Cisco Unified Communications Manager Authentication and Encryption

- Cisco Unified Communications Manager Authentication and Encryption, on page 1

Cisco Unified Communications Manager Authentication and Encryption

Introduction

A potential point of vulnerability for a Cisco Unity Connection system is the connection between Unity Connection and Cisco Unified Communications Manager. Possible threats include:

- Man-in-the-middle attacks (a process in which an attacker observes and modifies the information flow between Cisco Unified CM and the Unity Connection voice messaging ports)
- Network traffic sniffing (a process in which an attacker uses software to capture phone conversations and signaling information that flow between Cisco Unified CM, the Cisco Unity Connection voice messaging ports, and IP phones that are managed by Cisco Unified CM)
- Modification of call signaling between the Unity Connection voice messaging ports and Cisco Unified CM
- Modification of the media stream between the Unity Connection voice messaging ports and the endpoint (for example, a phone or gateway)
- Identity theft of the Unity Connection voice messaging port (a process in which a non-Unity Connection device presents itself to Cisco Unified CM as a Unity Connection voice messaging port)
- Identity theft of the Cisco Unified CM server (a process in which a non-Cisco Unified CM server presents itself to Unity Connection voice messaging ports as a Cisco Unified CM server)

Cisco Unified CM Security Features

Cisco Unified CM can secure the connection with Unity Connection against these threats. The Cisco Unified CM security features are used by Unity Connection as described in Table 7.

Cisco Unified CM Security Features Used by 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. **Impact on Threats: :**This feature protects against • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Unity Connection voice messaging ports. • Modification of the call signaling. • Identity theft of the Unity Connection voice messaging port. • 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 Unity Connection voice messaging ports 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. **Impact on Threats: :**This feature protects against • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Unity Connection voice messaging ports. • Modification of the media stream. • Identity theft of the Unity Connection voice messaging ports. • Identity theft of the Cisco Unified CM server.

Security Feature	Description
Signaling encryption	The process that uses cryptographic methods to protect (through encryption) the confidentiality of all SCCP signaling messages that are sent between the Unity Connection voice messaging ports 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. **Impact on Threats: :**This feature protects against • Man-in-the-middle attacks that observe the information flow between Cisco Unified CM and the Unity Connection voice messaging ports. • Network traffic sniffing that observes the signaling information flow between Cisco Unified CM and the Unity Connection voice messaging ports.
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 Unity Connection voice messaging ports 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 Unity Connection and the endpoint, and securing the delivery of the keys while the keys are in transport. Unity Connection and the endpoint use the keys to encrypt and decrypt the media stream. **Impact on Threats: :**This feature protects against • Man-in-the-middle attacks that listen to the media stream between Cisco Unified CM and the Unity Connection voice messaging ports. • Network traffic sniffing that eavesdrops on phone conversations that flow between Cisco Unified CM, the Unity Connection voice messaging ports, and IP phones that are managed by Cisco Unified CM .