Cryptanalyse : « les yescards »

La progression des moyens informatiques et des outils d'analyse mathématique entraîne une course poursuite entre la cryptologie (la science de la cryptographie) et la cryptanalyse (l'art de briser un cryptosystème). Gare à ceux qui sont à la traîne ! Ce fût le cas du groupement interbancaire (GIE) qui certifie les cartes bleues. Bien qu'averti par des spécialistes de l'obsolescence de leur système face aux techniques modernes, le GIE a utilisé durant plus de 15 ans un système initialement prévu pour ne durer que 5 années. A la fin des années 2000, Serge Humpich a découvert la faille… Avant de voir celle-ci présentons comment fonctionnent les cartes bleues.

Formation d'une carte bleue

En 1983, le GIE s'appuie sur la cryptographie RSA (voir article) pour former un cryptosystème à clé privée, clé publique basé sur un nombre $n = pq$ de 96 chiffres décimaux (soit 320 bits). Ce cryptosystème permet de former une signature permettant d'authentifier la carte bleue. Plus précisément, lorsqu'un usager fait une demande de carte bancaire, sa banque produit un certain nombre d'informations qu'elle produit au GIE. A partir de celles-ci, le GIE forme un numéro d'identifiant I correspondant au numéro à 16 chiffres visible sur la carte. Parallèlement, à l'aide de sa clé secrète, le GIE forme un numéro d'authentification J. Ces différentes données ainsi que quelques autres sont emmagasinées dans les quelques Ko de mémoire EEPROM de la carte à puce qui peut dès lors être transmise au client.

Chez le commerçant

Une fois chez un commerçant agréé, le client insère sa carte dans un terminal et commence alors une phase d'authentification (ce message apparaît souvent sur l'écran du terminal). Lors de celle-ci, les numéros I et J sont lus et le terminal contrôle, par le biais de la clé publique du GIE, que ces numéros se correspondent. Si le montant de la transaction est faible et selon la nature de la carte, la phase d'authentification peut en rester là, sinon le terminal contacte un serveur général pour voir s'il n'y a pas d'interdit bancaire, d'opposition ou pour savoir si le compte est suffisamment alimenté. Le client saisit ensuite son code personnel.

A quoi sert le code PIN ?

A chaque carte bancaire est associé un code PIN (Personnel Identifer Number) de 4 chiffres. Celui-ci sert à identifier le porteur de la carte bleue. Lorsque le client tape son code PIN sur le terminal, celui-ci est transmis à la puce de la carte qui vérifie son exactitude. Si la puce reçoit successivement 3 codes incorrects, elle se fige et la carte devient inutilisable. Si le code reçu est correct, la puce mémorise le montant et la date de la transaction, elle vérifie que la somme des montants des transactions écoulées dans la semaine n'excède pas un certain plafond et donne son accord au terminal en produisant un numéro de transaction (qui apparaîtra sur la facturette). Le client peut alors repartir avec sa marchandise et le commerçant transmettra dans la soirée à sa banque l'ensemble des transactions réalisées dans la journée.

Les « yescards »

S'interrogeant sur la fiabilité des cartes bancaires, Serge Humpich est parvenu à comprendre les mécanismes d'authentification d'une carte bleue. En 1997, il factorise le nombre n de 96 chiffres défini par le GIE notamment à l'aide du logiciel de calcul formel Maple. Il lui est alors facile, à partir d'un numéro d'identifiant farfelu I de calculer le numéro d'identification J correspondant. Il conçoit alors de fausses cartes bleues dont la puce répond « oui » à n'importe quel code PIN : ce sont les fameuses « yescards ».

L'affaire Humpich

Serge Humpich contacte le GIE pour négocier sa découverte d'une faiblesse dans le protocole d'authentification des cartes bancaires. Le GIE lui demande alors de prouver ses dires et Humpich achète 10 carnets de tickets de métro auprès d'un distributeur de la RATP à l'aide de 10 numéros de cartes bancaires inexistant de la forme :

xxxx xx98 7654 321x, xxxx xx09 8765 432x, xxxx xx10 9876 543x,…

Le GIE semble alors prêt à négocier mais mène parallèlement une enquête lui permettant de remonter jusqu'à l'auteur de ses pratiques « frauduleuses ». Il ordonnera une perquisition du domicile de Serge Humpich qui diffusera alors publiquement sa découverte en juin 1999 et sera condamné à 10 mois

Est-il licite de factoriser ce nombre ?

