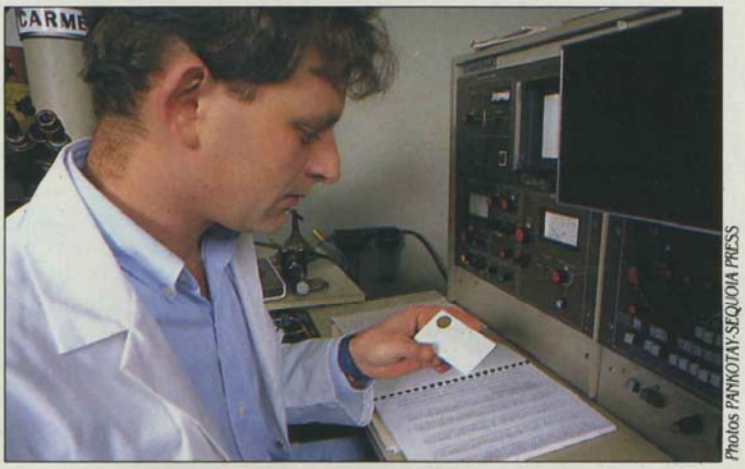
PEUT-ON PIRATER

Les secrets du silicium au microscope électronique



Photos PANNOTAY-SEQUOIA PRESS

LA CARTE À PUCE ?

Peut-on voir à l'intérieur d'un circuit intégré, d'un microprocesseur, d'un composant de mémoire ? La réponse est oui, grâce au microscope électronique. Mieux, par effet stroboscopique, on peut visualiser l'écoulement des électrons à l'intérieur des circuits, et suivre la circulation des bits, la vibration des instructions, le scintillement des informations dans les mémoires. De là à pouvoir démonter les mécanismes de la carte à puce et les contrefaire, il n'y a, en apparence, qu'un pas. Mais le passage à la pratique réserve bien des surprises aux faussaires du futur. Avec une équipe de micro-espionnage, nous vous proposons dès à présent un fabuleux voyage au cœur du silicium et au centre de ce micro-bunker génial qu'est la carte à puce.

LA CARTE À PUCE A RÉVOLUTIONNÉ les problèmes de sécurité par rapport à la carte de crédit classique. Avec cette dernière, et au grand désespoir des banquiers, il suffit, en effet, d'un matériel relativement simple pour lire les informations de n'importe quelle piste magnétique, laquelle ressemble à s'y méprendre à une disquette ou à une bande de sauvegarde d'ordinateur. En revanche, il est considérablement plus difficile de venir à bout d'un circuit intégré de quelques millimètres de côté, enchâssé dans une carte plastique, ce qui en fait probablement le meilleur système pour préserver l'information des regards indiscrets. Il faut du matériel sophistiqué, un ou deux ingénieurs très spécialisés et du temps. En conséquence, bricoleurs s'abstenir.

Mais la possibilité existe depuis la fin des années 60, et les informations qui suivent ont été obtenues, non pas auprès de pirates invétérés, mais d'un grand laboratoire français qui, justement, travaille pour les fabricants de circuits intégrés, nationaux et étrangers : le CARME, Centre d'applications et de recherches en microscopie électronique. Installé au milieu des pins entre Bordeaux et Arcachon, ce centre accueille des ingénieurs de formations diverses qui travaillent essentiellement sur microscopes électroniques à balayage. Pour l'anecdote, il faut savoir, qu'actuellement, le CARME est aussi (et surtout) à la pointe de la police scientifique européenne. Grâce à ses experts, capables d'analyser des échantillons infimes, poussières ou grains de sable, prélevés sur le lieu d'un crime, sur une

d'un crime, sur une victime ou un suspect, le laboratoire a fait plusieurs fois la une des journaux pour avoir aidé à conclure les enquêtes les plus obscures.

