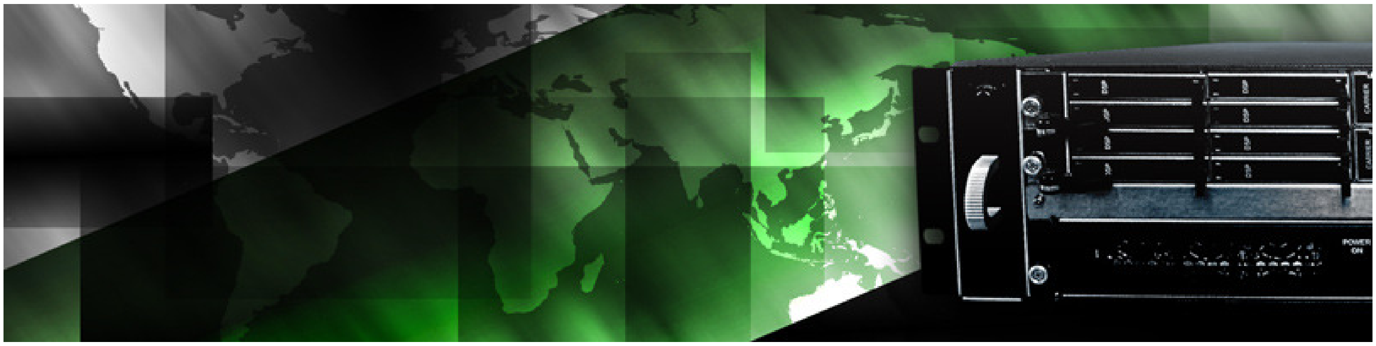
compunetix

ae.net conference



EVERGREEN SECURITY FEATURES

Introduction

This document outlines the various security features of the Evergreen Multipoint Control Unit (MCU) Video Conferencing System.
It will highlight those security features inherent in the **hardware architecture** of the system as well as the **software security** features for achieving access to the system for operational control and maintenance and **security for endpoint access** into a conference.

Security Aspects of System Architecture

The Evergreen system is a **custom hardware-based MCU** dedicated and optimized for video conferencing multipoint applications.
It is **not a general purpose** server running multipoint software.
Because of this **proprietary architecture**, it is significantly **less vulnerable** to security threats that target general purpose servers running common server software operating systems.

The Evergreen has **two types of network access points**, one for control and one for media. System access for control and maintenance is accessed via a control PC running a Windows-based webserver.
The application that interfaces between the Evergreen and the control PC is call the **Compunetix Platform Manager (xPM)**.
The Control Network connection with the Evergreen is on a dedicated, isolated network that only connects the Evergreen with the xPM and is a 100% proprietary interface.
Therefore, a security breach on this network connection is highly unlikely and would have to be targeted specifically at our MCU and have knowledge of our proprietary API used in this communication link.

The xPM application interfaces with a **dedicated Operations Client (xOC)** located on this PC or on a private network connection with the xPM as well as the Windows Web Server for web interface and control.
All web connections are encrypted using HTTPS and require a secure login. Vulnerabilities on the web interface can be kept to a minimum by keeping up to date with security patches from Microsoft. However, keep in mind that even if this interface is breached, there is still the **proprietary link** between the xPM PC and the MCU that actually runs the conferences.

The **media network interfaces** on the Evergreen are 10/100/1000 Mbps Ethernet interfaces. These interfaces communicate over the standard H.323 and SIP protocols and ports used in video communications.
Other protocols and port activity is **locked out**, eliminating many security threats.
The operating systems inside the Evergreen are a **stripped down version of Linux** on the network processors and a proprietary operating system on the Digital Signal Processors (DSPs) that do the audio and video processing.
Internally, the network processors take media off of the Ethernet interfaces and distribute them over an **internal proprietary Serial Rapid I/O (SRIO) network** to the DSPs.
This network isolation of the media packets on the SRIO network from the Ethernet networks provides **another level of isolation and security**.
Security vulnerabilities are tested with each software release and the latest patches from the open source Linux community are applied as needed with each release (since the Linux software on the Evergreen is a stripped down version, not all patches are applicable).
Alterations to the internal operating systems on the Evergreen **can only be managed over the proprietary interface** coming from the xPM.

