CHAPTER 3

Securing the Connection Between Cisco Unity Connection, Cisco Unified Communications Manager, and IP Phones

In this chapter, you will find descriptions of potential security issues related to connections between Cisco Unity Connection, Cisco Unified Communications Manager, and IP phones; information on any actions you need to take; recommendations that will help you make decisions; discussion of the ramifications of the decisions you make; and best practices.

See the following sections:

Security Issues for Connections Between Cisco Unity Connection, Cisco Unified Communications Manager, and IP Phones

A potential point of vulnerability for a Cisco Unity Connection system is the connection between Connection voice messaging ports (for an SCCP integration) or port groups (for a SIP integration), Cisco Unified Communications Manager, and the IP phones.

Possible threats include:

- Man-in-the-middle attacks (when the information flow between Cisco Unified CM and Connection is observed and modified)
- Network traffic sniffing (when software is used to capture phone conversations and signaling information that flow between Cisco Unified CM, Connection, and IP phones that are managed by Cisco Unified CM)
- Modification of call signaling between Connection and Cisco Unified CM

- Modification of the media stream between Connection and the endpoint (for example, an IP phone or a gateway)
- Identity theft of Connection (when a non-Connection device presents itself to Cisco Unified CM as a Connection server)
- Identity theft of the Cisco Unified CM server (when a non-Cisco Unified CM server presents itself to Connection as a Cisco Unified CM server)

Cisco Unified Communications Manager Security Features for Cisco Unity Connection Voice Messaging Ports

Cisco Unified CM can secure the connection with Connection against the threats listed in the "Security Issues for Connections Between Cisco Unity Connection, Cisco Unified Communications Manager, and IP Phones" section on page 3-1. The Cisco Unified CM security features that Connection can take advantage of are described in Table 3-1.

Table 3-1 Cisco Unified CM Security Features That Are Used by Cisco Unity Connection

Security Feature	Description
Signaling authentication	The process that uses the Transport Layer Security (TLS) protocol to validate that no tampering has occurred to signaling packets during transmission. Signaling authentication relies on the creation of the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and Connection. • Modification of the call signalling. • Identity theft of the Connection server. • Identity theft of the Cisco Unified CM server.
Device authentication	The process that validates the identity of the device and ensures that the entity is what it claims to be. This process occurs between Cisco Unified CM and either Connection voice messaging ports (for an SCCP integration) or Connection port groups (for a SIP integration) when each device accepts the certificate of the other device. When the certificates are accepted, a secure connection between the devices is established. Device authentication relies on the creation of the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and Connection. • Modification of the media stream. • Identity theft of the Connection server. • Identity theft of the Cisco Unified CM server.

Table 3-1 Cisco Unified CM Security Features That Are Used by Cisco Unity Connection (continued)

Security Feature	Description
Signaling encryption	The process that uses cryptographic methods to protect (through encryption) the confidentiality of all SCCP or SIP signaling messages that are sent between Connection and Cisco Unified CM. Signaling encryption ensures that the information that pertains to the parties, DTMF digits that are entered by the parties, call status, media encryption keys, and so on are protected against unintended or unauthorized access. This feature protects against: • Man-in-the-middle attacks that observe the information flow between Cisco Unified CM and Connection. • Network traffic sniffing that observes the signaling information flow between Cisco Unified CM and Connection.
Media encryption	The process whereby the confidentiality of the media occurs through the use of cryptographic procedures. This process uses Secure Real Time Protocol (SRTP) as defined in IETF RFC 3711, and ensures that only the intended recipient can interpret the media streams between Connection and the endpoint (for example, a phone or gateway). Support includes audio streams only. Media encryption includes creating a media master key pair for the devices, delivering the keys to Connection and the endpoint, and securing the delivery of the keys while the keys are in transport. Connection and the endpoint use the keys to encrypt and decrypt the media stream. This feature protects against: • Man-in-the-middle attacks that listen to the media stream between Cisco Unified CM and Connection. • Network traffic sniffing that eavesdrops on phone conversations that flow between Cisco Unified CM, Connection, and IP phones that are managed by Cisco Unified CM.

Authentication and signaling encryption serve as the minimum requirements for media encryption; that is, if the devices do not support signaling encryption and authentication, media encryption cannot occur.

Cisco Unified CM security (authentication and encryption) only protects calls to Connection. Messages recorded on the message store are not protected by the Cisco Unified CM authentication and encryption features but can be protected by the Connection private secure messaging feature. For details on the Connection secure messaging feature, see the "How Cisco Unity Connection Handles Messages That Are Marked Private or Secure" section on page 9-1.

Security Mode Settings for Cisco Unified Communications Manager and Cisco Unity Connection

Cisco Unified Communications Manager and Cisco Unity Connection have the security mode options shown in Table 3-2 for voice messaging ports (for SCCP integrations) or port groups (for SIP integrations).

Caution The Cluster Security Mode setting for Connection voice messaging ports (for SCCP integrations) or port groups (for SIP integrations) must match the security mode setting for the Cisco Unified CM ports. Otherwise, Cisco Unified CM authentication and encryption will fail.

Table 3-2 Security Mode Options

Setting	Effect
Non-secure	The integrity and privacy of call-signaling messages will not be ensured because call-signaling messages will be sent as clear (unencrypted) text and will be connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream cannot be encrypted.
Authenticated	The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text. In addition, the media stream will not be encrypted.
Encrypted	The integrity and privacy of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages will be encrypted. In addition, the media stream can be encrypted. ⚠ **Caution** Both end points must be registered in encrypted mode for the media stream to be encrypted. However, when one end point is set for non-secure or authenticated mode and the other end point is set for encrypted mode, the media stream will not be encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream will not be encrypted.

Best Practices for Securing the Connection Between Cisco Unity Connection, Cisco Unified Communications Manager, and IP Phones

If you want to enable authentication and encryption for the voice messaging ports on both Cisco Unity Connection and Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager SCCP Integration Guide for Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/integration/guide/cucm_sccp/cucintcucmskinny.html.