Les lundis de la cybersécurité
14 février 2022

- Hommage à Michel Ugon
- Ma découverte des cartes à puce
- 1ère Application militaire envisagée
- Carte à puce = arme de guerre!!!
- Sécurisation des cartes à puce
- Certification des composants de cartes à puce
- L'affaire Humpich


THALES
Jean-paul MARTIN
CONFIDENTIEL DEFENSE
1
2 abc
3 def
4 ghi
5 jkl
6 mno
7 pqrs
8 tuv
9 wxyz
*
0 +
#

L'évolution des composants pour cartes à puce

Aujourd'hui, l'industrie européenne de la carte à puce est représentée par EUROSMART, une association fondée en 1994 par les pionniers de cette activité afin de promouvoir la carte à puce dans le monde entier.

Michel UGON
Président d'EUROSMART

Les membres d'Eurosmart (voir figure 1) témoignent de l'avance technologique européenne en s'appuyant sur un historique unique et une expertise sans égale :

EUROSMART représente aujourd'hui

EUROPEAN SMART CARD INDUSTRY ASSOCIATION

Associated Members:

Bull CP8*
Dassault AT*

SECURITE

son terminal.

Pour contrecarrer les attaques physiques au niveau du composant, des protections particulières doivent être intégrées au moment de la conception de façon à interdire les pénétrations, les investigations, les altérations, et déclencher des blocages ou des alarmes utilisés par le système d'exploitation. On atteint ce but en utilisant des contre-mesures, ou des techniques de diversion qui nécessitent, bien entendu une assez grande expérience de ces phénomènes. On se trouve ainsi inévitablement dans un processus de perfectionnement permanent vers des niveaux de sécurité de plus en plus élevés. Ainsi, chaque jour voit augmenter les ressources matérielles et logicielles nécessaires à ces fonctions de la carte dédiées spécifiquement à la sécurité.

Peu de gens savent que 30 % du logiciel du système d'exploitation est ainsi consacré à la sécurité physique. C'est une part très importante complètement cachée et ignorée du monde extérieur qui ne voit que la partie visible purement fonctionnelle. C'est pourquoi un système d'exploitation conçu pour un certain type de composant ne peut être transposé intégralement sur un autre. Ainsi les dévelop-

