Verschlüsseln und Entschlüsseln des IM&P Compliance Encryption Key

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie der von IM&P für die Compliance-Verschlüsselung generierte Verschlüsselungsschlüssel verschlüsselt und entschlüsselt wird.

Voraussetzungen

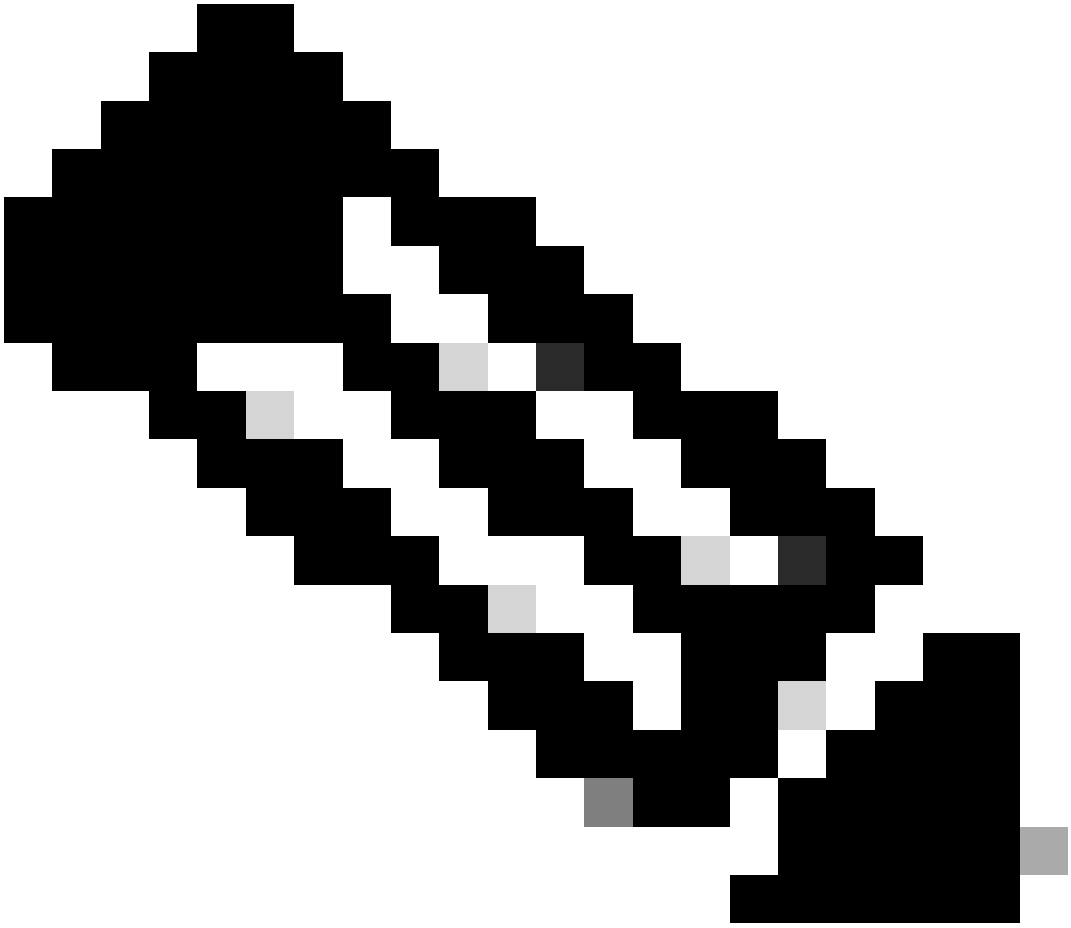
Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration des Nachrichtenarchivs
- OpenSSL

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- MacOS 15.5
- IM und Presence (IM&P) Version 15su2
- OpenSSL 3.3.6



Anmerkung: Die in diesem Dokument aufgeführten Befehle können je nach OpenSSL-Version oder -Plattform variieren. Das Internet ist eine gute Quelle, um diejenigen zu finden, die zu Ihrer Umgebung passen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Message Archiver-Funktion bietet eine grundlegende IM-Compliance-Lösung. Mit dieser Funktion kann Ihr System Vorschriften einhalten, die die Protokollierung des gesamten Instant Messaging-Datenverkehrs in Ihrem Unternehmen vorschreiben. In vielen Branchen gelten für Instant Messages dieselben gesetzlichen Vorschriften wie für alle anderen geschäftlichen Aufzeichnungen. Um diese Vorschriften einzuhalten, muss Ihr System alle Geschäftsdatensätze

protokollieren und archivieren, und archivierte Datensätze müssen abrufbar sein.

