- Aggressive mode

  IKE SA values, the Diffie-Hellman public keys, and nonces are exchanged in three messages. Aggressive mode is used by default in MX-ONE installations. It is less resource demanding than main mode.

- Main mode

  IKE SA values, the Diffie-Hellman public keys and nonces are exchanged in six messages, and the identities of both peers are encrypted during negotiations. If the number of hosts exceeds a threshold, the IKE negotiations may start to time out and this limits the number of LIMs in the system. Therefore it is not recommended to use main mode.

2. **Note:**
3. It is strongly recommended to use aggressive mode and not main mode.
4.
5. IKE Phase 2
   IKE negotiates and sets up IPSec SA parameters between the peers.
6. IPSec
   IPSec protected data starts to flow between the peers.

The following two types of IPSec deployments are possible in a network:

- Host-to-host

  Offers end-to-end encryption and/or authentication between the hosts in a network. Each host will set up SAs (both inbound and outbound) to all other hosts, which makes this type of deployment very resource demanding if the number of hosts in the system increases, see Figure 2. It can be used in systems with up to 18 LIMs.

- Net-to-net

  Offers gateway-to-gateway encryption and/or authentication in a geographically scattered network, see Figure 3. Dedicated hardware handles securing of tunnels between the networks. The net-to-net solution lowers the CPU overhead from individual LIMs. It is the recommended solution for MX-ONE systems with more than 18 LIMs.