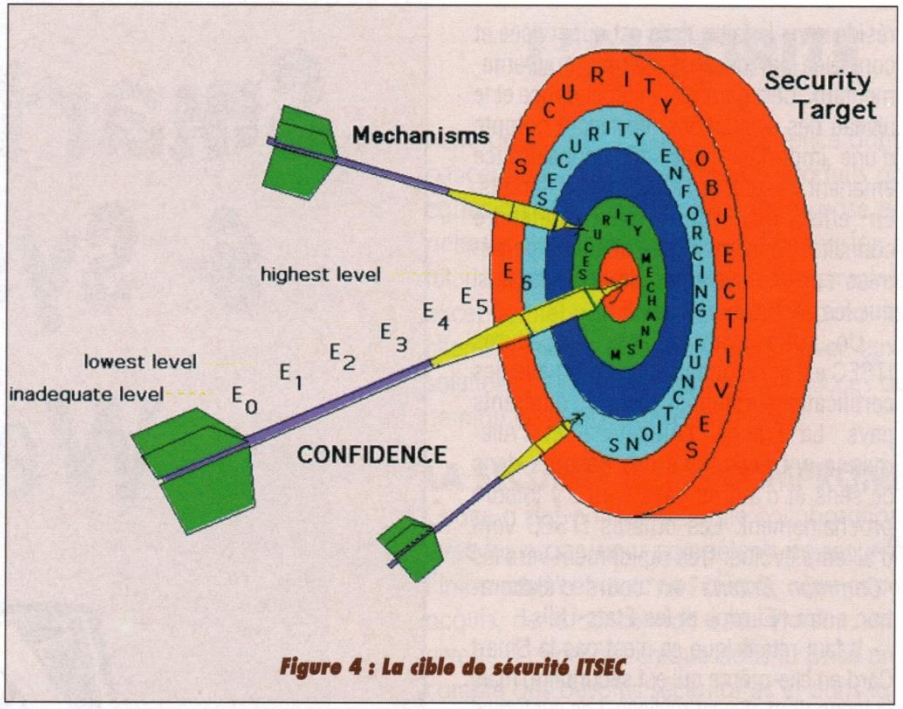


Figure 4 : La cible de sécurité ITSEC

Comment connaître le niveau de securité ?

son logiciel associé : c'est comme si dans un coffre fort, fut-il électronique, on séparait la serrure de son infrastructure. A quoi cela servirait-il d'avoir un composant très sécuritaire si la sécurité de l'ensemble est compromise par un logiciel inadapté, et réciproquement ?

SÉCURITÉ

La politique française en matière d'évaluation de la sécurité des cartes

Par le General Jean-Louis DESVIGNES
Responsable du Service Central
de la Sécurité des Systèmes d'information (SCSSI)

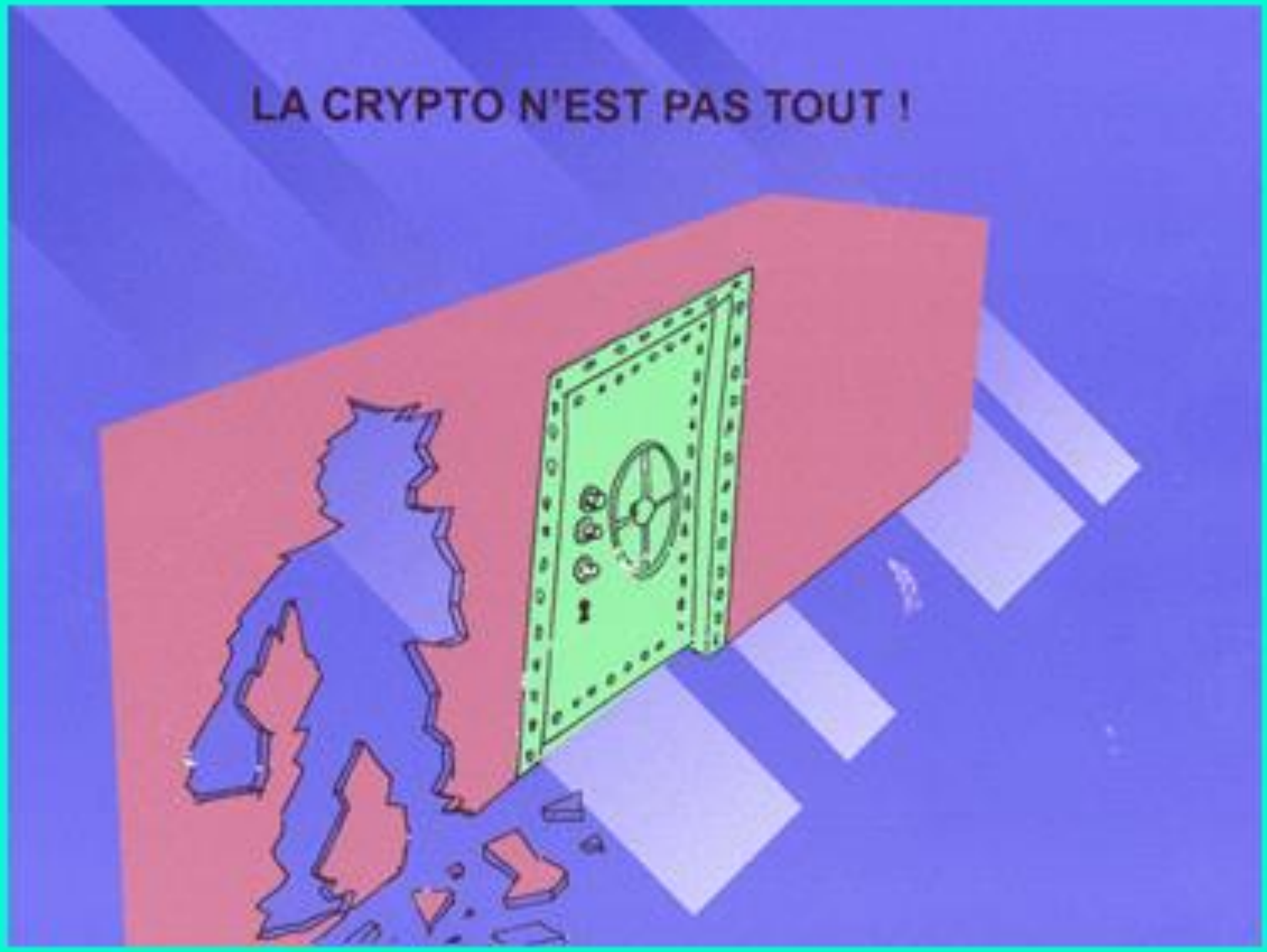
Ceux qui, parmi vous, ont assisté aux journées précédentes ont dû observer qu'il était difficile de parler de cartes ou d'ap-

