

# Securicom : la course vers le complexe

PAR JACQUES MAISONVERTE

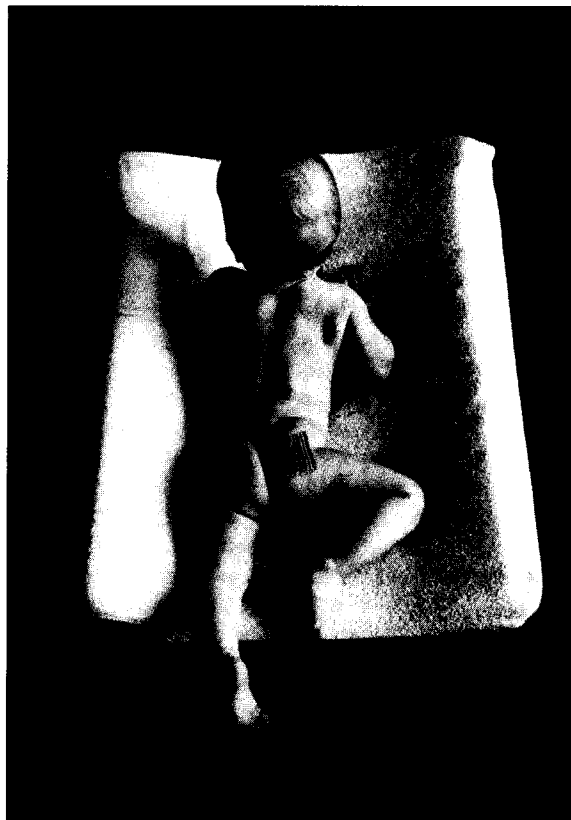
Cette année encore, au SECURICOM, l'événement est venu d'Allemagne. En 88, Wernery, membre du célèbre *Chaos Computer Club* de Hambourg était arrêté par la police française à sa descente d'avion. En 89, on apprenait le dernier jour du colloque \* l'arrestation en RFA de jeunes *hackers* qui espionnaient pour le compte de l'Est. L'impression générale est que les systèmes informatiques sont de plus en plus sophistiqués et que, parallèlement et peut-être exponentiellement, les dispositifs de sécurité se complexifient, et que la maîtrise des uns et des autres tend à échapper à l'entendement.

Encore plus que les années précédentes, au colloque Securicom, on ressentait une étrange impression de course éperdue vers une complexification croissante des systèmes de protection. En particulier les réseaux, *tremendly complex*, qui s'étendent en l'absence de norme permettant la protection des données de manière cohérente de bout en bout des lignes, inquiètent les responsables de la sécurité des grandes entreprises. Comment assurer efficacement la protection et la fiabilité d'un réseau de 200 000 terminaux points de vente britanniques ou les 30 000 micros de la Poste ? Seules des solutions partielles sont mises en place, telle une carte de sécurité intégrée dans les micros de la Poste.

## Mots de passe...

Les systèmes de codage sont nombreux : à clé publique, à clé privée, asymétrique tel le RSA, symétrique tel le DES, algorithme de Fiat Shamir, de Rabin, protocoles à connaissance zéro, entièrement logiciels ou en partie matériels. Aucun ne suscite l'adhésion générale des spécialistes, mais plutôt des discussions passionnées entre leurs divers supporters.

De nouvelles techniques de protection ont été présentées, mais les orateurs ont tous pris soin de terminer en disant que leur dispositif était bon *pour le moment*. L'unanimité s'est faite par contre sur l'idée qu'il ne faut protéger une installation que jusqu'à un certain niveau de sécurisation, où le coût de son effraction devient dissuasif. Ainsi a été présenté un système de cryptage utilisant une simple calculatrice, et qui donne pour une somme modique une protection correcte sans



*En ce qui concerne les transferts d'analyses médicales, la CNIL impose un codage dans les deux directions...*

\* Organisé par  
SEDEP, 8, rue de la  
Michodière,  
75002 Paris..  
Tél. 47 42 40 30.  
Prochain  
SECURICOM du  
13 au 16 mars 1990.

prétention à l'invulnérabilité. En définitive, les failles des dispositifs de sécurité, avec ou sans cartes à puces, tournent autour des questions suivantes : qui gère les clés ? où sont-elles mémorisées ? qui en est le responsable ? comment sont-elles protégées ? comment sont-elles distribuées ? comment est initialisé le système ? La multiplication des mots de passe et des clés de codage (pour le PC, les réseaux, les systèmes...) conduit bien souvent les utilisateurs à opter pour les mêmes, à l'inverse du but recherché. Vaste sujet donc, dont la complexité est réelle si l'on désire se prémunir efficacement.