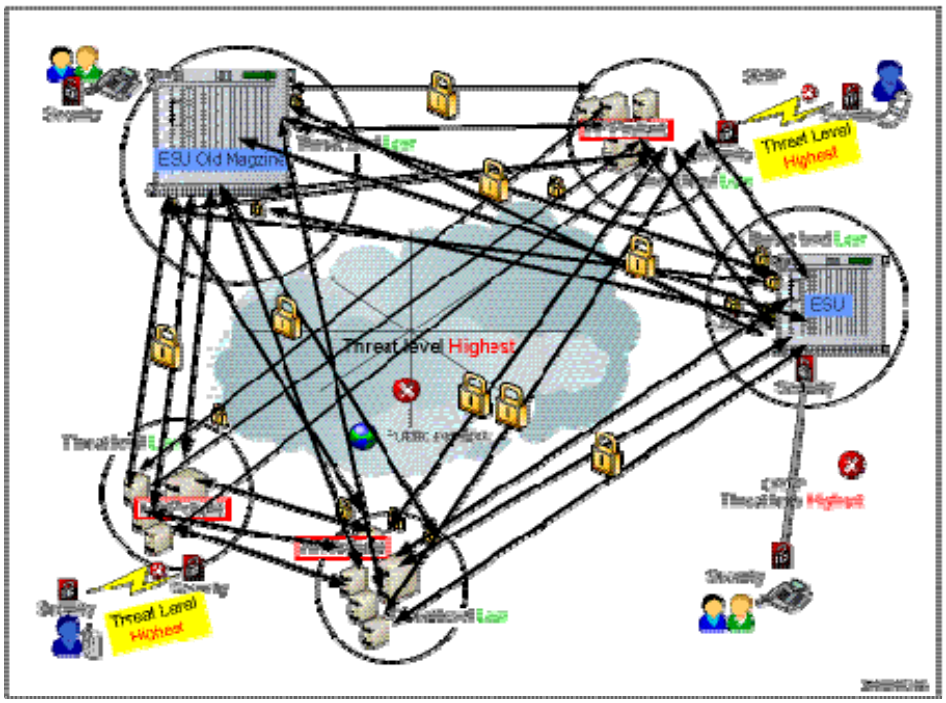

Figure 2 IPSec host-to-host tunnels

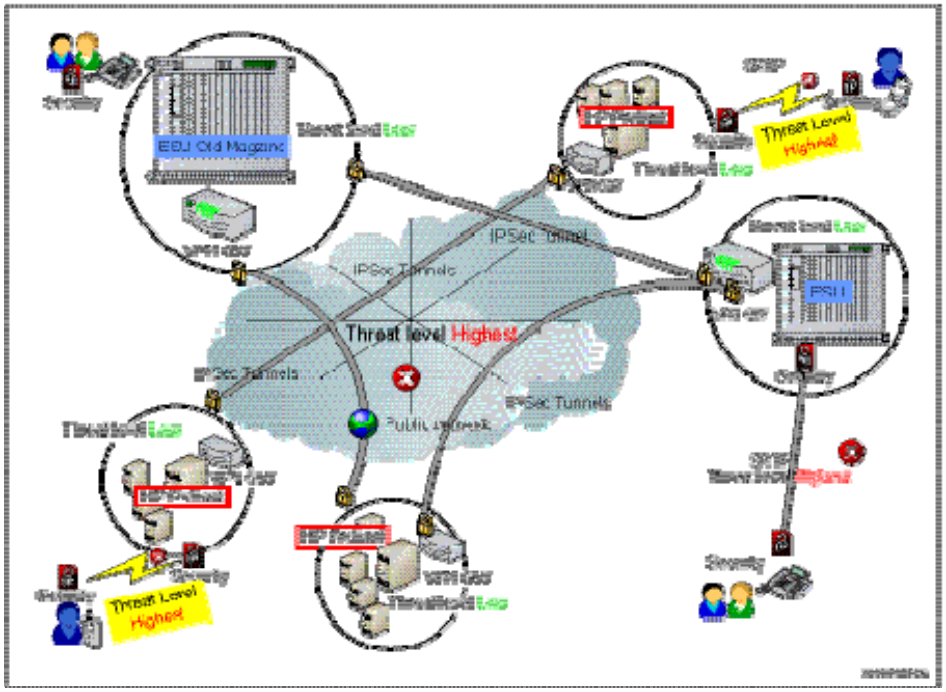

Figure 3 IPSec net-to-net solution for larger MX-ONE systems

Note:

During the installation the system administrator will be asked if IPSec should be set up on the Telephony servers. If host-to-host deployment is used IPSec should be set up on the Telephony servers. If net-to-net deployment is used it

should not be configured on the Telephony servers, rather it should be left for VPN gateways to establish the IPSec tunnels.

2.4 Client Server Communication

Generally, no assumption can be made as to the location of the clients within the Intranet. This is a major difference compared to the server-to-server communication. For this reason, it is important to protect the communication from the MX-ONE clients to the MX-ONE servers.

If the clients are used from the public Internet, the use of an IPSec-based VPN system is the best solution as it is not a recommended practice to open the corporate firewall for all ports used by the Personal Assistant clients.

2.5 Connection to PSTN and PLMN

The MX-ONE Telephony System can communicate with the Public Switched Telephony Network (PSTN) or the Public Land Mobile Network (PLMN) using the trunk interfaces. Such trunks are always located in the Media Gateway or in the Media Gateway Classic.

To enhance the security of the system, ISDN signaling is always terminated in the Media Gateway (or Media Gateway Classic). Communication with the Telephony Server is done by internal signaling protocols. Additionally, ISDN D-channel services are not implemented. This means that for example X.25 over an ISDN D-channel is not allowed and it is thus not possible to access the LAN from an external line.

Communication with MX-ONE Messaging is currently only supported via IP networking. Communication through digital trunks is not supported.

2.6 Mobile Extension

When using the Mobile Extension feature, security of the system is provided by mechanisms available in the mobile operator's network. It is recommended that the user make use of a PIN code to protect access to the phone and to prevent possible misuses of the system if the phone is lost.

2.7 Analog Connections

The MX-ONE system supports the use of analog extensions. Only telephony services are supported through such interfaces. Data connections through Point-to-Point Protocol (PPP) using a modem are not possible to get access to the corporate LAN infrastructure.

