Security for Mobile Instant Messaging

IBM Lotus Sametime for Android

Conundrum Software, LLC

www.conundrumsoftware.com

Contact us: sales@conundrumsoftware.com

13 March, 2011

Contents

Overview

Regardless of its convenience, no instant messaging client is acceptable in a business environment, unless the client provides at least the same level of security provided by other forms of access to the instant messaging server.

QuipIM achieves this level of security in three tiers, depending on the nature of the enterprise's operations, and its required level of security. Each tier addresses two components of the security of the client and its communications:

1. Storage of sensitive account information
2. Security of over-the-wire communications

Before we address any of these tiers, it is worth noting that in all three tiers, QuipIM communicates with the the server utilizing a direct connection. We have concluded that it is never acceptable for either private account information or messages to be routed through an intermediary server owned by us at any time. Many IM clients do choose to pass through an intermediary server by design – this is one way we have chosen to set QuipIM apart.

We present the three tiers of security offered by QuipIM in ascending order of security and complexity.

Tier 1 – Sametime protocol using 128-bit RC2 encryption

Providing a robust security framework for most needs.

Storage of sensitive account information

All account information, including the user id and password, is stored in the Android OS account manager (not in our own database). The stored password (intended for the account's authenticator which resides inside the QuipIM application) can only be accessed by a caller who holds the permission AUTHENTICATE_ACCOUNTS and has the same UID as the account's authenticator. When installed, applications are given a unique UID, and the application will always run as that UID on that particular device. Applications signed with a different key can never request to be run with the same UID, enforced by Android's PackageManager. What this means is that *QuipIM is the only app that can request passwords that it entrusts to the Android account manager*.

Security of over-the-wire communications

The login process involves a number of different messages going back and forth between the Sametime server and the device. The first set of messages establishes a secure connection for the duration of the user's session. All messages from that point are encrypted with a key derived with Diffie-Hellman key exchange and utilizing the RC2 cipher, created specifically for Lotus Notes. Your password is not sent until after the secure connection has been established. The password itself is encrypted inside of the surrounding login message which is encrypted in its entirety. So in a sense, there are two levels of encryption operating on your password before it is sent over the wire. In short, QuipIM uses the same level of encryption and the same procedure that the IBM Sametime Connect Client and Lotus Notes uses. A login request from QuipIM is indistinguishable in this respect from a login request by the Sametime Connect Client.

