INFO910 Cryptologie

Sujet :

« Protocole cryptographique du paiement par carte bancaire »

M2 informatique et systèmes coopératifs

Réalisé par :

- Chaimaa HASKA
- Nouhaila AIT LHADJ

Année universitaire : 2020-2021

Table de matières

Introduction

Dans un monde où la technologie est chaque jour de plus en plus performante, on se pose la question “est ce que nos données bancaires sont sécurisées?”.Surtout ces dernières années ont amorcé l’explosion des technologies du numérique, et on entend de temps en temps des incidents de pénétration et de violation des données bancaires des gens, alors en demande à quelle point les méthodes actuelles utilisées pour sécuriser nos données , plus particulièrement les données bancaires, sont elles fiables.

Aujourd’hui et dans le milieu bancaire, la technologie ou bien la technique utilisée pour la sécurité des échanges est la cryptographie. La sécurité existe au cœur de ces protocoles cryptographiques, et dans notre sujet on va se concentrer sur le protocole cryptographique de paiement par carte bancaire (que ce soit par machine ou en ligne), qui constitue une succession d’échanges de messages chiffrés par des méthodes cryptographiques. Et on va répondre principalement aux questions suivantes :

Comment nos données bancaires sont-elles sécurisées ? Comment la cryptographie est utilisée pour sécuriser le paiement en ligne et par machine ?

1. Les composants d'une carte bancaire :

La carte bancaire est un moyen de paiement, il en existe beaucoup (classique, Premier, Gold), de différents réseaux (Visa, MasterCard), à des prix disparates (d'une carte bancaire gratuite à plusieurs centaines d'euros par an), chez de nombreuses banques. Ces cartes contiennent des éléments qui jouent un grand rôle dans leur sécurité.

Les éléments qui composent une carte bancaire, dans sa face recto, sont les suivants :

- Des informations concernant la banque et des sigles (Visa ou MasterCard,...)
- Le nom du propriétaire de la carte
- La date d'expiration de la carte
- Le numéro de la carte
- La puce
- Un hologramme

La puce est l'élément central de la carte, elle est au cœur de sécurité des cartes bancaires. C'est une sorte d'ordinateur miniature avec un processeur assez peu puissant qui permet d'effectuer des calculs, et dont la mémoire contient les données importantes de la carte (enregistrement de l'historique des transactions).

Elle contient en particulier des clés cryptographiques spécifiques à chaque carte, le code secret, et le compteur d'essai qui permet de bloquer la carte au bout d'un certain nombre d'essais.

Pour l'hologramme, il est destiné à rendre plus difficile la fabrication de fausses cartes bancaires. Pour les cartes Visa, l'hologramme est une colombe qui semble voler lorsque vous inclinez la carte. Au lieu d'un hologramme de colombe sur le recto, il se peut que l'on trouve au verso de la carte également.

L'hologramme MasterCard composé de deux globes représentant le monde est en trois dimensions avec une répétition de MasterCard imprimé en arrière-plan. Lorsqu'on le fait tourner, l'hologramme reflète la lumière et semble bouger.

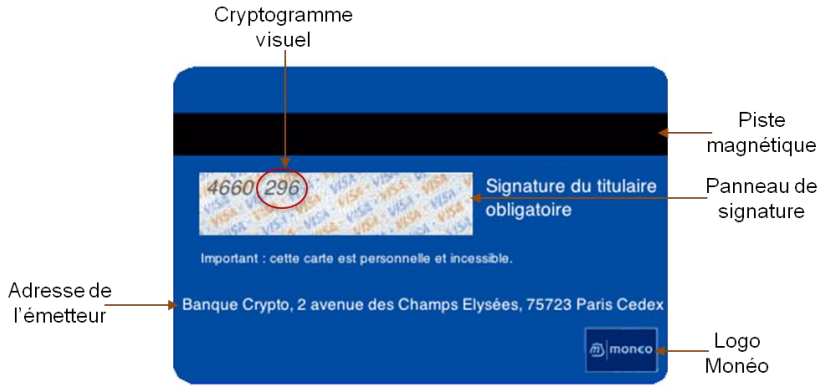
Pour le numéro de la carte bancaire, il est composé de 16 chiffres:
Les 6 premiers chiffres identifient le type de la carte et la banque à laquelle elle appartient. Si le 2 premiers chiffres sont 51,52,53,54 ou 55 il s'agit donc d'une MasterCard et si le 1 premier chiffre est 4, il s'agit d'une carte Visa. Si les 2 premiers chiffres sont 34 ou 37 c'est une carte américaine express et le reste des six premiers chiffres identifient la banque.

