Ravon Technical Architecture : Call Recordings with Encryption and Decryption

Ravon Technical Architecture : Call Recordings with Encryption and Decryption

Introduction

The document describes the high level approach to Ravon Hosted Phone System call recordings with encryption, decryption and playback. The document does not address the technical architecture components but the methodology and approach.

1.1 Glossary

- IVR (Interactive Voice Response). A technology that allows a computer to interact with humans through the use of voice and DTMF keypad inputs.
- DTMF (dual tone multi frequency). The signal to the phone company that you generate when you press an ordinary telephone's touch keys.
- PAN. Permanent Account Number.
- MP3 (MPEG Audio Layer 3). Common digital audio codec. Ravon call recordings use MP3 at a rate of 128 kbps.
- PBX Manager Web. Application used to manage behavior and users of Ravon Hosted Phone Service.
- ANI (Automatic Number Identification). ANI captures and displays the phone number of a calling party.
- DNIS (Dialed Number Information Service). The phone number which the calling party called.
- GPG GNU Privacy Guard. Cryptographic software which is used for recording encryption /decryption.
- PCI DSS2. HTTPS Protocol used to securely transmit WWW data. See https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

1.2 Assumptions

1. Customer is in compliance with PCI DSS2 Requirement 3.2. PAN information will not be stored in Ravon Hosted Phone System call recordings because agents will manually start call recording after the caller has provided PAN.
2. Security of the LAN and agent workstations (PCI DSS2 Requirement 1) are the responsibility of Customer.
3. Customer is in compliance with PCI DSS2 Requirement.
    3.1. Customer will use PBX Manager to define the period of time that recorded calls are stored. (After the expiration of this period, Ravon Hosted Phone System will automatically delete recordings.)
4. Customer will define access control for playback of recordings (PCI DSS2 Requirement 7).

1.3 References

Ravon Hosted Phone Service provides several different ways to record calls:

1. All of an agent's calls can be recorded in their entirety.
2. All of a queue's calls can be recorded in their entirety.
3. While a call is in progress, an agent may request that the call be recorded in its entirety by pressing the "one-touch record" button or key sequence (e.g., *7).
4. While a call is in progress, an agent may request that the call be recorded starting from the point at which the agent made the request. This is done via a call to a function exposed by the PBX Manager API. The PBX Manager API can be accessed via a Web Services Call. Access to the different ways of call recording is controlled through the PBX Manager. For example, if it is not appropriate for all of an agents calls to be recorded, then this feature should be turned off. This is the default behavior. Similarly, the default behavior is not to provide agents with the ability to record their own calls from the beginning of the call. In situations where a caller may provide PAN information, it is recommended to use only method #4 to record calls. This will ensure the PAN data is not recorded. The PBX Manager also allows administrators to control access to playback of recordings. For example, supervisors may be granted access to listen to recordings of the employees they are responsible for (1.8.2).

1.4 Recording Calls

The following diagram shows Ravon call recording at a high level. Calls recordings in progress are recorded and stored on the local file system of the PBX server. Immediately after the call completes, it is converted (from WAV) to MP3 format and then encrypted using RSA. Finally, the encrypted call is stored to the database along with metadata describing the call (e.g., agent, date/time), and the original call recording (i.e., WAV file) is deleted.

1.5 Retrieving Recorded Calls

Recorded calls are retrieved and played back using the PBX Manager. The diagram below shows how the call is retrieved from the database, decrypted on the web server, and the decrypted call is sent over HTTPS to the workstation. The PBX Manager uses a Flash player to request the decrypted call recording. The agent is not presented with a facility to save the decrypted call on their workstation.

Implementation

1.6 Call Recording

Recordings are stored in the database as encrypted 128kbps MP3s. Playbacks are also 128kbps MP3s.

1.7 Database

Every call stored in the database is encrypted. The database is MySQL 5.5 allowing a maximum file size of 4096 MB for the call recording. Replication is enabled on the database. Read more about this in section 1.7.2.

