Thèse de doctorat Décembre/ 2014

Université Panthéon - Assas

Ecole doctorale d'Économie, Gestion, Information et Communication

Thèse de doctorat en Informatique

soutenue le 18 Décembre 2014

L'expertise et la lutte contre la fraude monétique

Université Panthéon-Assas

Thomas Souvignet

Sous la direction de David Naccache, Professeur à l'Université Panthéon-Assas

Rapporteurs :
Jean-Jacques Quisquater, Professeur à l'Université Catholique de Louvain
Christophe Rosenberger, Professeur à l'ENSI de Caen
Membres du jury :
David Billard, Professeur à l'Université des Sciences Appliquées de Genève
Christof Paar, Professeur à l'Université de la Ruhr à Bochum
Pierre Paradinas, Professeur au Conservatoire National des Arts et Métiers
Marc Watin-Augouard, Général d'armée (2S), directeur du CREOGN

Avertissement

L'université n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à leur auteur.

Remerciements

Je tiens à remercier l'ensemble de ceux qui ont contribué, de près ou de loin, à la réalisation de cette thèse.

Je remercie ainsi l'ensemble du personnel des départements Informatique-Electronique de l'IRCGN et KT52 du BKA pour leur coopération de tous les jours ; les enquêteurs des différents services d'enquête qui ont cru en mes idées et systèmes irrationnels ; les membres de l'OSCP qui ont échangé avec moi et permis de lever certaines zones d'ombre ; les étudiants qui ont participé au développement de l'application FPCA ; mes supérieurs hiérarchiques qui ont bien voulu que je reprenne mes travaux personnels dans mon travail quotidien et su valoriser les résultats obtenus ; et tous ceux que j'oublie...

Mon extrême gratitude va également à ceux sans qui mes trois articles et cette thèse n'auraient pas pu être publiés : Dan, Francis, Matthieu, Eric, Jürguen, Thomas, Julien et tous les autres...

Mes remerciements les plus respectueux vont également à mon jury, qui a bien voulu accepter d'évaluer ces 4 années de travail sur mon temps libre résumées en quelques pages, et tout spécialement au Professeur David Naccache, mon directeur de Thèse, sans qui tout cela n'aurait pu se faire.

J'adresse enfin mes remerciements à ma compagne qui a su faire preuve d'une extrême patience et à mon fils qui, s'il a légèrement bouleversé mon planning, aura su m'apporter les moments de distraction nécessaires à la finalisation de cette thèse.

Résumé :

Le montant annuel de la fraude européenne à la carte de paiement se monte à plus d'1,5 milliard d'euros. Cette manne aiguise l'appétit des groupes criminels qui exploitent la moindre faille de la monétique (écosystème de la carte de paiement).
Les cinq principaux acteurs de la monétique (porteurs, émetteurs, accepteurs, acquéreurs et systèmes de paiement) s'appuient pourtant sur des systèmes et réseaux normalisés dont la sécurité est encadrée par des standards internationaux contraignants. Néanmoins, la fraude monétique ne cesse de progresser alors que les moyens de lutte (étatiques, collaboratifs ou individuels) restent limités.
Après étude de la fraude monétique, cette thèse propose différentes actions (passives, réactives et proactives) visant à améliorer la lutte contre la fraude monétique. D'abord, il convient de mieux connaître la fraude en étudiant la provenance des données volées et plus seulement leur usage. Ensuite l'expertise de ces fraudes doit être améliorée, en développant par exemple une captation du progrès scientifique. Une expertise qui doit être en partie transmise aux enquêteurs afin qu'ils puissent conduire leurs enquêtes. Enquêtes qui peuvent être dynamisées par des opérations réactives associant investigateurs et sachants techniques. Enfin, de manière proactive, les enquêtes et analyses de demain doivent être facilitées par les technologies monétiques conçues aujourd'hui.

