Compte-rendu de réunion, 9

Florian Guilbert

13 février 2013

Participants :

- Zakaria Addi ;
- Baptiste Dolbeau ;
- Florian Guilbert ;
- Emmanuel Mocquet ;
- Maxence Péchoux.
- Romain Pignard.

Absents :

- Yicheng Gao ;
- Giovanni Huet ;

Ordre du jour : Point sur l'avancement pour chaque membre de l'équipe

Zakaria Addi : (Travaille à 100% sur l'extension)

- Accompli pour le moment : création d'une extension firefox, modification du DOM avec JQuery, communication sécurisé Extension/FaceCrypt (SSL).
- Prochains objectifs : développement de classe implantant le protocole de communication entre FaceCrypt et l'extension (Tunnel), intégrer la partie communication dans l'extension.

Baptiste Dolbeau : (Travaille à 100% sur FaceCrypt)

- Accompli pour le moment : Chiffrement symétrique (test des algorithmes disponibles), mise en place d'un système client/serveur (SSL), modifications de ce système pour communiquer avec SoftCard et l'extension, création des certifications pour des authentifications bidirectionnelles entre les parties.
- Prochains objectifs : mettre en place la communication avec l'extension via des objets JSon.

Yicheng Gao : (Travaille à 100% sur le projet SmartCard)

- Accompli pour le moment : La mise en place de l'environnement de développement de JAVAcard, compiler et charger une applet Javacard sur une carte physique ainsi l"application cliente pour un simulateur et une vrais carte, les documentations d'applet Cypher
- Prochains objectifs : Test sur l'applet GenRadom pour les bits différents (en ce moment le test concerne 2 bits) et le compte-rendu complet.

Giovanni Huet : (Travaille à 50-50 entre SmartCard et SoftCard)

- Accompli pour le moment : développement d'une applet réalisant la signature/vérification, un jeu de test permettant de vérifier le bon fonctionnement et le temps requis :
  - du chiffrement rsa
  - du déchiffrement rsa
  - de la signature rsa
  - de la vérification correspondante
  - de la génération d'un nombre aléatoire
- Prochains objectifs : rédaction du cahier de recette (à vérifier et compléter)

Emmanuel Mocquet : (Travaille à 60% sur SoftCard et 40% sur SmartCard)

- Accompli pour le moment : manuel d'installation de l'environnement de developpement, classe Cypher permettant de chiffrer/déchiffrer et d'obtenir la clef publique, tunnel avec FaceCrypt.
- Prochains objectifs : mise à jour du manuel, intégration de SoftCard, administration, test sur le déverrouillage par code PIN (timing).

Maxence Péchoux : (Travaille à 95% sur l'extension et 5% sur FaceCrypt)

- Accompli pour le moment : création d'une extension firefox, modification du DOM avec JQuery, interception d'un Post (message de statut), insertion/récupération clef publique.intégration de l'extension finale (en cours).
- Prochains objectifs : Terminer l'intégration, créer FBExt qui dialogue avec la classe Tunnel, commenter et documenter le code.

Romain Pignard : (Travaille à 90% sur SmartCard et 10% sur SoftCard)

- Accompli pour le moment : applets echo (pour les tests), génération des nombres aléatoires, vérification de PIN, tunnel sécurisé (authentification, confidentialité et intégrité) entre la carte et le lecteur, développement de classe outils (concaténation, extraction IV, ...), un peu de test.
- Prochains objectifs : Intégration des applets avec SoftCard, test de performance et amélioration si possible, poursuite de la documentation.

Florian Guilbert : (Travaille à 50-50 entre FaceCrypt et l'extension)

- Accompli pour le moment : Sur FaceCrypt, développement de classes de chiffrement asymétrique, de hachage et une classe permettant de manipuler la base de données contenant la liste des amis. Création de cette même classe en JavaScript pour l'extension.
- Prochains objectifs : développer l'IHM de l'extension pour gérer les listes d'amis et étudier l'upload d'images sur Facebook.

Prochaine réunion

mercredi 20 février 10h