Par Daniel Renard

L'«Anti-piratage» de Canal+

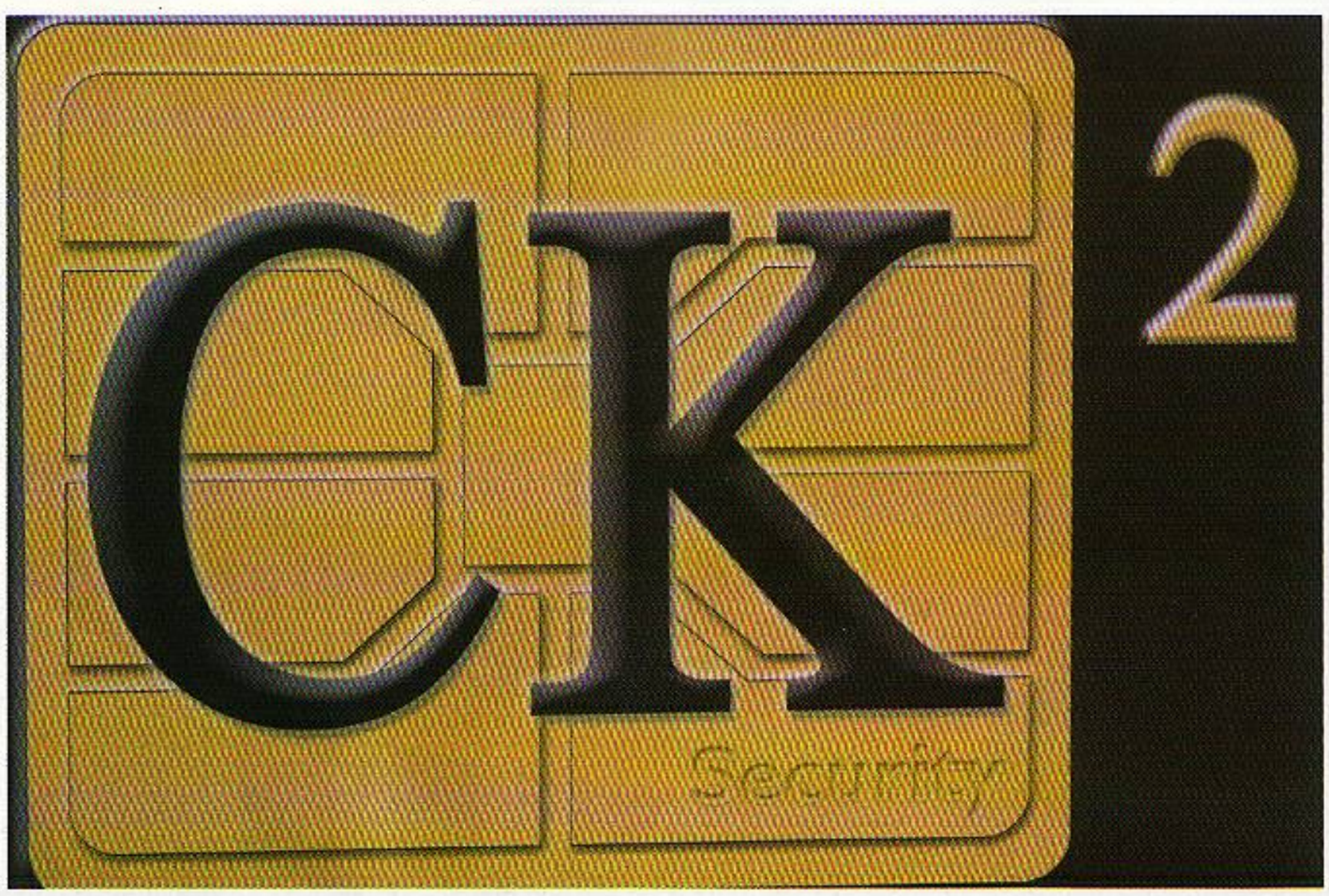
Installé sur la Côte d'Azur, dans la zone d'activités de Sophia Antipolis, le centre Anti-piratage du groupe CANAL+. baptisé « CK2 Security » abrite des installations techniques de pointe, permettant à une équipe d'ingénieurs spécialisés chargée de mettre en place les moyens technologiques pour combattre le piratage existant, mais aussi et surtout de préparer les futurs systèmes de cryptage en les rendant le plus inviolables possible. Parallèlement, une équipe de spécialistes en Droit intente des actions légales en collaborant avec les autorités policières et juridiques des différents pays concernés.

Les premiers actes de piratage des cartes Médiaguard, le cryptage développé par Canal+ Technologies, sont apparus en Grande-Bretagne en mars 1999 ; la croissance fut très rapide puisque, dès l'année suivante, le piratage fut tellement massif qu'il conduisit par exemple le bouquet italien au bord de la faillite… Devant cette constatation, les responsables du Groupe CANAL+ décidèrent fin 2000, sous l'impulsion de Gilles Kaehlin, de mettre sur pied une structure "Anti-piratage" chargée d'étudier la sécurité des systèmes de contrôle d'accès de manière indépendante. Cette indépendance vis-à-vis des fabricants de contrôle d'accès était d'autant plus importante que Canal+ Technologies était vendu à deux concurrents, Kudelski (exploitant du Nagravision) pour la partie contrôle d'accès Médiaguard et NDS / News Corporation (Rupert Murdoch) pour le moteur d'interactivité Médiahighway.

Unique en Europe.

Il parut rapidement évident au responsable sécurité du groupe, Gilles Kaehlin, que cette situation justifiait grandement la constitution d'une "cellule" chargée de combattre le piratage, essentiellement sous deux angles, la technique et la justice. De plus, la meilleure façon de combattre le piratage étant de mettre au point des systèmes les plus inviolables possible, il fallait se donner les moyens efficaces pour y parvenir. Il faut dire que le budget de fonctionnement de la cellule anti-piratage de CANAL+ coûte environ 3,5 millions d'euros par an… pour une vingtaine de salariés permanents et des consultants extérieurs.