Descripteurs :

Fraude monétique , Terminaux, Carte de paiement, Expertise, Enquête, Cybercriminalité, Outils criminalitisques

Title and Abstract:

Solid forensic assessment and the fight against payment card fraud

Every year, payment card fraud exceeds 1.5 billion euros in Europe. Organised crime groups are exploiting any vulnerability possible to take a piece of this lucrative activity.
Even though the five principal entities in the payment card industry (cardholders, issuers, acceptors, acquirers and payment system providers) are implementing binding security measures throughout standardized systems and networks, fraud continues to increase. Efforts by the state, industry collaboration, and individuals have been unsuccessful in decreasing criminal advances.
Having analysed the elements of payment card fraud, this thesis proposes several actions (passive, reactive and proactive) to help improve the fight against this fraud. First, it is relevant to gain knowledge of the source of the card details and not to focus only on its reuse. Next, forensic assessment has to be improved, for example by developing an increased scientific understanding of the technology. Such an expertise should then be passed on to investigators through effective training and knowledge transfer. Investigations should also be made more dynamic with reactive operations conducted in concert by investigators and technicians. Finally, in an ideal proactive spirit, future investigations and assessments should be oriented and facilitated by studying and influencing current payment card technology developments.

Keywords:

Payment card industry, Terminals, Payment card, Forensic assessment, Investigation, Cybercrime, Forensic tools

Principales abréviations

2CENTRE *Cybercrime Centres of Excellence Network for Training Research and Education.*

AES *Advanced Encryption Standard.*

AFSIN Association Francophone des Spécialistes de l'Investigation Numérique.

APDU *Applicative Protocol Data Units.*

ATICA *Acquirer To Issuer CArd.*

ATM *Automatic Teller Machine.*

BCE Banque Centrale Européenne.

BFMP Brigade des Fraudes aux Moyens de Paiement.

BKA *Das Bundeskriminalamt.*

CAPE *CArd Payments Exchanges.*

CB Cartes Bancaires.

CB2A « CB Accepteur Acquéreur ».

CB2C « CB Compensation Cartes ».

CBAE « Cartes Bancaires Acquéreur-Emetteur ».

CECyF Centre Expert contre la Cybercriminalité Français.

CIR *« Common Implementation Recommendations »* .

CNP *Card Not Present.*

CoFrOSIN Communauté Francophone OpenSource pour l'Investigation Numérique.

CORE COmpensation REtail.

CP Code Pénal.

CPP Code de Procédure Pénale.

DAB Distributeur Automatique de Billets.

DAC Distributeur Automatique de Carburant.

DACG Direction des Affaires Criminelles et des Grâces.

DEFS Département de lutte contre la délinquance Économique, Financière et Stupéfiant.

DLCC Division de Lutte Contre la Cybercriminalité.

DPA *Differential Power Analysis.*

EAST *European ATM Security Team.*

EC3 *Europol CyberCrime Center.*

EMV Europay-Mastercard-Visa.

ENFSI *European Network of Forensic Science Institutes.*

EPAS *Electronic Protocols Application Software.*

ETSI *European Telecommunications Standards Institute.*

FFA UK *Financial Fraud Action UK.*

FIB *Focused Ion Beam.*

GAB Guichet Automatique Bancaire.

ICC Investigateur en CyberCriminalité.

INHESJ Institut National des Hautes Études de la Sécurité et de la Justice.

INL INformatique-éLectronique.

IRCGN Institut de Recherche Criminelle de la Gendarmerie Nationale.

NFC *Near Field Communication.*

NTech Enquêteur en Technologies Numériques.

OCLCTIC Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.

ONDRP Observatoire National de la Délinquance et des Réponses Pénales.

OSCP Observatoire de Sécurité des Cartes de Paiement.

PAN *Primary Account Number*.

PCI *Payment Card Industry*.

PIN *Personal Identification Number*.

POS *Point Of Sale*.

SCITT Service Central de l'Informatique et des Traces Technologiques.

SEPA *Single Euro Payments Area*.

SEPA-FAST « *Financial Application Specification for SCS Volume Compliant EMV Terminals* ».

SER2S Société d'Exploitation de Réseaux et de Services Sécurisés.

SIT Système Interbancaire de Télécompensation.

SSC *Security Standards Council*.

STRJD Service Technique de Recherches Judiciaires et de Documentation.

SWIFT *Society for Worldwide Interbank Financial Telecommunication*.

TPE Terminal de Paiement Électronique.

TVA Taxe sur la Valeur Ajoutée.