Les 9 chiffres qui suivent identifient le numéro de compte dans la banque, chaque banque ayant son propre système d'identification.

Enfin, le dernier chiffre représente ce qu'on appelle la clé de Luhn. Il est calculé à partir des autres chiffres avec l'algorithme suivant :

1. On multiplie par 2 le 1er chiffre du numéro de la carte, le 3eme, le 5ème,... (que les chiffres ont des emplacements impairs)
2. Si le résultat est plus grand que 9, on retranche 9. chaimaa haska#2395
3. On calcule la somme de tous les chiffres.
4. On divise la somme par 10 et on prend le reste de la division.
5. On calcule 10-reste de la division = la clé de Luhn.

Les éléments qui composent une carte bancaire, dans sa face verso, sont les suivants :



- La piste magnétique.
- Une fenêtre pour apposer la signature du propriétaire. Cette fenêtre comporte aussi souvent quelques chiffres, dont les derniers constituent le cryptogramme de sécurité de la carte (cryptogramme visuel).
- Diverses informations et sigles.

Pour la piste magnétique, elle comporte toutes les informations qu'on peut lire en ayant la carte en mains (nom de la banque, numéro, date d'expiration,...) sauf le cryptogramme de sécurité.

2.Paiement en ligne :

Dans cette partie on va s'intéresser au protocole de cryptographie utilisé pour effectuer un paiement en ligne (pour des achats par internet).

Lors de ce paiement les informations qui sont demandées sont les suivantes :

- Le numéro de la carte bancaire.
- Le nom du porteur.
- La date de validité de la carte.
- Le cryptogramme de sécurité *CVV*.

La question qui se pose ici , c'est comment mes données sont protégées dans ce cas? et si quelqu'un arrive à les violer est ce qu'il peut payer avec la carte?

L'un des composants des cartes bancaires, qui joue un rôle dans la sécurisation de ce type de transition, est le cryptogramme de sécurité, puisqu'il permet de s'assurer que la personne qui est en train de payer possède effectivement la carte.Vue que contrairement aux autres données, le cryptogramme de sécurité n'est pas stocké dans la piste magnétique donc ceci empêche qu'une personne (commerçant par exemple) capture les données de la carte lors d'un paiement par lecture de la piste magnétique et l'utiliser pour effectuer des paiement.

Parmi les protocoles les plus utilisés dans les solutions de sécurité pour le paiement en ligne :

1.1. Le protocole SSL :

Les informations saisies par le porteur de la carte, sont acheminées sur internet à l'aide du protocole SSL (Secure Socket Layer).

Ce protocole est utilisé par le navigateur (internet explorer, Google chrome, mozilla firefox), et permet la transmission sécurisée des renseignements sur internet. Il repose sur un procédé de cryptographie par clé publique afin de garantir la sécurité de la transmission de données sur internet. Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur).

Par exemple, si un utilisateur souhaite effectuer un achat par internet (en ligne), il utilise un navigateur internet pour se connecter à un site de commerce électronique sécurisé par SSL enverra des données chiffrées (les informations de sa carte bancaire) sans aucune manipulation nécessaire de sa part. Un serveur web sécurisé par SSL possède une URL commençant par https, où le « s » signifie bien évidemment secured (sécurisé). Qui a été renommé en 2001 "Transport Layer Security (TLS)".