3 Platform Security

The MX-ONE servers run on commercially available operating systems. From a security point of view, this is both an advantage and a disadvantage. The advantage is that these operating systems are being used by millions of users and security vulnerabilities are quickly discovered, announced and fixed. However the disadvantage is that these operating systems are the preferred target of the malicious crackers community.

3.1 MX-ONE Telephony System

3.1.1 MX-ONE Telephony Server

The MX-ONE Telephony Server runs on the Suse Linux Enterprise Server (SLES) operating system, which is the enterprise version of the well-known Linux distribution. One of the main advantages of this operating system is the enhanced security features that it is equipped with. It is worth mentioning that SLES is being evaluated for compliancy with the Common Criteria Evaluation Assurance Level (EAL) 4+.

The Telephony Server is the most relevant node in the system whose security must be guaranteed to keep the system available. For this reason, beside the already strict security features of the operating system, a number of additional measures are enabled by default on the Telephony Server to improve its security, its reliability, and its resiliency to a number of malicious attacks.

Only needed packages of the operating system are installed on the Telephony Server. The SLES operating system is extremely feature-rich but the more features that are installed and enabled, the more are the potential security breaches. To decrease the risk of security vulnerabilities, the Telephony Server is delivered with only the necessary operating system packages installed by default.

Another important security measure is to only enable services and network ports that are necessary for the system's correct functioning. As an example, well known insecure services, such as Telnet and FTP are disabled by default. Additionally, the Linux packet filter IPTables has been configured to block access to certain services that are needed for the system but should not be reachable from the network interfaces connected to the corporate LAN. IPTables is also able to block certain kinds of attacks that have a well-known pattern and make use of certain deficiencies of the TCP/IP protocol stack.

To manage the server using the Command Line Interface, SSH is the preferred solution. SSH is enabled by default on the Telephony Server. To increase security, direct root access is disabled by default. If a system administrator needs to carry out tasks that need root access, the administrator first needs to log on as a non-root administrator and

then require the system to be granted root privilege by performing a second authentication procedure.

To guarantee the integrity of the system and detect possible unauthorized or unwanted changes to the file system, the AIDE (Advanced Intrusion Detection Environment) tool has been configured on the Telephony Server. All relevant system files are being monitored and changes are notified as soon as they are detected. The system administrator can of course change the default settings to further increase the security level by increasing the frequency when the tool performs the integrity check of the file system.

The SLES operating system is equipped with a security tool named Seccheck. This tool is installed and enabled by default on the Telephony Server. Seccheck comprises three scripts that are run respectively each day, each week and each month. If something is detected that might indicate a security breach, a mail is sent to the root user with a description of the problem.

File permissions have to be accurately set, especially for those files that are relevant to the correct functioning of the system. The Linux operating system allows the use of the Least Necessary Privilege approach, the security golden rule that protects sensitive files of the system and avoids misfunctioning due to wrong configuration actions done by inexperienced users having accidentally gained access to the system.

3.1.2 MX-ONE Media Gateway

The Media Gateway runs on a Linux distribution known as Monta Vista Linux Professional 2.1. It is an embedded version of the well-known operating system equipped with real-time features and characterized by a smaller memory footprint than other versions of the Linux operating system, obtained by reducing the number of features, services, and applications. This makes the operating system implicitly more secure than other much more feature-rich distributions.

The Media Gateway Linux operating system includes support for IPTables, the Linux built-in firewall. It is delivered to the customer with the firewall correctly configured. In particular, all undesired traffic on the network interfaces connected to the corporate network is blocked. Examples of allowed traffic are Internet Control Message Protocol (ICMP) reply, signaling messages between the Media Gateway and the Telephony Server, NFS traffic, and so on. RTP and RTCP streams (being sent on random User Datagram Protocol (UDP) ports) are directly forwarded to the Digital Signal Processors (DSPs) by the network processor and are never sent to the Linux kernel (and hence the IP stack) running on the main processor.