Sommaire

Introduction

La carte de paiement, simple morceau de plastique âgé d'une cinquantaine d'année, s'est imposée comme l'instrument de paiement préféré des Européens avec 42% des transactions, loin devant les virements, les prélèvements ou les chèques.
En 2012, pas moins de 738 millions d'entre-elles étaient en circulation dans l'espace unique de paiement en euros – ou *Single Euro Payments Area* (SEPA) –, permettant la réalisation de près de 40 milliards de transactions pour un montant total de plus de 2000 milliards d'euros [21].
Derrière ces chiffres et cette suprématie se cache tout un écosystème, la monétique, pouvant s'avérer complexe mais fascinante de diversité pour les non-initiés. Il se cache aussi une manne providentielle que la criminalité organisée ne peut occulter. Ainsi, avec 1,33 milliard d'euros de paiement frauduleux pour l'année 2012, la fraude monétique constitue un marché lucratif pour les groupes criminels.

Par ses aspects numériques, son écosystème massivement dématérialisé et ses possibilités de paiement à la fois physiques (paiements de proximité) et virtuelles (paiement à distance), la fraude monétique fait partie intégrante de la sphère de la cybercriminalité [32].
Réduire la fraude monétique constitue donc un enjeu important de la lutte contre la cybercriminalité. L'*Europol CyberCrime Center* (EC3) dédie d'ailleurs l'un de ses trois points de convergence à lutter contre cette activité criminelle à faible risque et haute profitabilité.

Face à l'importance de cette fraude et l'intérêt affiché de lutter contre elle, il nous parait important de l'analyser, de lister les moyens de lutte existants, pour enfin étudier s'il n'est pas possible d'améliorer ces derniers. Nous proposons d'opérer ces études sous un angle technique, proche du terrain et de la réalité de la fraude au quotidien.

Pour ceci, nous proposons dans un premier temps de présenter l'écosystème de la carte de paiement en détaillant le fonctionnement du système de paiement bancaire, la carte de paiement et les terminaux. La monétique constitue un environnement fermé, dont la connaissance générale se limite souvent à la manipulation d'une carte et d'un terminal. La présentation des acteurs de cet environnement permet de mieux en comprendre les responsabilités et limites ainsi que les systèmes qu'ils mettent en œuvre. La présentation, à travers leurs évolutions et leurs technologies, de la carte de paiement et des terminaux de paiement permet également de mieux en apprécier la nature et d'en expliquer les forces et faiblesses actuelles.

Dans un second temps, nous nous attacherons à présenter les fraudes, aussi bien en nature qu'en volume, ainsi que les moyens de lutte. Nous nous attacherons toutefois à avoir un regard concret sur les fraudes actuelles, en occultant celles qui demeurent de l'ordre

du possible. La nature des fraudes est en effet multiple, qu'elle soit basée sur la carte, le terminal, le système ou encore qu'elle soit conceptuelle, matérielle ou logicielle. Une taxonomie des fraudes monétiques s'avère donc nécessaire afin d'effectuer un inventaire ordonné le plus exhaustif possible des différentes formes qu'elles peuvent revêtir. Ceci permet également d'avoir un regard structuré et critique sur les chiffres de la fraude actuelle et d'en proposer une évolution possible. Les moyens de lutte aussi s'avèrent nombreux et nous essaierons de les identifier, qu'ils soient étatiques, collaboratifs ou individuels.

Puis, fort des précédentes analyses, nous proposerons des solutions pratiques et techniques permettant d'améliorer ces moyens de lutte. Les cinq principales améliorations proposées consistent en une meilleure connaissance des sources de la fraude, une amélioration de l'expertise judiciaire, une meilleure diffusion de l'information et des outils d'analyse, une dynamisation de l'enquête judiciaire ainsi que la prise en compte préalable des nécessités d'analyse. Afin d'appuyer les concepts passifs, réactifs et proactifs proposés, nous développerons des solutions concrètes mises en œuvre par ou au profit de services d'enquête pour la plupart.

Enfin, nous discuterons les résultats obtenus et tenterons d'analyser les limites identifiées. La question du financement sera ainsi mise en avant avec de possibles solutions participatives à cette problématique. Les défis de demain seront abordés avec des réflexions sur les évolutions possibles de la monétique et des fraudes.

1 Le système monétique

1.1 L'architecture du système monétique

La monétique est un écosystème s'appuyant sur de multiples acteurs, qu'ils soient institutionnels, industriels ou simples particuliers.

