Projet M2-SSI : Transchiffrement SSL **Client: Magali Bardet**
Compte Rendu Réunion

Date :
02/12/2013

Présent :
Souchal - Hamdani - Générat - Bourdon - Bardet

Excusé (procédure administrative) :
Nouafo

Objet :
Point d'avancement du projet + Précision du travail à faire pour la collision de certificats MD5

Tâches réalisées :

- Récupération de certificats MD5
- Analyse des modifications à faire sur un certificat facilitant une recherche de collision MD5

Action à faire :

- Rechercher des certificats MD5 d'autorité intermédiaire
- Expliquer, en détail, la collision MD5 sur des certificats
- Ajouter les étapes de la réalisation d'une collision MD5 dans la STB et DAL
- Vérifier les politiques des navigateurs web sur l'acceptation de certificats MD5
- Mesurer l'impact et la détection d'une attaque par proxy (man in the middle)
- Réaliser un programme cherchant une collision MD5 pour des certificats

Prochaine réunion :

- Présenter la nouvelle version de la STB au client

Précision sur la collision MD5 :

- Garder la signature + l'algorithme du certificats source
- Le sujet et l'émetteur doivent être identique sur les deux certificats
- Effectuer les plus gros changements sur la clé public, donc prendre une clé public de grande taille pour avoir une marge de manoeuvre importante.
- A part le sujet, l'émetteur, la signature et l'algorithme, aucune restriction de modification sur les autres champs du certificats pour obtenir une collision.

Programme de recherche de collision MD5 :

- Utiliser un programme parallélisable pour optimiser les temps de calculs