C'est ainsi que le laboratoire "CK2" fut mis sur pied : des hommes compétents, si possible les plus compétents dans le domaine, et le meilleur matériel haut de gamme existant sur le marché. Ces deux critères étant réunis, le "CK2" constitue, aux dires de ses responsables, « *une unité unique en Europe* », de par son expertise en matière de microprocesseurs et de cryptologie. Il est vrai que les personnels recrutés, en dehors de quelques jeunes ingénieurs passionnés, viennent en grande partie du milieu des "hackers", ces génies de l'informatique qui passent leur temps à essayer de pirater tous les systèmes… C'est le cas de la "star" Olivier Kömmerling (voir encadré) qui est devenu la clef de voûte du "CK2". Dés son arrivée en 2000, il a mis au point le microprocesseur utilisé actuellement



dans le Médiaguard V1+, lequel a su résister, jusqu'à aujourd'hui, aux assauts des pirates...
On considérait à l'époque qu'un microprocesseur devait résister au moins 2 ans, s'il était bien conçu. Le Médiaguard V1+ approche de ses trois ans !

la meilleure façon de combattre le piratage étant de mettre au point des systèmes les plus inviolables possible

Une bonne conception

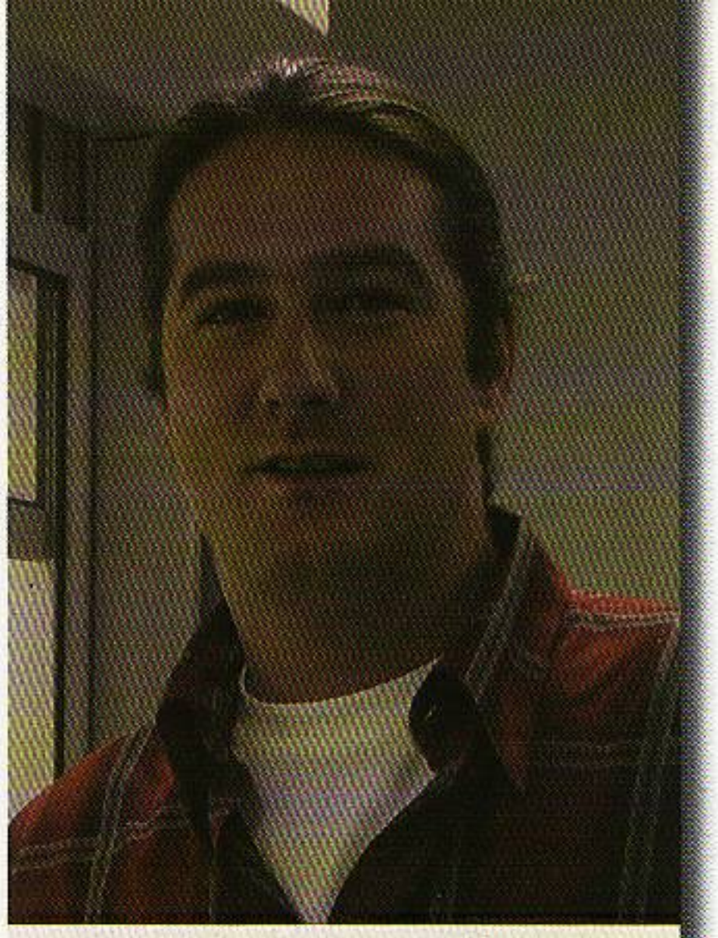
Vous l'aurez compris, la lutte contre le piratage ne doit pas se faire uniquement lorsque le produit est piraté mais bien avant. C'est sa conception et sa résistance aux attaques qui vont faire du microprocesseur l'élément majeur de tout le système sécuritaire. Pour faire simple, on peut le comparer à un coffre-fort qui contient des codes secrets. Si l'accès à l'intérieur du coffre est aisé, il est facile de comprendre que l'accès aux codes secrets sera facile et qu'ils seront décryptés d'autant plus rapidement qu'ils seront accessibles. Par contre, s'il est très difficile de pénétrer à l'intérieur du coffre pour y retirer les codes secrets, ceux-ci étant inaccessibles, ils ne pourront pas être décryptés... D'où l'importance de la conception du microprocesseur ! Il faut le rendre quasiment impénétrable aux attaques extérieures.

La veille technologique.

Les couches qui le constituent mesurent seulement 0,18 micron. Comme il peut y en avoir jusqu'à huit l'une sur l'autre, on estime qu'il peut, si sa conception est bonne, résister au moins 4 ans.
Autre aspect de la lutte anti-piratage, la veille technologique : elle consiste essentiellement à voir ce qui se passe dans le monde de piratage en utilisant tous les moyens possibles, parmi lesquels la veille sur Internet semble la plus utilisée. Pour cela, des experts surfent sur la toile à la recherche des sites diffusant des infos sur le piratage ainsi que les forums sur lesquels se retrouvent *"les pirates et leurs amis pour discuter de leurs exploits"*. Cette veille est décentralisée et ne se fait pas uniquement depuis les locaux de CK2. Partout dans le monde, des consultants externes, rémunérés par la société, se livrent à une « surveillance » consciencieuse.

L'investigation

Toutes les informations recueillies sont traitées de manière centralisée afin de pouvoir mener de véritables enquêtes et investigations, en rapport étroit avec les services de police et de douane des pays concernés : ainsi ces actions débouchent ponctuellement (pas assez souvent aux dires de CANAL+ !), sur des poursuites judiciaires avec des condamnations assorties de peines d'amendes, voire de prison avec sursis ou de prison ferme. La politique affichée par les responsables de CK2 est la "tolérance zéro". Mais ils nous confient qu'à leur avis, *« il y a parfois trop de laxisme de la part de certains opérateurs de bouquets »* : cette attitude est préjudiciable à la lutte contre le piratage car elle semble encourager les pirates dans leurs actions en ne luttant pas techniquement de manière efficace. Tout le monde l'aura compris sans qu'ils soient explicitement nommés, TPS et Noos sont directement visés. Il est vrai que depuis 7 ans qu'elles sont utilisées par ces opérateurs, les cartes Viaccess 2.3 sont allégrement piratées... alors que l'on sait parfaitement que la seule façon efficace