Le fonctionnement du système monétique est souvent présenté comme un système « quatre coins » (figure 1.1) qui met en œuvre les cinq principaux acteurs d'une opération de paiement : porteur, accepteur, acquéreur, système de paiement et émetteur.

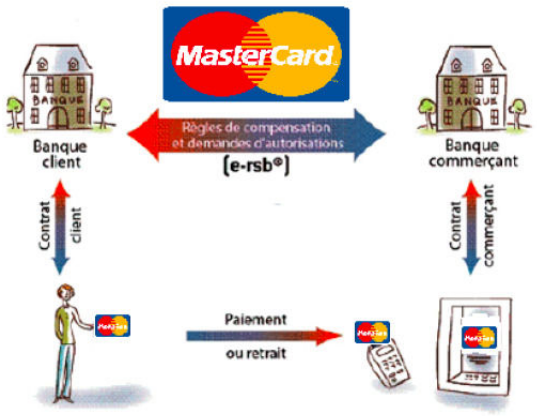


FIGURE 1.1 – Systèmes « quatre coins » de Mastercard - *source : Autorité de la concurrence [3]*

Ainsi lors d'un classique paiement par carte, le client (porteur) insère sa carte dans le terminal du commerçant (accepteur). Dans certains cas, ce dernier va contacter la banque du commerçant (acquéreur), qui, via le réseau d'un opérateur de routage (système de paiement), va interroger la banque du client (émetteur) afin de savoir si le paiement peut être honoré.

1.1.1 Porteur

Le terme « porteur » d'une carte bancaire désigne le client qui se voit remettre une carte bancaire par son organisme financier.
La carte est le plus souvent personnalisée à son nom par embossage ou sérigraphie. Il est existe toutefois des cartes prépayées ne faisant pas apparaître le nom du porteur. Ces cartes sont dites « anonymes » [33].

La responsabilité du porteur est engagée par contrat établi auprès de l'établissement émetteur lors de la demande de mise à disponibilité d'une carte de paiement. En règle générale, le porteur s'engage notamment à « tenir absolument secret son code [confidentiel] et ne pas le communiquer à qui que se soit » ainsi que de « veiller à le composer à l'abri des regards indiscrets » sous peine d'engager sa responsabilité [8, 5].

1.1.2 Émetteur

L'émetteur d'une carte de paiement est un établissement de crédit (e.g. une banque) ou un établissement de paiement (e.g. un fournisseur de cartes prépayées) qui va émettre une carte liée au compte d'un de ses clients.

Il définit le visuel ainsi que les fonctionnalités qu'il souhaite incorporer à sa carte. Ainsi, au regard de ses politiques de gestion de risques et commerciale, il pourra proposer à ses clients différents produits : des cartes sans contact, au visuel personnalisé, à interrogation permanente du solde du compte lié mais aussi des cartes avec différentes générations de mécanismes sécuritaires internes. L'ensemble des propriétés sécuritaires liées à la carte de paiement est décrit dans le paragraphe 2.4.

1.1.3 Accepteur

Le terme « accepteur » désigne l'entité (e.g. un commerçant) ayant signé un contrat d'acceptation en paiement (de proximité ou à distance) par cartes de paiement avec sa banque (e.g. contrat commerçant).
Ce contrat permet ainsi à son souscripteur d'être en mesure d'accepter les paiements par carte de paiement.

Ces contrats imposent néanmoins de nombreuses mesures de sécurité aux accepteurs en contrepartie desquelles les opérations de paiements sont garanties. En cas de non respect d'une de ces mesures, l'accepteur devient alors responsable des fraudes éventuelles et les paiements frauduleux ne sont alors pas crédités sur son compte bancaire.
Ces mesures de sécurité dépendent du contrat commerçant et du système de paiement associé mais prévoient le plus souvent [12, 11] l'utilisation de terminaux agréés, le contrôle

de la validité de la carte, l'utilisation d'une technologie (e.g. carte à puce), un mode de contrôle du porteur (e.g. code confidentiel), une limite haute de transaction, etc.