Um die Sicherheit zu erhöhen, können Sie eine verschlüsselte Datenbank für den Nachrichtenarchiver aktivieren. Wenn diese Option aktiviert ist, verschlüsselt der IM- und Presence-Dienst Instant Messaging-Nachrichten, bevor sie in der externen Datenbank archiviert werden. Mit dieser Option werden alle Daten in der Datenbank verschlüsselt, und Sie können archivierte Instant Messages nur lesen, wenn Sie den Verschlüsselungsschlüssel besitzen.

Der Verschlüsselungsschlüssel kann vom IM- und Presence-Dienst heruntergeladen und zusammen mit dem Tool verwendet werden, mit dem Sie Daten anzeigen, um archivierte Daten zu entschlüsseln.

Verschlüsseln/Entschlüsseln

1. Öffnen Sie Ihr OpenSSL-Terminal.
2. Generieren Sie einen privaten Schlüssel.

```
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
```

3. Extrahieren Sie den öffentlichen Schlüssel aus dem privaten Schlüssel.

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

4. Zu diesem Zeitpunkt haben wir 2 Dateien private_key.pem und public_key.pem.

- private_key.pem: Wird zum Entschlüsseln des verschlüsselten Schlüssels aus IM&P verwendet.
- public_key.pem: Dies ist der Schlüssel, den Sie mit dem IM&P-Server teilen, damit dieser den AES-Schlüssel und den IV verschlüsseln kann.

Darüber hinaus fügt der IM&P-Server dem verschlüsselten Verschlüsselungsschlüssel die Base64-Verschlüsselung hinzu.

5. Laden Sie den Verschlüsselungsschlüssel vom IM&P-Server herunter. Weitere Informationen finden Sie im Abschnitt Verschlüsselungsschlüssel herunterladen im Instant Messaging Compliance Guide for the IM and Presence Service.
6. Zu diesem Zeitpunkt haben Sie 3 Dateien private_key.pem, public_key.pem und encrypted_key.pem.
7. In diesem Fall ist encrypted_key.pem für die sichere Übertragung mit Based64 codiert.
8. Decodieren Sie den mit Base64 verschlüsselten Schlüssel.

```
base64 -D -i encrypted_key.pem -o encrypted_key.bin
```

Dadurch wird die Base64-Codierung entfernt und eine 256-Byte-Datei erzeugt, die ursprünglich mit dem öffentlichen RSA-Schlüssel verschlüsselt wurde.

9. Entschlüsseln Sie den verschlüsselten Schlüssel mit Ihrem privaten RSA-Schlüssel.

```
openssl pkeyutl -decrypt -inkey private_key.pem -in encrypted_key.bin -out decryptedkey.bin
```

Dadurch werden der AES-Schlüssel (K) und der IV für die IM&P-Nachrichtenverschlüsselung entschlüsselt.

Beispiel für entschlüsselte Datei:

key = 0ec39f2a22abf63d4452b932f12de

iv = 683bb3d7e59e82e3fa9f42

10. Entschlüsseln Sie die AES-verschlüsselten Nachrichten.

```
openssl enc -aes-256-cbc -d -in encrypted.bin -out decrypted.txt -K <hex_key> -iv <hex_iv>
```

Fehlerbehebung

Ein häufiger Fehler beim Entschlüsseln der verschlüsselten Datei ist:

```
Public Key operation error 60630000:error:0200006C:rsa routines:rsa_ossl_private_decrypt:data greater t
```

Dieser Fehler tritt auf, wenn Sie versuchen, Daten zu entschlüsseln, die zu groß für die Größe Ihres privaten RSA-Schlüssels sind. RSA kann Daten nur bis zur Größe des Moduls entschlüsseln. In unserem Fall kann ein 2048-Bit-RSA-Schlüssel nur 256 Byte entschlüsseln.

Wenn Sie die von IM&P generierte verschlüsselte Schlüsseldatei überprüfen, ist sie 344Byte groß (344 Byte). Sie können nur 256 Bytes mit unserem privaten Schlüssel entschlüsseln.

```
-rw-rw-rw-@ 1 testuser staff 344 Jun 5 13:10 encrypted_key.pem
```

Wie bereits in diesem Dokument erwähnt, ist der verschlüsselte Schlüssel für eine sichere Übertragung mit Base64 verschlüsselt, wodurch Bytes zur Dateigröße hinzugefügt werden.

Sobald wir die Base64-Codierung entfernt haben, haben Sie eine 256-Byte-Datei, die mit unserem privaten Schlüssel leicht entschlüsselt werden kann.

```
-rw-r--r-- 1 testuser staff 256 Jun 12 09:16 encrypted_key.bin
```

Best Practices für die Sicherheit

- Speichern Sie Ihren privaten Schlüssel (private_key.pem) sicher.
- Geben Sie Ihren privaten Schlüssel nicht für andere frei und laden Sie ihn nicht auf nicht vertrauenswürdige Systeme hoch.
- Bereinigen Sie temporäre Dateien wie decryptedkey.bin nach der Entschlüsselung.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.