Son fonctionnement est comme suit :

La sécurisation des transactions par SSL est basée sur un échange de clés entre client et serveur. La transaction sécurisée par SSL se fait selon le modèle suivant:

- Dans un premier temps, le client se connecte au site marchand sécurisé par SSL.
- Le serveur envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA).
- Le client vérifie la validité du certificat, puis crée une clé secrète aléatoire, chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat (la clé de session).
- Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée.

Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. Le reste des transactions peut se faire à l'aide de clé de session, garantissant l'intégrité et la confidentialité des données échangées.

1.2. Le protocole 3D Secure:

C'est un protocole de paiement sécurisé sur internet pour renforcer la sécurité des transactions électroniques, il a été développé par Visa, connu par les cartes Visa sous le nom "Verified by Visa" et pour les cartes Mastercard sous le nom "Mastercard Secure Code".

Il ajoute une étape supplémentaire au paiement en ligne pour garantir une meilleure authentification du détenteur de la carte de paiement lors d'achats effectués sur des sites web. Concrètement après avoir saisie les données de la carte afin d'effectuer un achat sur le site du marchand, le client est renvoyé vers le site de sa banque, dont il va saisir un code d'authentification à usage unique, afin de finaliser la transaction.

La plupart des banques utilisent des SMS (envoie d'SMS sur le téléphone portable du client) pour communiquer ce code.

Pour résumer, la procédure se poursuit ensuite comme suit :

- La banque envoie un code à usage unique par téléphone (sms) ou via Internet (e-mail) à l'acheteur.
- En plus du code, il peut également être demandé une information personnelle, telle qu'une date de naissance.
- Une fois le code confirmé, la banque valide la transaction.
- Si la confirmation du code échoue trois fois d'affilée, la transaction est annulée et le paiement par carte se trouve bloqué sur les sites 3D Secure.

3. Paiement par machine :

Nous nous intéressons ici au protocole utilisé pour effectuer un paiement chez un commerçant. Ce protocole met en œuvre des agents qui sont les acteurs, humains ou matériels, de cette transaction.

Imaginons que: Alice est la détentrice de la carte bancaire, C la carte bancaire à puce détenue par Alice, T le terminal du commerçant sur lequel Alice compose son code secret et B, la banque d'Alice.

Ces agents réalisent le protocole suivant :

- Alice introduit sa carte C dans T
- Le commerçant saisit le montant m de la transaction sur T
- T authentifie C, le message « Authentification » est affiché sur T
- Le message « Code ? » est affiché sur T
- Alice tape son code sur T
- T transmet le code à C
- Si le code est valide, C le signale à T

Jusqu'à cette étape, tout se passe localement sur T. Vient ensuite une phase de vérification distante, Cette dernière n'est pas réalisée pour toutes les transactions,

mais seulement pour celles dépassant un certain montant (typiquement 100 euros), et encore uniquement pour 20% d'entre elles.

- T demande l'autorisation à B pour C et le montant m
- B donne l'autorisation

En effet cette phase est longue et considérée parmi les causes directes de l'augmentation des temps d'attente et l'allongement des files aux caisses dans les grandes surfaces. Le seuil de 20 % de vérification a donc été choisi afin de pallier ce problème tout en gardant un quota de vérification dissuasif contre la fraude.

- Dernière étape, le montant m est débité

Ces différentes étapes constituent la vue de l'extérieur du protocole, nous expliquerons dans ce qui suit le réel fonctionnement ou la vue d'intérieur de ce protocole.

3.1. Le chiffrement asymétrique :

La notion centrale des protocoles cryptographiques est celle du chiffrement, une opération visant à transformer un texte intelligible en une version incompréhensible, à l'aide d'une clé. À l'inverse, le déchiffrement permet de produire la version intelligible à partir du texte chiffré.