Ce centre tient le rôle d'expert dans différents domaines, dont la micro-électronique. Les constructeurs apportent au CARME leurs circuits expérimentaux afin de déterminer l'origine de pannes ou de dysfonctionnements. Dans certains cas, les constructeurs apportent également le dernier circuit sorti sur le marché par la concurrence, afin qu'il en détermine les spécificités. Une activité aussi courante dans le monde des fabricants de circuits que dans tous les autres secteurs de l'industrie : c'est la fameuse « veille technologique ». Les constructeurs ont souvent leurs propres laboratoires pour effectuer ces analyses, mais préfèrent parfois les sous-traiter. Ces compétences font que l'équipe du

Le travail du processeur au ralenti vu au microscope électronique à balayage.

CARME est capable de démonter n'importe quel circuit, mémoire ou microprocesseur, « *qui n'est qu'un circuit comme un autre* » explique-t-on. Avec deux difficultés de plus tout de même. Dans le cas d'une carte à puce : l'inclusion dans le plastique (« *Un problème mineur : pour dégager un circuit de sa protection plastique, nous avons des outils bien au point, comme tous les laboratoires de micro-électronique* » explique un ingénieur) et, le plus rude, le codage des données et les protections diverses concoctées par les fabricants.

Les premiers à être conscients de la possibilité de fraude sont donc à l'évidence les concepteurs de cartes eux-mêmes, qui étudient des techniques subtiles pour rendre plus difficiles encore la lecture des informations et la simulation du fonctionnement. Principal talon d'Achille : la technologie employée pour fabriquer les puces des cartes est forcément la même que celle utilisée pour tous les circuits intégrés du monde, des commandes d'ascenseurs aux calculatrices de poche en passant par les machines à laver à microprocesseur. La littérature abonde sur ce sujet et les ingénieurs sont maintenant au

LES RÉACTIONS DE ROLAND MORENO

SVM – À votre avis, les techniques du « reverse engineering » ou démontage de puce peuvent-elles s'appliquer à la carte à mémoire ?

Roland Moreno – Les laboratoires spécialisés dans le « reverse engineering » ont généralement pour vocation d'anticiper sur la fabrication d'un circuit par une seconde source. C'est un mécanisme classique : pendant les longues négociations qui visent, pour un constructeur, à obtenir la fabrication en seconde source d'un circuit, on démonte la puce, et le jour de la signature du contrat, la production est prête à commencer. Ces laboratoires travaillent sur des puces honnêtes, normales, des puces qui ne sont pas sensibles. Les cartes à micro-circuits utilisent des circuits spécifiques (Motorola ou Thomson) qui bénéficient de sécurités spéciales. Ce qui fait que bon nombre des méthodes classiques du reverse engineering sont impossibles à réaliser avec ces circuits. En particulier, dès le début des années 80, ont été mises au point des méthodes qui interdisent la vision de la carte en fonctionnement à l'aide d'un microscope à contraste de potentiel.

SVM – Pourriez-vous rappeler les grands principes de fonctionnement des sécurités d'une carte à puce ?

R.M. – Dans toute application informatique où la machine est distante du système qui lit la carte, tout ce que voit arriver cette machine, ce sont des bits, des 1 et des 0, dont rien ne permet de distinguer s'il s'agit de bits honnêtes ou malhonnêtes. Par bits malhonnêtes, on entend, par exemple, des informations en provenance d'un système pirate, branché sur la ligne entre la carte et la machine. Donc une simulation serait, en effet, concevable. Moi-même suivi par Bull et Philips après 1978, nous nous sommes attaqués à ce problème. Aussi, avons-nous mis en place des procédures d'authentification. Sans entrer dans le détail, il s'agit d'une technique de cryptage dont la clé est une combinaison d'un nombre aléatoire et du produit de deux grands nombres premiers. Ce cryptage permet de faire en sorte que le dialogue entre la carte et l'ordinateur qui la lit ne soit jamais le même. Imaginez, par exemple, une session au cours de laquelle vous faites un virement de 10 francs sur votre compte ; le même virement

A. NOGUES-SYGMA

Roland Moreno, inventeur de la carte à mémoire.

réitéré donnera lieu à une session complètement différente. C'est tout l'échange qui est codé et toute comparaison est impossible.

SVM – Mais qui fournit la clé de codage ?

