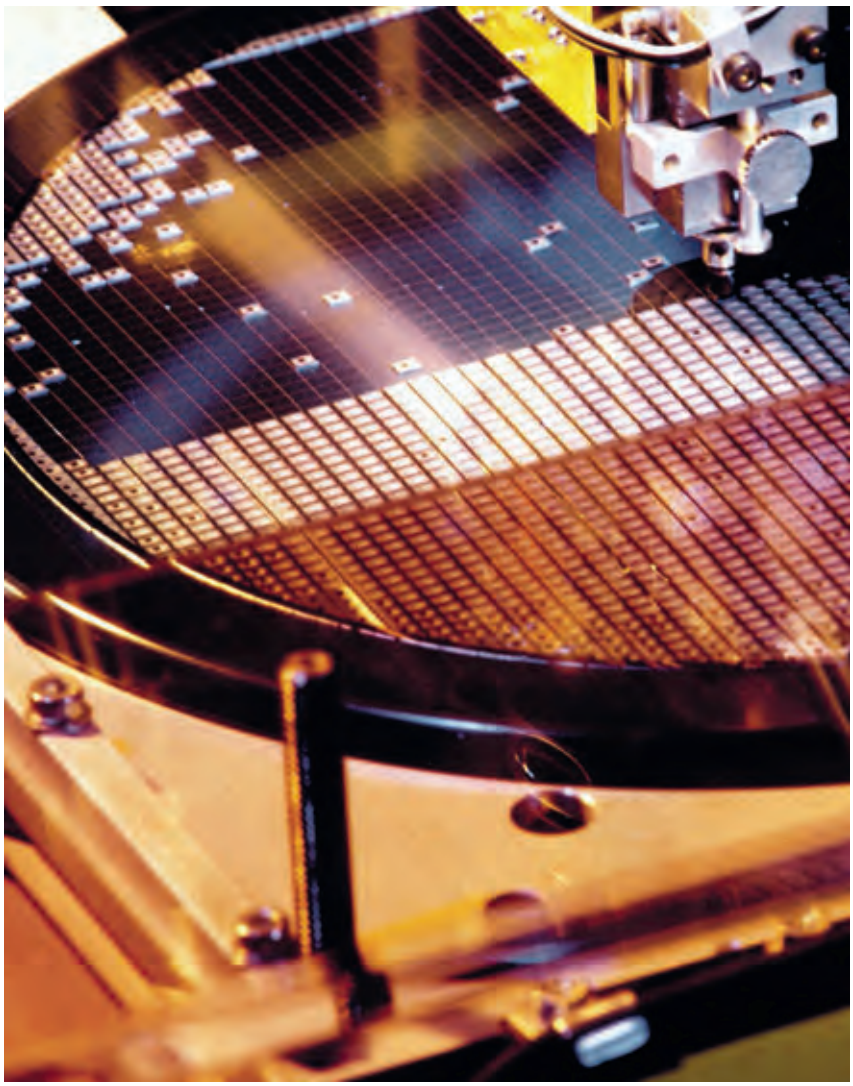
PAR PHILIPPE GEYRES (70)
Directeur général délégué,
Oberthur Technologies

La clé du monde numérique

La France est aujourd'hui le leader mondial de la carte à puce, depuis les débuts du Publiphone en 1984 puis avec les cartes bancaires et les cartes SIM du téléphone mobile (3 milliards seront vendues en 2008). Et cette réussite économique devrait continuer grâce aux nouveaux besoins d'identification et de sécurité. Le développement d'Internet et les services en ligne, comme la banque à domicile et les achats électroniques, demandent identification et transactions sécurisées. Le téléphone portable à tout faire permet les mêmes services avec la mobilité en plus. Il est déjà possible de réaliser des achats sur Internet depuis son mobile.
Demain, cartes de crédit et titres de transport seront dans notre mobile.
Une identité électronique pour chaque citoyen, internaute ou pas, augmente la sécurité et le contrôle des personnes tout en pouvant leur garantir le respect de leur vie privée.
L'industrie française continue d'investir en recherche et applications-pilotes sur ces sujets, et conserve son avance dans les technologies de sécurité.