3.2 MX-ONE Messaging

The MX-ONE Messaging server run on the Microsoft Windows Server 2003 operating system. This version of the well-known Windows operating system is supplied with much stronger security than its previous versions. For this reason, no further security measures are performed beside the ones already enabled by default on the operating system.

3.3 Patch Management Policy

As the MX-ONE components run on commercially available operating systems, vulnerabilities to these systems are discovered and fixed with high frequency. It is necessary to make sure that the MX-ONE components are always updated and equipped with all critical patches to guarantee the highest level of security. On the other hand, Ericsson must guarantee the availability of the MX-ONE servers. In the unlikely event that a patch released by an operating system vendor should conflict with the MX-ONE software, the installation of such patch without prior testing would jeopardize the availability of the system.

To guarantee the availability of the MX-ONE system and hence the customer's satisfaction, Ericsson recommends its customer not to modify (by for example installing not approved software) the Ericsson products without prior verification and approval from Ericsson.

Ericsson Enterprise has developed best practices as the management and installation of security patches released by the operating system vendors aiming to guarantee the highest level of security and the correct functioning of the system.

3.3.1 MX-ONE Telephony Server

Ericsson constantly monitors updates released by the Operating System supplier. Concerning the Linux OS, patches and updates fixing several types of problems are released daily. Some of them address security vulnerabilities that can be exploited to attack the system; such patches and updates must be installed as soon as possible.

In order to allow customers to keep a high security level without compromising the system's functionality, Ericsson tests all patches and updates released by the OS suppliers that can be installed on the Telephony System. In case one of these packages breaks the Telephony System software preventing its correct functionality, Ericsson will provide a hot fix solving the conflict, if deemed necessary by the nature of the update. A fix will always be provided for all security-related updates that conflict with the system functionality.

Ericsson will make all OS patches and updates including possible conflict-fixing hot fixes available to customers regularly. Ericsson is continuously working to decrease the time from the release date by the OS supplier until the OS patches and updates are available, but it is always guaranteed that the system functionality is not compromised.

3.3.2 MX-ONE Messaging

The MX-ONE Messaging server run on the Microsoft Windows 2003 server. Microsoft has developed an efficient way of managing and classifying updates to their operating systems.

All updates released by Microsoft that are classified as *Critical updates* can be installed on the above-mentioned products without prior explicit approval from Ericsson Enterprise. In the unlikely event of a malfunctioning caused by any of these updates, the customer should contact Ericsson (or its service partner) immediately and a Service Ticket with Priority A will be issued. This guarantees that the problem will be solved with the highest priority.

All updates released by Microsoft that are classified as *Recommended updates* should not be installed by the customer without prior approval from Ericsson. Ericsson guarantees to verify these updates before the release of the next service pack.

Occasionally, Microsoft releases service packs for their operating systems. Service packs have a broad scope and address problems of application compatibility, driver updates, reliability, security, and so on. Since Microsoft service packs include a broad range of changes, Ericsson Enterprise must thoroughly test all Computer Telephony Integration (CTI) products running on each service pack before we can support these service packs in the field. Therefore, before installing any new Microsoft service pack, it is necessary to check that it has been fully tested and qualified by Ericsson. Use of unqualified service packs may prevent Ericsson Enterprise Technical Support from properly supporting customer installation.

3.4 Antivirus Policy

Virus attacks on the IS/IT infrastructure are becoming increasingly frequent. For this reason, a valid antivirus policy is a necessary aspect of any valid security policy. The formulation of such a policy is a task that must be carried out by the IS/IT system administrator. Ericsson Enterprise, as a supplier of equipment that might be subject of a virus attack, guarantees that their products do not contrast with antivirus policies in force in the IT environment.

3.4.1 MX-ONE Telephony Server

The Telephony Server is based on the Linux OS, which has traditionally only marginally been object of virus-related attacks. However, since there is a slight possibility to be hit by a virus targeting the Linux OS, it is possible to install antivirus software on the Telephony Server, if desired.