1.1.4 Acquéreur

Un acquéreur est un organisme financier qui va véhiculer et/ou acquérir les données de transaction générées par le terminal d'un accepteur. Dans le cas d'un contrat commerçant, il s'agit de la banque de ce dernier ou d'un sous-traitant.

L'acquéreur est notamment responsable de réaliser la compensation des opérations de paiement enregistrées par ses accepteurs. Cette opération consiste à échanger avec les banques émettrices des cartes concernées afin de procéder conjointement à une opération de débit du compte bancaire du porteur ainsi qu'à une opération de crédit du compte bancaire de l'accepteur.

1.1.5 Systèmes de paiement

Pour qu'une transaction carte soit permise, il est nécessaire que cette dernière soit reconnue par un système de paiement, national ou international. Au terme d'un contrat délimitant les engagements et responsabilités de chacun, la carte sera donc reconnue dans les commerces également liés à ce système de paiement.
Par exemple, un émetteur français désirant mettre en œuvre une carte de paiement à usage international pourra choisir deux systèmes de paiement : Cartes Bancaires (CB) pour les paiements domestiques, s'assurant ainsi des frais moindres, et Visa pour les paiements internationaux, permettant ainsi à son porteur des achats à l'étranger. La carte ainsi créée sera dite « cobadgée CB-Visa ».

Le choix du ou des systèmes de paiement par l'émetteur d'une carte se fait donc en fonction de la destination souhaitée de la carte (e.g. retrait/crédit, nationale/internationale) et des détails du contrat liant les deux entités (e.g. frais, responsabilités, etc.).
Il existe en effet des systèmes de paiement dits « nationaux », tels que Cartes Bancaires en France, Girocard en Allemagne, et des systèmes de paiement dits « internationaux », tels que Visa ou Mastercard. Les systèmes de paiements « nationaux » n'ont qu'une portée régionale, limitée à quelques pays, alors que les systèmes « internationaux » ont une portée mondiale.
Par ailleurs, chaque système de paiement dispose de sa propre politique en matière de tarifs (e.g. frais fixe et/ou pourcentage du montant de la transaction) et de responsabilités (e.g. sécurité à mettre en œuvre par l'émetteur). L'imputabilité du recouvrement d'une transaction frauduleuse est ainsi fortement dépendante du système choisi.

Sous la pression de l'autorité de la concurrence, les taux des trois systèmes de paiement présents en France se sont rapprochés au 1er septembre 2013. Ainsi un paiement de 20 euros chez un commerçant de proximité sera facturé à l'acquéreur 5,6 centimes alors qu'il était auparavant de :

- par Cartes Bancaires : 9,4 centimes [13] ;
- par Visa : 14,4 centimes [4] ;
- par Mastercard : 9,9 centimes [3].

1.2 Les réseaux monétiques

Les réseaux monétiques sont les réseaux d'information reliant l'ensemble des acteurs du système monétique.

Ils permettent ainsi de véhiculer de bout en bout l'ensemble des informations nécessaires à la réalisation d'une opération de paiement. Ils permettent aussi de véhiculer les données nécessaires au paramétrage des terminaux de paiement. Enfin, ils constituent un support important pour la veille et la lutte contre la fraude.

On peut distinguer trois types majeurs de réseaux :

- les réseaux d'acquisition et de paramétrage ;
- les réseaux de routage des autorisations interbancaires ;
- les réseaux de compensation.

1.2.1 Réseaux d'acquisition et de paramétrage

Les réseaux d'acquisition et de paramétrage sont ceux mis en place entre l'accepteur et l'acquéreur (figure 1.2).
Ils permettent de véhiculer localement les demandes d'autorisation générées par les paiements. Ils sont également le support des actions de gestion de réseau, de télécollecte et de téléparamétrage.

La télécollecte permet à l'acquéreur de régulièrement récupérer l'historique des transactions (*online*[1], *offline*[2], réalisées et annulées) effectuées par les terminaux de ses accepteurs.
Le téléparamétrage permet à l'acquéreur de connaître l'état fonctionnel et de configurer les terminaux de ses accepteurs. Ces configurations à distance permettent notamment de transmettre des paramètres de sécurité tels que des seuils de déclenchement pour les paiements *online* ou des actions à réaliser pour certains numéros de carte (blocage de la carte, appel systématique, rejet).