1.7.1 Call Recording Metadata. The following metadata is available for each call recording:

- Date/Time
- Duration of the call (in seconds)
- Agent
- Queue
- ANI
- DNIS

Type (inbound, outbound, internal)

1.7.2 Database Backup & Replication. The database is replicated to a separate database server. Replication occurs in real-time. In practice, this is typically 1-5 seconds behind. Monitoring is set up for the replication process to make sure it is always up-to-date. If an error occurs, or if replication falls more than 10 seconds behind, an alert is sent to administrators. This process is executed every 15 minutes. In addition to replication, the database is backed up nightly.

1.8 PBX Manager

The PBX Manager is a web application that is used to manage the behavior of the phone system, control user access (1.8.2), and listen to recordings.

1.8.1 Retrieving Call Recordings. Retrieval of recorded calls is available exclusively from the PBX Manager over HTTPS. The web server will not serve recordings over HTTP. When the web server receives a request for a call recording, it retrieves the call from the database and decrypts it using the private key. Following this, it responds to the request with the decrypted recording.

1.8.2 User Authentication. User authentication and validation is a central concept of the PBX Manager. Each user of the PBX Manager has his/her own login and security profile. This security profile controls the features of the PBX Manager the user has access to. In addition, the PBX Manager has another method that provides greater granularity in controlling access to the call recordings. It is possible to grant specific users access to review the call recordings of another user or group of users. For example, a supervisor can be granted privileges to listen to the recordings of those employees he/she is responsible for.

1.8.3 PBX Manager Web Services. The PBX Manager exposes web services that can be used to start, stop, pause, or resume call recording. The following diagrams show the requests and responses for accomplishing call recording. The following diagram shows an example of a call to the PBX Manager web services to record a phone call. An agent initiates the process by selecting the record link/button from the application on his workstation. This sends a request to the server to start call recording. The server sends a "List Calls request to Ravon web services and it responds with the call in progress for the agent. Next, the server sends a "Manage Call Recording" request to Ravon Web Services. Ravon Web Services responds with a "Success" message.

1.9 Call Encryption & Decryption

The encryption algorithm used is RSA with a 4096-bit key. Refer to section 1.9.4 for a description of the process used to generate a key. The application GPG is utilized to carry out the encryption process.

1.9.1 Encryption Process. Initially, a call is recorded in WAV format on the PBX server's file system. Once the call completes, it is converted to MP3 and encrypted using the public key. Finally, the encrypted recording is stored to the database along with metadata for the recording and the original unencrypted WAV recording is deleted.

1.9.2 Decryption Process. Decryption occurs exclusively on the web server. It uses the private key to decrypt the recording and the decrypted call is transferred in the HTTPS response.

1.9.3 Key Storage Public keys, which are used for encryption, are stored on the PBX servers' file system. Private keys, which are used for decryption, are stored on the Web servers' file system. The keys on the Web server and PBX server file systems are encrypted using 4096-bit key-encrypting keys. These key-encrypting keys are stored in the database and are themselves encrypted using AES with a 128- bit key. The key for that operation is stored on the web server.

1.9.4 Key Management. Key management is one of the features provided by the PBX Manager. This is shown in the screenshot below. Administrators may cycle the current key by using the PBX Manager to securely generate new 4096-bit keys. The keys are generated on the server and saved to the key store on the appropriate servers. The PBX Manager does not provide access to the newly generated keys, nor is the administrator able to upload self- generated keys for additional security. When a new pair of keys is generated, these are now used for encrypting and decrypting new calls. Recordings that were previously stored in the database will require the old key to decrypt. The web server and GPG take care of the logic to choose the correct key for decryption.

1.9.4.1 Retiring Keys PCI DSS2. Requirement 3.6.5 describes the need for retirement/destruction of keys that have had their integrity compromised. In this situation, calls stored in the database will need to be decrypted using the old compromised key and then re-encrypted using a new key. This process is accomplished by an administrator on the command line and is not provided by the PBX Manager.