... et secrets

En ce qui concerne le cryptage, le code dit DES à 8 itérations a été cassé par le mathématicien israélien Shamir sur un simple PC, en trois minutes, grâce à une nouvelle technique mathématique et non, comme on le pense souvent, par un surcroît de puissance de calcul. On estime donc que le DES d'IBM à 16 itérations devrait être percé dans les années à venir ; cette annonce n'a pas surpris outre mesure C. Meyer, le spécialiste du codage d'IBM. Shamir s'est refusé à donner des informations sur sa technique, il s'est contenté d'en faire la démonstration. C'est là une attitude qui révèle l'importance stratégique de tels personnages.

Au centre des préoccupations, les virus ont suscité beaucoup de recherches sur les parades. Mais étant donné la variété des virus, aucune technique n'est polyvalente. Toutefois une méthode a été présentée qui, à partir d'un programme *off line* sur disquette, permet de savoir si les programmes et les fichiers ont été modifiés, si des entrées-sorties ont été opérées depuis la dernière utilisation par le titulaire. Ce dispositif utilise des contrôles sur l'éventuelle modification de la taille des fichiers, sur le contenu (par un *cheksum*, image condensée d'un fichier) et sur les interruptions d'écriture.

Dossiers médicaux

Les virus sont pris au sérieux par les responsables informatiques : toutes les techniques permettant l'identification, l'authentification, l'intégrité s'avèrent de plus en plus nécessaires, et même si elles coûtent du temps et de l'argent, leur usage ne peut que s'étendre.

La prolifération des fichiers médicaux destinés soit à la recherche, soit à la gestion des dossiers des malades posent des problèmes de protection et de déontologie. Il en est de même de la transmission de données sensibles, telles que des résultats d'analyses, par le biais de réseaux, en particulier celui du minitel.

Les déontologies européennes ne protègent pas toutes également le secret médical ; alors que se passe-t-il si l'on transmet vers un pays à faible protection, des données qui en France bénéficient d'un bon niveau de confidentialité ? Le secret médical n'est pas partageable ; alors comment le respecter dans le cadre de l'informatisation d'une équipe médicale ? En ce qui concerne les transferts de données sensibles telles que les analyses médicales, la CNIL impose, pour donner son accord, un codage dans les deux directions pour en garantir la confidentialité, une protection par cartes à puces en ce

qui concerne la sécurité et l'authenticité, et une redondance de la transmission pour en assurer l'intégrité. Ce dispositif doit être obligatoirement doublé d'un document écrit et signé, le seul qui vaille légalement.

La spirale infernale

Le problème est complexe, alors... on en rajoute un peu pour rendre le système moins vulnérable, ce qui évidemment introduit une couche supplémentaire et une faille nouvelle. Pour sortir de cette spirale infernale, certains ont proposé une approche globale, bien difficile à concrétiser car les utilisateurs, en particulier, ont rarement la maîtrise complète des réseaux mis en œuvre.

Les pays développés n'ont plus le privilège de la vulnérabilité : des informaticiens chinois ont en effet annoncé qu'au moins trois escroqueries s'étaient produites dans des banques ; les autorités chinoises commencent donc à s'en préoccuper et se proposent de légiférer en la matière. Un des spécialistes chinois a souhaité qu'une coopération se mette en place « avec les experts et amis à travers le monde » pour « garantir le sain développement de l'informatique et la rendre profitable à l'humanité ».

Et pour terminer, une anecdote : un orage de grêle s'est abattu sur le toit de la salle du colloque, couvrant la voix de l'orateur, et l'instant d'après une panne de courant a contraint l'orateur à s'arrêter faute de lumière, de sono et de rétro-projecteur ! Les cordonniers seraient-ils vraiment les plus mal chaussés ? ■

LISEZ LE MENSUEL

SILENCE

• L'ÉCOLOGIE : les relations des personnes avec la nature (l'environnement) et avec les autres (social) nous semblent une bonne base politique.

• LA NON-VIOLENCE : le rejet de la violence... mais sans passivité nous semble une bonne méthode.

• LES ALTERNATIVES : la mise en pratique de nos idées nous semble indispensable pour être crédible.

VOUS AUSSI

PARTICIPEZ AU DÉBAT

Pour un exemplaire gratuit

NOM ..... PRÉNOM .....

ADRESSE .....

CODE POSTAL ..... VILLE .....

A retourner à *Silence*, 4, rue Bodin, 69001 LYON