Faculté des Sciences de Limoges
DESS Sécurité de l'Information
Cryptographie

2002–2003

Travaux pratiques, séance 5

Exploration d'une carte Java

Installation du lecteur

1. — Récupérer l'archive `all-for-smartcards.tar.gz`.

```
$ su
# cd /usr/local
# tar -xzf <path>/all-for-smartcards.tar.gz
# cd pcsc
# cp -p etc/limoges-reader.conf /etc/reader.conf
# ln -s /usr/local/pcsc/sbin/pcscd /usr/local/sbin/pcscd
# ln -s /usr/local/pcsc/bin/sectok /usr/local/bin/sectok
# ln -s /usr/local/pcsc/bin/mksolo+ /usr/local/bin/mksolo+
# echo "/usr/local/pcsc/lib" >> /etc/ld.so.conf
# mv /usr/local/pcsc/lib/libc.so.5 /lib      % for mksolo
# mv /usr/local/pcsc/lib/ld-linux.so.1 /lib  % for mksolo
# ldconfig
```

2. — Brancher le lecteur de cartes sur le PC. Le connecteur série sert à transmettre les données. Le connecteur PS/2 à alimenter le lecteur. Editer le fichier `/etc/reader.conf` pour l'adapter au lecteur utilisé, ainsi qu'au port série sur lequel vous l'avez branché.

3. — Lancer le *daemon* `pcscd` à partir d'un shell root. Insérer une carte *Cyberflex Access 16k* dans le lecteur (recto du côté du logo Gemplus pour les lecteurs PC-410, et en haut pour les lecteurs Reflex 72). La lampe verte des lecteurs Gemplus doit devenir fixe.

Installation du kit Java de Sun

4. — Vous avez déjà (en principe) un kit Java, nommé Kaffe. Il n'a pas l'air compatible avec nos cartes Cyberflex. Donc, récupérez le fichier auto-extractible de Sun `j2sdk-1_3_1_06-linux-i586.bin`. Puis :

```
# chmod a+x j2sdk-1_3_1_06-linux-i586.bin
# cd /usr/local
# <chemin>/j2sdk-1_3_1_06-linux-i586.bin
```

Exploration

5. — Utiliser l'interpréteur de commandes `sectok`, pour explorer la carte. la première commande à utiliser est `reset`. Ensuite `ls -l` peut vous indiquer la mémoire disponible dans la carte (13506 octets) et les fichiers existants (dans une carte neuve, il y a un fichier `0011` de 58 octets contenant des clés, un fichier caché `0000` contenant deux PINs). Commande `quit` pour sortir.

6. — Compiler l'applet `secbdes.java` (une implémentation JavaCard de DES par Jim Rees) avec la commande

```
$ /usr/local/jdk-1_3_1_06/bin/javac -g -classpath /usr/local/pcsc/lib/access secbdes.java
```

Vous obtenez le fichier Java compilé `secbdes.class`.

7. — Préparer le fichier à charger dans la carte avec la commande `mksolo+ secbdes.class`. Vous obtenez le fichier `secbdes.bin`.

8. — Charger l'applet `secbdes.bin` dans la carte et lui donner le statut d'applet par défaut :

```
$ sectok
> login -d
> jload secbdes.bin
> reset
> fid sc
> jdefault
> reset
```

9. — Utiliser l'applet pour chiffrer/déchiffrer des blocs de 8 octets (ou des données plus longues, en mode CBC). La clé utilisée est `AUT2 = 3812a419c63be771`. La classe de l'applet est CLA=04, les instructions sont INS=0e pour chiffrer, INS=10 pour déchiffrer. Par exemple :

```
> apdu -c 04 0e 00 00 08 12 34 56 78 9a bc de f0
> apdu -c 04 10 00 00 08 61 78 22 61 aa d3 fc b4
```

10. — Changer la clé `AUT2` utilisée. C'est la troisième clé contenue dans le fichier `0011`, elle commence à l'octet 0x0020. La commande utilisée est `UpdateBinary` (CLA=00, INS=D6).

```
> login -d
> fid 3F00
> fid 0011
> apdu -c 00 d6 00 20 08 xx xx xx xx xx xx xx xx
```

Chiffrer/Déchiffrer avec la nouvelle clé.

Rangement

11. — Restaurer la clé `AUT2` initiale, désactiver l'applet et la supprimer de la carte.

```
> login -d
> fid 3F00
> fid 0011
> apdu -c 00 d6 00 20 08 38 12 a4 19 c6 3b e7 71
> jdefault -d
> reset
> junload sp
> quit
```

12. — Sous un shell root, faire `killall pcscd`. Vous pouvez débrancher le lecteur.