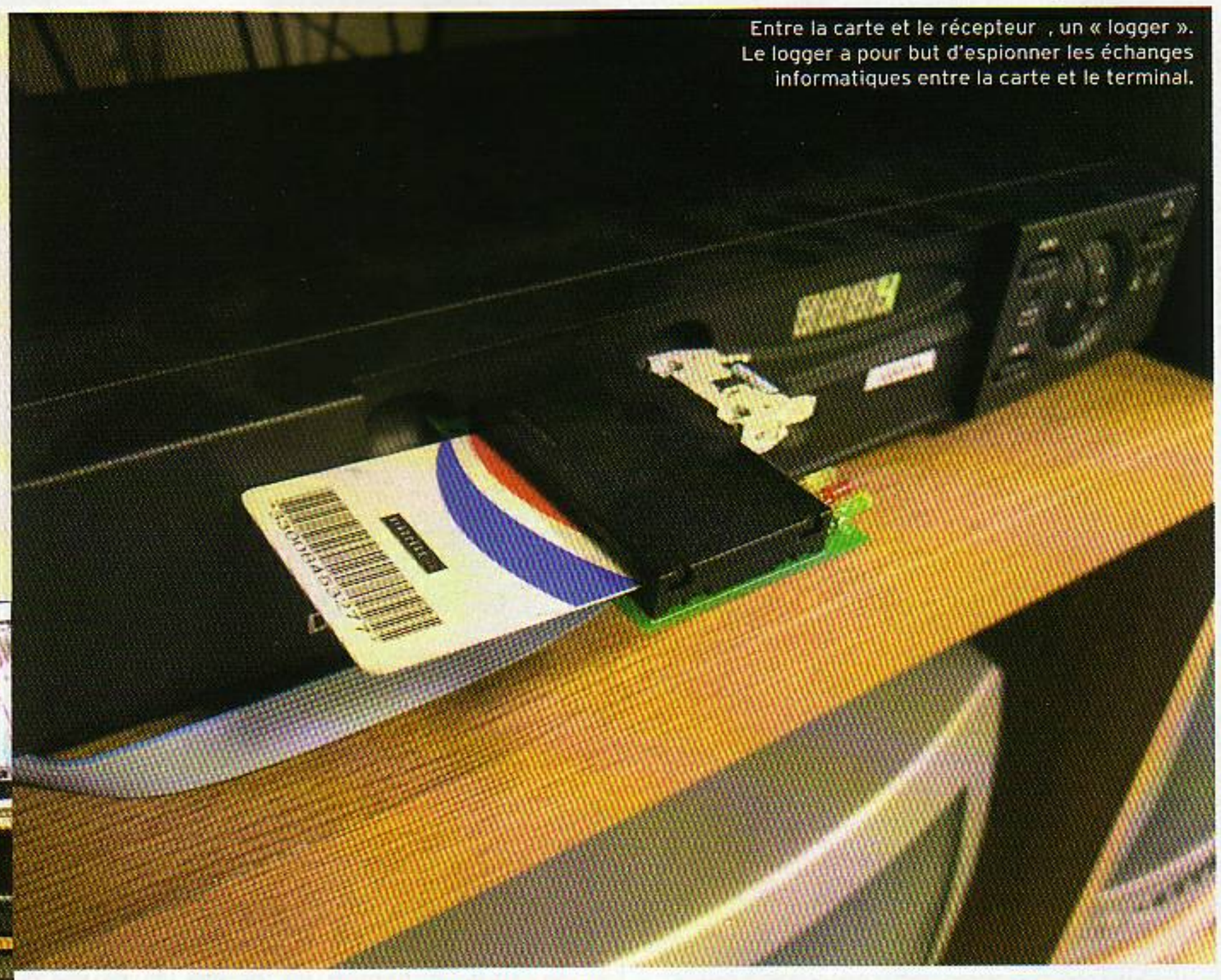
Une histoire policière :

➤ **L'histoire commence avec une arrestation :** celle d'Oliver Kömmerling, un jeune Allemand, génie de l'informatique et des cartes à puce, connaissant parfaitement les microprocesseurs et des logiciels de sécurité. Les faits qui lui sont reprochés : être à l'origine du piratage du contrôle d'accès élaboré par la société NDS pour la télévision à péage. NDS est aujourd'hui la filiale technologique du groupe de Rupert Murdoch, News Corporation (82 %). Dirigée par Abraham Peled, son Pdg, elle a mis au point les cryptages Videocrypt, utilisés alors principalement par une des sociétés du groupe, le bouquet analogique britannique Sky Television, et le Videoguard, que l'opérateur DirecTV, aux États-Unis, a été le premier à employer dès 1994. Et ce sont justement ces opérateurs qui ont été les victimes d'Oliver Kömmerling. Très vite, NDS propose à Oliver Kömmerling de le relaxer en échange d'une collaboration pour renforcer sa propre technologie, afin de la rendre, si possible, quasi infaillible. Le procès d'Oliver Kömmerling aboutit à un non-lieu. Et, dans la foulée, fin 1996, ce dernier part en Israël pour former des ingénieurs travaillant chez NDS. Il leur apprend comment arriver à déjouer les pièges des technologies de contrôle d'accès. Il illustre ses propos avec le cryptage mis au point par NDS qu'il a lui-même piraté. Mais, très vite, les trois ingénieurs travaillent sur les systèmes concurrents dans un but pédagogique... C'est ce que l'on a coutume d'appeler le "reverse engineering" qui peut conduire n'importe quel laboratoire de recherche à pirater ou " contrefaçonner ", c'est-à-dire tout simplement faire des recherches illégales à seule fin d'apprentissage technologique... Tout le monde en fait et c'est légal ! Même CANAL+ a reconnu avoir travaillé sur les systèmes de ses concurrents, mais de là à les rendre public...
Premier contrôle d'accès à apparaître sur le marché de la télévision numérique en Europe et dans le monde, après le Videoguard américain de Rupert Murdoch: l'Irdeto. Celui-ci est utilisé à l'époque, entre autres, par le bouquet italien Telepiù. L'Irdeto sera aussi le premier à être piraté, étant alors peut-être un des moins bien protégés.
(Lire l'article complet dans TS n° 154)

Par Daniel Renard

Le banc de test

→ Dans cette pièce sont installés des récepteurs satellites et des téléviseurs pour capter les principaux bouquets européens. Chaque terminal numérique est équipé d'un "logger" supportant la carte de décryptage qui est branchée sur son contrôle d'accès. Le logger a pour but d'espionner les échanges informatiques entre la carte et le terminal. Ces informations sont transmises à des ordinateurs qui les analysent. On peut ainsi monitorer en temps réel les contre-mesures, en vérifier l'efficacité et tenter de comprendre comment les pirates peuvent procéder.