R.M. – Il y a un algorithme de cryptage dans la carte. Celui-ci fonctionne avec une clé secrète qui est, elle aussi, dans la carte et un nombre aléatoire qui, lui, est envoyé à la carte par l'ordinateur distant.

SVM – À partir du moment où l'on peut lire dans le silicium, ne peut-on lire à la fois l'algorithme et la clé secrète ?

R.M. – Oui, mais on ne sait pas où il sont logés dans la carte. Comment faire la différence entre un simple sous-programme d'émission d'un bit et les informations que l'on cherche ?

SVM – Supposons que l'on puisse faire du reverse engineering suffisamment pointu, et qu'effectivement on parvienne à démonter complètement le mécanisme de la carte. Ne pourrait-on pas alors fabriquer un programme qui simulerait complètement cette carte ?

R.M. – Je ne sais pas, c'est une question discutable. Un autre paramètre intervient alors : celui de la vitesse de réaction. En gros, il faudrait fabriquer un composant identique à celui de la carte.

SVM – Vous voulez dire que si on utilisait un programme d'ordinateur, le système ne réagirait pas assez vite ?

R.M. – En effet. Sauf si l'on dispose d'un très gros ordinateur du type de ceux de Cray, car l'unité centrale qui lit les informations en provenance de la carte mesure aussi les temps de réactions pour savoir si son interlocuteur est bien un circuit spécifique et non un circuit programmé. Ceci ne concerne que la carte à microprocesseur pour laquelle le jeu d'instructions a été sensiblement modifié pour que la vitesse soit un élément difficile à reproduire.

SVM – Les organisations criminelles ne peuvent-elles pas recruter des ingénieurs capables de maîtriser toutes ces technologies ?

R.M. – Les ingénieurs capables de démonter les mécanismes d'un circuit ne sont pas si nombreux ; quelques dizaines en Europe. Rien à voir avec les hackers, les pirates des réseaux d'ordinateurs. Ceci est un point important. Pendant encore longtemps, peut-être un quart de siècle, il sera impossible au crime organisé – le seul qui nous intéresse – de débaucher ces ingénieurs sans que cela se voit. Or, il en faut un bon nombre pour commencer à faire le travail.

Propos recueillis par Yves HEUILLARD.

nombre de plusieurs centaines en Europe. Il faut se rendre à l'évidence : ce qui nous semblait, il y a plusieurs années, être une technologie inaccessible tend à se banaliser aujourd'hui. Le support physique de la carte, aussi « hi-tech » qu'il en ait l'air, ne suffit plus à garantir la sécurité absolue de l'information qui s'y trouve. C'est bien pourquoi les concepteurs de cartes ont recours au codage des informations enregistrées sur la carte et à des protocoles de communication invraisemblablement complexes.

Etude minutieuse du plan du circuit à partir des photos.

Deux grands types d'action sont envisageables : d'une part, l'écriture et la lecture d'informations dans la mémoire de la carte et, d'autre part, la simulation d'une vraie carte par une fausse ou par un dispositif informatique. L'écriture sur la carte est un sport délicat. Les circuits de mémoire morte programmable (PROM), une fois écrits, ne peuvent pas être réécrits et les opérations possibles sont donc plus limitées. Sur une Télécarte, par exemple, un fraudeur masochiste pourrait se retirer des unités. L'intérêt est plus que douteux... La simulation d'une carte, activité nettement plus ambitieuse, consisterait à fabriquer une « vraie-fausse » carte, opération concevable, ou encore à bricoler un support plastique relié à un ordinateur par un petit fil.

