Retour page d'accueil site sur les failles des cartes bancaires

EXPLOREZ VOTRE CARTE BANCAIRE A PUCE : PAS BESOIN DU CODE SECRET A 4 CHIFFRES, LES BANQUES N'ONT JAMAIS EXPLOITE LES DISPOSITIFS DE SECURITE DE LA PUCE

Plan

Résumé

L'objectif de ce document est d'explorer une carte bancaire à puce.
Cela n'a rien de très compliqué et est abordable pour un budget de 400 francs environ (il faut disposer au minimum d'une carte bancaire à puce et d'un lecteur de carte à puce).
Cela peut être fait par quiconque un peu curieux arrivant à se débrouiller tout seul en informatique (ne comptez pas sur nous pour vous assister).
Ce n'est pas très long non plus (cette page est longue car toutes les étapes sont détaillées).
Cette page n'a pas pour objectif, et ne sert pas pour fabriquer des "Yescard", ce thème n'est pas abordé mais seulement l'observation objective d'une carte bancaire à des fins d'information, d'éducation : en effet, il s'agit principalement de démystifier la puce sur la carte bancaire, ce n'est pas parce qu'il y a une puce que c'est forcément sûr.
mais aussi d'interfaçage [lecture de l'historique des transaction, vérification de carte, ultérieurement mise au point d'une solution logicielle de paiement par carte (pas besoin de se conformer à la procédure d'agrément pour accepter les cartes bancaires car cette procédure de certification est illégale)].
Cependant, la simple observation de la carte bancaire permet de réduire à néant certains mythes bien tenaces répétés par des institutionnels doués pour la manipulation.
Notamment :
1. Le code secret à 4 chiffres ne sert pas pour l'authentification, il ne sert que pour insérer une transaction dans l'historique des transactions (ce qui est quasiment inutile)
2. Les cartes émises depuis novembre 1999 comportent 2 valeurs d'authentification : l'une de 320 bits créée à l'aide de la clé cassée révélée sur Internet le 04/03/2000, l'autre de 768 bits
3. Comme toutes les données servant à l'authentification sont situées dans des zones publiques accessibles sans le code, TOUTES les cartes bancaires à puce (même celles émises depuis novembre 1999) peuvent être recopiées à l'insu du porteur et retranscrites sur un émulateur dit "Yescard"
Ces 3 points constituent bien entendu des fautes lourdes de conception de la part des banques.
Elles sont d'autant moins excusable que ces failles subsistent depuis 1983 et que les banques étaient prévenues depuis au moins 1988 de leur existence, problème jamais corrigés depuis.
A cela s'ajoute un 4ème bug secondaire mais impardonable quand même car il génère déjà des litiges (des victimes se font débiter une somme en euro alors qu'elles croyaient effectuer une transaction en franc) :
4. L'historique des transactions ne contient que la date de la transaction donnée par le terminal de

Conclusion :
les banques n'ont exploité aucunes des sécurités de la puce :
Le code aurait dû servir à restreindre l'accès des secrets (la valeur d'authentification et l'identifiant composé du numéro de carte bancaire) aux seuls titulaires du code secret, mais ces secrets sont accessibles sans le code !
La puce peut faire des calculs cryptographiques complexes permettant de prouver qu'elle détient un secret sans le révéler, ce qui permet d'éviter les attaques par clonage de carte ou le rejeu. Cette possibilité de la puce n'a pas non plus été utilisée dans les cartes bancaires.

MATERIELS ET DOCUMENTS UTILISES POUR L'EXPERIENCE :

Pour les observations sur la carte bancaire, l'auteur de cette page a rassemblé les matériels suivants :

(note : le matériel réellement nécessaire est réduit)

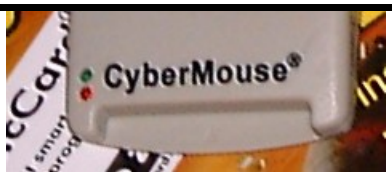
Le matériel utilisé pour l'expérience comprend donc

1. Kit BasicCard	Ce kit permet de programmer facilement des cartes à puce par exemple pour des projets d'identification, contrôle d'accès, porte-monnaie électronique, conservation de codes secrets... Son prix assez bas (650 francs), la facilité d'utilisation et la diversité des applications possibles le rend très attractifs. Les possibilités de programmation de ce kit n'ont pas été utilisées dans l'expérience décrite sur cette page : seul le lecteur cybermouse compris dans le kit a été utilisé Ce kit ne permet de programmer que des cartes asynchrones en mode T=1 (pour info, la carte bancaire est en mode T=0) Les cartes fournies supportent les algorithmes DES, triple DES, IDEA, courbes elliptiques, SHA-1 mais pas RSA (est annoncé pour mai 2001 des cartes programmables en T=0 ou T=1 supportant l'algorithme RSA).
2. Applied Cryptography	Livre sur les techniques de cryptographie, permet de comprendre l'algorithme RSA, mais il existe des livres plus simples. Pour la carte bancaire, il n'y a pas besoin de ce gros livre puisque l'algorithme d'authentification est décrit dans cet article de 1988 publié par Louis Claude Guillou et Professeur Jean-Jacques Quisquater et Marc Davio (Philips) dans le numéro 43 des annales des télécommunications.
3. Lecteur XiPuce de Xiring	Ce lecteur de carte à puce de poche permet de lire le solde d'une télécarte, les informations d'une carte vitale ou l'historique d'une carte bancaire à puce. Il sert ici pour vérifier et comparer les inscriptions dans l'historique des transactions entre ce qui est lu sur la puce à l'aide du lecteur Cybermouse. Accessoirement, il peut servir pour entrer un code bon après des manipulations hasardeuses (au bout de 3 code faux consécutifs, la carte est bloquée, si vous avez fait une fausse manipulation avec le lecteur cybermouse et craignez d'avoir présenté un code faux, vous pouvez rentrer la carte bancaire dans le lecteur XiPuce et entrer le bon code puis continuer vos expériences sans risquer de bloquer la carte.
4. Livre PC et Cartes à Puce	Ce livre écrit en 1995 par Patrick Gueulle aux éditions Dunod, collection ETSF décrit les cartes à puce, comment faire un lecteur de carte, comment émuler une carte à puce... Pratiquement la moitié du livre est consacrée à la découverte de la carte bancaire. Une disquette avec des programmes d'exploration de la carte bancaire et de consultation de l'historique des transactions est fourni. Ces programmes sont un peu obsolètes (écrits en GWBasic) mais les sources sont utiles. Cette page a été principalement conçue à partir des informations glanées dans ce livre.

	couverture) sur amazon.fr. Cette page n'a été conçue par Patrick Gueulle mais par Laurent PELE
5. Maple V édition Etudiant	Ce logiciel de calcul mathématique grand public est disponible au prix de 500 francs environ à la Fnac. Il permet de faire des calculs sur les grands nombres comme fait pour la vérification de carte bancaire (la carte bancaire ne fait pas de calcul RSA mais les terminaux de paiements en font). Voir la "petite feuille Maple" démontrant la révélation du secret de la carte bancaire
6. Carte bancaire expirée	Pour commencer l'exploration d'une carte bancaire à puce, une carte bancaire expirée a été utilisée, ce qui permet de prendre moins de risque de griller une carte bancaire récente. Ici une carte expirée en septembre 1998 a été utilisée. Seul problème : à cette époque, les puces n'étaient pas placées au même endroit : elles étaient plus situées sur le côté (la norme a évolué depuis). Comme le lecteur Cybermouse ne lit pas les puces situées à cet endroit, il a fallu découper la carte avec des ciseaux autour de la puce (cela détruit la piste magnétique située derrière), la RETOURNER (le côté de la puce qui était près du bord devient près du centre), puis l'insérer dans un support au bon emplacement. Le support utilisé ici est un carte plastique SIM ISO (de téléphone GSM) qui contenait une puce au format mini SIM. Pour fixer la puce au support, du ruban adhésif ("scotch") a été mis au dos de la carte. Ensuite il suffit d'insérer la carte dans le lecteur XiPuce pour voir si on arrive à la lire et si la puce a été mise à la bonne position. Cette manipulation n'est heureusement pas à faire avec les cartes bancaires actuelles. Note : vous ne devez utiliser que des cartes dont vous êtes le légitime porteur.
7. Carte bancaire actuelle	Prenez votre carte bancaire actuelle pour vérifier la persistance des failles de sécurité Ici nous avons utilisé des cartes émises à partir de novembre 1999 Note : vous ne devez utiliser que des cartes dont vous êtes le légitime porteur.

MATERIELS ET DOCUMENTS NECESSAIRES :

Il n'y a besoin que du lecteur de carte à puce, un logiciel de lecture de puce et une carte bancaire à puce non grillée pour réaliser l'expérience.
L'expérience a été faite ici à l'aide d'un lecteur Cybermouse ACR 20S sur port série présent dans le kit de vévelopppement pour carte à puce Basiccard, le lecteur est disponible séparément sur site Cybermouse (prix de 30$ + port) mais d'autres lecteurs de carte à puce peuvent convenir car il existe des normes ISO 7816 de dialogue avec les cartes à puce.
L'expérience a été faite avec le logiciel CardEasy version 2.3 qui peut se télécharger ici (avec DLL pour lecteur Cybermouse ACR20S sur port série, il a été testé sous Win98 et Win2000)
[il existe aussi le programme ACS20ev.zip sous DOS pour envoyer des commandes ISO à la carte sur cette page du constructeur,
note 1 : le logiciel CardEasy.zip de la page du constructeur est incomplet, il faut aussi les utiliser DLL correspondant au lecteur dans le fichier SDK ACSR20.zip
note 2 : si votre navigateur vous demande si vous voulez installer les caractères chinois, vous pouvez lui répondre NON].
L'expérience peut donc être faite pour un coût très modique : 30 $ plus frais de port mais vous pouvez également bricoler un lecteur de carte à puce si vous bidouillez en électronique.



Un lecteur de carte à puce (prix 350 F) est le seul matériel nécessaire pour l'expérience (avec une carte bancaire).