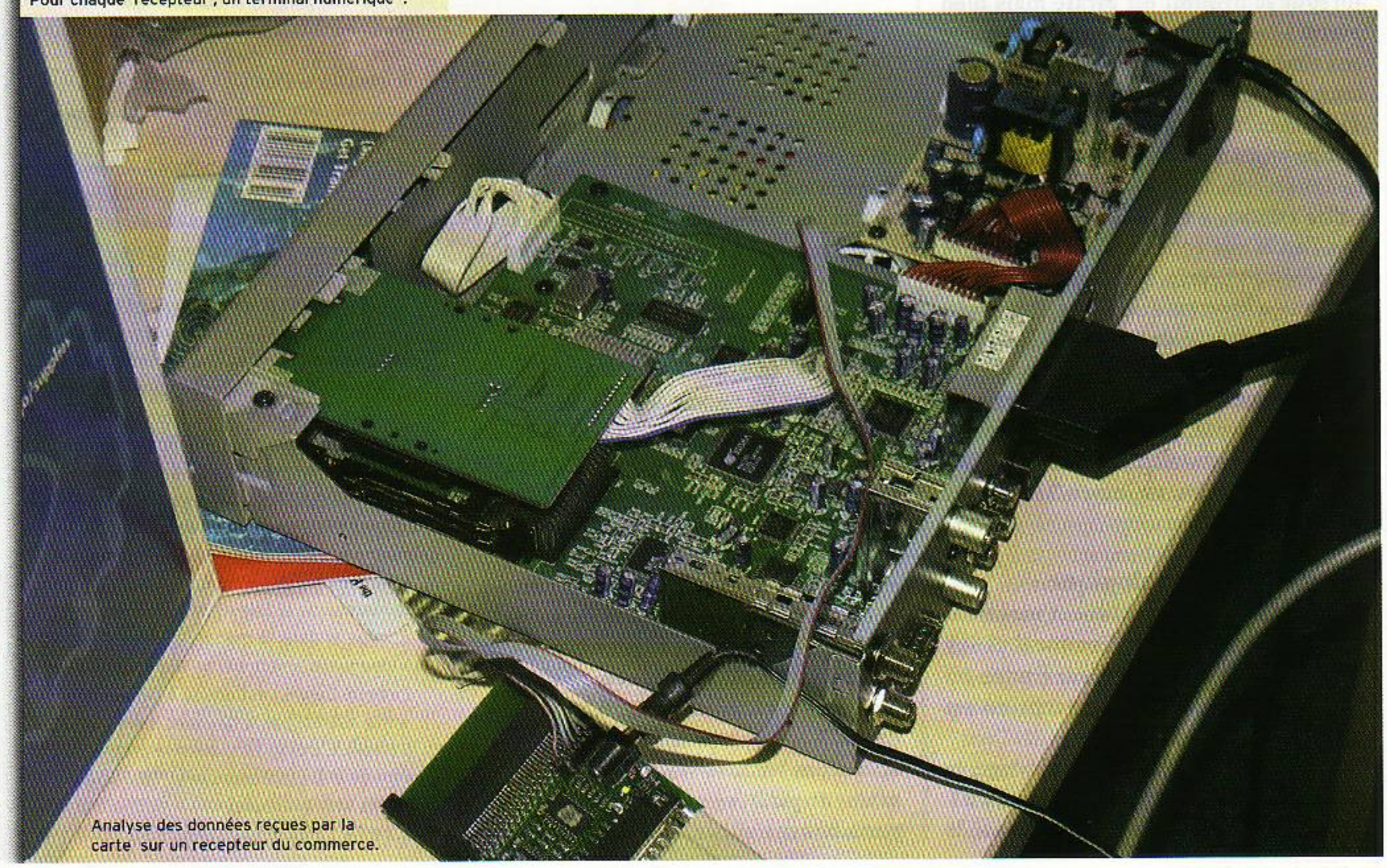
Entre la carte et le récepteur , un « logger ». Le logger a pour but d'espionner les échanges informatiques entre la carte et le terminal.

Local de réception des principaux bouquets cryptés . Pour chaque récepteur , un terminal numérique .

→ d'enrayer le phénomène est de remplacer les cartes actuelles à la technologie et de passer au Viaccess 2.5, encore inviolé à ce jour…

Le V1+ piraté !

Pour mieux comprendre les enjeux technologiques posés par les microprocesseurs, nous allons passer en revue les principales étapes permettant de les attaquer afin qu'ils livrent tous leurs secrets. C'est grâce à ces opérations qu'il est possible aux équipes de CK2 d'étudier les produits mis sur le marché afin de choisir le meilleur, celui qui saura protéger le mieux possible les algorithmes de cryptage. Il faut savoir, ce qui semble de prime abord étonnant, que le Médiaguard V1+ utilisé par Canal+ France est piraté ! Oui, piraté par… les équipes de CK2. Elles se sont piratées elles-mêmes afin de mieux préparer les contre-mesures électroniques qui seront utilisées quand il sera réellement piraté… Ainsi, CANAL+ ne donnera pas le temps aux pirates d'utiliser leur découverte : immédiatement le "remède électronique" →

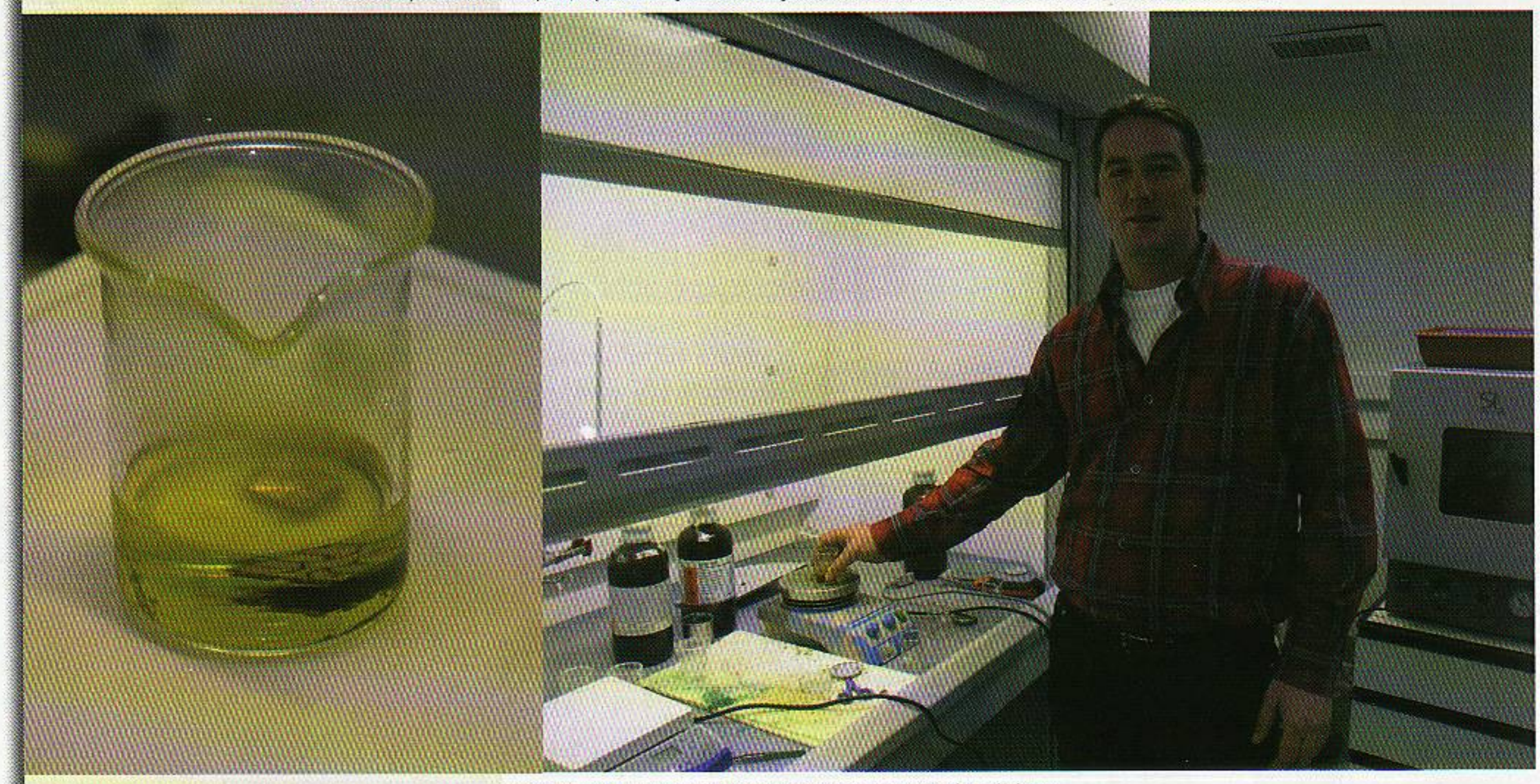


Analyse des données reçues par la carte sur un recepteur du commerce.