MCU Access Security

Access to the Evergreen over any of the public facing maintenance or conference control interfaces **require a Username and Password**. Strong password security is available on the Evergreen and controlled by the System Administrator.
The System Administrator can control **minimum password length**, minimum number of **lowercase and uppercase characters**, minimum number of numeric characters and minimum number of special characters for each password.
Passwords can be set to expire after a configurable period and the warning period for expiration also set by the System Administrator.
The System Administrator can also set **reuse rules on how many unique passwords** must be used before one can be used again as well as set lockout rules for failed password attempts. This includes setting the **number of attempts** before the Username is locked out as well as the **period of lockout** (from minutes to indefinitely).

System Administrators **can also disable any user account** at any time as well as set accounts to become disabled if not active after a configurable number of days.

When a user account is created on the Evergreen, **the user account is assigned** to one or more groups as well as having a role defined for it.
The Evergreen **supports multi-tenancy**. That means that multiple groups can use the MCU without any knowledge of the other groups.
Each group can have its **own set of users, contact lists, and stored conferences**.
Therefore, user accounts assigned to specific groups are another level of system security which **restricts the visibility** of that user to affect operations only within their respective group(s) to which they are assigned.
Each user account **is also assigned a role**.
The role defines what permissions that user has access to in the system.
System Administrators have full access.
Group Administrators can just affect the activities of their Group and ***Group Operators*** can control conferences only within their assigned group(s).
The system allows for **custom role creation** and these can further restrict the rights of a user, for example by only allowing them to view, but not control any of the conference parameters.

Conference Level Security

Security at the conference level can be considered from two perspectives: **who has access to join** the conference and **security of the data being transmitted** to and from each participant in the conference.

In order to join a conference on the Evergreen, a connection must be established with a video endpoint either by dialing out to the participant or having the participant dial into the MCU.
The Evergreen can be operated in **attended and/or unattended mode**.
In attended mode, a **trusted operator** can dial out to each participant, verify the party's identity and then transfer that participant to the target conference.
Similarly, a dial-in attended service can be set on the Evergreen such that all incoming calls to one or more specific IP address can be placed in an **attended incoming call queue** where they must be greeted and checked by a trusted operator before placing the party into the conference.
Attended conferencing provides the highest level of conference access since each participant is screened before joining the selected meeting.

Various levels of security can also be enforced for unattended conferencing.
At its most basic level, security can be enforced through the use of passcodes.

The Evergreen supports **three types of passcodes**: guest passcodes, host passcodes, and conference level passcodes.
A ***guest*** passcode will provide access to a conference, but rules can be set that will not allow the conference to continue if a host is not present.
Therefore, a ***host*** passcode should be used by a limited and trusted party or parties to allow all participants to be joined to the conference.
A ***conference level*** passcode is a further prompt to a user in addition to either the guest or host passcode in order for them to join the conference.
A conference operator can turn on or change the conference level passcode at any time during the meeting at which point all participants will be placed on hold and prompted to enter the conference level passcode again in order to rejoin the conference.

There is an additional level of connectivity for security for unattended dial-in callers.
This is called **placing a party in Standby state**.
When in a standby state, the party calling in must match a predetermined calling IP address in order to be allowed into the conference.

Further security can be enforced **through the use of a Gatekeeper**.
The Evergreen has its own internal gatekeeper or a third party gatekeeper can be used.
With the use of a gatekeeper, only registered endpoints with the gatekeeper can be permitted to join a video meeting.

Finally, security can be enforced on the media connection **through the use of encryption**.
The Evergreen supports **three modes of operation** in this area: **no** encryption required, encryption **preferred**, and encryption **required**.
The second and third modes are the more secure means of connecting.
In an encryption required conference, only endpoints capable of encrypting the media will be allowed into the conference. All others are not permitted.
For H.323 calls, the Evergreen supports H.235 which uses **AES encryption**.
This encryption is supported by a hardware encryption engine in the network processors of the Evergreen and supports **both 128 and 256 bit keys**.
An encryption preferred conference will prefer encryption but also allow non-encrypted terminals to be joined. This can be advantageous if one or more parties may have terminals that do not support encryption but are connected on a private, secure network.

The Evergreen can also interface to different **Gateway** devices.
Gateways are another means of bridging between private and public networks or for connecting via ISDN dial-up connections.
Unlike an Ethernet connection, **H.320 ISDN connections** are inherently more secure because any third-party tap in the line would disrupt the end to end signaling for the connection.