JEU DE COMMANDE ET MAPPING CARTE BANCAIRE :

JEU D'INSTRUCTIONS :

La classe ISO de la puce Bull CP8 (ce masque équipe les cartes bancaires et les cartes France Télécom anciennement Pastel, la carte FT utilise le même système d'authentification que la carte bancaire avec des clés de 320 bits, par contre la clé publique RSA diffère sûrement de celle de la carte bancaire qui a été cassée) est BC en hexadécimal.
Les cartes EMV auront normalement une classe ISO 80 en hexa.
D'après le livre "PC et Cartes à Puce" de Patrick Gueulle (édité en 1995), le type de la carte bancaire est 3F E5, stocké en 09E0, la carte bancaire admet le jeu d'instruction suivant :

Instruction (Hexa)	**Description ordre**
0E	Effacement
10	Présentation de la clé banque (dite "CB") (en clair)
20	Présentation du code confidentiel (dit "CC") ou du code de déblocage de la carte (en clair)
30	Présentation de la clé d'ouverture (CO) (en clair)
40	Validation de lecture
50	Ecriture de verrou
70	Validation d'écriture
80	Certification avec 1er jeu secret
82	Certification avec 2ème jeu secret
84	Certification avec 3ème jeu secret
86	Certification avec 4ème jeu secret
88	Certification avec 5ème jeu secret
A0	Recherche du premier mot vierge ou sur argument
A8	Recherche du premier mot non vierge
B0	Lecture d'octets
C0	Lecture de résultat
D0	Ecriture d'un mot
D2	Changement code porteur

Bien entendu, ces instructions sont à utiliser avec précaution (surtout celle d'effacement) on peut noter également que les instructions du masque B0' 18h , 28h et 38h permettant de présenter des clés sous forme chiffrée n'est pas utilisée non plus : les codes à 4 chiffres sont échangés en clair entre la carte et le lecteur.

MAPPING DE LA CARTE BANCAIRE :

ADC	Zone confidentielle (effacement intedit, lecture protégée, écriture interdite) ou zone de travail n°2 (l'application définit les droits d'accès à cette zone)
ADT	Zone de travail n°1 (l'application définit les droits d'accès à cette zone)
ADL	Zone de lecture (effacement intedit, lecture libre, écriture interdite)
ADMAX-8h	Zone de fabrication (effacement intedit, lecture libre, écriture interdite sauf verrou)

La description des zones mémoires correspond à celle d'une carte bancaire émise avant novembre 1999.
A titre indicatif, le livre de Patick Gueulle donnait la cartographie suivante (pour une vieille puce bancaire) :
ADL en 08E0h (zone de lecture libre à partir de cette adresse, il faut le code confidentiel pour lire dans la zone située avant).
ADM en 0290h
ADC et ADT en 02B0h
AD2 en 0278h
AD1 en 0210h
ADS en 0230h
Prestataire 03 :
à l'adresse ADL (08E0), se trouve le "prestataire 03" correspondant à la valeur d'authentification codée sur 320 bits avec l'entête suivant :
08E0 : 2E 03 30 33
Le 3ème octet 30h représente la taille en octets : le prestataire 03 a donc une taille 48 octets (30h= 48 en décimal). Cela correspond à 320 bits car il y a des quartets avec des "3" de redondance tous les 4 octets.
La clé de la valeur d'authentification est codée à partir de 08F0
Prestataire 02 :
à l'adresse 0948, se trouve le "prestataire 02" correspondant à l'identifiant de la carte, elle contient le numéro de la carte, les dates de validité, le nom du porteur, la devise. ce sont des données a valeur d'authentification codée sur 320 bits avec l'entête suivant :
0948 : 2E 02 38 F1
Le 3ème octet (38h) indique que cette zone a une taile de 56 octets.
Ensuite on a un 3 , un code enregistrement 00 le numéro de carte sur 19 caractères BCD, le code usage (7FF), le code service (101), la date de début de validité sur 4 caractères BCD, la langue (250 pour le français), la fin de validité sur 4 caractères BCD, la devise (franc : 250), l'exposant

EXPLORATION SUR UNE VIEILLE CARTE EXPIREE :

Intérêt :

Faire une expérimentation sur une carte périmée permet de s'initier sans trop de risque à la découverte de la puce de la carte bancaire sans prendre le risque de griller sa carte actuelle.
Si vous préférez vous pouvez cependant faire directement l'expérience sur une carte bancaire à puce récente.
En effet, la puce des cartes bancaires périmées restent lisibles et on peut lire l'historique des transactions, même si on ne peut pas théoriquement faire de paiement dans les terminaux de paiements avec (cela reste cependant facilement possible en rusant, voir aussi ici).
Pour faire cette manipulation, l'auteur a utilisé une vieille carte arrivée à expiration en septembre 1998.
Il s'agit surtout de vérifier que les indications fournies dans le livre "PC et Cartes à Puce" de Patrick Gueulle sont exactes et de s'initier à la manipulation des cartes à puce sans prendre trop de risque puisque la carte est expirée.

Préparation :

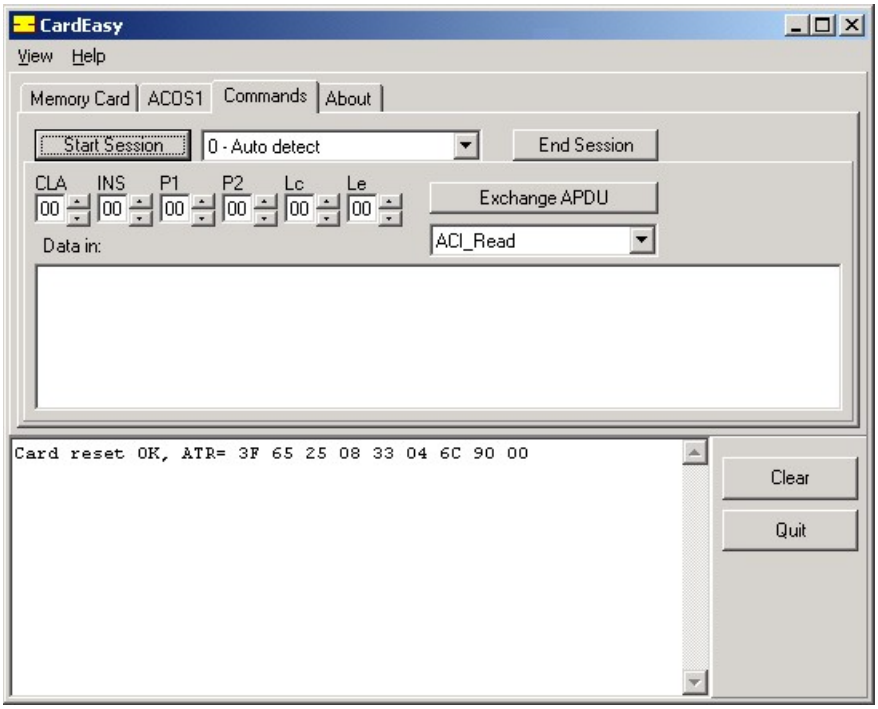
port série (vous pouvez utilisez celle d'un autre ordinateur allumé)).
On prépare une carte bancaire expirée, éventuellement après avoir déplacé et retourné la puce comme expliqué précédemment s'il s'agit d'une très vieille carte avec une puce située au dessus de la piste magnétique (et non en position dite "centrée").
On installe le logiciel CardEasy et on le lance, il détecte automatiquement le port (COM1 ou COM2 généralement) où est installé le lecteur de carte à puce.

La puce de la carte bancaire expirée découpée prête à être insérée dans le lecteur de carte

Note : il n'y a pas besoin d'installer le kit BasicCard pour faire la manipulation décrite dans cette page.
On introduit la puce de la carte bancaire dans le lecteur.
Dans le logiciel CardEasy, on choisit l'onglet "Commands", il n'y a pas besoin de changer le type de carte (le laisser à 0 -Auto Detect).
Maintenant on va pouvoir commencer à lire la puce.

Réponse au reset de la puce :

Pour initialiser la puce on lance la commande Reset sur le logiciel CardEasy.
Cela correspond au bouton "Start Session" dans l'onglet "Commands"
Le résultat suivant s'affiche :



CardEasy affiche après une réponse au reset "Card reset OK, ATR= 3F 65 25 08 33 04 6C 90 00 "

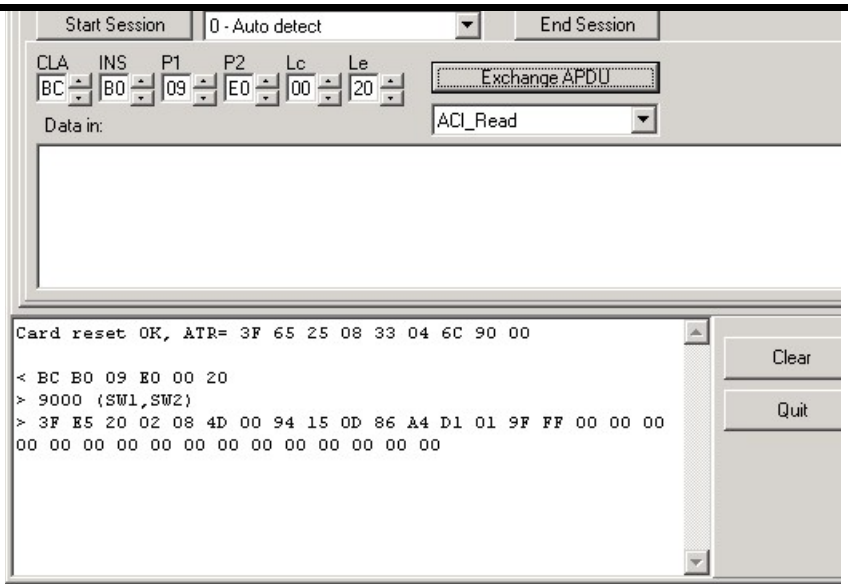
De son côté les 2 voyants vert et rouge du lecteur Cybermouse se sont allumés

Cela semble assez encourageant, cela marche, on arrive à envoyer des commandes à la carte et elle répond (fenêtre du bas de CardEasy), et il faut moins de 5 minutes pour installer le lecteur de carte et le logiciel CardEasy, les 2 derniers octets sont 90 00, ce qui signifie que la commande ISO s'est déroulée correctement.

Première lecture zone libre de la puce :

Maintenant on va lire une zone libre de la carte bancaire expirée, on lit par exemple 32 octets à partir de l'adresse 09 E0. Cela correspond aux valeurs suivantes à saisir dans la fenêtre de commande ISO envoyée à la carte (voir image suivante) :
Classe (CLA) : BC
Instruction (INS) : B0
Paramètre P1 : 09
Paramètre P2 : E0
Nombre d'octets lus (Le) : 20 (20h en hexadécimal est égal à 32 en décimal).

On appuie sur le bouton "Exchange ADPU" pour envoyer la commande à la carte et on obtient le résultat suivant dans la fenêtre du bas.