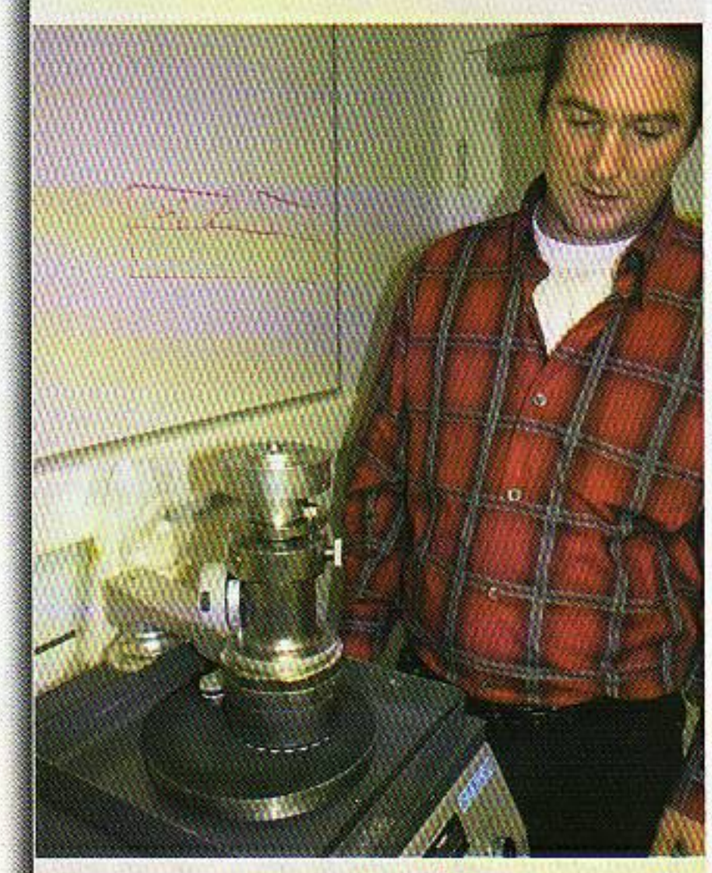
DOSSIER] → CK2

Par Daniel Renard

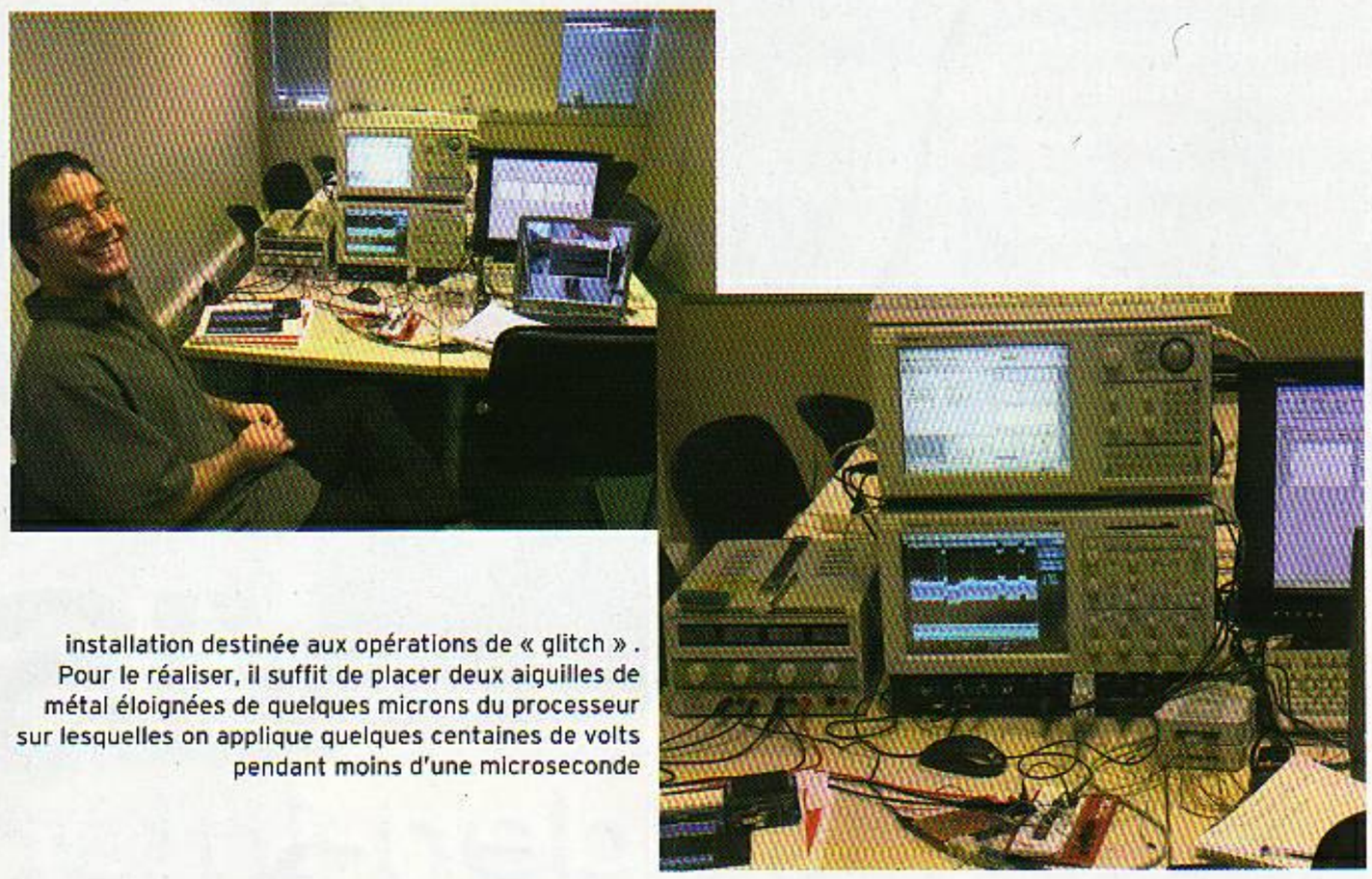
De nombreux produits chimiques, liquides et gazeux, dangereux sont utilisés pour démanteler les microprocesseurs.



