Manuel utilisateur

L'équipe SSN

1er mars 2013

Table des matières

1 Installation

Le projet est livré dans un paquet `tar.gz` à décompresser. Pour l'installation de la carte, il est d'abord nécessaire d'installer les librairies et programmes à utiliser en exécutant le script installSmartCard/lib/install.sh. Il est ensuite possible d'installer les applets sur la carte en lançant le script pkgSoftCard/install.sh. Exécutez ensuite SoftCard.jar du sous-dossier pkgSoftCard. Quant à Facecrypt, assurez vous d'avoir installé une machine virtuelle Java, puis placez-vous dans le sous-dossier pkgFaceCrypt, vous pourrez ainsi lancer le *daemon* FaceCryptServer.jar.

Pour installer l'extension, le fichier concerné est dans le sous-dossier pkgSSNExt et s'appelle ssnext.xpi. C'est en fait une archive dans laquelle toutes les sources sont organisées dans une structure compréhensible par Firefox. Vous disposez de deux choix : soit vous installez manuellement dans Firefox un fichier dans le gestionnaire d'add-on, soit vous lancez le fichier `xpi` directement avec firefox, qui l'installera automatiquement. Votre extension est maintenant prête à l'emploi.

2 Utilisation

Une fois les serveurs lancés, il suffit de lancer Firefox pour que tout soit prêt. En arrivant sur la page Facebook, il faut rentrer le code PIN de la carte depuis le terminal du serveur SoftCard. Dans le cas d'une première connexion, vous aurez alors à rentrer sur Firefox vos identifiants actuels dans une popup qui permettra d'initialiser la carte correctement. Dans les connexions suivantes les champs de login seront remplis automatiquement, toujours après avoir entré le code PIN, et vous n'aurez qu'à cliquer sur le bouton de connexion.

Une fois authentifié auprès de Facebook, il est conseillé d'utiliser la carte pour générer un nouveau mot de passe. Pour cela, accédez à la page de vos paramètres de compte et cliquez sur « modifier » pour la section du mot de passe. L'extension demandera automatiquement à la carte un nouveau mot de passe sûr, *via* Facecrypt, et SSNExt remplira les champs adéquats.

L'étape suivante consiste à publier votre clef publique sur votre profil pour que vos amis puissent la récupérer. Pour cela il suffit de cliquer sur le bouton « publier ma clef » sur votre journal d'évènements (page principale de Facebook où l'on voit les posts de nos amis). Si vous avez peu d'amis, vous n'arriverez pas sur la *timeline* car Facebook vous recommandera d'en trouver. Il faudra alors cliquer sur le logo Facebook en haut à gauche de la page afin d'y accéder. Dans ce cas vous devrez ensuite rafraîchir la page avec un F5 par exemple. Ceci est nécessaire pour ré-injecter les scripts dans la bonne page, car Facebook fonctionne majoritairement en Ajax, qui ne "recharge" pas les pages et donc pas nos scripts. Vous pouvez cliquer sur le bouton et publier votre clef.

Enfin la dernière étape d'initialisation importante est la synchronisation des clefs publiques de vos amis. Ceci va permettre à notre extension d'aller chercher sur les pages de vos amis toutes les clefs disponibles et les stocker en base. Il est conseillé de relancer cette commande de temps à autre dans le cas d'un changement éventuel de clef d'un ami. La seule action à effectuer pour cela est un clic sur le

bouton « Synchroniser les clefs ». Il faut ensuite rafraîchir la page pour que les popup de listes soient actualisés.

Pour chiffrer un message, vous devez bien sûr d'abord créer des listes d'amis. Un panneau est prévu à cet effet sur le côté gauche de la page, où un « Ajouter » est visible. Une fois le nom choisi, vous devez modifier la liste créée afin d'y ajouter les amis désirés. Vous pouvez à tout moment gérer ces listes via ce panneau.

Vous pouvez maintenant poster un message sur votre mur, en cliquant sur notre bouton « Chiffrer ». Une popup apparaîtra alors pour vous demander les listes auxquelles vous désirez donner l'accès. Les modes « non anonyme » et « anonyme » sont alors à choisir. Un chiffrement anonyme empêchera quiconque de savoir à qui est destiné le message, si ce n'est lui-même, mais les ressources demandées à la carte seront plus importantes. Le principipe inverse est appliqué pour le chiffrement non anonyme.

Il est également possible de chiffrer les commentaires *via* un bouton « Chiffrer » et grâce à la clef de message du post correspondant. Le commentaire ne sera alors lisible que par les destinataires du post d'origine.

Le déchiffrement des messages anonymes se feront par un clic sur le bouton « Déchiffrer » correspondant, qui déchiffrera également les commentaires de ce post. Pour les posts non anonymes, le déchiffrement sera fait automatiquement. Dans le cas où ces messages ne vous sont pas destinés, un message vous le notifiera.

2.1 Exceptions

De manière générale, si quelques éléments ne sont pas affichés alors qu'ils le devraient, pensez à rafraîchir la page, afin de réinjecter les scripts. Si les boutons ont perdu leur « look'n feel » Facebook, il faut vider le cache et les cookies de Firefox. Pour cela vous pouvez exécuter la commande CTRL+MAJ+SUPPR. Enfin, si des erreurs de chiffrement se produisent ou que vous n'arrivez pas à déchiffrer, pensez à vérifier l'état des serveurs, et relancez-les au besoin.

Bonne utilisation,

L'équipe SSN.