Lecture de la carte à 09E0 : la carte répond "3F E5 20 02 08 4D 00 94 15 0D 86 A4 D1 01 9F FF"

La fenêtre du bas affiche
< BC B0 09 E0 00 20 ce qui correspond à la commande envoyée à la carte (selon la convention de CardEasy)
puis
> 9000 (SW1,SW2) c'est le statut de la réponse de la carte, 90 00 signifie qu'il n'y a pas d'erreur.
Enfin
> 3F E5 20 02 08 4D 00 94 15 0D 86 A4 D1 01 9F FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3F E5 correspond bien au type de la carte bancaire stocké en 09 E0 d'après le livre de Patrick Gueulle.
On a ainsi réussi à lire une partie de la carte (ici une partie de la zone de lecture et de la zone de fabrication)
Vous noterez que le 16 derniers octets renvoyés sont nuls, c'est parce que l'adresse 09 E0 est une adresse exprimée en quartets et la dernière adresse lisible est 09FF, on ne peut pas lire après car il n'y a rien.
Il n'y a donc que 16 octets entre les adresses 09 E0 et 09 FF, or nous avons demandé à lire 32 octets
Comme la zone d'adresse de la carte bancaire commence en 0200, il n'y a donc qu'un kilo-octets de stockage sur cette carte.
Les autres octets après 3F E5 (aux adresses à partir de 09 E4) sont expliqués dans le livre de Patrick Gueulle.

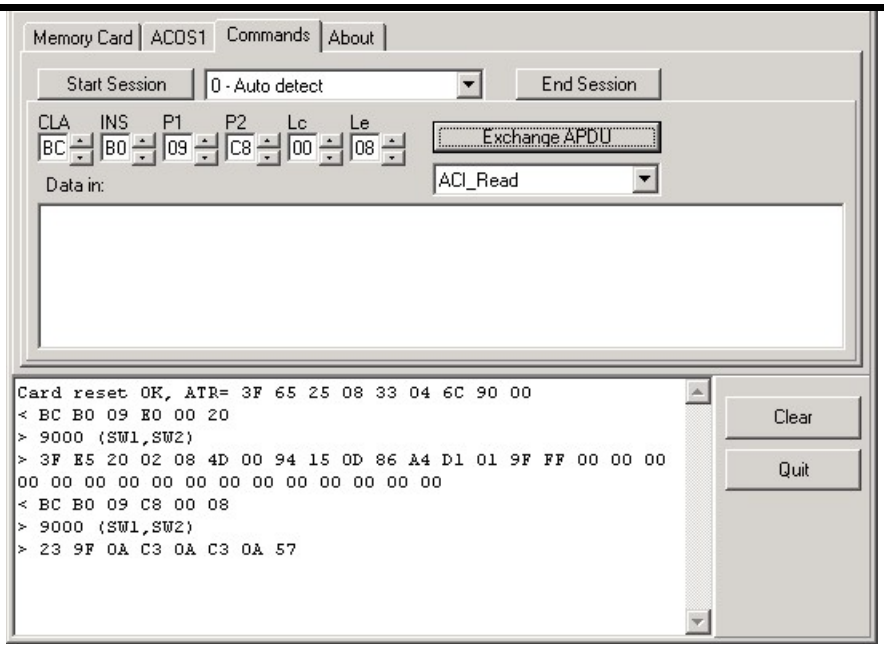
Lecture zone d'adressage en 09 C0 :

Sur les cartes Bull CP8, se trouve à partir de l'adresse 09 C0 le début de la zone d'adressage donnant les adresses de début de chacunes des zones de la carte, à savoir ADL, ADS, ADT, AD1, AD2, ADM.
Pour lire ces adresses, il faut répéter des manipulations au niveau des bits, si cela vous gonfle, passez au paragraphe suivant en vous contentant des résultats des recherches (cette étape n'est pas essentielle).

Lecture ADL, début zone lecture :

ADL (adresse de début de la zone de lecture libre) est défini en 09C8 et se retrouve de la façon suivante :
Cela correspond aux valeurs suivantes à saisir dans la fenêtre de commande ISO envoyée à la carte (voir image suivante) :
Classe (CLA) : BC
Instruction (INS) : B0
Paramètre P1 : 09
Paramètre P2 : C8
Nombre d'octets lus (Le) : 08

On appuie sur le bouton "Exchange ADPU" pour envoyer la commande à la carte et on obtient le résultat suivant dans la



Lecture 8 octets en 09C8

on lit ainsi sur cette carte en 09C8 : 23 9F 0A C3 0A C3 0A 57 11 premiers bits en 09C8 :
00100011100
on multiplie par 8 (soit ajout de 3 bits à 0) :
00100011100000
soit
00 1000 1110 0000
soit 0 8 E 0 en hexadécimal
on a donc ADL =08E0
C'est la même valeur que donne le livre de Patrick Gueulle.

Lecture ADT, début zone travail :

ADT est défini en 09CC :
on lit sur la carte en 09CC : 0A C3
0000 1010 1100 0011
11 premiers bits :
00001010110
on multiplie par 8 :
00001010110000
soit
00 0010 1011 0000
0 2 B 0 ADT ok
On a ADT = 02 B0

Lecture ADC, début zone confidentielle :

ADC est défini en 09D0 :
< BC B0 09 D0 00 20
> 9000 (SW1,SW2)
> 0A C3 0A 57 09 F1 08 D9 3F E5 20 02 08 4D 00 94 15 0D 86 A4 D1 01 9F FF 00 00 00 00 00 00
00 00
soit en binaire :
0000 1010 1100 0011
11 premiers bits :
0000 1010 110

0 2 B 0 ADC OK
On a ADC = 02 B0 (égal à ADT, en fait c'est une zone de travail à cette adresse, elle contient l'historique des transactions)

Lecture ADM, début zone d'accès :

ADM est défini en 09D4 :
on lit sur la carte en 09D4 : 0A 57
soit en binaire :
0000 1010 0101 0777
11 premiers bits :
0000 1010 010
ajout 3 bits à 0:
00001010010000
soit
00 0010 1001 0000
soit
0 2 9 0
d'où ADM = 0290

Lecture AD2, début zone de travail 2 :

AD2 est défini en 09D8 :
on lit sur la carte en 09D8 : 09 F1
soit en binaire :
0000 1001 1111 0001
11 premiers bits :
0000 1001 111
ajout 3 bits à 0:
00001001111000
soit
00 0010 0111 1000
soit
0 2 7 8
d'où AD2 = 0278

Lecture ADS, début zone secrète :

ADS est défini en 09DC :
on lit sur la carte en 09DC : 08 D9
soit en binaire :
0000 1000 1101 1001
11 premiers bits :
0000 1000 110
ajout 3 bits à 0:
00001000110000
soit
00 0010 0011 0000
soit
0 2 3 0
d'où ADS = 0230

Lecture AD1, début zone de travail 1 :

AD1 est défini en 09E8 :
on lit sur la carte en 09E : 08 4D
soit en binaire :
0000 1000 0100 1101
11 premiers bits :
0000 1000 010
ajout 3 bits à 0:
00001000010000
soit

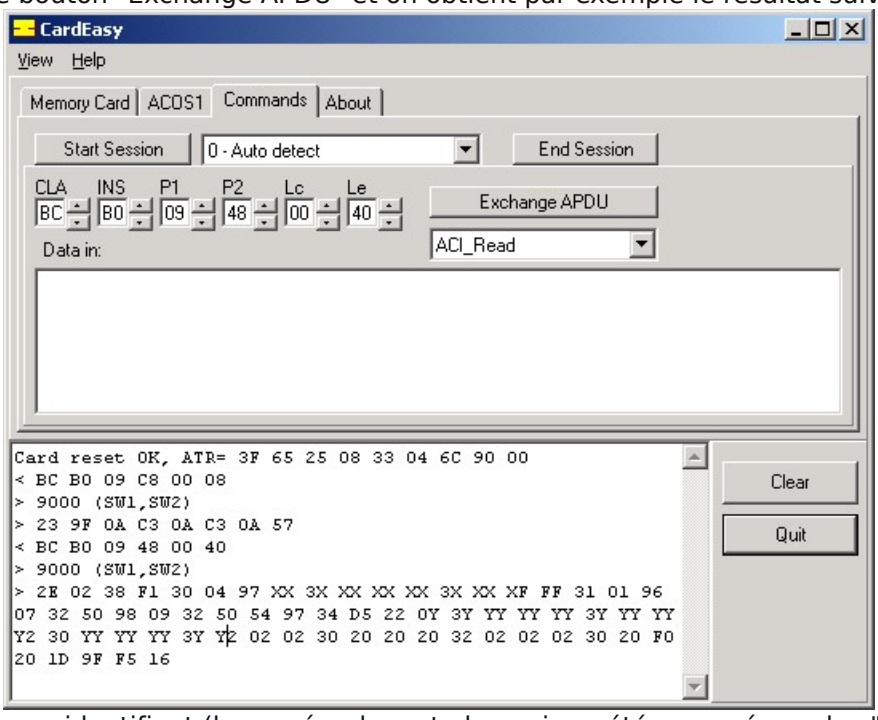
Conclusion lecture zone d'adressage :

On trouve pour cette carte ayant une date d'expiration 09/98 les mêmes valeurs que dans le livre de Patrick Gueulle :

ADL	08E0
ADT	02B0
ADC	02B0
ADM	0290
AD2	0278
ADS	0230
AD1	0210

Lecture zone identifiant de la puce :

Fort de cette expérience réussie, nous allons continuer l'exploration de la carte en regardant la zone identifiant du prestataire 02 supposée stockée à partir de 09 48 sur notre carte expirée et commençant par l'entête 2E 02
Cela correspond aux valeurs suivantes à saisir dans la fenêtre de commande ISO envoyée à la carte (voir image suivante) :
Classe (CLA) : BC
Instruction (INS) : B0
Paramètre P1 : 09
Paramètre P2 : 48
Nombre d'octets lus (Le) : 40 (40h en hexadécimal est égal à 64 en décimal).
On appuie sur le bouton "Exchange APDU" et on obtient par exemple le résultat suivant :



Lecture de la zone identifiant (le numéro de carte bancaire a été masqué par des "X", le nom du porteur a été masqué par un "Y")

La fenêtre du bas affiche donc les résultats suivants :
< BC B0 09 48 00 40
> 9000 (SW1,SW2)