manière globale et cohérente; il ne sert en effet à rien d'avoir une superbe clef si la serrure est rouillée, ou si la porte blindée repose sur des chambranles en bois

porter un soin tout particulier à l'élément le plus visible et le plus accessible aux gens malveillants : la carte.

L'attention qu'il convient de lui

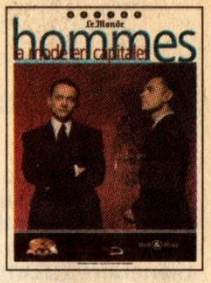
Les limites de la cryptographie



Le Monde

CAHIER SPÉCIAL

■ D'Amsterdam à Paris, la mode hommes 2000 en capitales



EURO FRANCE MÉTROPOLITAINE — SAMEDI 11 MARS 2000 — FONDATEUR : HUBERT BEUVE-MÉRY – DIRECTEUR : JEAN-MARIE COLOMBANI

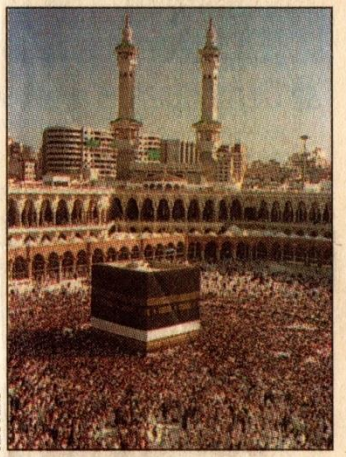
Alerte à la sécurité des cartes bancaires

● Les cartes à puce ne sont plus inviolables ● Le responsable de la sécurité des systèmes d'information demande aux banques de réagir vite ● La Banque de France s'inquiète du retard pris ● Les transactions via Internet sont à l'origine de la majorité des fraudes

LA SÉCURITÉ des 35 millions de cartes de paiement bancaires détenues par les Français est-elle menacée ? Les autorités et les banquiers commencent à s'inquiéter de la multiplication des piratages, notamment via Internet. Quant au mythe de l'inviolabilité de la carte à puce, il a vécu. La récente publication anonyme, sur Internet, d'une clé de cryptage secrète a levé un tabou. *« La carte à puce a bénéficié d'une réputation d'inviolabilité qui a écarté les attaques mafieuses, mais la technologie de ces cartes devient accessible, et avec des moyens relativement modestes on peut les attaquer »*, affirme le général Jean-Louis Desvignes, chef du Service central de la sécurité des systèmes d'information. Il demande aux banques et à leurs autorités de tutelle *« des actions ambitieuses pour être à l'abri pendant les années qui viennent »*. La Banque de France s'inquiète du retard pris. Le Groupement d'intérêt économique Cartes bancaires se veut pourtant rassurant. *« Ce n'est pas parce que l'on peut briser un verrou que l'on peut ouvrir la porte »*, affirme le porte-parole du GIE. La carte à puce a offert jusqu'à présent aux Français une sécurité nettement supérieure à celle des cartes ordinaires. Le taux de fraude représente 0,02 % des transactions contre 0,1 % à 0,4 % pour les cartes sans puce.