Ericsson has tested the product Sophos Anti-Virus for Linux 6.1 to make sure that it works correctly with the MX-ONE 3.1 Telephony Server without affecting its functionality. For more information about Sophos products, see http://www.sophos.com. If Sophos Anti-Virus for Linux is used, disable the Sophos Anti-Virus GUI. To use this feature requires local access to the Web GUI and this is not possible on a Telephony server as there is no Linux GUI running on it. Other antivirus products may also work on the Telephony Server but they have not been tested.

When installing an antivirus application containing more than antivirus, all features except antivirus must be disabled. Features such as firewall and integrity protection can safely be disabled in the antivirus application since they are already covered by the hardening installed with the Telephony Server application.

When deploying antivirus software, it is important to guarantee that the virus definition files are always updated.

Note:
Ericsson does not provide any antivirus applications with MX-ONE.

3.4.2 MX-ONE Messaging

As a real-time system performing business-critical and computationally-intensive functions, MX-ONE Messaging cannot be expected to perform to specification if a third party application periodically makes essential Central Processor Unit (CPU), memory, and disk resources unavailable. The preferred solution is naturally to schedule virus scanning on a daily basis and during low server activity. The selected time should not coincide with scheduled daily maintenance or updates to the system. Should a periodic scan not be acceptable, the virus scanning software may have multiple configurations or approaches for continuous or active scans.

All virus scan solutions including periodic, active and continuous background scans of directories or disks may significantly impede operating system resources, and prevent Ericsson products from responding as specified. It is the customer's responsibility to test the virus scanning software in conjunction with Ericsson products during a high load condition to assure correct system operation. When configuring the virus scan software, the preferred choice will be the one that uses the least amount of CPU and generates the least amount of disk activity.

3.5 IP Phones

The IP phones for the MX-ONE system are based on a Real-Time OS (RTOS) with strict control over which applications are running on the phones and with limited privileges. Additionally, only signed firmware can be uploaded on the phones. For these reasons, it is unlikely that such a phone can be infected by a virus or some other form of mal-ware. The IP phones are endowed with an SSH server to perform configuration and troubleshooting activities. The SSH server public and private keys are hard-coded in the phones and cannot be updated.

4 Operation and Maintenance Security

Management of the MX-ONE system is performed according to the FCAPS paradigm. In particular, the following mechanisms are available to manage the system:

- Manager Telephony System: Web-based tool located on the Telephony Server used for system-wide configuration
- Manager Device: a tool for remote software maintenance in MX-ONE based on HP Radia
- Manager Availability: an optional fault and performance tool based on BMC® PATROL
- Windows GUIs located on the MX-ONE Messaging
- CLI-based management of the Telephony System
- SNMPv1

4.1 Manager Telephony System

The Manager Telephony System is a Web-based tool that allows monitoring and configuration of a number of relevant objects.

To protect access to this tool, SSL in server authentication mode can be enabled during the installation procedure. The administrator (client/Web browser) will be authenticated by the means of username/password. It is assumed that the Web server has a valid pair of RSA keys and a digital certificate that can be verified by the client. This certificate can either be a self-signed certificate or issued by a well-known Certification Authority (CA). After successful authentication, the administrator is mapped to one of four possible administrator profiles, each of them holding different access privileges. The following four profiles are defined within Manager Telephony System:

- Secretary/Administrator
- System Administrator
- Engineer

- Advanced Troubleshooter

For each operation requested by the administrator, the access privileges are checked against the requested privileges for that specific operation, thus implementing a fine-grained access control policy. The system administrator can configure the access privileges assigned to each role.

4.2 Manager Device

Manager Device handles remote software upgrades of MX-ONE applications on the Telephony Server and MX-ONE Messaging server. It is based on HP Radia, which is a part of the HP OpenView Management Suite.