Pour simplifier les principes mathématiques des algorithmes cryptographiques ainsi que les détails de programmation de ces protocoles, nous utilisons les notations suivantes :

- {m}K, le message m chiffré par la clé K,
- A → B : m, l'envoi par l'agent A (Alice) d'un message m à l'agent B.
- $K_{PUB/B}$: clé publique de B
- $K_{PRIV/B}$: clé privée de B

Le chiffrement asymétrique emploie une combinaison d'une clé privée et d'une clé publique. La clé privée est connue uniquement par son propriétaire respectif, tandis que la clé publique est mise à disposition de tous sur une base de données ou un

annuaire publiquement accessible. Un message chiffré avec la clé $K_{PUB/B}$ ne pourra être déchiffré qu'avec la clé inverse $K_{PRIV/B}$. Réciproquement, un message chiffré avec la clé $K_{PRIV/B}$ ne pourra être déchiffré qu'avec la clé inverse $K_{PUB/B}$. Toute tentative de déchiffrement réalisée avec une mauvaise clé échoue.

Les messages chiffrés permettent également d'assurer d'autres propriétés comme la confidentialité et l'authentification car :

- Le message $\{m\}K_{PUB/B}$ ne pourra être déchiffré que par *B*, vu que c'est le seul qui détient la clé inverse $K_{PRIV/B}$. En conséquence, c'est un moyen simple pour n'importe quel agent d'envoyer de façon confidentielle un message *m* à *B*.

- Le message $\{m\}K_{PRIV/B}$ pourra être déchiffré par tous les agents et leur permettra ainsi d'authentifier l'émetteur de ce message. On appelle aussi ce type de procédé signature numérique. La raison pour laquelle il est possible d'associer ce message à *B* est due au fait que seul *B* détient $K_{PRIV/B}$ et qu'il est donc le seul agent en mesure de construire ce message.

3.2. Description intérieure du protocole cryptographique :

Les clés et les données utilisées dans ce protocole sont les suivantes :

- La banque B possède un couple de clés asymétriques $K_{PUB/B}$ et $K_{PRIV/B}$.
- La carte C possède la donnée Data= nom, prénom, numéro carte, date de validité, ainsi qu'une valeur de signature $\{Data\}K_{PRIV/B}$.
- Le terminal T possède la clé publique de la banque, $K_{PUB/B}$.

3.2.1. Authentification de la carte :

Lorsqu'Alice introduit sa carte dans le terminal, ce dernier a besoin de savoir à qui elle appartient, et s'il s'agit effectivement d'une carte valide.

Ceci est réalisé grâce à la cryptographie asymétrique. En effet, dans la puce on trouve des données stockées en deux façons : d'une part, en clair, et d'autre part, sous forme chiffrée, en utilisant la clé privée de la banque. Ainsi, sur la carte, on

trouve le couple (Data, {Data}$K_{PRIV/B}$), et ce sont ces informations qui sont transmises par la carte au terminal.

Le terminal peut donc identifier la carte par la connaissance de "Data". Il peut aussi vérifier la validité de la carte, on calculant {{Data}$K_{PRIV/B}$} $K_{PUB/B}$ puis vérifier si cela est bien égal à "Data" Si c'est le cas, c'est que la carte est valide et authentifiée.

3.2.2. Code confidentielle :

Le client est invité à entrer son code secret sur le terminal. Celui-ci le communique (en clair!) à la puce de la carte bancaire, qui le compare avec la valeur stockée. Si les deux valeurs coïncident, la carte retourne "OK" au terminal.

3.2.3. Authentification en ligne (Vérification distante) :

Le terminal interroge un centre de contrôle à distance, qui envoie à la carte un message aléatoire **R**. La carte calcule **y=f (K, R),** où **K** est une clé secrète, inscrite dans la partie illisible de la carte, et **f** est un algorithme de chiffrement symétrique. La valeur **y** est retransmise au centre, qui lui-même calcule **f (K, R)**, compare les deux les deux valeurs et donne ou non l'autorisation. Ceci nécessite que le centre connaisse la clé secrète de toutes les cartes. Cette authentification hors-ligne n'est pas réalisée à chaque transaction, car elle demande un temps assez long.

