PROTOCOLE D'AGREMENT DE CLES Key agreement protocol

Type de contenu : Images animées

Titre(s) : PROTOCOLE D'AGREMENT DE CLES Key agreement protocol ; PARRAUD ; Professeur ROY, Bimal ; SLT de BISSCHOP, Quentin

Autre(s) responsabilité(s) : PARRAUD (Directeur de thèse)
Professeur ROY, Bimal (Directeur de thèse)
SLT de BISSCHOP, Quentin (Secrétaire)

Editeur, producteur : Ecoles Militaires de Saint-Cyr Coëtquidan

Note de thèses et écrits académiques : Filière Scientifique - Option Informatique Promotion Chef d'Escadron Francoville Date de soutenance : 01/01/2011

Résumé ou extrait : Etude: PRESENTATION : Le domaine de la cryptographie inclue les techniques de chiffrement et de déchiffrement des informations. Plus précisément, lorsque deux individus souhaitent établir une communication cryptée, il doivent au préalable s'être mis d'accord sur l'utilisation d'un algorithme de chiffrement particulier et partager une ou plusieurs clés permettant le cryptage et le décryptage des messages. Or le partage de cette clef peut se révéler compliqué, car celui-ci doit se faire de façon confidentielle: si un adversaire obtient la clef, il peut accéder aux informations échangées. Notre but est donc d'étudier les différents protocoles permettant l'échange d'une clé sur un canal non protégé. Ces protocoles sont appelés protocoles d'agrément de clés. Plus ou moins élaborés, ils peuvent dans certains cas assurer l'authentification des utilisateurs ou l'intégrité des données échangées. Nous proposerons par ailleurs une solution au partage de clés sous la forme d'un protocole d'agrément de clés authentifié et destiné à un groupe d'utilisateurs. CONTRAINTES ET IMPERATIFS : La première contrainte est de pouvoir faire des calculs sur de grands nombres. En effet, et même si notre objectif n'est pas d'aboutir à programme opérationnel, les algorithmes cryptographiques impliquent la plupart du temps de manipuler de grands nombres qui peuvent d'une part, poser problème lors de l'implémentation, et d'autre part, entraîner des temps de calculs relativement longs. Nous choisissons, par ailleurs, d'utiliser les courbes elliptiques dans l'exécution des différents protocoles. Cela impose d'étudier le groupe particulier des points d'une courbe elliptique E: y2=x3+ax+b modulo p, où p est premier. DEMARCHE : Dans un premier temps, il nous a été necessaire de cerner au mieux les enjeux et problèmes soulevés par les protocoles d'agréments de clés. Puis nous avons étudié l'utilisation des courbes elliptiques dans le domaine de la cryptographie. Enfin, nous proposons notre propre solution après nous être intéressé à des protocoles particuliers (authentifiés par mot de passe, ou destinés à des groupes d'utilisateurs). Nous avons choisi d'implémenter les différentes algorithmes et protocoles étudiés. Le principale problème est alors venu de la manipulation des grands nombres. Enfin, dans le protocole que nous proposons, la difficulté a été de trouver une approche qui soit à la fois différente de celles précédemment étudiées, tout en étant théoriquement sûre et apportant une réelle plus-value. RESULTATS OBTENUS : L'utilisation d'une bibliothèque de manipulation de grands nombres nous permet d'apporter une solution au premier problème. Cette bibliothèque effectue les opérations de façon dite naïve. Loin d'être une solution optimale, elle permet cependant le fonctionnement de tous les algorithmes et protocoles que nous avons

implémenté. Le protocole que nous proposons, quant à lui, se veut à la fois authentifié par mot de passe et destiné à un groupe d'utilisateurs. Il ne requiert pas d'utilisateur maître, chacun étant authentifié par un seul de ses voisins. Un des utilisateurs peut toutefois prendre le rôle de contrôleur, dont la tâche est d'exclure un utilisateur qui ne serait pas en mesure de s'authentifier. LIMITES : La limite majeure qui intervient dans l'implémentations des protocoles est le temps de calcul requis par l'analyse des courbes elliptiques, préalable indispensable à leur utilisation. Ainsi pour une courbe d'équation E: y2=x3+ax+b mod p où p est de l'ordre de 107, on obtient une durée de calcul de 300s. Il est bien entendu possible d'effectuer ces calculs en amont et de stocker les résultats. Toutefois, il est clair que l'utilisation de telle procédés de calcul est impossible pour manipuler des clés de 256 bits, longueur couramment utilisée en cryptographie sur les courbes elliptiques. CONCLUSION : Nous comprenons mieux, suite à cette étude, les enjeux et problématiques du partage de clés cryptographiques. Notre protocole app

Sujet(s) : confidentialité
cryptographie
information chiffrée
protocole de transmission