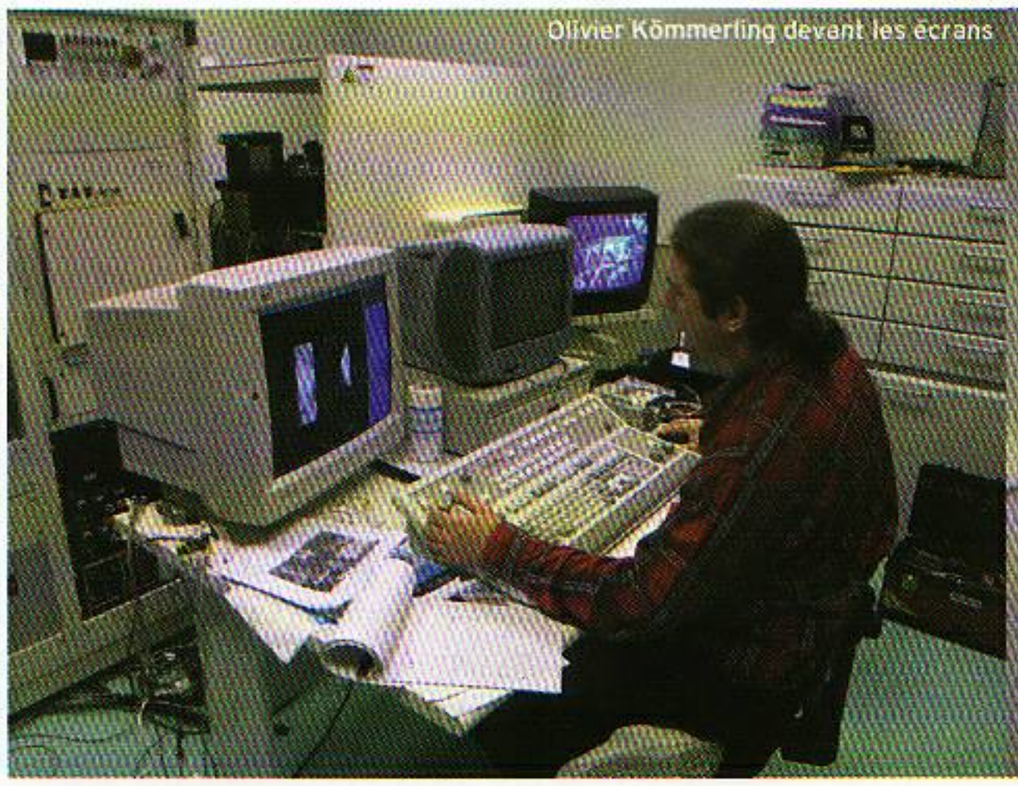
Olivier Kömmerling plonge le microproceseur dans l'acide nitrique



Olivier Kömmerling surveille « l'épluchage » du microprocesseur sur la machine



installation destinée aux opérations de « glitch ». Pour le réaliser, il suffit de placer deux aiguilles de métal éloignées de quelques microns du processeur sur lesquelles on applique quelques centaines de volts pendant moins d'une microseconde



Olivier Kömmerling devant les écrans

le « Plasmalab » permet de pratiquer une analyse sous ambiance gazeuse.

Olivier Kömmerling analyse le microprocesseur au microspcope électronique pour pratiquer les opérations de microprobing

sera administré et la brèche colmatée ! Le diffuseur français veut défendre son image de marque. D'ailleurs, la nouvelle génération de cartes Médiaguard, plus performante est actuellement en préparation avec une nouveauté technique qui permettra de la "patcher", via le signal diffusé pour mieux la protéger.

Un "sport" ancien

On peut faire remonter les origines du piratage des cartes d'accès aux années 1994 : à partir de cette époque, tous les bouquets cryptés, que ce soit en Europe, en Amérique du Nord et du Sud, en Asie, ont vu leurs cartes copiées et le système de cryptage piraté. Ce "sport" repose sur différentes techniques que nous allons passer en revue.

Les origines du piratage des cartes d'accès remonte aux années 1994 ou tous les bouquets cryptés, en Europe, en Amérique du Nord et du Sud, en Asie, ont vu leurs cartes copiées et le système de cryptage piraté.

Parmi elles, certaines sont dites "invasives" et nécessitent l'attaque physique de la carte comme le "microprobing" ; d'autres, plus douces, comme les attaques logicielles, les "écoutes clandestines" et les recherches de défaillances. Notons que les attaques "douces" sont dangereuses car elles ne se repèrent pas immédiatement et que les moyens mis en œuvre sont relativement modestes. Elles sont basées sur la connaissance détaillée à la fois du processeur et du logiciel.

Les attaques "invasives" dues au microprobing demandent peu de connaissances spécialisées puisqu'elles utilisent des techniques largement répandues dans des technologies similaires. C'est pourquoi les attaques contre les cartes commencent par le "reverse engineering", lequel permet ensuite d'utiliser les techniques douces... Nous allons expliquer, le plus clairement possible, les principales techniques de ces attaques dont nous venons de décrire les principes basiques.

Les attaques invasives.

Le principe repose sur l'étude du microprocesseur et celle-ci passe par son démantèlement systématique ; la première étape consiste à chauffer la carte pour extraire le microprocesseur, afin de le plonger dans de l'acide nitrique à 60°C, ce qui va provoquer la dissolution complète de la résine époxy qui enveloppe le silicium. On la nettoie ensuite à l'acétone dans un bain à ultrasons. Cette "puce" mise à nu est engluée dans un cadre qui permet de faire des tests en reliant ses contacts à une machine.

Puis vient le "découpage en tranches" du microprocesseur qui va permettre d'en dresser une carte précise en utilisant un microscope électronique, équipé d'une caméra qui le grossit 1 000 fois. On peut ainsi découvrir son architecture, comme les liaisons qui transportent les données, les interconnexions, les emplacements des mémoires (ROM, RAM, EEPROM, etc...) .

Cet "effeuillage" physique détruit le microprocesseur et, en cas de fausse manœuvre, il faut recommencer les opérations depuis le début.

Le microprobing.

