Jean-Baptiste MARTIN et Lucas SOLTIC - IRM promotion 2014
Tuteur : Traian MUNTEAN

Projet de synthèse : sécurisation d'une communication à travers le réseau Jabber

Introduction

Le réseau Jabber est utilisé pour le transfert de messages suivant le protocole XMPP. Plusieurs logiciels permettent d'exploiter ce réseau, comme Google Talk, Skype ou encore Pidgin. Nous avons choisi Pidgin car c'est un client graphique open source, léger et multiplateforme. Pidgin est basé sur la bibliothèque libpurple qui gère de nombreux protocoles de messagerie instantanée, dont XMPP. Pidgin et libpurple sont écrits en C.

Problème actuel

Le protocole XMPP permet de gérer le chiffrement des données entre le client et le premier serveur, mais le serveur est capable de déchiffrer et lire les conversations. L'objectif de ce projet est de rajouter une couche de sécurité ne permettant qu'au destinataire de lire les messages.

Objectifs

Les modifications apportées pour atteindre les objectifs seront effectuées sur la bibliothèque libpurple. Ainsi, tous les clients utilisant cette bibliothèque pourront bénéficier d'une connexion sécurisée. Dans le cadre de ce projet nous considérons uniquement le cas d'une conversation entre 2 personnes.

Dans un premier temps, nous créerons une communication utilisant un protocole cryptographique afin de chiffrer les messages envoyés par un émetteur A. Le recepteur B devra être en mesure de déchiffrer ce message. Les clés publiques seront connues des 2 utilisateurs et chaque utilisateur connaîtra sa clé privée associée.

Dans un second temps, les clés publiques n'étant pas connues à l'avance des utilisateurs, nous assurerons la protection contre les attaques de type "Man in the middle". Pour cela, nous utiliserons un tiers de confiance soit pour délivrer les clés publiques signées, soit pour permettre l'authentification de la clé publique délivrée par le destinataire, en vérifiant que cette dernière a bien été signée par le tiers de confiance.