Une chose est sûre : dans tous les cas, les opérations à effectuer sont très complexes, car la carte à puce, véritable ordinateur en réduction, possède suffisamment d'intelligence pour se protéger. Pour pénétrer dans le cœur du circuit, aucun espoir de passer par l'extérieur, c'est-à-dire par les huit contacts dorés figurant au recto. En effet, la lecture traversant ce bus est soumise à de multiples vérifications. Première d'entre elles, l'authentification. Elle utilise un puissant système de chiffrement. Le logiciel de décodage est présent dans l'ordinateur effectuant les transactions ainsi que dans la carte. L'ordinateur tire un nombre au hasard et l'envoie à la carte. Chacun de leur côté, ils utilisent alors le programme de chiffrement pour le coder et la carte envoie à l'ordinateur le résultat obtenu. Si les deux sont identiques, la transaction peut continuer. Le fait que la vérification utilise un nombre tiré au hasard est très important. En effet, il faut se prémunir contre le plus simple des moyens de piratage technologique des cartes : l'écoute branchée sur la connexion. Elle est tout indiquée pour les télétransactions où le lecteur de carte est relié à l'ordinateur par une liaison téléphonique. Si l'ordinateur envoyait toujours les mêmes messages pour les mêmes opérations, il suffirait de détecter précisément les signaux, puis, sans avoir besoin de les décoder, d'envoyer exactement les mêmes au moment de la transaction frauduleuse. Reste l'identification, opération servant à reconnaître le porteur de la carte, par la frappe du code confidentiel (le seul moyen employé aujourd'hui). Pour des applications très sensibles (militaires, par exemple), d'autres méthodes pourraient être utilisées : observation des empreintes digitales, de la forme de la main, examen du fond de l'œil, de la voix, etc.

La carte, donc, n'accepte pas de travailler avec n'importe quel ordinateur. Et elle n'accepte pas non plus de faire n'importe quoi. Certaines zones de mémoire, par exemple, sont protégées en lecture et le simple fait de tenter de les lire plus de trois fois provoque des catastrophes dans le circuit : une sorte de suicide, ou, au mieux, un blocage du processeur. Pour la télé-écriture, l'ordinateur maître de la transaction doit utiliser le code secret de la carte (qui n'a rien à voir avec le code confidentiel à quatre chiffres utilisé par le porteur), calculé à partir du numéro de série.

Techniques de déshabillage

La puce paraît bien protégée de toutes les attaques extérieures. Mais qu'en est-il lorsque des experts, armés de mauvaises intentions et d'instruments sophistiqués, s'en prennent à elle directement et s'attaquent au circuit lui-même ? Le problème n'est pas le même pour tous les types de cartes à circuit. Sur une carte à mémoire, comme la Télécarte des PTT, les informations sont stockées dans un circuit mémoire spécifique de type PROM. Ces mémoires mortes programmables peuvent être enregistrées une seule fois. L'écriture se fait de la même manière que celle d'une mémoire vive d'ordinateur, à ceci près que l'intensité de courant est plus forte et que les éléments de mémoire fonctionnent comme des fusibles. Au moment de la lecture, ils se comportent exactement comme une mémoire quelconque. Pour aller y chercher l'information, il suffit de fabriquer un connecteur s'adaptant aux broches de la carte – les

petites zones métalliques dorées. Ensuite, il reste à les lire comme des mémoires d'ordinateurs. Pour cela, il faut connaître parfaitement le principe utilisé, c'est-à-dire la forme du bus de données. Dans le cas contraire, le violeur doit retrousser ses manches et observer le circuit pour le comprendre.

Dans le cas d'une carte bancaire à micro-calculateur, on a vu que les protections de lecture et d'écriture sont bien trop contraignantes pour passer par cette porte ouverte que constituent les huit contacts dorés. Une seule solution : sortir la puce de son plastique protecteur et l'attaquer directement, sous le microscope. Les spécialistes parlent de la « déshabiller » ou de « l'effeuiller ». L'opération consiste en une abrasion du vernis de protection puis du plastique de la carte ou d'une attaque chimique à l'acide. Dans les deux cas, une main de maître est indispensable, sous peine de destruction définitive de la carte.

Commence alors le long travail d'étude du circuit. Le procédé est simple dans son principe mais complexe dans sa réalisation. En fait, il reprend la technique des réparateurs de vieux postes de radio testant les composants un à un avec des électrodes reliées à un appareil de mesure. Pour étudier un circuit intégré, les électrodes changent d'échelle : les connexions entre composants ne dépassent pas six microns. Quant aux appareils de mesure, ce ne sont pas, loin de là, des multimètres achetés chez le quincaillier. L'appareillage doit, en effet, être capable de stimuler des groupes de composants logiques pour essayer de comprendre à quoi ils servent.