à dire tous les 4 octets, il convient d'ignorer ces quartets avec des "3" pour analyser la chaine convenablement.
La chaine initiale 30 04 97 XX 3X XX XX XX 3X XX XF FF 31 01 96 07 32 50 98 09 32 50 54 97 34 D5 22 0Y 3Y YY YY YY 3Y YY YY Y2 30 YY YY YY 3Y Y2 02 02 30 20 20 20 32 02 02 02 30 20 F0 20 1D 9F F5 16
devient donc, après suppression des 3 de redondance tous les 4 octets :
0 04 97 XX X XX XX XX X XX XF FF 1 01 96 07 2 50 98 09 2 50 54 97 4 D5 22 0Y Y YY YY YY Y YY YY Y2 0 YY YY YY Y Y2 02 02 0 20 20 20 2 02 02 02 0 20 F0 20 1D 9F F5 16
Maintenant en groupant par octets :
00 49 7X XX XX XX XX XX XX FF F1 01 96 07 25 09 80 92 50 54 97 4D 52 20 YY YY YY YY YY YY YY 20 YY YY YY YY 20 20 20 20 20 20 20 20 20 20 F0 20 1D 9F F5 16
On reconnait, au début après l'octet 00, le numéro à 16 chiffres 497X XXXX XXXX XXXX gravé sur la carte bancaire, il est tout simplement codé sur la puce en BCD (Binaire codé décimal)
Ensuite suivent 3 "F", car le numéro de carte pourrait passer sur 19 caractères.
Puis il y a 3 quartets codés en BCD avec 101 correspondant au code usage (aussi appelé code service),
Suit ensuite la date de début de validité sur 2 octets codés en BCD : 96 07 soit juillet 1996, c'est la date d'émission de la carte
Suit ensuite 3 quartets codés en BCD 250 qui représente le code langue (250 = français)
Suit ensuite 2 octets codés en BCD correspondant à la date de fin de validité de la carte : 98 09, la date d'expiration indiquée sur la carte est bien septembre 1998.
Suit ensuite 3 quartets codés en décimal codés binaire avec le code devise ici 250, cela correspond au code numérique ISO du franc français.
Suit ensuite 1 quartet 5 qui correspond à l'exposant. 5 signifie unité, 3 signifie centième. Cela indique comment sont stockés les montants dans l'historique des transactions.
Comme sur cette carte il y a un 5, les décimales ne sont pas stockées dans l'historique des transactions :
si un paiement de 133.33 francs est effectué, seul 133 apparaîtra dans l'historique des transactions.
Ensuite suit 3 quartets 497
Ensuite suit une longue chaine de 26 caractères ASCII stockée à partir de l'adresse 0980 qui vaut comme vu plus haut (après suppression des "3" de redondance tous les 8 quartets) :
4D 52 20 YY YY YY YY YY YY YY YY YY YY YY 20 20 20 20 20 20 20 20 20 20
C'est l'identité du porteur stockée en ASCII
ainsi le code hexa 4D correspond à 77 en décimal et au code ascii de "M" [vous pouvez le voir avec l'utilitaire Charmap.exe de Windows ou en ouvrant un éditeur de texte (tel que le Bloc Note), vous appuyez sur la touche ALT de votre clavier et sans la relâcher, vous tapez sur les chiffres 0 puis 6 puis 9 puis relâchez la touche ALT, un M devrait apparaître)
52h correspond à la lettre "R" et le code 20h à l'espace
On arrive ainsi à lire le nom du porteur : "MR " suivi du prénom du porteur, d'un espace et du nom du porteur de la carte.
On a donc réussi à lire avec succès toute la zone identifiant de la carte bancaire à puce expirée et comprendre la signification des données qui y sont stockées.

Lecture zone Valeur d'authentification de la puce :

Maintenant on va lire la valeur d'authentification de la puce (prestataire 03) de la carte bancaire expirée qui commence selon le livre de Patrick Gueulle en 08E0 (égale aussi à l'adresse ADL) et commence par l'entête 2E 03
Une lecture avec CardEasy de 16 octets en 08 E0 nous donne :
< BC B0 08 E0 00 10
> 9000 (SW1,SW2)
> 2E 03 30 33 30 00 03 90 37 83 46 D4 3A CC B5 E6
On trouve bien l'entête 2E 03 avec une taille de 30h soit 48 octets.
Pour avoir la valeur d'authentification en entier, il suffit donc de lire 48 octets à partir de l'adresse 08 E8:
La fenêtre du bas de CardEasy affiche :
< BC B0 08 E8 00 30
> 9000 (SW1,SW2)

Vérification Valeur d'authentification de la puce :

On va maintenant vérifier l'authenticité de la carte bancaire expirée en faisant des calculs cryptographiques, par exemple à l'aide du logiciel de calcul Maple.
En supprimant les quartets de "3" tous les 4 octets de la valeur d'authentificaiton obtenue précédemment, on a :
0 00 03 90 7 83 46 D4 A CC B5 E6 X XX XX XX X XX XX XX X XX XX XX X XX XX XX X XX XX XX X XX XX XX X XX XX XX X XX XX XX X XX XX XX
sans les espaces :
000039078346D4ACCB5E6XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
On remarque que cette valeur d'authentification fait bien 320 bits codée en hexadécimal.
Dans Maple, on ouvre une nouvelle feuille.
on rentre dans Maple :
> produit :=
2135987035920910082395022704999628797051095341826417406442524165008583957746445
(ce produit de 321 bits (aussi appelé clé publique) provient notamment du [Message de "mail" du 04/03/2000](#))
Ensuite on rentre dans Maple la valeur d'authentification >
VA_LP0998:=convert(`000039078346D4ACCB5E6XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
decimal, hex);
Maple affiche l'équivalent en décimal de la Valeur d'authentification.
Ensuite on demande à Maple d'élever cette valeur d'authentification au cube modulo le produit de la clé publique RSA :
>exp_3_VA_LP0998:=VA_LP0998 &^ 3 mod produit;

Maintenant on convertit en hexa dans Maple :
> hex_exp3_VA_LP0998:=convert(exp_3_VA_LP0998, hex, decimal);
On voit s'afficher dans Maple comme résultat :
hex_exp3_VA_Laposte0998 :=
10A00000497XXXXXXXXXXXXFFF109607980900010A00000497XXXXXXXXXXXXFFF1096079809
(Note : le numéro de carte bancaire a été masqué).
On peut voir l'identifiant du prestataire 02 "497XXXXXXXXXXXXFFF1096079809" qui est dupliqué 2 fois. Cet identifiant contient bien le numéro de carte bancaire 497XXXXXXXXXXXX.
En effet, comme expliqué dans ce document de [1988](#) (publié par [Louis Claude Guillou](#) dans le numéro 43 des annales des télécommunications) , en élevant au cube la valeur d'authentification, on peut voir une redondance d'un motif de 160 bits composé de l'identifiant (numéro de carte, date de début de validité et date d'expiration).
Nous avons donc vérifié que cette carte bancaire est réputée émaner de l'autorité bancaire. Celui qui a créé cette carte est supposé connaître la clé secrète associée à la clé publique.
Cependant cette clé n'est plus du tout secrète puisqu'elle a été révélée le 04/03/2000 et il est maintenant possible d'inverser ce calcul et de voir apparaître que le dit Louis Claude Guillou dans cet article de [1988](#), des "simulacres de carte bancaires" créés par des fraudeurs mais reconnus par les terminaux de paiement comme émanant de l'autorité bancaire.
A noter que, outre l'identifiant du prestataire 02, on peut voir 3 quartets "10A" dans la valeur hex_exp3_VA_Laposte0998, ces 3 quartets dépendent de la carte, ces 3 quartets ne sont pas très importants, ils permettent de faire en sorte que la Valeur d'authentification ait 320 bits et non 321 bits (taille du produit).
Ces informations identifiant (prestataire 02) et valeur d'authentification (prestataire 03) en lecture libre suffisent pour authentifier la carte bancaire. Pourquoi sont elles en lecture libre alors qu'elles permmettent à n'importe qui de faire des émulations de carte bancaire ?
En conclusion de cette section, nous avons vérifié l'authenticité de la carte bancaire, vérifié la signification de cette valeur d'authentification stockée dans le prestataire 03. et vous noterez que nous n'avons toujours pas rentré le code secret !

De plus, [En substituant la puce par une autre puce dont on connait le code secret au cours de l'authentification par un](#)

Préparation lecture zone protégée de la puce

Maintenant nous allons lire la zone de la mémoire de la puce de la carte bancaire protégée par un code secret.
Ces informations "ultra-confidentielles" (puisque protégées par un code secret à 4 chiffres) sont tout simplement l'historique des transactions de paiement effectuées avec la puce chez un commerçant.
Non ne cherchez pas, il n'y a rien d'autre d'intéressant dans cette zone.
On va quand même lire la zone, elle commence à l'adresse ADT (02B0) et va jusqu'à 08DF (ADL-1).
Mais pour lire cette zone, il faut d'abord présenter le code secret.
Pour cela il faut présenter de façon spéciale le code secret :
Supposons que le code secret soit 1515 (ce qui n'est pas le cas sur les cartes testées) il faut envoyer la séquence de 4 octets 05 45 7F FF à la carte.
Pour obtenir cette séquence de 4 octets, est fourni dans cette page un logiciel de codage/décodage.
On rentre 1515 dans le champ "Code secret à 4 chiffres" et on appuie sur le champ "Codage -->", la séquence en héxadécimal à présenter à la puce (05 45 7F FF pour 1515 comme code PIN) apparait alors dans le champ suivant.

Logiciel de codage/décodage code secret envoyé à la puce :

Pour convertir un code secret en séquence hexadécimal, il suffit de renter le code secret à 4 chiffres dans le 1er champ suivant et d'appuyer sur le bouton "Codage -->"
Ce logiciel est assez simple, il est a été conçu à partir des explications du livre de Patrick Gueulle (qui fourni un autre logiciel avec des fonctions analogues), ceux qui veulent comprendre comment il fonctionne n'ont qu'à examiner le source de la page.

Code secret à 4 chiffres :

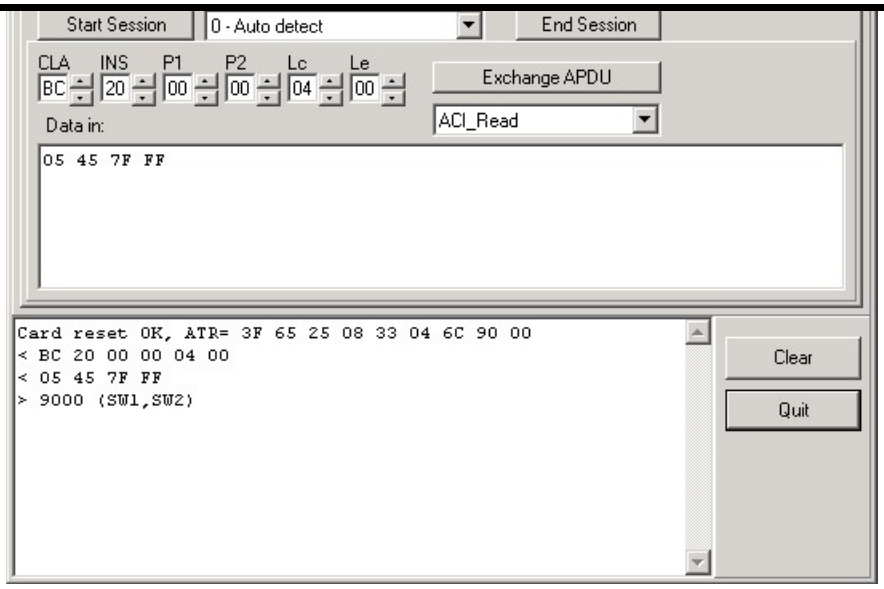
Codage --> Décodage <--

Séquence en héxadécimal à présenter à la puce :

A utiliser à des fins éducatives exclusivement. Bien entendu les codes ne sont pas échangés sur le réseau (attention tout de même aux yeux indiscrets derrière vous).