1. Transactions pour lesquelles une autorisation de paiement a été transmise à l'émetteur de la carte.
2. Transactions pour lesquelles le terminal n'a pas émis d'autorisation de paiement.

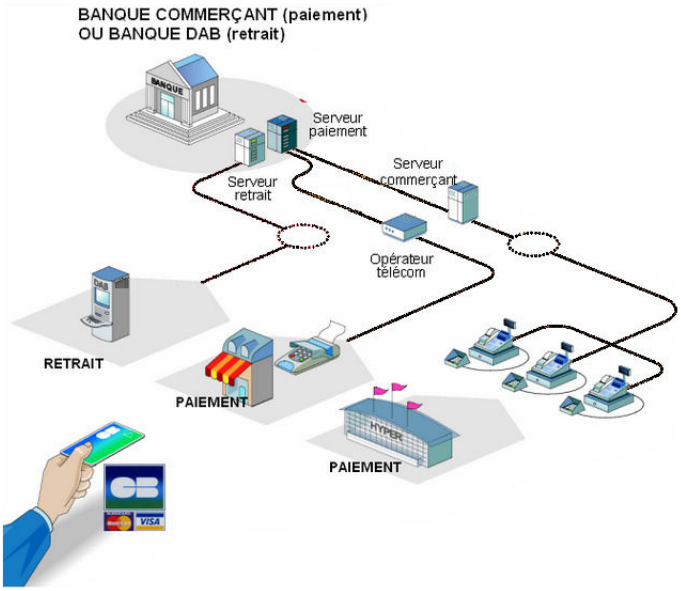


FIGURE 1.2 – Représentation d'un réseau d'acquisition et de paramétrage - *source : e-rsb.com (modifée)*

1.2.2 Réseaux de routage des autorisations interbancaires

Les réseaux de routage des autorisations interbancaires sont ceux mis en place entre acquéreurs et émetteurs (figure 1.3) afin de véhiculer les demandes d'autorisation de transaction.

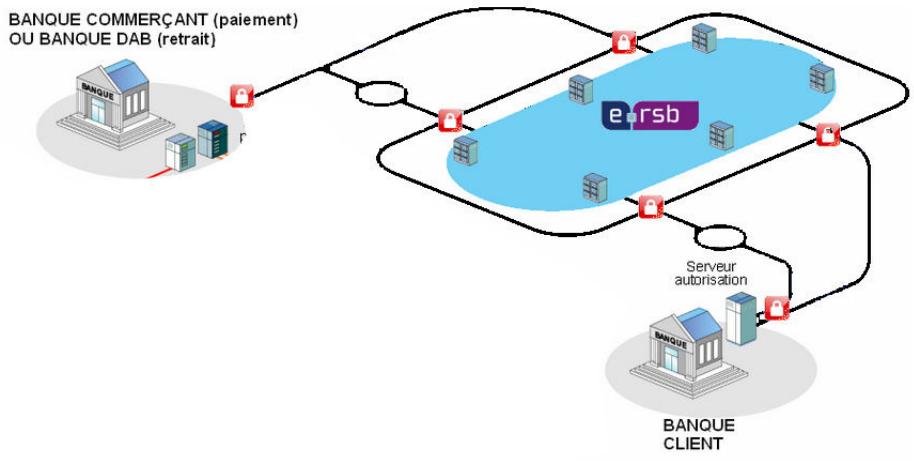


FIGURE 1.3 – Représentation du routage des autorisations interbancaires e-rsb - *source : e-rsb.com (modifée)*

En France, le réseau e-rsb (Réseau de Service aux Banques) exploité par la Société d'Exploitation de Réseaux et de Services Sécurisés (SER2S) [3] véhicule la quasi-totalité des demandes d'autorisation effectuées sur le territoire national avec une moyenne de plus de 13 millions de demandes par jour [4].
Lorsqu'une banque émettrice est étrangère ou en cas d'accord commerciaux hors Cartes Bancaires, des réseaux de routage tiers sont utilisés, tels que *Visanet* de Visa ou le *MasterCard Worldwide Network* de Mastercard.

1.2.3 Réseaux de compensation interbancaire

Les réseaux de compensation interbancaire sont ceux mis en place entre institutions financières (ex. acquéreurs et émetteurs) afin de permettre des opérations de compensation interbancaire (calculer un solde net à partir de différentes transactions, dont celles de paiement/retrait par carte).