La véritable menace pour le consommateur n'est pas, pour le moment, celle de l'informaticien de génie fabriquant une fausse carte. Le danger tient surtout à l'usage grandissant par des fraudeurs de numéros de cartes existant qu'ils ont dérobés, par exemple sur des facturettes abandonnées imprudemment. Ils effectuent ensuite des achats à distance par téléphone, Minitel ou Internet. Cette délinquance augmente avec le développement du commerce électronique. Les transactions sur Internet représentent en France 2 % de l'ensemble des paiements par carte bancaire, mais elles sont à l'origine de plus de 50 % des fraudes.

Lire page 20



REUTERS

PÈLERINAGE

Paris-La Mecque

19 000 musulmans sont partis de France pour participer au *« hadj »*, le grand pèlerinage de La Mecque, qui a commencé le 7 mars et culmine le 16 avec l'Aïd-el-Kébir. Ils n'étaient que 14 000 en 1996. Cette augmentation s'explique par l'attrait grandissant des jeunes « beurs » pour ce voyage, mais aussi par le fait que des ressortissants étrangers passent par la France pour éviter les quotas imposés par l'Arabie saoudite aux pays musulmans. p. 10

Serge Humpich, 36 ans, ingénieur, a percé le secret des cartes bancaires. Il attend son jugement aujourd'hui.

Gentleman décodeur

Une Opel Manta rouge sous le ciel plombé de la Brie, un jour d'hiver. Serge Humpich, lunettes et costume gris, s'excuse, «*je fais un peu Starsky*». D'habitude, il roule en Fiat 500. La Manta, qui démarre au tournevis, c'est un copain des pompes funèbres qui a le filon: «*Les gens qui meurent ont toujours une vieille caisse. Les héritiers sont soulagés de s'en débarrasser pour deux ou trois mille balles en liquide.*»

A chaque époque, sa combine. En juillet 1998, Humpich pesait des francs lourds dans un conte des mille et une nuits version grand Satan. Alchimiste de la Carte bleue, il savait transformer les chiffres en billets… Le sésame lui était apparu un soir tard, après quatre ans de bidouilles sur un terminal bancaire de récupération. «*Un moment dingue, je pouvais dialoguer avec les centraux et me faire admettre par n'importe quel réseau. Seul au monde à pouvoir retirer 15000 francs tous les quarts d'heure, et acheter absolument tout ce que je voulais…*» «*Une mine d'or*», résume-t-il, fatigué d'exposer à des néophytes «*comment il a inversé les algorithmes de cryptage*». Le but n'était pas de s'enrichir, pas «*en voleur*» en tout cas. Un sens profond de l'honnêteté, «*mon fond alsacien sans doute*», a arrêté

«*C'est intéressant de louer à des religieux, ils ne viennent que le dimanche.*»

SERGE HUMPISH EN 6 DATES
Mars 1963. Naissance

Grâce à leur code secret, les achats par cartes sont sécurisés. Mais gare aux oublis de facturettes. Photo DR

Un million pour les violeurs de puces

Roland Moreno, l'inventeur de la carte à puce, défie les pirates qui affirment avoir percé le secret des cartes bancaires

Eric JUHERIAN

Un million de francs. C'est le pactole offert par Roland Moreno à toute personne réussissant à pénétrer dans le microprocesseur d'une carte bancaire. « Je ne suis pas fou, ajoute l'inventeur de la carte à puce, je mets cette somme en jeu car j'affirme que personne ne peut violer la puce qui équipe les cartes de paiement : elle reste une citadelle imprenable. »