The Management Server can be setup to use SSL for communication with Radia Clients and also to provide HTTPS for access to the Management Portal from a web browser. This is configured during installation time and requires SSL/HTTPS port numbers to be configured and certificate/key files provided. This certificate can be a commercial certificate from any certificate vendor, a certificate issued from a local Certification Authority (CA) or self-signed certificate. The administrator (client/Web browser) will be authenticated by the means of username/password. It is possible to use a VPN for communication between the Management Server and the Managed System.

4.3 Manager Availability

The Manager Availability is an optional tool used for advanced fault and performance management. It is based on a number of agent-components installed on each managed server, and on a set of server-side components.

Communication between the agents and the server side components is based on BMC PATROL security level 2, which provides integrity and confidentiality protection based on SSL. The server-side components need to authenticate to the agent by the means of a username and a password, which are verified against the operating systems of the managed servers. Credentials are sent though the SSL connection.

The system administrator using Manager Availability accesses the tool's Web-based interface. Communication between the browser used by the system administrator and the Web server are also protected by HTTPS.

4.4 Windows GUI

The Messaging server is running on the Microsoft Windows Server 2003 operating system. All management operations related to the operating system need to be carried out through Windows-specific GUIs. Additionally, the Messaging server is equipped with a proprietary GUI in order to carry out system configuration activities. Access to these GUIs requires physical access to the host where the tool is being installed. Standard Windows security applies for controlling access to the hosts.

It is possible to gain remote access to the host where the Messaging Server is installed by making use of the PcAnywhere tool, which has been tested for this purpose. In this case, security features provided by the tool apply.

4.5 CLI-based Management of Telephony System

Most of the management operations necessary on the Telephony System are carried out through a proprietary Command Line Interface known as MD-shell. In order to have access to this tool remotely, SSH shall be used to log on to the system. It is obviously necessary to set up authentication keys before being able to use SSH.

4.5.1 Protection Mechanism of the MD-Shell

The MD-shell is a console-based mechanism to manage the MX-ONE Telephony Server. All possible management operations can be performed by the means of this tool, which makes it very powerful but also potentially dangerous. It is built on top of the Linux bash shell, which in turn is built on top of the operating system kernel.

It is necessary to guarantee that only authorized users (administrators) can manage the system; additionally, different groups of administrators might have different privileges. The MX-ONE Telephony Server defines eight different levels of user privileges for managing the system. Each time a command is issued by an administrator, the required privilege level to issue that command is checked against the privilege level assigned to the administrator issuing the command: if it is higher, the command is not performed. The root user is automatically assigned the highest privilege level, that is seven.

The mapping between different commands to access privileges is stored in a configuration file that can only be modified by the root user. Additionally, it contains the

mapping between Linux user groups and access privileges. The following briefly describes which operations are entitled to the different access privilege levels:

- Level 0: Visualizing of non-sensitive system configuration
- Level 1: Some Unix non-sensitive commands, call diversion, some operator-related operations
- Level 2: Operations on analog, IP, and generic extension, operations concerning abbreviated dialing
- Level 3: Simple accounting operations, number analysis, simple routing
- Level 4: Logging-related and dump operations, interception service, blocking operations, configuration, traffic recording
- Level 5: Inter-LIM signaling, Control system, LIM switch
- Level 6: Advanced management operations
- Level 7: Advanced troubleshooting; advanced diagnostic tools; advanced configuration, system-critical operations

4.6 SNMP

When monitoring the system with SNMP, it is only possible to read data that is not considered sensitive. It is not possible to set the value of a MIB II object.

5 Event Logging

All MX-ONE components log relevant events using tools available on the target operating system and MX-ONE specific tools or files.

The MX-ONE Telephony Systems has two main types of logs. The actual telephony application makes use of the common Linux logger known as Syslog. The MX-ONE Manager Telephony System allows the administrator to view relevant logs through its Web interface.

The MX-ONE Messaging is also equipped with a number of tools to monitor and visualize information concerning mailboxes, port usage, call handling statistics, network activity report, subscribers' setup, and so on.

6 Definitions

For definitions, see ACRONYMS, ABBREVIATIONS AND GLOSSARY.