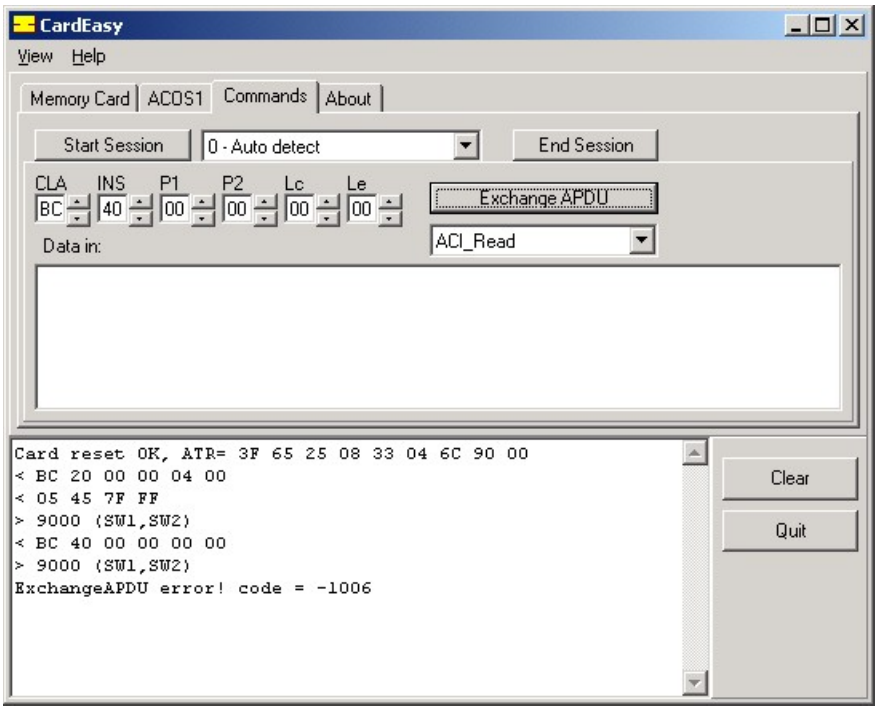
Lecture zone historique de la carte bancaire :

Pour lire proprement dit cette zone protégée de la carte bancaire, on envoie d'abord une commande de présentation du code à la carte.
Cela correspond aux valeurs suivantes à saisir dans la fenêtre de commande ISO envoyée à la carte (voir image suivante) :
Classe (CLA) : BC
Instruction (INS) : 20
Paramètre P1 : 00
Paramètre P2 : 00
Nombre d'octets envoyés (Lc) : 04
Nombre d'octets lus (Le) : 00
Data in : 05 45 7F FF (cela correspond au code secret 1515 qui ne correspond à aucune carte testée)
On appuie sur le bouton Exchange ADPU et on obtient le résultat suivant :



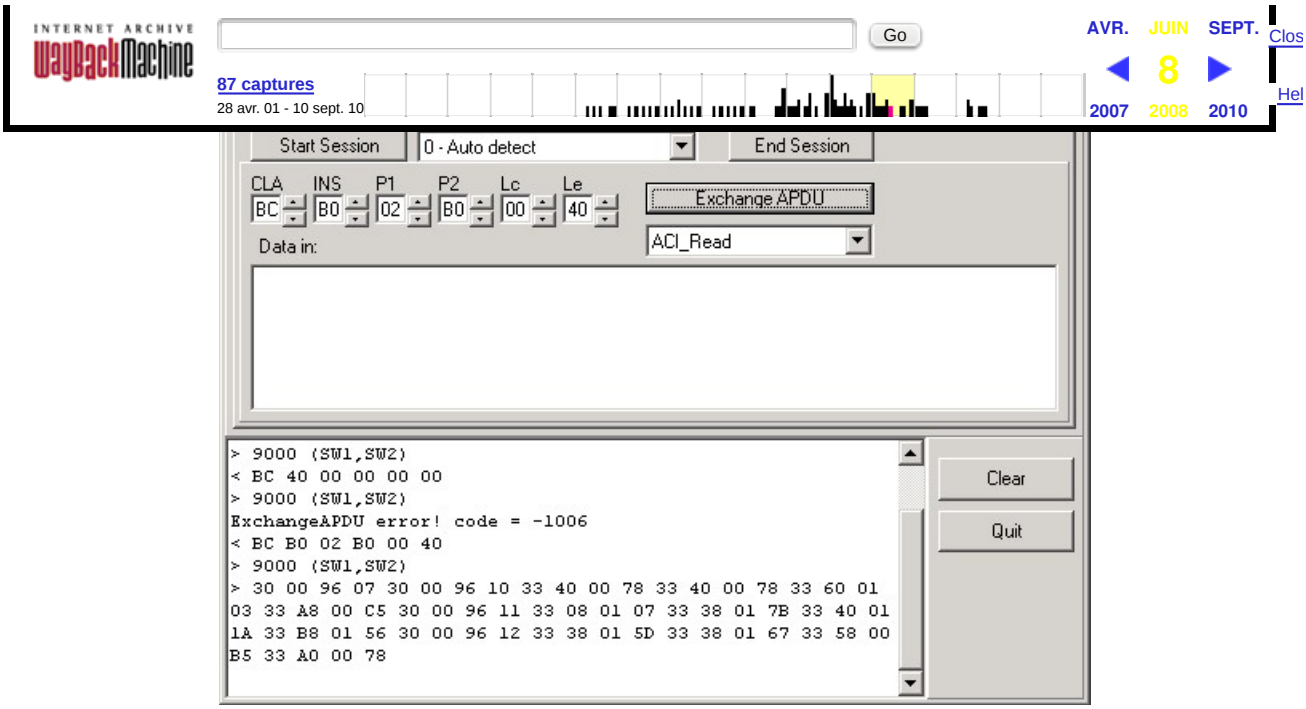
Exemple de commande d'envoi de code secret 1515 à une carte

Maintenant il faut "ratifier" le code secret envoyé précédemment à l'aide d'une commande BC 40 et appuyer sur Exchange ADPU :



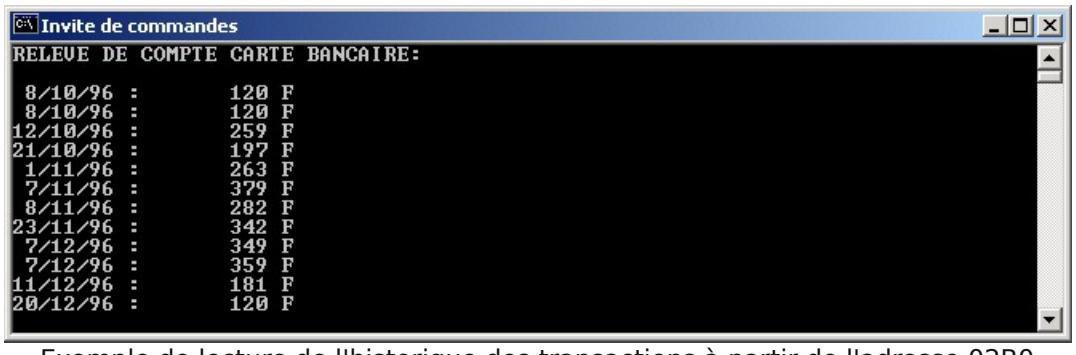
Exemple de commande de ratification de coe secret

Maintenant on peut enfin lire sur la carte à l'adresse 02B0 à l'aide d'une commande BC B0 :



Exemple de lecture de l'historique des transactions à partir de l'adresse 02B0

On obtient comme résultat :
< BC B0 02 B0 00 40
> 9000 (SW1,SW2)
> 30 00 96 07 30 00 96 10 33 40 00 78 33 40 00 78 33 60 01 03 33 A8 00 C5 30 00 96 11 33 08 01 07 33 38 01 7B 33 40 01 1A 33 B8 01 56 30 00 96 12 33 38 01 5D 33 38 01 67 33 58 00 B5 33 A0 00 78
[Note : si vous n'obtenez rien, vous avez peut être entré un mauvais code secret, il est alors préférable] Pour lire tout l'historique il est possible d'utiliser le programme DECADT en GWBasic de Patrick Gueulle (pas besoin de lecteur de carte à puce connecté pour exécuter ce programme) en créant un fichier adt.hex de la forme (on rajoute B0 au début, on supprime les espaces, on rajoute FFF9000 à la fin):
B03000960730009610334000783340007833600103 33A800C5300096113308010733380 17B3340011A33B80156300096123
on lance le programme DECADT.EXE (existe avec sources en GWBASIC) fourni avec le livre de Patrick Gueulle
On dit que l'exposant est de 5 (unité) (voir exploration zone identifiant) pour cette carte. On observe le résultat de l'historique suivant :



Exemple de lecture de l'historique des transactions à partir de l'adresse 02B0

Si on compare avec ce qu'affiche le lecteur XiPuces pour cette période allant d'octobre 1996 à décembre 1996, on a bien les mêmes transactions (notamment la transaction en double de 120 francs le 08/10/1996).
Si on compare maintenant avec les relevés de carte bancaire du porteur de cette carte, on constate une transaction de 120 francs le 8 octobre 1996 chez un coiffeur (et non 2, c'était sûrement parce que le code secret a été rentré une première fois mais la facturette ne s'est pas imprimée alors un autre essai a été effectué, parfois les gens sont débités en double dans ce genre de cas), une transaction de 259.02 francs le 12/10/1996, un paiement de 197.65 francs le

DECADT.bas fourni avec le livre de Patrick Gueulle pour voir le mode de stockage de l'historique.

Fin exploration carte expirée :

Maintenant que l'on a tout vu sur la carte bancaire à puce expirée, il est préférable d'appuyer sur le bouton "End Session" de CardEasy et de retirer la carte du lecteur.