Une carte à puce en 2008

Une carte à puce a aujourd'hui un microprocesseur aussi puissant que celui d'un ordinateur de 1990, communique avec USB2.0 et sa mémoire embarquée se compte en gigaoctets. Elle peut ainsi contenir 500 fichiers MP3 ou JPEG, quelques DIVX, ou même devenir serveur de pages Web...

La clé du monde numérique

Cette carte à puce est la clé du monde numérique. Citons, par exemple, la clé d'accès à la télévision, hier dans un décodeur de salon aujourd'hui dans un mobile, la clé d'accès à des services de voix sur IP (téléphonie *via* Internet) avec une clé USB identique à une carte SIM permettant de retrouver le carnet d'adresses de son portable sur un ordinateur.

La convergence numérique, c'est la disponibilité de tous les services sur un même outil – PC, téléphone mobile ou voiture.

Déjà, un titre de transport peut être téléchargé dans la carte SIM d'un téléphone mobile. Celui-ci avec NFC (Near Field Communication) va communiquer en mode sans contact avec les terminaux de contrôle d'accès. Là encore, la carte SIM est l'identité numérique de l'abonné.

La nouvelle identité électronique

Décliner son identité et, au nom de celle-ci, se voir reconnaitre certains droits par un tiers est néces-

Le cryptosystème RSA est l'algorithme le plus employé dans le monde pour les chiffrements et signatures électroniques

Pour cacher l'information contenue dans un message m, cela consiste à effectuer le calcul $y = m^e \text{ modulo } n$ où e et n sont des paramètres publics. Pour retrouver m à partir de y, il faut être capable d'inverser l'exponentiation modulaire, ce qui revient à trouver un élément d tel que $e\ d = 1 \bmod n$. Ce calcul est réputé être très difficile si l'on ne sait pas décomposer n en un produit de plus petits nombres et devient facile (*via* un algorithme dû à Euclide) dans le cas contraire. Malgré son étonnante simplicité, l'algorithme RSA a depuis quarante ans résisté avec succès aux attaques des mathématiciens du monde entier.

Même si l'algorithme RSA est très résistant aux cryptoanalyses théoriques, sa mise en œuvre (comme celle de n'importe quel autre algorithme) peut être facilement attaquée si elle a été faite sans précautions particulières. Le but de l'attaquant va être de retrouver la valeur secrète d stockée dans la carte, par exemple en la perturbant avec un laser qui génère à la surface de la puce un courant photoélectrique et donc « injecte des fautes » pour changer des bits en mémoire ou les états de portes logiques.

Le RSA est souvent mis en œuvre en utilisant l'astuce d'Henri Garner et le théorème dit *des restes chinois* qui permet de diviser par 4 le temps d'exécution. Notons p et q deux nombres premiers tels que $n = pq$, le mode de calcul RSA dit CRT permet d'obtenir la signature $y = m^d \bmod n$ en calculant tout d'abord $Sp = m^d \bmod p$ et $Sq = m^d \bmod q$ puis à appliquer la recombinaison de Garner pour finalement obtenir $y = ((Sp-Sq)\ q^{-1} \bmod p)*q + Sq$. Nous pouvons alors remarquer que l'on a $y = a\ Sp + b\ Sq$ où $a \equiv 1 \bmod p$, $a \equiv 0 \bmod q$, $b \equiv 0 \bmod p$ et $b \equiv 1 \bmod q$. S'il perturbe par exemple le calcul de Sp, un attaquant va obtenir une signature erronée y' qui sera égale à $a\ Sp' + b\ Sq$, où Sp' désigne le résultat de calcul erroné de Sp. En soustrayant y à y', l'attaquant va obtenir la valeur $a(y' - y)$. Or, cette valeur est un multiple du paramètre secret q et l'attaquant peut donc retrouver la valeur de ce paramètre en calculant le *plus petit diviseur commun* entre le $n = pq$ et $y'-y$.

saire dans une société organisée. L'identité est aujourd'hui électronique.