4. Attaque sur le protocole de paiement 'Affaire Serge Humpich' :

Le protocole de paiement par carte bancaire comporte plusieurs faiblesses qui ont été exploitées par Serge Humpich en 1998.

Cet informaticien, ayant essayé de négocier, sans succès, son savoir-faire auprès du groupement des cartes bancaires, il fait une démonstration publique en achetant un carnet de tickets de métro en utilisant une carte de sa fabrication. Cela lui valut en février 2000 une condamnation à 10 mois de prison avec sursis, alors qu'il n'avait pas utilisé sa trouvaille à des fins crapuleuses.

Cette attaque (la méthode de Humpich) concernait uniquement les transactions avec authentification hors-ligne, donc a priori il était impossible d'attaquer les distributeurs qui pratiquent systématiquement l'authentification en ligne avec un central, mais celle-ci n'est utilisée en France que pour une minorité de transactions

En réalité, Humpich avait pointé du doigt deux failles dans le protocole utilisé :

- Une faille logique : Le couple « Data, {Data} $K_{PRIV/B}$ » était inscrit en clair sur chaque puce donc il était possible de les lire, et de les reproduire sur une autre carte à puce vierge. D'autre part, il était aisé de fabriquer des cartes bancaires qui, quel que soit le code secret rentré, répondait "OK" au terminal de paiement, ce que l'on appelle des "Yescard". Ainsi en fusionnant ces deux étapes, le pirate peut fabriquer une fausse carte à partir d'une carte bancaire valide qui réalise les mêmes transactions sans aucun problème ou blocage de terminale T.

- Une faille cryptographique : L'algorithme utilisé pour le chiffrement asymétrique n'est autre que le célèbre RSA. Mais la clé utilisée en 1998 (inchangée depuis 1990) ne comportait que 320 bits. Or, en 1998, factoriser un tel entier n'était plus impossible (le record se situait à 512 bits). Humpich, en utilisant simplement un logiciel japonais de factorisation, avait réussi à découvrir la clé secrète $K_{PRIV/B}$.

Si on combine la faiblesse logique et la faiblesse cryptographique, Il devient ainsi possible pour le pirate de fabriquer de toute pièce une fausse carte bancaire, sans avoir besoin de partir des informations d'une carte bancaire valide.

Soit par exemple XXX un ensemble de coordonnées : nom, prénom, numéro de carte, date de validité imaginaires. Puisque le pirate dispose maintenant de la clé $K_{PRIV/B}$, il lui est possible de construire $\{XXX\}\ K_{PRIV/B}$. il peut ainsi construire une Yescard en ajoutant *XXX* et $\{XXX\}\ K_{PRIV/B}$ dans la zone publique de la carte .Les transactions effectuées à l'aide de cette Yescard deviennent :

- T → Pirate : « Authentification »
- C → T : XXX, $\{XXX\}\ K_{PRIV/B}$
- T → Pirate : « Code ? »
- Pirate → T : 0000
- T → C : 0000
- C → T : ok

5. Corrections du protocole :

Le groupement des cartes bancaires a retenu ses erreurs et a apporté plusieurs réponses. Les premières étaient purement matérielles comme :

- Augmentation de la taille des clés RSA utilisées : ce qui rend la factorisation et par conséquent le calcul de la clé secrète de la banque et la création d'identités bancaires factices impossible
- Changement de l'algorithme de chiffrement utilisé dans la méthode d'authentification en ligne pour un algorithme plus sûr.

En revanche, la possibilité de copier les données publiques d'une carte valide vers une Yescard subsistait toujours, c'est d'ailleurs un principe très exploité qui donne

aujourd'hui encore régulièrement lieu à des escroqueries. Une des dernières en date, révélée le 9 février 2007, a ainsi atteint un montant estimé à 640 000 euros.