Conclusion lecture carte expirée :

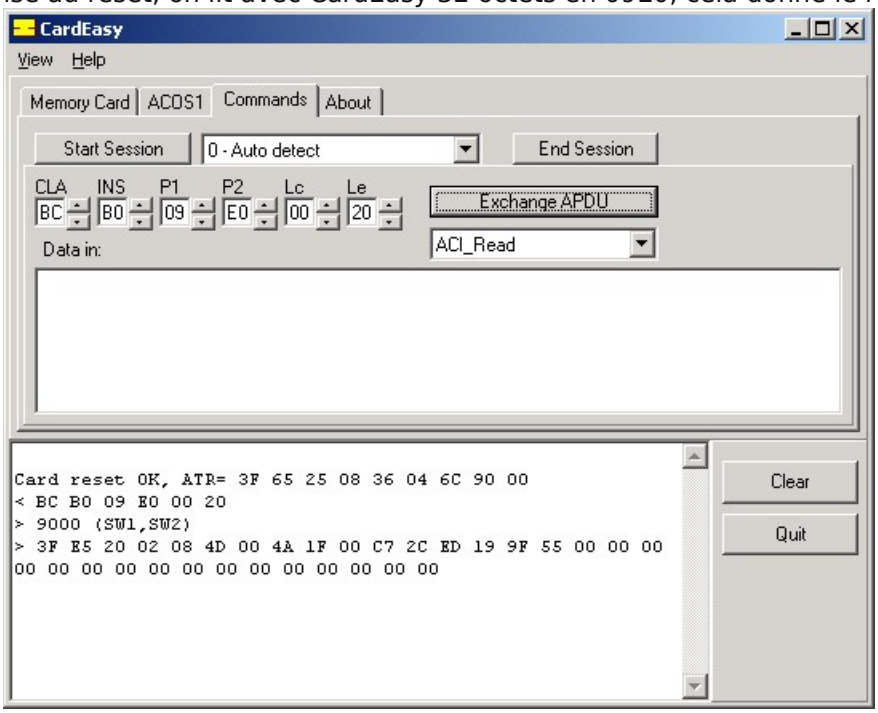
Maintenant que nous avons vu à quoi correspondait toutes les données d'une carte bancaire émise avant novembre 1999, que le code secret ne protège que l'historique des transactions et pas la valeur d'authentification et n'empêche pas les clônages de la puce, nous allons voir si les cartes bancaires émises depuis sont aussi sûres qu'on le prétend et notamment si elles comportent toujours une Valeur d'Authentification calculée avec une clé cassée et si le code secret sert à quelque chose.

EXPLORATION SUR UNE CARTE EMISE DEPUIS NOVEMBRE 1999 :

Pour l'expérience, a été utilisée une carte bancaire émise en novembre 1999.
Cependant, les résultats trouvés coincident exactement avec une expérience faite sur 2 autres cartes, l'une émise en janvier 2000 et l'autre émise en avril 2001 (les 2 cartes correspondant à un compte bancaire en euro mais la carte était en franc aussi)
Si vous faites l'expérience sur votre propre carte bancaire émise depuis novembre 1999, vous pourrez donc reproduire l'expérience.
Dans ce paragraphe, on suppose que vous êtes familier avec l'exploration d'une carte bancaire car vous avez essayé le paragraphe précédent.

LECTURE NOUVELLE CARTE en 09 E0 :

Après une réponse au reset, on lit avec CardEasy 32 octets en 09E0, cela donne le résultat suivant.



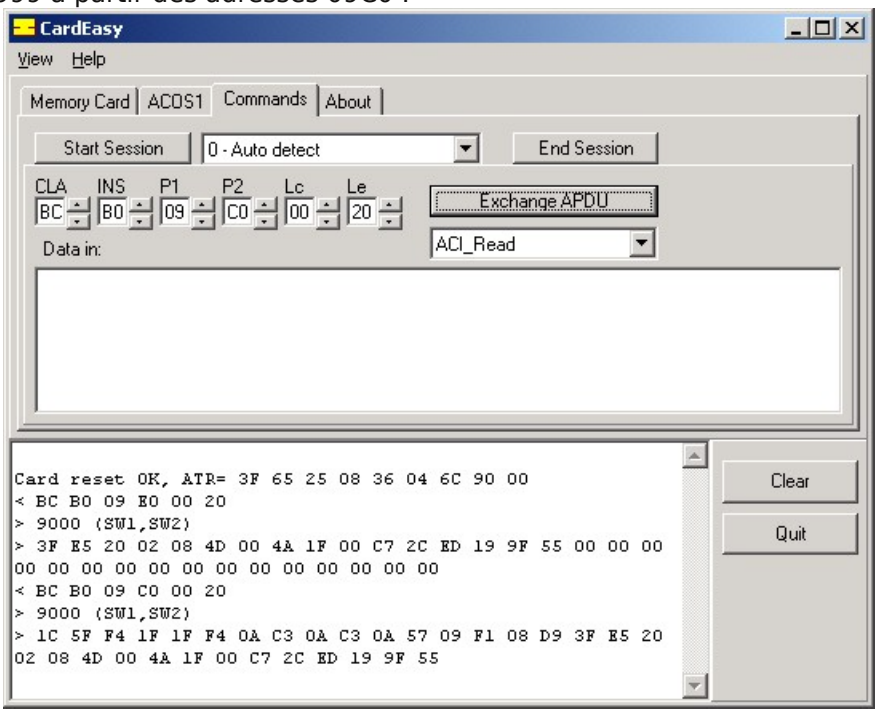
Exemple de lecture à partir de l'adresse en 09E0 sur une carte émise en novembre 1999

On peut constater apparemment qu'il n'y a pas beaucoup de nouveautés, le type de carte reste 3F E5, ce qui correspond à une

< BC B0 09 E0 00 20
> 9000 (SW1,SW2)
> 3F E5 20 02 08 4D 00 4A 1F 00 C7 2C ED 19 9F 55 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

ZONES D'ADRESSES DE LA NOUVELLE CARTE :

Selon la méthodologie vue pour une carte expirée, on décode les données lues sur une carte émise en novembre 1999 à partir des adresses 09C0 :



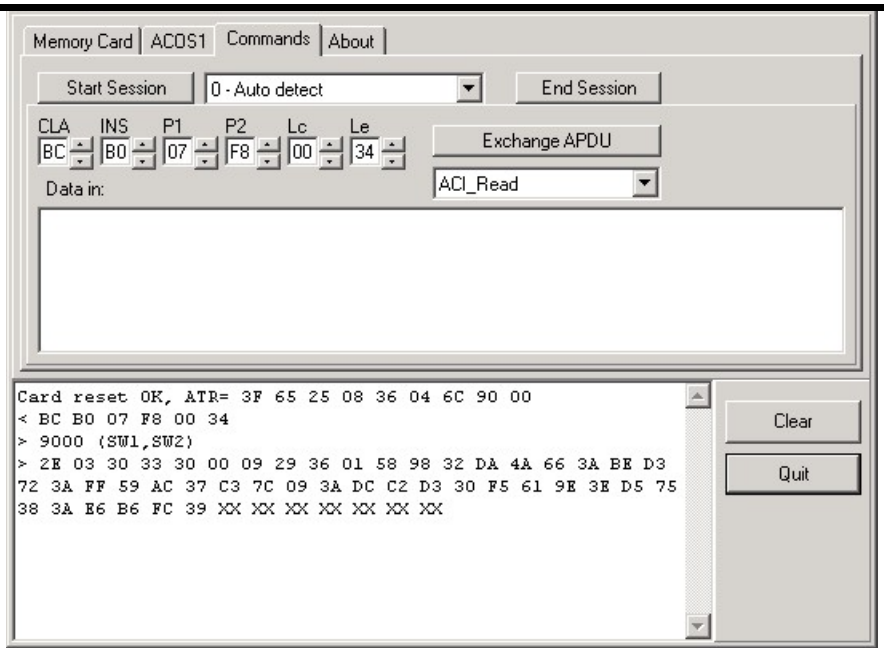
Exemple de lecture à partir de l'adresse en 09C0 sur une carte émise en novembre 1999

Résultats lecture en 09 C0 :
< BC B0 09 C0 00 20
> 9000 (SW1,SW2)
> 1C 5F F4 1F 1F F4 0A C3 0A C3 0A 57 09 F1 08 D9 3F E5 20 02 08 4D 00 4A 1F 00 C7 2C ED 19 9F 55

Nom zone	Adresse définition	Octets à l'adresse définition	Traduction en binaire des données à l'adresse définition	11 premiers bits et ajout 3 bits à 0 (*8)	Résultat zone d'adresse
ADL	09C8	1F F4	0001 1111 1111 1000	00 0111 1111 1000	**07 F8**
ADT	09CC	0A C3	0000 1010 1100 0011	00 0010 1011 0000	**02 B0**
ADC	09D0	0A C3	0000 1010 1100 0011	00 0010 1011 0000	**02 B0**
ADM	09D4	0A 57	0000 1010 0101 0111	00 0010 1001 0000	**02 90**
AD2	09D8	09 F1	0000 1001 1111 0001	00 0010 0111 1000	**02 78**
ADS	09DC	08 D9	0000 1000 1101 1001	00 0010 0011 0000	**02 30**
AD1	09E8	08 4D	0000 1000 0100 1101	00 0010 0001 0000	**02 10**

Comme on peut le voir, ADL est maintenant à 07 F8, la zone de lecture libre s'est donc agrandie, on va lire à cette adresse maintenant :

Lecture zone Valeur d'authentification de la puce carte émise en novembre 1999 :



Exemple de lecture à partir de l'adresse en 09C0 sur une carte émise en novembre 1999

< BC B0 07 F8 00 34
> 9000 (SW1,SW2)
> 2E 03 30 33 30 00 09 29 36 01 58 98 32 DA 4A 66 3A BE D3 72 3A FF 59 AC 37 C3 7C 09 3A DC C2 D3 30 F5 61 9E 3E D5 75 38 3A E6 B6 FC 39 XX XX XX XX XX XX XX

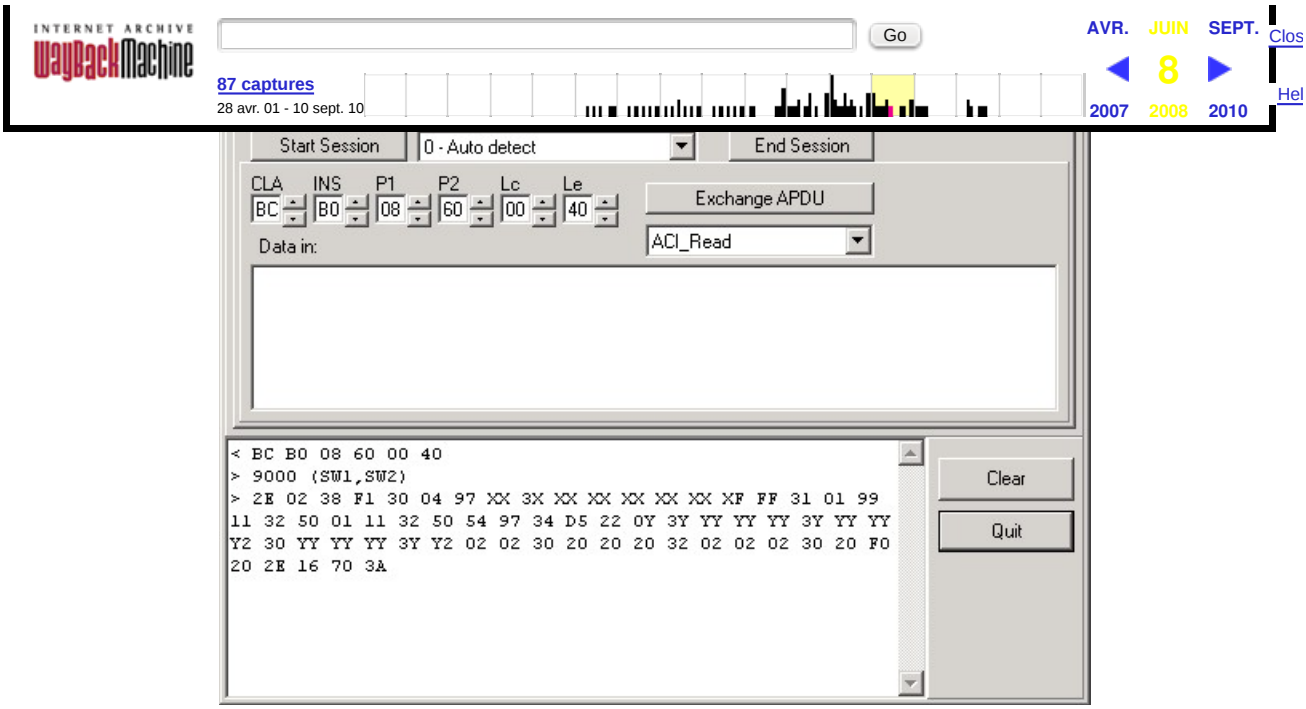
Mais comme c'est étrange ! On trouve un prestataire 03 et une Valeur d'authentification de 320 bits à l'adresse ADL ! On croyait que les cartes émises depuis novembre 1999 avait une valeur d'authentification allongée ???