Cette opération, que l'on pourrait appeler "essais microscopiques", se déroule à l'aide d'une station de travail spécialement équipée : elle comporte un microscope électronique dont l'objectif est placé à 8mm maximum de la surface à tester et d'un minuscule instrument en forme de tige, télécommandé, équipé à son extrémité d'un filament de tungstène de 5 mm de

Police et Justice s'en mêlent

Le second volet de l'action du CK2 repose sur la traque des pirates, que ce soient des individus isolés ou des réseaux constitués. La mondialisation de toute l'économie, y compris celle du piratage, impose une lutte transfrontière. Au-delà de la veille technologique qui permet de débusquer les actions de piraterie, il faut agir et poursuivre les auteurs, que ces soient "les petits", ceux qui en profitent en commercialisant des logiciels ou des matériels pirates, ou mieux, "les gros poissons", ceux qui sont à l'origine de cette fraude et de sa commercialisation. Dans tous les cas il est nécessaire de faire appel aux services de Police des pays concernés, puis de porter l'affaire devant la Justice. CANAL+ et le CK2 se sont donnés comme mission de débusquer et de poursuivre toutes les affaires dont ils ont pris connaissance.

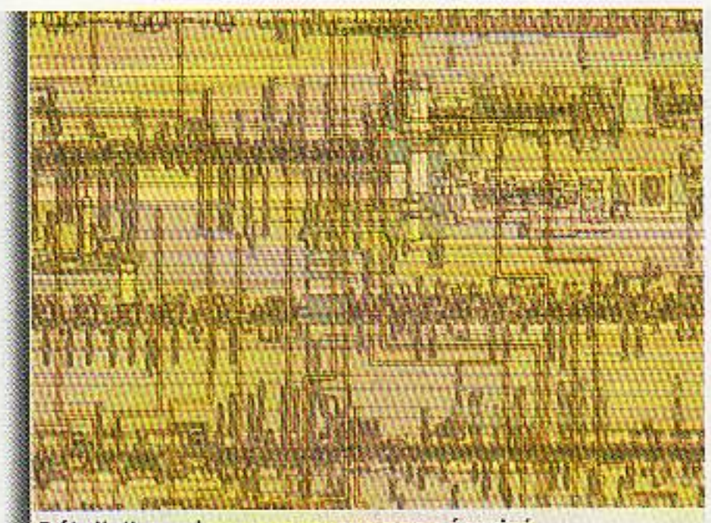
C'est la raison pour laquelle, régulièrement, nous avons des informations sur des actions policières et judiciaires qui débouchent sur des arrestations, plus ou moins importantes, et souvent sur des condamnations. Parmi les dernières actions, celle engagée en Italie par Nagravision France, le nouveau propriétaire de la licence Médiaguard, autrefois possédée par CANAL+. Plus de quinze personnes ont été interpellées, ce qui fait qu'aujourd'hui l'essentiel du réseau de piratage italien est fortement atteint.

De son côté, CANAL+/ CK2 a fait procéder, début décembre 2004 à Malte, à l'arrestation d'un certain Tonydo, bien connu dans le milieu des administrateurs de sites.

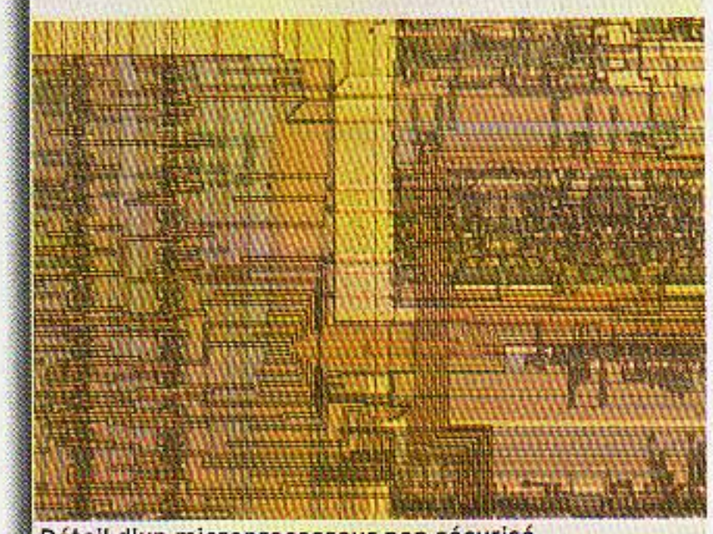
En Espagne, c'est Zacky Files (pseudo) qui s'est retrouvé menottes aux poignets en novembre pour le piratage du syster... suite à une plainte qui date de décembre 2003.

D'autres chantiers sont en cours : les cibles se situent au niveau des chercheurs, des concepteurs et des penseurs. Il est évident que le revendeur dans la rue ne présente pas un grand intérêt, si ce n'est, comme dans le cas de tout trafic, pour remonter la filière jusqu'à la tête. Notez que par ailleurs, dans le cadre de procédures judiciaires, « CK2 » répond régulièrement à des réquisitions formulées par des magistrats ou autorités de police pour expertiser des cartes à puce ou tout autre équipement lié au piratage audiovisuel

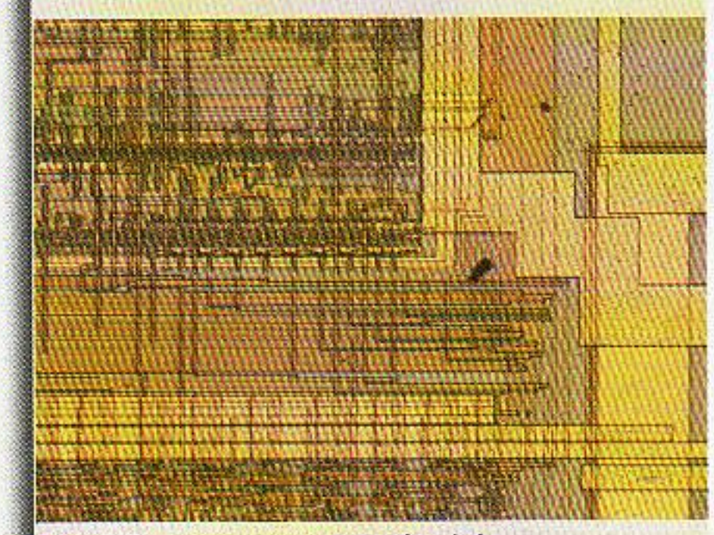
Par Daniel Renard



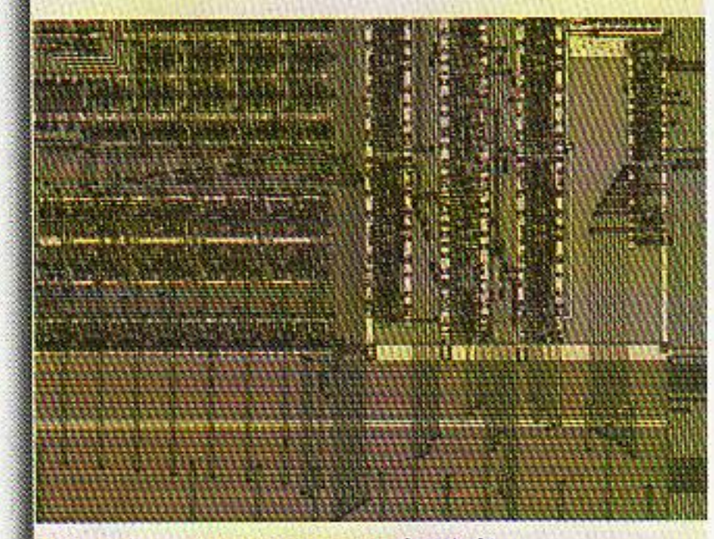
Détail d'un microprocesseur non sécurisé en technologie 0.50 µm (*ancienne génération*)