Le passeport électronique embarque une carte à puce dans sa couverture. La Belgique a été le pionnier en Europe, la réglementation américaine après le 11 septembre a accéléré son adoption partout dans le monde.
Le développement d'Internet a rendu plus prégnant le besoin d'identification électronique, mais a également vu émerger le vol ou l'usurpation d'identité. Aujourd'hui la plupart des identifications requises pour accéder à des cyberservices reposent sur des numéros d'identification associés à des mots de passe, avec un niveau de sécurité très insuffisant.
Une carte à puce sous la forme d'une clé USB comme Webstick™ d'Oberthur allie les moyens cryptographiques d'une carte à puce, à la facilité d'utilisation d'une clé USB. Il suffit d'insérer cette clé dans un PC, pour ouvrir un accès sécurisé aux services de banque en ligne, par exemple, authentifiant son porteur grâce au code PIN associé ou à la reconnaissance d'une empreinte digitale.

Le développement des services de téléphonie mobile exige une sécurité accrue

Utiliser son téléphone mobile pour des applications autres que la téléphonie, et en particulier le paiement sans contact, impose de nouvelles exigences sécuritaires.

La coexistence d'applications fournies par différentes sociétés, telles que banques, opérateurs de transports ou chaînes de magasins, demande des silos indépendants et sécurisés dans une carte SIM.

L'activation des droits aux services et la gestion des cartes SIM se font par le réseau (OTA, Over the Air), avec des plateformes sécurisées. C'est le concept de TSM « Trusted Service Management », véritable autorité de confiance entre les opérateurs de téléphonie, les fournisseurs de services et les usagers.

Une course incessante entre l'arme et la cuirasse

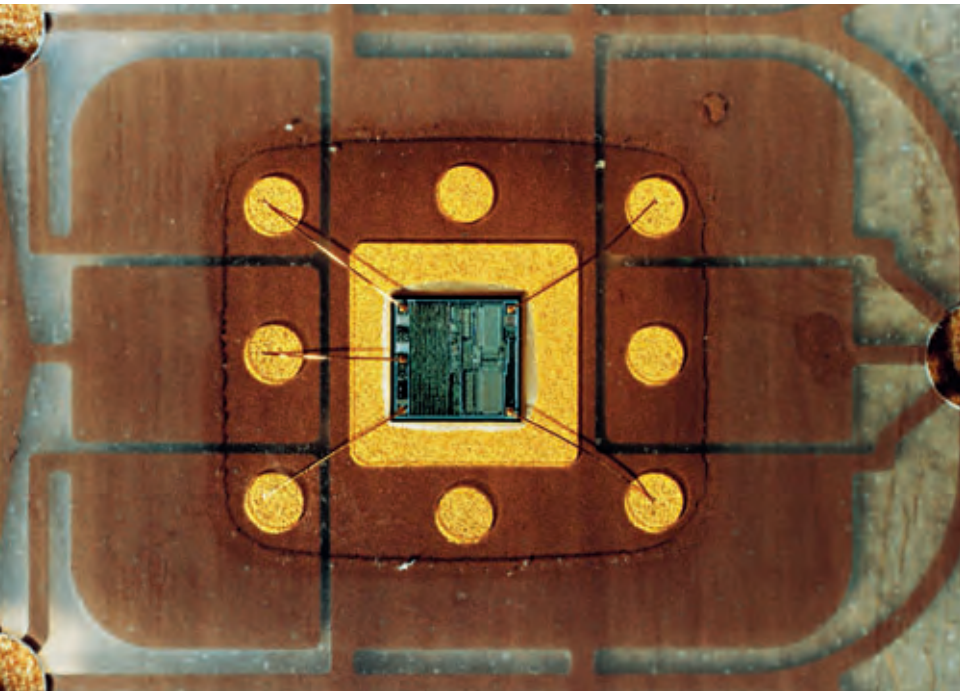
La sécurité des systèmes et des protocoles a historiquement été pensée pour protéger les communications d'un utilisateur placé dans un environnement hostile. Le monde numérique a fondamentalement modifié cette hypothèse. Aujourd'hui la sécurité d'un système ne peut reposer sur l'honnêteté supposée de ces utilisateurs.