On nous aurait menti ?

On verra par la suite que cette Valeur d'authentification (VA) à 320 bits a bien été calculée à l'aide de la clé cassée mais qu'il y a une autre valeur d'authentification, de 768 bits cette fois ci.

Lecture zone identifiant de la puce carte émise en novembre 1999 :

Juste après le prestataire 03 se trouve la zone identifiant du prestataire 02 à l'adresse 0860 :
On lit 64 octets (40h en hexa) à partir de l'adresse 0860 sur la carte émise en novembre 1999 : on trouve cela :



Lecture de la zone identifiant sur une carte émise en novembre 1999 (le numéro de carte bancaire a été masqué par des X et le nom du porteur a été masqué par des Y)

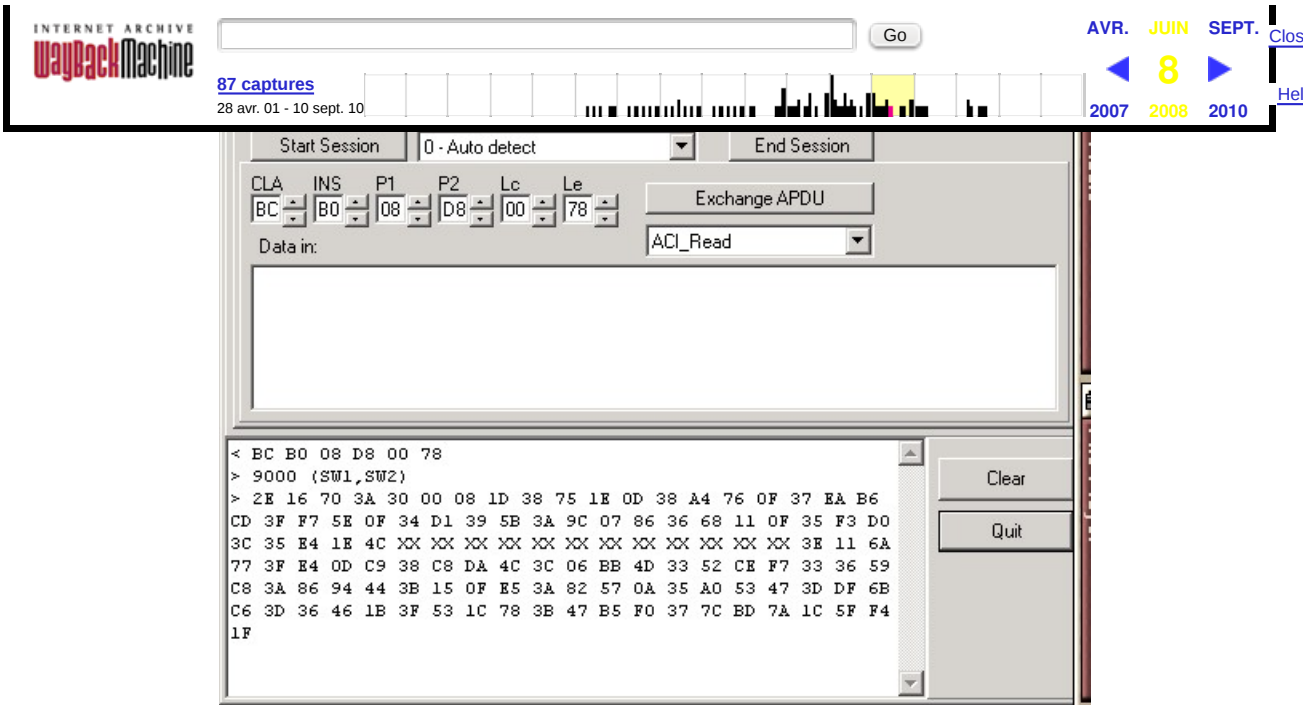
Résultat de la lecture de 64 octets en 0860 :
< BC B0 08 60 00 40
> 9000 (SW1,SW2)
> 2E 02 38 F1 30 04 97 XX 3X XX XX XX XX XX XF FF 31 01 99 11 32 50 01 11 32 50 54 97 34 D5 22 0Y 3Y YY YY YY 3Y YY YY Y2 30 YY YY YY 3Y Y2 02 02 30 20 20 20 32 02 02 02 30 20 F0 20 2E 16 70 3A

Vérification de la Valeur d'authentification

Voir les calculs faits pour une carte expirée pour les détails
En élevant au cube les 48 octets de la valeur d'authentification stockée à partir de l'adresse 08 00 (en supprimant les quartets de "3" de redondance tous les 4 octets) modulo la clé publique cassée, on retrouve :
8E00000497XXXXXXXXXXXXFFF1099110111000008E00000497XXXXXXXXXXXXFFF1099110111
(les X représentent le numéro masqué)
soit la redondance du motif de l'identifiant (stockée à partir des adresses 0868) de la date d'expiration et de la date de début de validité de la carte.

Lecture Valeur d'authentification "allongée" de la puce carte émise en novembre 1999 :

Juste après le prestataire 02 se trouve la zone VA allongée correpsondant au prestataire 16 à partir de l'adresse 08D8 :
On lit 78h octets (120 octets en décimal) à partir de l'adresse 08D8 sur la carte émise en novembre 1999 : on trouve cela :



Lecture de la valeur d'authentification allongée sur une carte émise en novembre 1999 (elle est masquée partiellement par des X)

Compte tenu de la taille de 120 octets de cette zone, elle correspond à une clé de 768 bits (en supprimant les quartets "3" de redondance)
Il y a donc bien une valeur d'authentification allongée **mais pourquoi la clé cassée subsiste t'elle ?**
(Parce que seuls les terminaux de paiement en version 5.2 lisent cette clé allongée qu'il est prévu de lire la clé cassée jusqu'en 2004) !
Surtout **pourquoi peut on toujours lire cette Valeur d'authentification sans avoir besoin du code secret ?** Elle est en effet située dans une zone publique en lecture, c'était tout de même possible de la stocker ailleurs.
On croit rêver, pas besoin du code secret à 4 chiffres pour cloner une carte allongée, et cela jusqu'à quand ? 2020 ?

Lecture de l'historique des transactions

L'historique des transactions n'a guère changé, sauf que sa taille est plus réduite du fait de l'apparition de la Valeur d'authentification allongée, voir le paragraphe correspondant.

EXPLORATION SUR UNE CARTE EN "EURO" :

C'est une blague, il n'y a pas de carte bancaire en euro !
Nous avons fait la même expérience sur une carte associée à un compte bancaire en euro de l'auteur émise en janvier 2000, ainsi qu'une autre en avril 2001 il n'y a pas de différence, la carte bancaire a "franc" (code 250) comme code devise et "français" (code 250) comme langue
L'historique des transactions n'indique pas la devise de la transaction, par exemple, pour une opération d'achat de 82 francs de tickets à la SNCF (correspondant à 12.50 EURO), l'historique indiquera 12 si le porteur choisit de faire une transaction en euro et 82 s'il choisit de passer la transaction en franc (en plus les centimes ne sont jamais stockées dans l'historique des transactions de la puce).
cet historique est donc inutilisable (les retraits d'argent ne sont pas non plus indiqués dans l'historique, seuls les paiements avec un terminal de paiement chez un commerçant acceptant la puce sont indiqués).
Ce bug est impardonable car il génère déjà des litiges (des victimes se font débiter une somme en euro alors qu'elles croyaient effectuer une transaction en franc)
Note : le code du franc est 250, celui de l'euro est 978 mais il n'y a pas actuellement de carte bancaire en euro.

certaines banques.
L'expérience a pas été tentée sur une carte bloquée de l'auteur avec pour date d'expiration 05/1995 (bloquée sur un distributeur de billets de train la SNCF qui n'attendent pas 3 essais infructueux pour bloquer la carte).
Là aussi la zone de lecture avec la valeur d'authentification 320 bits, la zone identification du porteur entre 08E0 et 09FF ont pu être lue sans présenter le code secret.
Les cartes à puce bloquées peuvent donc toujours être clonées sans connaître le code secret !
Par contre il n'est pas possible de consulter l'historique des transactions car cela requiert le code secret et la présentation du code ne fonctionne pas si la carte est bloquée.