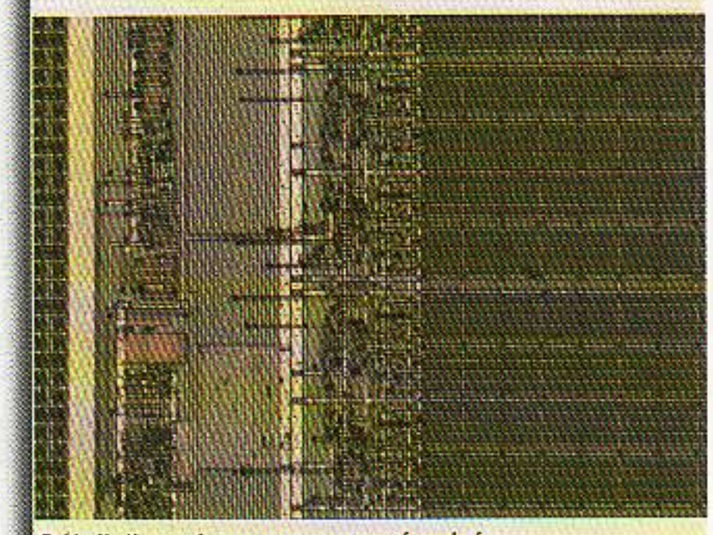
Détail d'un microprocesseur non sécurisé en technologie 0.50 µm (ancienne génération)



Détail d'un microprocesseur sécurisé en technologie 0.18 µm (*nouvelle génération*)



Détail d'un microprocesseur sécurisé en technologie 0.18 µm (*nouvelle génération*)



Détail d'un microprocesseur sécurisé en technologie 0.18 µm (*nouvelle génération*)

long qui se termine par une pointe fine de moins de 0,1 micron. Avec cette tige, l'opérateur peut viser précisément des points de contact sur la couche visible de la puce et établir des contacts électriques directement sur les liaisons apparentes sans les endommager, lesquels sont exploités par un générateur de signaux numériques qui peut à la fois enregistrer les informations recueillies et générer des signaux pour faire fonctionner le microprocesseur.

Parallèlement, un générateur laser vert est utilisé pour enlever les couches de protection permettant de faire apparaître une seule "bus line" (liaison). Le prix de telles installations peut dépasser 1 million d'euros, de même pour le prix du laser…

Les faisceaux à particules.

Les techniques exposées jusqu'à présent permettent d'explorer des dimensions comprises entre 0,5 et 1 micron, reparties sur deux couches métalliques. Pour pouvoir pousser plus avant les recherches pour les cartes exploitant plus de deux couches métalliques et dont la grandeur des éléments est inférieure à la longueur d'onde de la lumière visible, il est nécessaire d'utiliser une chambre à vide équipée d'un canon à électrons qui projette un faisceau d'électrons concentré pouvant être réduit à un diamètre de 5 à 10 nanomètres avec des courants électriques de 1 pA à 10 nA. Le rendement du système peut être amélioré en utilisant des injections de gaz iodine provoquant des réactions chimiques à la surface de la puce et qui se traduisent par des "trous" permettant d'établir de nouveaux contacts électriques. Il est possible ainsi d'attaquer la fréquence d'horloge du processeur pour l'abaisser en dessous de 100 KHz et permettre l'enregistrement en temps réel de toutes les connexions (bus lines).

Les attaques douces.

Un processeur est constitué de quelques centaines de systèmes électroniques à bascule (registres, verrous, SRAM, etc…) qui définissent son état physique, auxquels s'ajoute une logique informatique combinée qui calcule, selon les cycles de l'horloge interne d'après l'état présent, l'état suivant. Il faut savoir que chaque transistor et chaque interconnexion ont une capacité et une résistance qui déterminent la vitesse de propagation du signal, laquelle varie sous l'influence de différents facteurs comme la température et la tension d'alimentation. De même pour les systèmes de bascule dont les intervalles d'échantillonnage varient de l'un à l'autre.

L'attaque dite "glitch" (problème) consiste à générer un dysfonctionnement qui conduit un ou plusieurs systèmes à bascule à adopter un "mauvais état". On peut ainsi remplacer des instructions ou corrompre des valeurs informatiques qui sont transportées entre les registres et les mémoires. Cela permet de créer une "fenêtre de vulnérabilité" pouvant empêcher, au-delà de la barrière de la cryptographie, l'exécution du code détectant les attaques. Il est possible aussi d'agir sur l'horloge en accroissant sa fréquence, ce qui provoque des changements de cycle des systèmes à bascule. Pour le réaliser, il suffit de placer deux aiguilles de métal éloignées de quelques microns du processeur sur lesquelles on applique quelques centaines de volts pendant moins d'une microseconde. Les instructions ainsi envoyées provoquent des niveaux d'activité différents dans les instructions de décodage et les unités arithmétiques permettant de reconstituer des éléments de l'algorithme de cryptage.

Toutes ces opérations visent à permettre la lecture des informations contenues dans le microprocesseur, en accédant là où elles sont stockées en mémoire. C'est pourquoi ces accès doivent être minutieusement étudiés afin d'éviter le piratage. Pour re-prendre l'image du "coffre-fort", plus son ouverture est difficile, plus son contenu sera protégé. Voici comment, avec ces techniques de pointe, les ingénieurs peuvent pénétrer les microprocesseurs pour les "faire parler".

Pour reprendre l'image du "coffre-fort", plus son ouverture est difficile, plus son contenu sera protégé.

Vous comprendrez aisément que l'important est de rendre cette "pénétration" la plus difficile possible, afin d'interdire l'accès aux informations qui y sont contenues. En effet, une fois le microprocesseur "pénétré", l'information étant extraite et exploitable, il est trop tard pour réagir efficacement. C'est donc l'objectif que s'est fixé le CK2 et son équipe d'ingénieurs en déclarant une guerre sans fin aux pirates. ●

* 10-9 = nano - 10-12 = pico

Pour contacter CK2

Gilbert Borelli (*Directeur*)
CK2 SECURITY
Espace Beethoven
1200 route des Lucioles
BP 68
06902 SOPHIA ANTIPOLIS CEDEX
Tel : 04.97.21.42.42