Les circuits au microscope

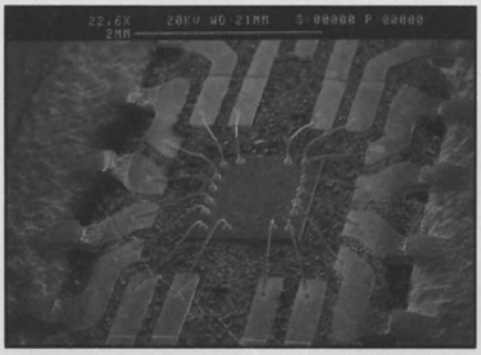
Au CARME, l'analyse de circuits nécessite une station micropointe, composée d'un microscope de métallurgie et de micro-manipulateurs. Le microscope utilisé en métallurgie se caractérise par une généreuse plate-forme porte-objet. Pour faciliter le travail, l'ensemble doit également être installé sur une table anti-vibrations. Sur la plate-forme sont posés quelques micro-manipulateurs, petites mécaniques de précision, munies d'un bras commandé par des molettes à travers un système de démultiplication. Ces micro-manipulateurs font partie du matériel courant dans tous les laboratoires travaillant en microscopie. Les électrodes – très fines – sont fixées sur ces bras. Le circuit vient prendre place au milieu du dispositif, sous l'œil du microscope et l'expérimentateur en approche l'extrémité coudée des électrodes. En grossissant quelques centaines de fois, on peut, grâce aux micro-manipulateurs, aller poser ses électrodes au pied d'un composant du circuit, transistor, porte logique, liaison du bus de données, etc.

Reste à ne pas les poser au hasard. Le circuit d'une carte à mémoire ou, pire, d'un microprocesseur, est extrêmement complexe. La question est de savoir où sont situées les informations et comment est conçu le bus de données. Parfois, les constructeurs fournissent eux-mêmes la solution en incluant sur la carte de véritables portes d'entrée. Pour pouvoir vérifier facilement leurs circuits fraîchement construits avant qu'ils ne soient enchâssés dans le support plastique, ils gravent sur le silicium des plots servant de points de contact qui, directement reliés au bus de données, constituent l'endroit idéal pour poser les électrodes. Il faut toutefois prendre la précaution de placer à ce niveau des connecteurs de type fusibles, qui, après vérification, seront grillés pour couper définitivement le contact entre les plots et le bus.

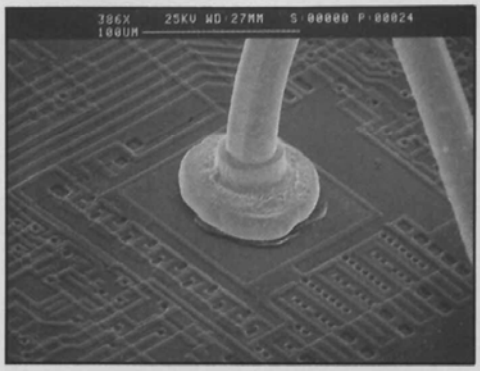
De toute façon, à moins que le technicien au travail ne connaisse la puce sur le bout des doigts, c'est par là qu'il faudra commencer. La première opération consiste donc à prendre une multitude de photos avec un appareil fixé sur le microscope. Les clichés obtenus sont collés les uns aux autres pour reconstituer le plan du circuit, qui dépasse alors facilement le mètre carré. Un passionnant travail de fourmi commence. Pendant des semaines ou des mois selon la complexité du circuit, les techniciens passeront leurs journées à plat-ventre sur le sol, où le plan sera étalé, pour suivre les pistes, identifier les composants et supputer des principes de fonctionnement. Quelques années d'études préalables dans une école d'ingénieurs en électronique et une bonne pratique des circuits intégrés en tous genres sont vivement conseillées.