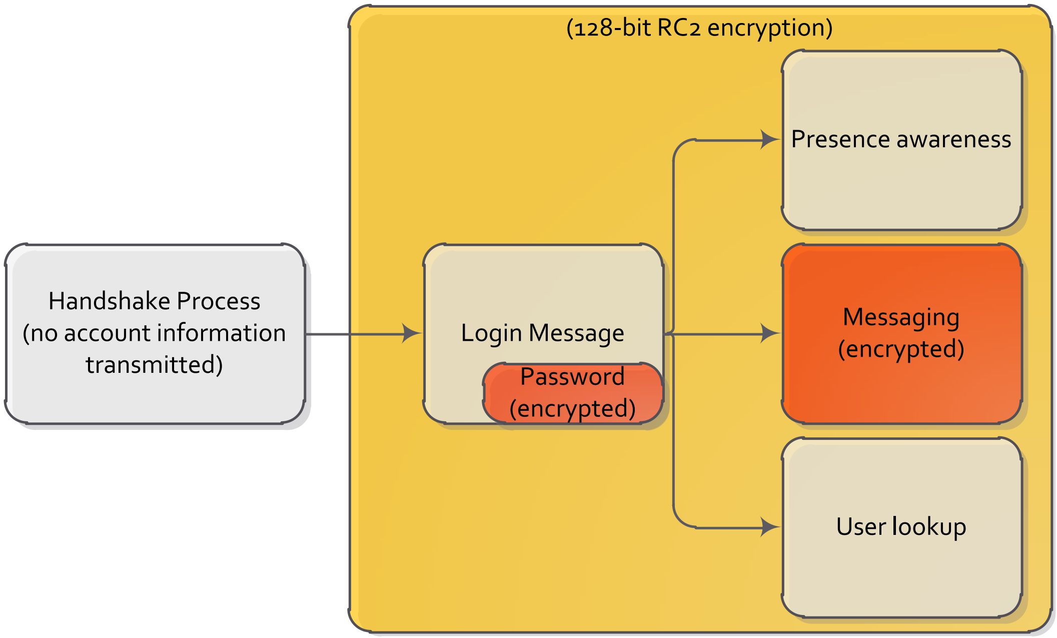

Figure 1 - The Tier 1 over-the-wire communications model

Tier 2 – RC2 Encryption plus VPN

Wrapping Tier 1 RC2 encryption in another layer of security by introducing VPN.

Storage of sensitive account information

Account information is stored in the same way it was in the Tier 1 implementation. Private account information is protected by the Android OS, and only accessible to the QuipIM app.

Securing over-the-wire communications even further

Many companies choose not to expose their Sametime servers to the internet, but do already provide at least limited VPN access to their employees. VPN can be an effective means of controlling unauthorized external probing of the corporate Sametime server while allowing employees to communicate with their coworkers while away from the corporate campus. Both the Android and iPhone come equipped to connect to VPNs.

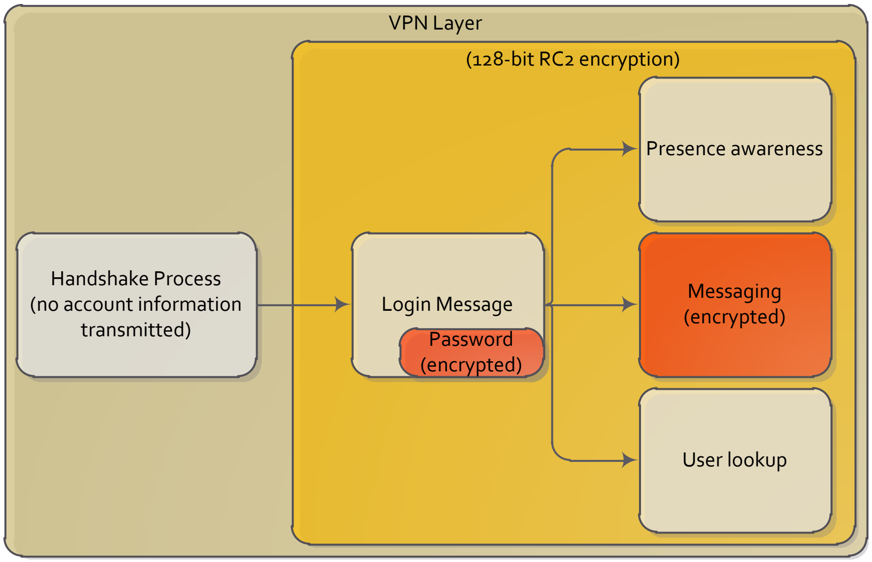

Figure 2 - The Tier 2 over-the-wire communications model

Tier 3 – QuipIM Enterprise

Avoiding storage of sensitive account information on the mobile device by using QuipIM Enterprise.

Circumventing the storage of sensitive account information

While Tier 1 and 2 provide a secure means of storing sensitive account information on the device and keeping it isolated from other apps installed on the device, the account information is only as secure as the physical device itself. If the device is lost or stolen, a persistent malicious party could, with some difficulty, retrieve that account information from the device by rooting the phone and ultimately extracting the account database stored on the device.

Additionally, some enterprises will desire to provide external access to Sametime only for a certain subset of its employees on a needs basis.

For these types of businesses, QuipIM Enterprise provides a solution for both. The Enterprise edition couples the familiar QuipIM client with a QuipIM Enterprise Gateway that is deployed on the corporate network. Authorized employees register their mobile device through a web interface exposed on the corporate intranet, and input their Lotus login data on the web interface. The Enterprise Gateway uses this information to retrieve a login token from the Sametime server, and stores this login token. The mobile device then hits the Enterprise Gateway to establish its connection without requiring any account information.

A lost or stolen device can be deregistered from the Enterprise Gateway to prevent unauthorized access.

Security of over-the-wire communications

QuipIM Enterprise connections are secured with HTTPS.