On the Web at www.AMEMusic.com

American Music Environments

Security White Paper

Prepared By: Tom Krikorian and Joshua Smith
Prepared On: 9/18/2012

American Music Environments
1133 W. Long Lake Road
Suite 200
Bloomfield Hills, MI 48302
Tel: 888-AME-5005
Fax: 888-AME-6006

Contents

Contents....3
1. Introduction....4
2. General Description....4
2.3. The AME Receiver....4
2.4. The Web Interface....4
2.5. The AME Communication Server....4
3. Server and Hosting Facilities....5
4. The AME Receiver....6
5. Communications....7
6. Web Interface....8

1. Introduction

1.1. This document contains confidential and proprietary information about AME business practices, computer systems, and related technology. The distribution or sharing of any part of this information with any party without the prior written consent of AME is strictly prohibited.

1.2. The information contained in this document is correct and accurate at the time of writing. AME constantly strive to improve and innovate and such endeavors will invariably result in changes to business practices and technology.

2. General Description

2.1. AME is a provider of background audio including music and messaging. Typical AME Clients include retail establishments, restaurants, malls, hotels, casinos, and any business that desires to enhance its public presentation with the addition of carefully selected audio.

2.2. The AME delivery platform comprises three main components. A detailed description of these components is deferred until later in this document. Briefly, the three main components of the AME system are as follows:

2.3. The AME Receiver

2.3.1. An AME Receiver device is installed in each client location where audio is to be played. The Receiver is connected to a standard audio system typically comprising amplifier and speakers. A standard AME Receiver can deliver four independent programs of audio through separate physical outputs.

2.3.2. Audio files and programming instructions are installed on the hard disk drive or solid state memory of the physical Receiver. The programming instructions determine how the installed audio should be played.

2.4. The Web Interface

2.4.1. An authorized user can use the AME Web interface to make changes to the programming instructions on a Receiver or to add or remove audio content. Changes are packaged in the form of an update that is placed on the AME Communication Server for retrieval by the Receiver during the next scheduled communication.

2.5. The AME Communication Server

2.5.1. Each AME Receiver routinely communicates with the AME Communication Server located at the AME headquarters and Colocation. In practice there may be multiple physical computers providing this server interface but for simplification these computers can be discussed as a single entity.

2.5.2. During these communications the Receiver will perform a number of functions including the retrieval of programming changes and new audio tracks as requested via the Web interface.

3. Server and Hosting Facilities

AME utilizes a Windows and Linux network that comprises multiple servers running Windows 2008 R2 Server or Linux Server which is Debian or RPM based.

3.1. All server computers are located in a locked server room onsite at AME headquarters. AME also maintains multiple servers in a collocation for redundancy.

3.2. Access to the server room is restricted to authorized personnel. Currently this would be as follows:

- Chief Technologist
- Network Administrator

3.3. All servers are patched to the latest security updates and hot fix levels.

3.4. Comprehensive corporate anti-virus protection is in place to protect servers and workstations real-time. Currently, AME uses AVG Antivirus Corporate Edition.

3.5. The internal network is protected by a firewall to prevent intrusion. Currently, AME uses a Cisco ASA5505 as well as a Cisco ASA5510.

3.6. All server and workstation computers are located behind the firewall.

3.7. Computer workstations are PC computers running Windows 7.

3.8. Users must log on to the internal network with individually assigned user id’s and passwords.

3.9. Users are restricted to AME staff.

3.10. Network access is only available from computers physically located on premise at AME headquarters.

3.11. Direct access to media files is restricted to authorized users such as audio editors and network administrators. Access is restricted by the use of secured folders.

3.12. All media files are encrypted using an RSA public-key cipher 40 bit streaming when they are added to the media library. Insecure, unencrypted files are permanently discarded at this time. A single private key is used to encrypt all audio files. A copy of the corresponding public key is required to decrypt the audio files. A copy of this public key is installed on each AME Receiver within the secure CSP (Cryptographic Service Provider) such that it cannot be exported. The CSP is the component of the Windows

platform that's responsible for securely storing certificates and keys and handling requests to decrypt files. See Microsoft documentation for further details.

3.14. Insecure, unencrypted media files are only accessible to authorized users such as audio editors.

3.15. Insecure files are only maintained to support file editing and are discarded as soon as the editing process is completed and the encrypted file is transferred into the media library. Audio editors perform tasks such as trimming silence and adjusting volume level for consistency with other audio material in the library.

