GPShell

Interpréteur de script pour communiquer avec les cartes à puces compatibles GlobalPlatform

Il utilise le plugin de connection PCSC pour accéder aux cartes à puces. Il peut établir un canal sécurisé avec une carte à puce, charger, instantier, supprimer et lister les applications sur les cartes supportées. Ces applications sont pratiquement toujors des applets JAVA.

Installer GPShell et GlobalPlatform

Ajouter dans /etc/apt/sources.list les entrées :
http ://ppa.launchpad.net/k-o-/globalplatform/ubuntu
http ://ppa.launchpad.net/k-o-/globalplatform/ubuntu
ou, pour compiler les sources :
aptitude install gcc libpcsclite-dev pkg-config zlib zlib1g-dev libcur14-openssl-dev make
wget http ://heanet.dl.sourceforge.net/sourceforge/globalplatform/globalplatform-6.0.0.tar.gz
tar xfvz globalplatform-6.0.0.tar.gz
cd globalplatform-6.0.0
./configure —prefix=/usr
make
make install
cd ..
wget http ://heanet.dl.sourceforge.net/sourceforge/globalplatform/gpshell-1.4.4.tar.gz
tar xfvz gpshell-1.4.4.tar.gz
cd gpshell-1.4.4
./configure —prefix=/usr
make
sudo make install
cd ..

Commandes

establish_context Établir le contexte, nécessaire avant d'établir une communication avec la carte.

card_connect -reader Connection à la carte dans le lecteur spécifié par son nom (-reader) ou son numéro (-readerNumber)

select -AID Sélectionner l'instance de l'applet

card_disconnect Déconnecter la carte

release_context Arrêter le contexte

mode_201 Sélectionne le mode OpenPlatform 2.0.1

mode_211 Sélectionne le mode globalPlatform 2.1.1

enable_trace Active le debug APDU

enable_timer Log le temps d'exécution d'une commande

open_sc -keyind x -keyver x -key xyz -mac_key xyz -enc_key xyz -kek_key xyz -security x -scp x -scpimpl x -keyDerivation x (mode_211) -scp et scpimpl ne sont pas nécessaires.

open_sc -keyind x -keyver x -mac_key xyz -enc_key xyz (mode_201)

Install -file appletFile -priv privilege -sdAID sdAID -AID AIDInPkg -pkgAID packageAID -instAID instanceAID -nvCodeLimit x -nv Installer une applet

install_for_load -pkgAID x -sdAID sdAID -nvCodeLimit x

load -file appletFile Charger une applet. A utiliser si la commande install ne fonctionne pas.

get_status -element e0 Liste les applets, packages et domaines de sécurité

get_status -element 20 Liste les packages

get_status -element 40 Liste les applets et les domaines de sécurité

get_status -element 80 Liste me gestionnaire de carte et les domaine fournisseur de sécurité

get_data -identifier identifier Retourne la donnée pour l'identifieur donné

put_sc_key -keyver 0 -newkeyver 2 -mac_key new_MAC_key -enc_key new_ENC_key -kek_key new_KEK_key -cur_kek current_KI
Ajouter un nouveau jeu de clé version 2

put_sc_key -keyver 1 -newkeyver 1 -mac_key new_MAC_key -enc_key new_ENC_key -kek_key new_KEK_key -cur_kek current_KI
Remplacer le jeu de clé version 1

put_dm_keys -keyver 0 -newkeyver 2 -file public_rsa_key_file -pass password -key new_receipt_generation_key Place les clés de gestion délégués en version 2 (mode_211)

put_dm_keys -keyver 0 -newkeyver 2 -file public_rsa_key_file -pass password -key new_receipt_generation_key -cur_kek current_KI
Place les clé de gestion délégués en version 2 (mode_201)

send_apdu -APDU x Envoyer un APDU

send_apdu -sc 0 -APDU x Envoyer un APDU sans canal sécurisé

send_apdu_nostop -APDU x Envoyer un APDU et ne stop pas en cas d'erreur

OPTIONS

-reader readerName Nom du lecteur de carte

-readerNumber x Numéro du lecteur de carte

-protocol x Protocole (0 : T=0 ; 1 : T=1)

-keyind x Index de clé

-keyver Version du jeu de clé

-newkeyver x Nouvelle version du jeu de clé

-key key Valeur de la clé en hexa

-mac_key key Clé MAC en hexa

-enc_key key Valeur de clé ENC en hexa

-kek_key key Valeur de clé KEK en hexa

-security x 0 : aucun, 1 :MAC, 3 :MAC+ENC

-scp x Protocol du canal sécurisé (1 SCP01, 2 SCP02)

-scpimpl x Implémentation du canal sécurisé (ne devrait pas être sopécifié implicitement)

-pass password Mot de passe pour le déchiffrement de la clé

-sc x mode canal sécurisé (0 off, 1 on)

-keyDerivation ('non', 'visa2', 'emvcps11')

-AID aid ID de l'applet

-sdAID aid AID du domaine sécurisé

-pkgAID aid AID du Package

-instAID aid AID de l'instance

-nvCodeLimit x Limite de taille du code non-volatile

-nvDataLimit x Limite de taille de donnée non-volatile

-vDataLimit x Limite de taille de donnée volatile

-file file Nom du fichier

-instParam param Paramètre d'installation

-priv x Privilège (ex : 0x04 Default Selected)

-element x Type d'élément à indexer en hexa

80 Card Manager / Card Issuer Security Domain only.

40 Applications (and Security Domains only in GP211).

20 Executable Load Files only.

10 Executable Load Files and their Executable Modules only (Only GP211)

-identifier Identifieur pour le tag pour la commande get_data (en hexa, ex : 9F7F)

-APDU apdu APDU à envoyer en hexa (ex : 80CA00CF00)

Variables d'environnement

GLOBALPLATFORM_DEBUG Active le mode debug depuis la librairie GlobalPlatform

GLOBALPLATFORM_LOGFILE Définis le fichier dans lequel écrire les logs

Installer une applet java sur une carte cyberflex 64k

```
mode_201
enable_trace
establish_context
card_connect
select -AID a000000003000000
open_sc -security 1 -keyind 0 -keyver 0 -mac_key 404142434445464748494a4b4c4d4e4f -enc_key
404142434445464748494a4b4c4d4e4f
delete -AID A0000003230101
delete -AID A00000032301
delete -AID A00000000101
delete -AID A000000001
install_for_load -pkgAID A000000001 -nvCodeLimit 13500 -sdAID A000000003000000
load -file CardEdgeCflex.ijc
install_for_install -instParam 00 -priv 02 -AID A00000000101 -pkgAID A000000001 -instAID A00000000101
-nvDataLimit 12000
card_disconnect
release_context
```

Ensuite il reste à intialiser le code pin à "00000000" :

opensc-tool -s 00 :A4 :04 :00 :06 :A0 :00 :00 :00 :01 :01 -s
B0 :2A :00 :00 :38 :08 :4D :75 :73 :63 :6C :65 :30 :30 :04 :01 :08 :30 :30 :30 :30 :30 :30 :30 :30 :08 :30 :30 :30 :30 :30 :30 :30 :30 :05 :02 :08 :30 :

Utiliser la carte avec opensc :

pkcs15-init -EC -p pkcs15+onepin