DEROULEMENT PAIEMENT PAR CARTE BANCAIRE :

Schématiquement les opérations suivantes sont faites lors d'un paiement par carte bancaire à puce sur un terminal de paiement électronique (cela dépend des versions du terminal de paiement) :
1. Le consommateur choisit un bien ou un service et souhaite présente sa carte bancaire à puce pour le réglement
2. Le porteur de carte introduit sa carte dans le lecteur
3. Le commerçant tape le montant de la transaction sur le terminal de paiement en choisissant la devise (Francs ou euro) et appuie sur le bouton pour déclencher la transaction
4. Le terminal de paiement lit la zone libre de la carte bancaire
5. Le terminal de paiement authentifie la carte bancaire (le mot "Authentification" apparait souvent sur le lecteur)
Pour cela le terminal de paiement élève le prestataire 03 (Valeur d'authentifcation à 320 bits) à la puissance 3 modulo la clé publique et vérifie que le résultat obtenu correspond bien à une redondance de l'identifiant du prestataire 02.
ou si le terminal de paiement est en version 5.2 et que la carte a été émise depuis novembre 1999, l'authentification est faite à partir du prestataire 16 (Valeur d'authentification allongée).
L'authentification de la carte est finie à ce moment là.
6. Le terminal vérifie que le numéro de la carte ne figure pas dans sa liste noire (stocke quelque milliers de numéros en opposition)
7. Le terminal demande au porteur de rentrer le code PIN secret à 4 chiffres
8. Le porteur rentre le code PIN secret à 4 chiffres
9. La transaction est inscrite dans la liste des transactions
10. La carte fait un calcul cryptographique DES à partir d'un jeu secret de la carte (le résultat ne sert que pour l'impression du certificat de paiement qui sera imprimé sur la facturette)
11. Le terminal de paiement fait un autre calcul cryptographique DES à partir du résultat de la carte et imprime le résultat de ce calcul sur 2 facturettes ainsi que les informations sur la transactions (montant transaction, date, nom commerçant, numéro de carte complet ou masqué,
12. Selon certaines circonstances (carte à appel systématique ou transaction supérieure à 600 francs ou autre), le terminal de paiement fait un appel téléphonique au central pour avoir une demande d'autorisation. Ce central indique si le numéro est en opposition ou pas et si le numéro est attaché à un compte valide ou non.
13. Si toutes les étapes ont été franchies avec succès, la transaction est validée,
14.la transaction est réputée irrépudiable en vertu de l'article L132-2 du code monétaire et financier (sauf cas de perte ou de vol).
15.le commerçant livre le bien ou fournitle service.
16. En fin de journée, la liste des transactions avec les numéros de carte sont transmises par la ligne téléphonique au central de la banque. La liste des numéros en opposition est également mise à jour.
17. En cas de contestation sur un paiement par un porteur, la banque du porteur transmet la contestation à la banque du commerçant, la banque du commerçant demande au commerçant de fournir la facturette et le descritif du produit ou service fourni en contrepartie du paiement, le commerçant fourni le justificatif avant l'ultimatum fixé, sinon il n'est pas payé, la banque du commerçant transmet la facturette à la banque du porteur de carte, la banque du porteur de carte

Ce certificat de paiement ne peut servir de preuve car les banques ne peuvent être juges et parties, seules elles peuvent le vérifier et elles mentent systématiquement.

En substituant la puce par une autre puce dont on connait le code secret entre les étapes 7 et 8, il est possible de débiter une carte dont on ignore le code

A t'on le droit d'explorer et d'observer sa carte ?

Désolé pour ce paragraphe triste voire inutile, il est nécessaire à cause des apprentis juristes des banques qui ne connaissent pas le droit et inventent des nouvelles règles de droit. Au moins, cela économisera des honoraires inutiles aux banques !
C'est clair, si les cartes bancaires présentent des failles, les banques n'ont à s'en prendre qu'à elles mêmes et retirer au plus vite toutes les cartes en circulation au lieu de continuer à fourguer de telles passoires.
Les banques s'effarouchent de tout, elles font n'importe quoi, commettent pleins d'erreurs, n'assument pas leurs responsabilités : au lieu de rembourser intégralement les victimes et payer le renouvellement du parc de cartes et de terminaux, elles s'enrichissent grâce à la fraude (augmentation des commissions, pas de garantie des paiements à distance, perception de frais d'opposition, d'assurance, de renouvellement de carte, d'enquêtes inutiles) mais elles n'aiment pas que l'on parle de la fraude car le chiffre d'affaire baisse et la confiance du porteur de carte et des commerçants s'effrite (ce qui est bien normal).
Du coup, les banques, au lieu de corriger les failles, ont pris pour bouc émissaire la presse.
Les banques aiment encore moins les détails techniques car cela permet aux victimes de mettre en évidence la faute des banques et donc d'engager leur responsabilité.
Cependant, la constitution est ainsi faite et garantie le droit à la liberté d'expression, ne peut être interdit que ce qui est illégal et prévu par la loi. La constitution prévoit aussi que la loi ne peut interdire que les actions nuisibles à la société. Une loi devrait donc interdire les cartels nuisibles à la société.
Même si une loi scélérate interdisait, par extraordinaire, de parler des cartes bancaires (ce qui n'est pas le cas, la France n'est pas encore le régime des talibans), la convention européenne des droits de l'homme prévoit que la liberté d'expression ne peut être restreinte que dans les cas nécessaires dans une société démocratique. Or il n'est nullement nécessaire de faire perdurer le mythe de l'inviolabilité des cartes bancaires à puce.
Pour savoir s'il est légal d'observer et d'explorer sa carte bancaire à puce, il suffit de lire son contrat carte bancaire. Ce contrat, intitulé "conditions générales d'utilisation de la carte de paiement" qui dit que la carte est rigoureusement personnelle. ce qui est bien, l'auteur de cette page a fait les observations sur les cartes qui lui ont été remises par sa banque et portant son nom. Vous êtes également invité à ne faire ces opérations que sur votre propre carte.
Il n'est pas indiqué dans le contrat qu'il est interdit d'observer la carte, il n'est pas non plus interdit de s'en servir pour dégivrer les vitres de sa voiture.
Si l'on considère que la carte de paiement comporte un logiciel installé sur le microprocesseur qui répond aux ordres que l'on envoie, il faut donc aussi voir les dispositions du code de la propriété intellectuelle relatives aux logiciels :
Article L 122-6
Sous réserve des dispositions de l'article L. 122-6-1, le droit d'exploitation appartenant à l'auteur d'un logiciel comprend le droit d'effectuer et d'autoriser :
1° La reproduction permanente ou provisoire d'un logiciel en tout ou partie par tout moyen et sous toute forme. Dans la mesure où le chargement, l'affichage, l'exécution, la transmission ou le stockage de ce logiciel nécessitent une reproduction, ces actes ne sont possibles qu'avec l'autorisation de l'auteur ;
2° La traduction, l'adaptation, l'arrangement ou toute autre modification d'un logiciel et la reproduction du logiciel en résultant ;
3° La mise sur le marché à titre onéreux ou gratuit, y compris la location, du ou des exemplaires d'un logiciel par tout procédé. Toutefois, la première vente d'un exemplaire d'un logiciel dans le territoire d'un Etat membre de la Communauté européenne ou d'un Etat partie à l'accord sur

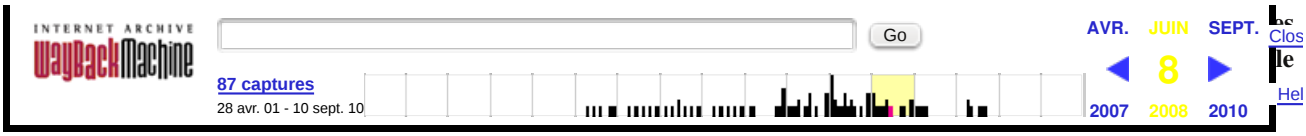
I. Les actes prévus aux 1° et 2° de l'article L. 122-6 ne sont pas soumis à l'autorisation de l'auteur lorsqu'ils sont nécessaires pour permettre l'utilisation du logiciel, conformément à sa destination, par la personne ayant le droit de l'utiliser, y compris **pour corriger des erreurs**.
Toutefois, l'auteur est habilité à se réserver par contrat le droit de corriger les erreurs et de déterminer les modalités particulières auxquelles seront soumis les actes prévus aux 1° et 2° de l'article L. 122-6, nécessaires pour permettre l'utilisation du logiciel, conformément à sa destination, par la personne ayant le droit de l'utiliser.
II. La personne ayant le droit d'utiliser le logiciel peut faire une **copie de sauvegarde** lorsque celle-ci est nécessaire pour préserver l'utilisation du logiciel.
III. La personne ayant le droit d'utiliser le logiciel **peut sans l'autorisation de l'auteur observer, étudier ou tester le fonctionnement de ce logiciel afin de déterminer les idées et principes qui sont à la base de n'importe quel élément du logiciel lorsqu'elle effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du logiciel qu'elle est en droit d'effectuer**.
IV. La **reproduction du code du logiciel** ou la traduction de la forme de ce code n'est pas soumise à l'autorisation de l'auteur lorsque la reproduction ou la traduction au sens du 1° ou du 2° de l'article L. 122-6 est indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels, sous réserve que soient réunies les conditions suivantes :
1° Ces actes sont accomplis par la personne ayant le droit d'utiliser un exemplaire du logiciel ou pour son compte par une personne habilitée à cette fin ;
2° Les informations nécessaires à l'interopérabilité n'ont pas déjà été rendues facilement et rapidement accessibles aux personnes mentionnées au 1° ci-dessus ;
3° Et ces actes sont limités aux parties du logiciel d'origine nécessaires à cette interopérabilité.
Les informations ainsi obtenues ne peuvent être :
1° Ni utilisées à des fins autres que la réalisation de l'interopérabilité du logiciel créé de façon indépendante ;
2° Ni communiquées à des tiers sauf si cela est nécessaire à l'interopérabilité du logiciel créé de façon indépendante ;
3° Ni utilisées pour la mise au point, la production ou la commercialisation d'un logiciel dont l'expression est substantiellement similaire ou pour tout autre acte portant atteinte au droit d'auteur.
V. Le présent article ne saurait être interprété comme permettant de porter atteinte à l'exploitation normale du logiciel ou de causer un préjudice injustifié aux intérêts légitimes de l'auteur.
Toute stipulation contraire aux dispositions prévues aux **II, III et IV du présent article est nulle et non avenue**.
Article L 122-6-2
Toute publicité ou notice d'utilisation relative aux moyens permettant la suppression ou la neutralisation de tout dispositif technique protégeant un logiciel doit mentionner que l'utilisation illicite de ces moyens est passible des sanctions prévues en cas de contrefaçon.
Un décret en Conseil d'Etat fixera les conditions d'application du présent article.

Donc en vertu de l'article L 122-6-1 III on est libre d'observer, étudier et tester le fonctionnement du logiciel pour en tirer les principes de fonctionnement. On ne va pas donc pas se gêner.

Les données inscrites dans la carte reproduites par la suite, ne sont pas du "code" source ou exécutable du logiciel mais juste des données inscrites sur la carte et ne sont pas des oeuvres de l'esprit, j'ai donc le droit de les reproduire librement

En vertu de l'article R335-2 du Code de la propriété intellectuelle, **L'UTILISATION DE MOYEN DE SUPPRESSION OU DE NEUTRALISATION DE TOUT DISPOSITIF TECHNIQUE PROTEGEANT UN LOGICIEL, EST PASSIBLE DES SANCTIONS PREVUES EN CAS DE CONTREFACON**.

Cependant, cette page ne s'intéresse pas à la contrefaçon de la puce et encore moins à la désactivation des protections de la puce puisqu'il n'y a pas de protection sur la puce des cartes bancaires !



Liens

04/03/2000 Secret carte bancaire	La formule secrète des cartes bancaires révélées sur Internet
Parodie.com	Page d'accueil site sur les failles des cartes bancaires