3.16. Audio file editors work rooms are locked to prevent access to insecure media files by unauthorized personnel.

3.17. All physical source media such as compact discs, video discs, and digital tapes are stored in a locked room. Currently, the room is locked with a conventional lock and key mechanism. Access to this room is restricted to authorized personnel such as Audio Editors and the Music Director.

3.18. Physical access to the AME suite is secured with an alarm system and coded entry pad.

3.19. Company policy strictly prohibits the taking of any media files off-premise.

3.20. General purpose workstations have no devices for transferring files to or from external media. Company policy strictly prohibits connecting external storage and removal media devices to workstations or the network.

4. The AME Receiver

4.1. The AME Receiver device is built using mostly standard PC hardware such as motherboard, hard disk drive, RAM, and microprocessor.

4.2. The AME Receiver currently uses Ubuntu Linux.

4.3. AME employs the use of Intel HD audio. Audio connections are made with standard RCA connections.

4.4. The device provides a local interface which allows control over communication parameters for limited onsite configuration. Settings accessible through the interface are receiver IP settings and communication parameters. Normal operation does not require the use of the local interface.

4.5. The device is not equipped with a keyboard, mouse, or monitor.

4.6. The software Shell provides no functionality to the user including no provision for the user to access data on the hard disk such as audio files.

4.7. All audio material stored on the hard disk drive are 16bit, 44K single channel mono files compressed to 64Kb using MPEG3.

4.8. All audio files stored on the local hard disk drive are encrypted so they are useless should the hard disk drive be removed or stolen. These files are encrypted at AME headquarters at the time they are added to the main audio library. All files installed on the hard disk drive of the AME Receiver or added as part of an update have been encrypted in this manner.

4.9. No facility is provided for the user to add their own music or audio content. Only audio material provided by AME can be installed and played on the AME system. Changes to audio content or programming can only be performed using the Web interface described elsewhere in this document.

4.10. No facility is provided for the user to extract or offload audio from system.

4.11. Playback output is analog.

4.12. A preloaded expiration date insures that receiver will automatically deactivate if services from AME discontinues. Because the date is loaded in advance the Receiver will expire even if it is disconnected from the AME network.

5. Communications

5.1. The AME Receiver communicates with the AME Communication Server on a routine basis in accordance with a preprogrammed schedule. During these communications the Receiver will:

- 5.1.1. Upload diagnostic data and logs that help AME insure the device is operating properly
- 5.1.2. Set the Receiver's expiration date
- 5.1.3. Perform miscellaneous maintenance functions such as clock synchronization
- 5.1.4. Retrieve and apply any software updates that may be needed
- 5.1.5. Retrieve and apply any programming updates (including requested audio files) that have been prepared via the Web Interface

5.2. Diagnostic data typically amounts to about 100 KB daily per Receiver.

5.3. Software updates and programming updates vary in size up to a maximum of 10 MB. This maximum size can be changed for each Receiver.

5.4. Communication between the AME Receiver and AME Communication Server uses standard HTTPS.

5.5. The AME Receiver initiates all communications with the AME Communication Server. There is no mechanism for AME to initiate a communication with any Receiver from the server side. This approach effectively eliminates most firewall issues.

5.6. Each AME Receiver communicates within a pre-programmed and configurable time window consistent with the client-specified schedule for that device.

5.7. TCP/IP configuration of the AME Receiver can be assigned statically or dynamically using DHCP.

5.8. All receiver ports on the AME Receiver are blocked to prevent intrusion.

5.9. No listening services or applications such as Telnet or SSH are running on the AME Receiver to respond to inbound connection requests.

5.10. AME rely on the diagnostic information retrieved during communication to diagnose and resolve problems. In the event a receiver cannot be made to communicate, it is replaced.

5.11. Receivers can communicate with AME using the Internet where a suitable network connection is available.

5.12. An AME Receiver may be configured to access an Internet connection via a proxy server or firewall device.

6. Web Interface

6.1. The system's user interface is a Web application hosted centrally on AME Web servers. The Receiver itself provides no user interface with which to interact with the Receiver device directly.

6.2. The client or AME personnel (the user) can use the Web interface to add or remove audio content from the Receiver.

6.3. The Web interface can be used to change the manner in which the installed audio is organized, mixed, and played on the Receiver.

6.4. Audio tracks can be played in several ways including:

- 6.4.1. Audio tracks can be organized into categories that are then mixed together and scheduled for random playback.
- 6.4.2. Audio tracks can be included in a play list where the order in which the tracks should be played is specified.
- 6.4.3. Audio tracks can be scheduled to play at specified times of the day and on recurring intervals.