Le défi de Roland Moreno, que bien des petits génies devraient tenter de relever dans les jours à venir, fait suite aux récentes révélations de Serge Humpich. Cet informaticien, récemment condamné à dix mois de prison avec sursis pour avoir fabriqué « une fausse carte bancaire », l'affirme : « Le système de protection des cartes à puces vient de tomber. »

Internet

La semaine dernière, la publication, sur un forum de discussion du Net, d'une clé de cryptage permettant de casser le code de protection des puces, confirmait ses prédictions. Même le Groupement Cartes Bancaires, qui gère les quelque 30 millions de cartes circulant en France, admettait « qu'un verrou venait de sauter ». En l'espace de quelques semaines, la réputation d'inviolabilité a pris du plomb dans l'aile. Pour Serge Humpich, « il est désormais possible de fabriquer une fausse carte bancaire, à l'aide de numéros dérobés sur un site Internet ou sur une facturette, et de payer grâce à elle ». Comme seul argument de défense, le Groupement Cartes Bancaires se retranche derrière un faible taux de fraudes en France (0,02 %, lire aussi page suivante).

« Insuffisant », proclame Roland Moreno, qui réaffirme « l'inviolabilité de son invention ». « Il n'existe pas de moyen de paiement plus sûr, même la plus modeste des cartes, la carte de téléphone, n'a jamais été violée. » Pour le patron d'Innovatron, ce qui fragilise ce mode de paiement, ce n'est pas la puce mais la cryptologie, les clés nécessaires pour avoir accès aux informations placées sur la bande magnétique. « Les banques ont choisi un format de clés très insuffisant, explique l'inventeur. Tout le monde sait qu'un digicode à six chiffres est plus sûr qu'un digicode à quatre chiffres. » Autrement dit, la porte d'accès au compte bancaire ne tient plus : n'importe quel génie informatique peut entrer et se servir.

Inviolabilité

Seule solution pour le Groupement en charge de ce moyen de paiement : le renouvellement complet des cartes bancaires. Depuis 1998, les banques, averties de la fragilité, ont décidé de remplacer les cartes par un chiffrement à 792 bits (actuellement, les cartes n'ont qu'une protection de 320 bits). « Le renouvellement total sera fini en 2001 », affirme-t-on au Groupement Cartes Bancaires. D'ici là, s'impose à chacun d'adopter un principe de méfiance. ■

curisés, il est possible qu'un pirate s'infiltre sur le serveur d'une entreprise et s'empare des numéros de cartes de ses clients.

Le Net favorise le développement des fraudes.

VRAI. Les transactions sur Internet, bien qu'elles ne représentent que 2 % des paiements par carte, sont à l'origine de près de 50 % des litiges. Dans la majorité des cas, les escrocs utilisent des numéros récupérés sur des facturettes.

Il est plus sûr de payer par chèque.

FAUX. Le taux de fraude par cartes bancaires est bas (142 millions de francs, sur les 800 milliards de transactions annuelles). Le niveau de sécurité apporté par ce système de paiement est sans commune mesure avec celui du papier : 0,27 % de fraude, soit 11 fois plus que les cartes !

Les cartes bancaires récentes sont mieux protégées.

VRAI. Depuis quelques mois, les nouvelles cartes diffusées par les banques disposent d'une clé de codage inviolable pour l'instant. Elles ne sont pas concernées par les découvertes faites par les pirates.

Tout débit frauduleux est à la charge du titulaire de la carte.

FAUX. En prévenant immédiatement sa banque, le titulaire de la carte se décharge de la responsabilité de la fraude. La banque paie à sa place. Un conseil : vérifiez attentivement vos relevés de comptes. A la moindre transaction suspecte, prévenez immédiatement votre banque. **E.J.**