Pour cela le groupement EMVCo, regroupant Europay, MasterCard et Visa, a publié sur le Web les spécifications détaillées de son successeur EMV. Celui-ci propose trois protocoles de transaction pouvant être activés en fonction de leur disponibilité sur la carte et/ou le terminal. Nous allons présenter DDA (Dynamic Data Authentification) qui utilise la notion challenge pour garantir une authentification plus sure.

5.1. Le protocole DDA :

Le protocole DDA met en jeu un autre couple de clés asymétriques $K_{PUB/C}/K_{PRIV/C}$, spécifiques à chaque carte. Donc sur la zone publique de la carte on trouve en plus de $\{Data\}K_{PRIV/B}$ et Data , la clé publique de la carte chiffrée par la clé privée de la banque $\{K_{PUB/C}\}K_{PRIV/B}$. Et sur la zone privée théoriquement inaccessible on trouve la clé privée de la carte $K_{PRIV/C}$. Une transaction avec DDA prend donc la forme suivante :

- T → A : « Authentification »
- C → T : Data, $\{Data\}\ K_{PRIV/B}$, $\{K_{PUB/C}\}K_{PRIV/B}$
- T : calcule $\{\{Data\}\ K_{PRIV/B}\}K_{PUB/B}$ et vérifie , puis calcule $\{\{K_{PUB/C}\}K_{PRIV/B}\}K_{PUB/B}= K_{PUB/C}$,il est maintenant en possession de la clé publique de la carte
- T → C : R un nombre aléatoire (le challenge)
- C → T : $\{R\}K_{PRIV/C}=M$
- T : calcule $\{M\}K_{PUB/C}$, s'il est égale à R donc que le challenge est rempli et la carte est authentifiée , vue qu'elle est la seule qui possède $K_{PRIV/C}$
- T → A : « Code ? »
- A → T : code
- T → C : $\{code\}\ K_{PUB/C}$
- C → T : ok

Le protocole DDA répare la faille logique du protocole initial car il n'est plus possible de cloner une carte bancaire grâce au $K_{PRIV/C}$. De plus, il améliore la phase "authentification du possesseur de la carte". En effet, le terminal ne communique plus à la carte directement le code secret entré par le client, mais l'information $\{code\}K_{PUB/C}$. Avec sa clé secrète, la carte, et elle seule, peut retrouver le code. Ainsi, le code secret circule sous forme chiffrée entre le terminal et la carte et ne peut plus être espionné.

Conclusion

Le monde des cartes bancaires et les opérations liées à ces dernières est très compliqué, il pose des problèmes concernant la sécurité des informations des détenteurs des cartes bancaires.

Chaque année on entend beaucoup d'incidents, par exemple quelqu'un a utilisé la carte d'une autre personne pour effectuer un paiement sans qu'il sache comment il a fait pour récupérer les informations de sa carte même s'il la possède physiquement,...etc.

Nous avons vu pas mal d'outils de sécurité, et technique de protection des données des gens, comme le protocole SSL , le protocole 3D Secure, … mais dernièrement et à cause de l'évolution rapide de la technologie et techniques de pénétration, nous avons constaté que certaines de ces protocoles utilisés n'est plus fiable, en peut donner comme titre d'exemple le protocole 3D Secure, qui consiste à la vérification par SMS de l'identité du détenteur de la carte, présente cependant un niveau de sécurité insuffisant selon le législateur européen, et devrait disparaître, en raison de l'entrée en vigueur de dispositions prévues par la DSP2 (deuxième directive européenne sur les services de paiement) qui dit que la validation de ces paiements par un code envoyé par SMS (3D Secure) devra être renforcée ou remplacée par d'autres solutions (reconnaissance biométrique, émission d'un code personnel envoyé par courrier, connexion obligatoire à l'application mobile bancaire, etc.) à compter du 31 décembre 2020.