6.5. Any changes the user makes via the Web interface are processed by the server and placed in an update package for retrieval by the remote Receiver during its next scheduled communication. There is no means by which to push updates to a Receiver.

6.6. The AME web control interface is a facility available on the amemusic.com web site and it available only to registered users via Id and password. Multiple users can be authorized with rights of "view only" or "update". A user with a view-only status can only look at the programming and details but cannot change anything. A user with update rights can see the programming content and make changes.

6.7. The web interface presents what we call a profile. The profile defines all of the program material such as music, spots, sound effects, etc., as well as the instructions about how and when to play the items. A profile can, in turn, be assigned to one or more AME digital receivers. Once a receiver is assigned to a profile, that receiver will only respond to the programming and rules of that profile. The profile allows the user to schedule certain blends of music categories with resolution down to half-hour segments for each day of the week.

6.8. A music blend can consist of one or more categories of music with instructions to play the music categories in certain percentages. For example, a user could specify the adult contemporary, light jazz and oldies categories with instructions to formulate a mix consisting of 50% adult contemporary, 20% light jazz and 30% oldies. This music blend is then given a name, such as “afternoon mix” and it is assigned a color code in the interface. When this color coded mix is used for a half-hour block, the receiver will play music according to the instructions above. The receiver actually selects music from each category at random and plays the selections in the desired percentages figured over the course of a one-hour period. A music mix can consist of only one category, in which case the percentage of play would be 100%.

6.9. The user can inspect the contents of each stock or custom music category song by song. The user can delete any song from any category. He can also take music from any category and place some or all of the songs in another custom category. This way, the user can divide the music into categories that make sense for their particular program needs and styles. The user can also assign additional rules to a give song or entire category. A permissible range of dates or time spans can be specified for play. For example, a song that has a strong summer theme can be specified to play only during the summer months. Likewise, a song with some reference to time of day can be set to play only during certain hours. When a song is assigned more specific rules, the receiver then takes these rules into consideration when populating the music mix. If a song is in a category that is being used but the song itself is not authorized to play, the receiver ignores the song when it makes the random selection from the category.

6.10. A user can also formulate a fixed order play list. Here, one or more songs are selected and placed in a fixed list. The list is given an ID. After the list

is formulated, the user can instruct the receiver to play the list of music at some given time. Lists can be used once or stored for use again. The fixed playlist is a seldom used feature that is designed more for special event programming. Since the fixed order play list will play and exhaust its' contents, it must be used in conjunction with a background music program that will take over after the fixed play list has played.

6.11. The interface differs from personal devices like iTunes because the AME receiver participates in the formulation of the program based on instructions specified by the user. Real-time control is not possible with the interface. In order for the receiver to respond to new instructions, the user must sign on to the web interface and specify the desired changes. He must then "release" the changes to instruct the interface to incorporate those changes into the clients' program. The AME receiver must then contact the AME server to pick up the new instructions. If the receiver does not communicate with the server, it will continue to operate based on the most current instructions it has received.

6.12. All receivers have an expiration date which is set by the AME server based on the billing and payment status of the client. If the expiration date is reached, the receiver will no longer play any audio. It will, however, continue to communicate with the AME server on its' established interval. A receiver can be set to communicate as often or seldom as indicated by the program needs of the client. If the receiver is unable to communicate with the server due to connectivity failure or even intentional act by the user, the receiver will still expire on the proper date and audio play will stop.

6.13. The system is not intended to function as a "jukebox" or real-time player. The complete program change cycle from entering the changes to the web interface to having the receiver pick up and process the new instructions takes up to an hour. The receiver can be forced to communicate with the server by powering off and on. On startup, the first thing every receiver does is contact the server. The receiver can communicate using an ordinary POTS line or any type of network connection. The telephone communication is by direct POTS connection to the AME RAS (Remote Access Server) server. The RAS server uses Microsoft's standard built-in RAS software. See Microsoft documentation for further details.

6.14. AME retains full control of all music content on the interface and all receivers. If a music selection is not placed in the inventory by AME, then it cannot be played or accessed by a receiver. Likewise, if AME removes or withdraws a song, it stops playing system wide after each Receiver is updated during the next communication. AME can also add new releases to the system as needed.

6.15. Each receiver keeps a complete log of every song or announcement played along with a date and time stamp. The data is uploaded to the AME server each time the receiver communicates. The log facility allows AME to track and measure every program element. We will be able to report exact number of plays of any song with as much detail as required. Since the receiver logs music as it is actually played, the client can make changes as often as desired and we will still have an accurate record of music use.

Visit us at: www.AMEMusic.com

Phone: (888) 263-5005

Fax: (888) 263-6006