Une fois connus les éléments détaillés du circuit, celui-ci pourra être testé au microscope, connecté à l'appareil de mesure par l'intermédiaire des micro-électrodes. Des modèles suffisamment fins peuvent atteindre pratiquement tous les composants des technologies CMOS. Lorsque les cartes utiliseront les composants, actuellement à l'état de prototypes, qui descendent à l'échelle du micron et même en dessous, les malfaiteurs de la hi-tech devront, à leur tour, changer leurs outils et leurs méthodes. Avec l'épaisseur des circuits du moment, de quatre à six microns, les composants peuvent être testés séparément et étudiés en détail. Le stimulateur pourra les faire fonctionner isolément comme s'ils étaient en situation normale d'opération. Le circuit révèlera ainsi tous ses secrets un par un. Ce genre de manipulations est le pain quotidien des ingénieurs travaillant sur le contrôle des circuits intégrés. C'est grâce à ce type de technique que l'on peut diagnostiquer les pannes.

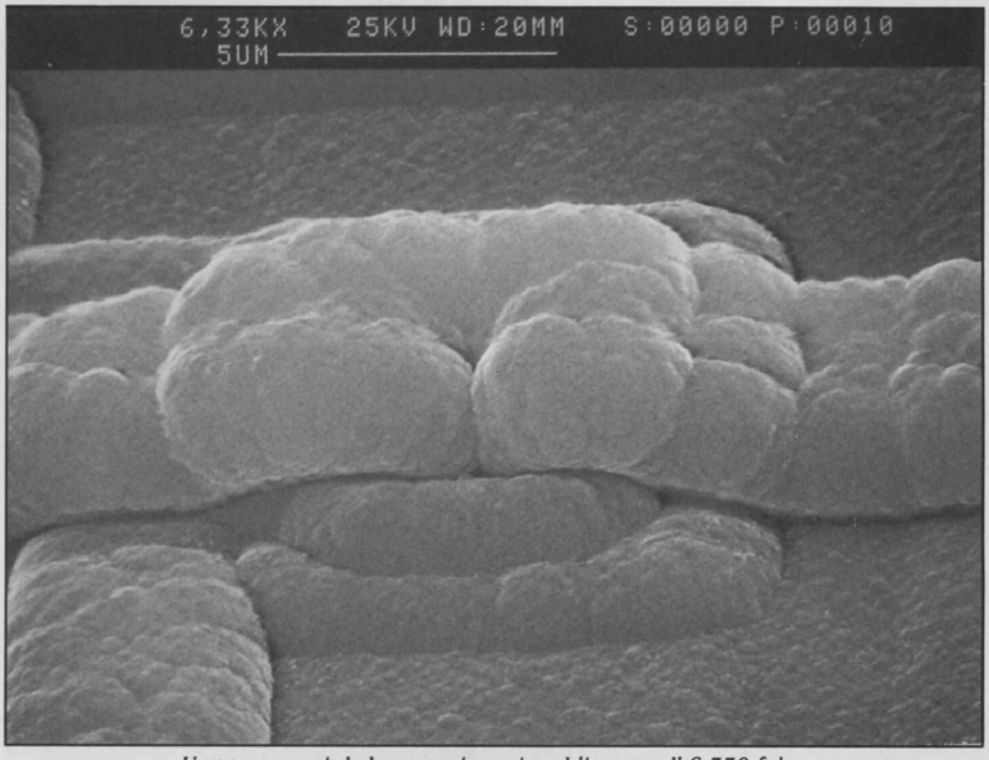
A la fin de ce travail de bénédictin, s'il s'agit d'une mémoire, l'équipe saura lire les don-



Le circuit-mémoire agrandi révèle les points de connexion intéressants.



Le fil d'or reliant la puce aux pattes du circuit, grossi 386 fois.



Un composant de base contenant un bit, agrandi 6 330 fois.