155088080278376929842392150075130787847102
021520671110279311199011387539455345999975
760530467173585609159755538979740893817334
404367470478098639006990667909672893308140
504493596951450867623994249344075058927001
5739962374529363251827

Ce nombre est celui de 230 chiffres déterminé par le GIE pour sécuriser les cartes bancaires. Il est dit qu'un groupe d'étudiants serait parvenu à le factoriser mais aurait préféré garder secret le résultat obtenu par respect pour leur passion… Cela semble douteux et à ce jour aucune factorisation n'a encore été diffusée.

Cependant certains sites peu scrupuleux proposent de communiquer cette factorisation moyennant paiement téléphonique… En tout cas dès que ce nombre sera factorisé, il est probable qu'un grand nombre de « yescards » feront leur réapparition !

de prison avec sursis en février 2000.

La correction du système

Pour combler la faille découverte par Humpich, le GIE est passé progressivement à un système de cryptographie basé sur un nombre $n = pq$ d'environ 230 chiffres ce qui lui a coûté l'adaptation des terminaux de paiement. Cela sera suffisant jusqu'à ce que l'on parvienne à factoriser ce nombre sachant que l'on est déjà parvenu récemment à factoriser un nombre de 200 chiffres décimaux. Malheureusement cela ne comble pas toutes les failles du système de paiement par carte bleue :

Le logiciel geZeroLee

En 2001 plusieurs institutions françaises sont averties de l'imminence d'une attaque informatique contre les systèmes de gestion des paiements par cartes bancaires. Quelques jours plus tard, un pirate informatique répondant au nom de code de « geoli » diffuse sur Internet le logiciel geZeroLee. Ce logiciel invite à suivre « le lapin blanc » et permet, à titre didactique, de fabriquer de fausses cartes bancaires ! Ce logiciel peut être encore trouvé sur le Net à condition de faire preuve d'un peu de courage.

La faille exploitée par les pirates consiste simplement à copier une carte existante. En effet la carte bancaire communique au terminal les numéros d'identification I et J avant même que le propriétaire de la carte ait inséré son code PIN. Il suffit alors au pirate de lire ses numéros et de les reproduire sur une fausse carte qui sera alors un « clone » de la première mais sans le code PIN… Cette manipulation ne prend que quelques secondes ! Méfiez-vous donc d'un emprunt de votre carte bleue pour quelques instants et a fortiori d'un vol de celle-ci car le code PIN ne vous protège en rien contre le clonage de votre carte et c'est alors votre compte qui sera débité ! Heureusement, les cartes bancaires sont aussi protégés par des moyens mécaniques comme les hologrammes, le relief de la carte qui compliquent sérieusement le travail des pirates.

De nos jours une vingtaine d'ingénieurs et d'anciens pirates de cartes bancaires travaillent ensembles à rechercher et à combler les failles de ce moyen de paiement qui reste l'un des plus sûrs.

Progression de la factorisation RSA :

Une liste de nombres de la forme $n = pq$ avec p,q nombres premiers a été formée depuis le 18 mars 1991 par la société RSA Security et est proposée comme défit de factorisation, certains étant même assortis de primes. Sur le graphe ci-contre, on trouve en abscisse le nombre de décimales de l'entier en question et en ordonné la date à laquelle il a été factorisé. Le dernier record date du 9 mai 2005, c'est la factorisation du RSA200, nombre à 200 chiffres décimaux. Celle-ci a été réalisée par une équipe du « German Federal Agency for Information Technology Security » déjà responsable de la factorisation du RSA 174 !

Sur ce graphe, on voit aussi que le nombre $n = pq$ à 96 chiffres déterminé en 1983 par le GIE était obsolète depuis le début des années 90.