Sécuriser les communications de façon fiable et économique pour un usage par le grand public a longtemps été un défi jusqu'à l'apparition des premières cartes à puce : une partie de la mémoire d'une carte peut en effet être protégée par des mécanismes hardware très efficaces (appelés inhibiteurs). Une telle protection n'existe généralement pas pour les mémoires des ordinateurs.

Dans les années quatre-vingt-dix, des équipes de chercheurs ont élaboré de nouveaux types d'attaques ne consistant plus à accéder directement aux données sensibles mais à analyser leurs manipulations par la carte. Ces attaques reposent sur le constat que le comportement d'un système embarqué est très fortement dépendant des valeurs des données qu'il manipule. Les échanges d'information entre une carte à puce et l'extérieur peuvent être décelés, par exemple, par la consommation d'énergie de la carte, son rayonnement électromagnétique, son temps d'activité ou son rayonnement calorifique. En observant le temps ou l'énergie nécessaire à un calcul, il est possible d'en déduire les opérandes. Supposons qu'une carte à puce ait à effectuer le produit entre une donnée publique x et une donnée secrète y. Le temps nécessaire au calcul $x*y$ est très différent selon que y est nul ou non, la plupart des microprocesseurs incluant des mécanismes d'optimisation. Un attaquant peut retrouver un peu d'information sur y. Depuis leur introduction, les attaques par analyse de canaux cachés ainsi que les mécanismes mis en place pour les contrer ont fortement évolué. Les attaques actuelles recourent à des analyses statistiques ou de traitement du signal tandis que les contre-mesures modifient les algorithmes. L'étude de la sécurité embarquée est ainsi au carrefour de domaines scientifiques divers comme l'algèbre, l'analyse statistique, le traitement du signal, la théorie de l'information, l'électronique, l'informatique.

Il existe une autre grande famille d'attaques, dites par injection de fautes ou par perturbation, qui essaient de mettre le système ciblé dans un état anormal de fonctionnement. Elles consistent, par exemple, à faire en sorte que certaines parties d'un code ne soient pas exécutées ou que certaines opérations soient remplacées par d'autres. La carte à puce pourrait alors se retrouver à agir contre son intérêt, par exemple en renvoyant des données sensibles comme des clefs de chiffrement.

Ces attaques ont en commun d'être des menaces de type externe. La carte à puce va essayer de les contrer comme on défend une place forte contre des envahisseurs. Tant que la carte à puce est restée un système fermé ne répondant qu'à un très petit nombre de requêtes et ne contenant que des applications validées et certifiées, ce modèle a été suffisant. Récemment, la carte à puce pour ses nouveaux usages est devenue une plate-forme ouverte sur laquelle sont chargées des applications bancaires ou multimédias par exemple. Notre place forte doit alors aussi faire face à des menaces internes. De ce point de vue, certaines problématiques de sécurité de la carte à puce ont rejoint celles du domaine plus vaste de la sécurité des systèmes et des réseaux.



L'authentification d'une identité numérique utilise des algorithmes de cryptographie complexes comme RSA (du nom de ses trois inventeurs, en 1977, Rivest, Shamir et Adleman) ou les courbes elliptiques (ECC).

Actuellement, la cryptographie ECC tend à s'imposer par ses performances bien meilleures que le RSA à mesure que la résistance cryptographique requise augmente. Le passeport biométrique de seconde génération, interopérable au niveau européen, utilisera l'ECC, sur lequel l'industrie de la carte à puce travaille depuis plus de dix ans. ■

REPÈRES

Oberthur est le 2e acteur mondial de l'industrie de la carte à puce, avec 5 500 collaborateurs, présents dans 40 pays.