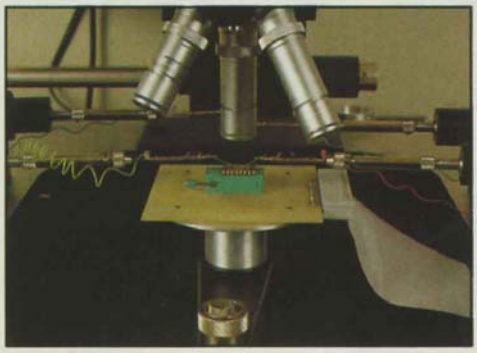
nées aussi facilement que dans un vulgaire ordinateur. S'il s'agit d'un microprocesseur, le travail sera plus long mais elle finira par le connaître aussi bien que si elle l'avait conçu. Si des doutes subsistent, dans le cas de structures très complexes, on peut franchir un palier supplémentaire grâce à un appareillage extraordinaire : le stroboscope sur microscope électronique à balayage. Dans ce microscope, où le circuit peut être installé en ordre de marche et alimenté, on obtient une magnifique image en noir et blanc et en perspective. Or, le parcours des électrons dans les composants modifie la façon dont le faisceau électronique du microscope est réfléchi et, du coup, son image est modifiée. Les événements sont normalement bien trop rapides pour être visualisés, mais on peut les ralentir par effet stroboscopique. En faisant exécuter un processus répétitif par le processeur, et, en envoyant le faisceau électronique du microscope par intermittence avec une période légèrement différente, on peut suivre au ralenti le cheminement des électrons le long des composants. En peaufinant les réglages, et en modifiant les stimulations envoyées au circuit, le technicien pourra, à loisir, observer les détails les plus intimes du fonctionnement du processeur. Bien sûr, il faut un microscope électronique à balayage, instrument plutôt coûteux : compter un minimum de un million et demi de francs...

Ultimes sécurités

À ce genre d'investigations, les constructeurs répondent par des astuces techniques de conception. Premier type de ruse : les faux bits. Parmi les vraies informations, le candidat à la fraude recueillera un peu n'importe quoi. Plus rusée encore : la technique des bits truqués. Très subtile à mettre en œuvre, elle consiste à réaliser des mémoires à l'apparence normale, dont les octets contiennent des suites de nombres semblant former une suite logique. Pourtant, cette information est entièrement fausse. Les véritables données se trouvent en réalité codées sous une autre forme physique, par exemple de légers décalages de phase dans la réponse de la mémoire. Enfin, le constructeur peut rendre active la pellicule de plastique qui recouvre la puce, de telle manière que, lorsqu'elle est enlevée, le circuit ne fonctionne plus et ne peut donc plus se prêter aux savantes investigations que nous avons décrites.

Au bout du compte, le codage des données reste le meilleur rempart contre l'intrusion étrangère dans le délicat mécanisme de la carte. Mais est-il infranchissable ? En allant très loin dans l'analyse des circuits, les fraudeurs peuvent lire isolément les mémoires de la carte, sans passer par les protocoles compliqués du dialogue normal. En étudiant très finement le fonctionnement de la carte en action, ils peuvent déterminer où sont stockées les informations confidentielles, le code secret, par exemple. En supposant qu'une équipe de spécialistes réussisse à percer tous les secrets d'une carte à micro-calculateur, pour utiliser de façon frauduleuse cette connaissance, il resterait à construire une « vraie-fausse » carte.

« Vraies-fausses » cartes ? Est-il possible de construire ou de faire construire des circuits sur mesure ? La réponse est oui depuis toujours, mais coûte un peu cher (5 à 10 millions de francs). En France et en Europe, plusieurs sociétés peuvent accomplir ce travail, mais quelques trimestres leur sont nécessaires.



La station « micropointe » pour étudier le fonctionnement intime des composants.

