Comparaison fonctionnelle et expérimentale d'une PKI sur mobile et de Kerberos sur mobile. Mise en oeuvre et comparaison rigoureuse des résultats expérimentaux. Automatisation du déploiement.

Jean-Philippe Blaise, Willian Jouot

Master SSIC, Metz University,
Ile du Saulcy, 57045 Metz, France
jeanphilippe.blaise@umail.univ-metz.fr
william.jouot@umail.univ-metz.fr

Mots-clés : PKI, Kerberos, mobile, mise en oeuvre, déploiement

1 Problématique

A l'heure actuelle, les téléphones ainsi que les smartphones se démocratisent de plus en plus, et il y a donc de plus en plus de données qui transitent via ces appareils, que cela soit via le wifi, bluetooth, ou directement le réseau téléphonique. On commence ainsi à faire des achats directement depuis son téléphone, où encore envoyer des informations personnels, comme des mots de passe, ou des documents que l'on veut garder secret. Malheureusement, toutes ces données transitent plus ou moins en clair dans l'air, à la portée de n'importe qui. Il faut donc sécuriser les données. Quelles solutions existent ? Des systèmes comme PKI ont déjà fait leurs preuves sur nos ordinateurs, mais existe-t-il des solutions concrètes pour nos mobiles ?

2 Travaux existants dans la littérature scientifique

Il existe de nombreux travaux dans le domaine, notamment pour la PKI. Le premier est basé sur une PKI pour un système de paiement[1]. Un autre document propose une solution d'implémentation d'une wireless PKI (WPKI)[2]. Beaucoup moins d'article parlant de Kerberos existe à ce jour. Quelques uns sont interessant comme ces articles parlant d'une authentification Kerberos par billets "réutilisables"[3,4].

3 Premières critiques des travaux existants

Les travaux existants proposent des solutions très bien et très complètes. Malgré tout, chacun propose sa propre solution ainsi que sa propre implémentation. Mais laquelle est la meilleure ? Très peu, voir aucunes, publications ne comparent sa solution avec celle des autres en pratique afin de déterminer la meilleure solution. Si l'on ne devait en choisir qu'une seule, laquelle choissirait-on ?

4 Objectifs et perspectives du projet de synthèse

L'objectif est d'implémenter le déploiement automatique d'un système de certification pour mobile. Pour cela, il faudra comparer le fonctionnement d'une PKI et de Kerberos aussi bien de manière expérimentale que fonctionnelle. Nous nous focaliseront sur une base théorique pour commenter les documents existants. Et a partir de ce qu'on nous aurons retenu, mettre en oeuvre une PKI pour mobile de la manière la plus efficace possible.

Références

1. H. Marko, H. Konstantin, and T. Elena, "Utilizing national public-key infrastructure in mobile payment systems," *Electronic Commerce Research and Applications*, vol. 7, pp. 214–231, 2008.
2. L. Yong, L. Jeail, and S. JooSeok, "Design and implementation of wireless pki technology suitable for mobile phone in mobile-commerce," *Computer Communications*, vol. 30, pp. 893–903, 2006.
3. P. S. Anish, C. Dong-You, R. K. Goo, and H. Seung-Jo, "Kerberos based authentication for inter-domain roaming in wireless heterogeneous network," *Computers & Mathematics with Applications*, vol. 60, pp. 245–255, 2010.
4. L. Yaohui, Q. Alejandro, and P. Samuel, "Mobile services access and payment through reusable tickets," *Computer Communications*, vol. 32, pp. 602–610, 2009.