Implémentation d'un protocole de sécurité niveau application pour les transactions du client mobile

Etabli par: GUEMINI Mustapha
Encadreur: Mr EUSCHI Salah
Département d'informatique et dess technologies d'information
Université Kasdi Merbah Ouargla 30000, Algérie

Résumé

L'utilisation fréquente et étendue des applications mobiles embarquées sur des dispositifs mobiles nous amène souvent à transmettre des données confidentielles et sensibles. Ces données, qui peuvent être des numéros de compte bancaire ou de carte de crédit lors des opérations de transaction et notamment lors de l'achat en ligne, des mots de passe lors d'ouverture d'une session web et même des code PIN, PUK pour ATM…etc, transmises en clair ne seront pas sécurisées donc exposées aux risques d'attaques et peuvent être interceptées.

L'objectif de notre travail est de concevoir et réaliser une solution fiable permettant de sécuriser les données sensibles de l'utilisateur mobile lorsqu'elles seront transmises via internet sans fil et filaire au serveur du marchand.

Nous devrons donc implémenter dans l'application mobile du client, des routines de sécurité basées sur des outils cryptographiques modernes et appropriés aux contraintes spécifiques de l'environnements mobiles et sans fil. Ces routines cryptographiques permettent d'assurer les critères de sécurité nécessaires à la protection contre les différentes attaques passives et actives, ces critères sont :

- La confidentialité des données pour fournir une protection contre l' attaque de type écoute passive.
- L'intégrité des données pour se protéger contre l'interception ou l'altération des données.
- L'authentification des entités communicantes pour se protéger contre le déguisement ou l'usurpation d'identité.

Mots clés: dispositif mobile, application mobile, transaction, cryptographie, authentification, intégrité, confidentialité.

1- Introduction

Avec l'utilisation de plus en plus répandue des applications mobiles et sans fil la face d'internet à complètement changé, les dispositifs mobiles dominent l'accès internet par rapports aux PCs, ils peuvent se connecter à l'internet n'importe ou? et n'importe quand? Ces dispositifs mobiles stockent des données personnelles (clés, code PIN et certificats) pour envoyer ou recevoir des données privées personnelles. Ils peuvent même réaliser des transactions financières liés aux opérations de m-commerce. Avec ces dispositifs mobiles, nous pouvons donc exécuter beaucoup d'applications mobiles qui nous permettent de communiquer, naviguer, ou faire des transactions sur internet …etc. Certaines applications mobiles comme celles réalisant les transactions financières nécessitent des solutions de sécurité qui sont basés généralement sur routines cryptographiques permettent de réaliser les critères de sécurité de confidentialité, d'intégrité et d'authentification.

2- Problématique

La sécurité est un défi important aux applications mobiles gérant des données sensibles. Ces applications mobiles nécessitent des transmissions sécurisés et des techniques d'authentification pour faire face aux différentes attaques passives et actives. La transmission sans fil est facile à l'écoute, donc il faut protéger les données personnelles (mot de passe, code pin, clé privée, n° de carte de crédit, compte bancaire, …) et authentifier les utilisateurs mobiles. Pour protéger les données personnelles et authentifier les utilisateurs mobiles nous utilisons des techniques cryptographiques. Mais le calcul crypto pose des problèmes de performance dans l'environnement sans fil et mobile, les protocoles de sécurité de l'internet filaire comme TLS ne sont pas appropriés aux applications mobiles car les dispositifs mobiles sont limités en ressources CPU, RAM et consommation d'énergie. Notre solution de sécurité doit être légère et adapté aux environnement sans fil et mobile.

4- Présentation de la solution

On se limite aux transactions clients mobiles avec un serveur web marchant (modèle client/serveur), ce type de transactions appelées B2C (Busines_to_consummer) sont les plus répandus dans le monde de commerce électronique et mobile.

Nous utilisons une cryptographie basée sur les courbes elliptiques (ECC) , elle offre un niveau de sécurité équivalent aux crypto systèmes traditionnels (comme RSA et DH) mais avec des tailles de clés plus petites. Elle offre une meilleur performance en calcul CPU, consommation d'énergie ainsi qu'une économie en mémoire et en bande passante, par conséquent les outils crypto ECC sont mieux adaptés pour les dispositifs mobiles et peuvent aussi alléger la charge crypto des serveurs de contenu Web.

5– Un protocole de sécurité léger

Le travail demandé consiste à implémenter un protocole de sécurité léger sur dispositif mobile du client et le serveur web du marchand. Ce protocole sera composé de trois modules suivants:

1. **Un module d'authentification** du client mobile permet d'enregistrer le client mobile et lui attribuer un login et un mot de passe, le client mobile se connecte au serveur web marchand en fournissant son login et son mot de passe , le mot de passe ne doit pas être transmis en clair au serveur web.
2. **Un module de gestion de clés** permet de générer la paire de clés ECDSA du client mobile pour la signature numérique ECDSA. La clé publique ECDSA sera communiqué au serveur marchand via une connexion HTPPs. Les clés de sécurité seront stockées dans le système RMS (Record Management System) du Java.
3. **Un module de sécurité** utilisé pour signer le message de la transaction du client mobile et le chiffrer par une clé secrète AES 256 bits transmis par le serveur au client mobile via une connexion HTTPs

Ces trois modules basés sur des routines cryptographiques seront par la suite intégrés dans l'application mobile utilisée pour réaliser la transaction du client mobile.

6– Conclusion

Dans ce travail, nous avons proposé une solution de sécurité légère niveau application pour sécuriser les transactions du client mobile. Elle est basée sur des routines cryptographiques de courbes elliptiques (ECC) associés à des certificats numériques. Cette solution de sécurité permet d'assurer la confidentialité ainsi que l'intégrité des données de la transaction et l'authentification des parties impliquées au même temps que la non-répudiation. Nous utilisons la plateforme Java SDK et J2ME avec l'éditeur de développement intégré Netbeens pour implémenter et tester notre solution.

7– Bibliographie

1. Certicom's Bulletin of Security and Cryptography, The Next Generation of Cryptography Public Key Sizes for AES, Code and cipher Vol. I, no. 1, en ligne http://www.certicom.com/codeandcypher.
2. Certicom's Bulletin of Security and Cryptography, The Next Generation of Cryptography Public Key Sizes for AES, Code and cipher Vol. 2, no. 2, en ligne http://www.certicom.com/codeandcypher.
3. David Hook, Beginning Cryptography with Java (Chapter 1 :The JCA and the JCE) , August 2005.
4. Bouncycastle.org, The Legion of the Bouncy Castle, http://www.bouncycastle.org/.
5. The Legion of the Bouncy Castle, SPECIFICATIONS, http://www.bouncycastle.org/specifications.html, September 2010.
6. Java SE Technical Documentation, Package javax.microedition.midlet Description, Sun Microsystems and Motorola, http://download-llnw.oracle.com/javame/config/cldc/ref-impl/midp2.0/jsr118/javax/microedition/midlet/package-summary.html.
7. Bouncycastle.org, Elliptic Curve Key Pair Generation and Key Factories, http://www.bouncycastle.org/wiki/display/JA1/Elliptic+Curve+Key+Pair+Generation+and+Key+Factories, September 2010.
8. Entrust, Inc., Elliptic Curve PKI An exploration of the benefits and challenges of a PKI based on elliptic curve cryptography, February 2008, http://www.entrust.com