Bien sûr, l'ensemble de ces opérations réclame une gamme de compétences et des moyens impressionnants. La fraude coûte très cher – on peut estimer l'investissement de cinq à dix millions de francs – et la vraie question à se poser est celle du rapport coût-profit. Pirater la Télécarte pour téléphoner tous les jours à Papeete ne paraît pas économiquement valable, tout comme s'attaquer à la carte de stationnement utilisée dans le « Piaf » de Roland Moreno, pour se garer gratuitement à Saint-Brieuc. En revanche, si la carte à puce finit effectivement par être adoptée par les banques, le jeu en vaudra peut-être la chandelle. Tout dépend des opérations qu'elle permettra d'effectuer. Si l'on en reste aux opérations actuelles, la carte à puce représente une meilleure sécurité que la carte à piste puisque le coût du déplombage est environ 1 000 fois supérieur. Si des opérations complexes, ordres de virement par exemple, sont possibles, si l'accès à des informations sensibles ou à d'importants fichiers informatiques est conditionné par une carte à puce, la contrefaçon pourrait être à la portée d'organisations criminelles ou de services secrets, dont les moyens financiers peuvent être mis à la hauteur de l'enjeu.

Jean-Luc GOUDET (SEQUOIA)

LES QUATRE TYPES DE CARTES

IL Y A CARTE ET CARTE. LA PREMIÈRE, ET la seule jusqu'à une époque récente, est la carte à piste magnétique utilisée actuellement. Aussi vulgaire qu'un ticket de métro, elle ne comporte qu'une piste magnétique dépourvue de toute inhibition de lecture ou d'écriture, sur laquelle une tête magnétique banale pourra lire et écrire comme le fait celle d'un magnétophone numérique ou d'un lecteur de disquettes. S'il y a trois pistes au verso, c'est tout simplement parce qu'il y a trois standards différents dans le codage, qui doivent coexister depuis la mise en place de « l'interbancarité ».

Les cartes munies d'un circuit intégré sont de trois types. La carte à mémoire, proprement dite, contient deux zones de mémoire. Exemple le plus connu : la Télécarte des PTT. Son circuit de deux millimètres carrés est composé essentiellement d'un circuit PROM (mémoire morte programmable). Au fur et à mesure de la consommation d'unités, le publiphone grille les bits de mémoire. Tout simple. C'est dans la zone de mémoire protégée que sont inscrites les données (numéro de série, référence de l'application) qui ne peuvent absolument pas être modifiées après fabrication.

La carte à logique câblée intègre l'équivalent de 300 portes logiques supplémentaires servant à gérer le détail des sécurités d'entrée-sortie. On ne peut donc pas y lire l'information depuis l'extérieur, c'est-à-dire en se branchant sur les contacts électriques dorés visibles au recto de la carte. Les PTT français et ouest-allemands utilisent ce composant en grand volume pour une carte de télécommunications plus évoluée qui permet d'imputer sur sa facture téléphonique les communications effectuées dans les cabines publiques.

La carte à puce est équipée d'un micro-calculateur ou microprocesseur. La plus sûre de toutes, quant à la sécurité des informations qu'elle contient, a été choisie par les banquiers dès 1982 pour devenir la future carte bancaire intelligente que l'on nous promet pour l'année suivante depuis cinq ans. C'est pratiquement un modèle réduit d'unité centrale d'ordinateur contenant des circuits de mémoire morte, de mémoire vive et des PROM. Le microprocesseur peut, lui-même, écrire dans la PROM, d'où le nom de microprocesseur autoprogrammable monolithique. Une zone de mémoire vive, assez restreinte, sert uniquement pour les calculs intermédiaires lorsque la carte est alimentée par le terminal. La présence du processeur permet les opérations les plus complexes. Une carte expérimentée pour les transports en commun, par exemple, module le prix du ticket en fonction de l'heure de la journée, du nombre de trajets déjà effectués et même de la proportion de déplacements ayant eu lieu pendant les heures creuses. Les opérations de contrôle qu'elle est capable d'effectuer sont évidemment beaucoup plus complexes. Le principe actuel consiste à lui faire exécuter au début de chaque transaction un algorithme de codage sur un nombre aléatoire tiré par l'ordinateur responsable de la connexion. Une moulinette mathématique effectivement très sécurisante qui a toutes les qualités pour refroidir les velléités de fraude, à moins que le jeu n'en vaille vraiment la chandelle.