Ces réseaux peuvent être bilatéraux ou mutualisés. En France, le système COmpensation REtail (CORE), géré par la société STET (pour Systèmes Technologiques d'Echange et de Traitement), a remplacé le Système Interbancaire de Télécompensation (SIT) en 2008 et assure la quasi-totalité des compensations interbancaires françaises.

1.2.4 Le rôle du terminal dans le système monétique

Le rôle du terminal dans le système monétique est principalement de faire l'interface entre la carte et le réseau d'acquisition et de paramétrage.

Il n'en demeure pas moins un élément actif, en charge de :
- la réception des paramétrages acquéreurs ;
- la sélection des applications de paiement ;
- l'évaluation et acception/refus d'une transaction ;
- véhiculer et opérer la transaction.

1.3 Normes et standards

1.3.1 Normes actuelles des réseaux monétiques

Les réseaux monétiques opèrent par envoi/réception de messages en suivant notamment l'ISO 8583. Néanmoins tous les pays ne suivent pas l'ISO 8583 à la lettre et beaucoup de systèmes de paiement l'ont adapté pour répondre à leurs besoins. Ainsi les réseaux

3. Filiale de Groupement des Cartes Bancaires.
4. Chiffres : semaine du 6 juillet 2013 - *source : http://www.e-rsb.com/index.php/fr/actualite*

monétiques français s'appuient sur cette norme pour concevoir leurs propres protocoles de communication.

1.3.1.1 Protocoles d'acquisition et de paramétrage

Les réseaux d'acquisition et de paramétrage français implémentent le protocole « CB Accepteur Acquéreur » (CB2A). CB2A est un protocole de présentation des données (couche 6 du modèle OSI [5]) qui prévoit la conception et l'interprétation des messages au format ISO 8583. Le transport de ces messages est assuré par le protocole CBCom ou « pseudo-session » (couches 4 et 5 du modèle OSI).

Les différents formats de données de CB2A sont décrits dans :

- « CB2A TLC-TLP-GR » pour les messages de télécollecte, téléparamétrage et de gestion de réseaux ;
- « CB2A FICHIER » pour les échanges de données volumineux entre acquéreur et accepteur, réservé aux grands remettants [6].

1.3.1.2 Protocole de transport des autorisations interbancaires

Le réseau de routage des autorisations interbancaires e-rsb utilise le protocole « Cartes Bancaires Acquéreur-Emetteur » (CBAE) qui définit les échanges, au format ISO 8583, entre un système acquéreur d'autorisation et un système émetteur d'autorisation.

1.3.1.3 Protocole de compensation interbancaire

Bien que le réseau de compensation interbancaire français ait évolué vers le système CORE-STET, le protocole de présentation « CB Compensation Cartes » (CB2C) (couche 6 du modèle OSI) déjà présent dans le système SIT reste d'actualité.

1.3.2 Normes des réseaux monétiques de demain

La mise en place d'un espace unique de paiement en euros (*Single Euro Payments Area* (SEPA)) par le conseil européen des paiements (*European Payments Council* - EPC) sur demande de la commission européenne, doit se faire en trois temps :

- mise en place du virement SEPA (*SEPA Credit Transfer* - SCT), effectif depuis 2008 ;
- mise en place du prélèvement SEPA (*SEPA Direct Debit* - SDD), effectif depuis 2010 ;
- mise en place du paiement électronique SEPA (*SEPA Cards Standardisation* - SCS), prévu pour 2017.

5. Modèle de référence d'interconnexion des systèmes ouverts.
6. Accepteurs qui se chargent de rassembler les transactions de leurs différents points de vente avant de les transmettre à leur acquéreur.

L'émergence d'un marché européen unique implique également une harmonisation des protocoles réseaux nationaux (adaptations locales de l'ISO 8583) et ouvre des perspectives en matière de normalisation des terminaux eux-mêmes.

Le passage au paiement électronique SEPA est l'occasion d'abandonner le protocole ISO 8583, devenu limité, pour adopter la norme d'échange de messages ISO 20022, initiée par la *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) et déjà utilisée pour les virements et prélèvements SEPA.

Ainsi le consortium EPASorg promeut le standard *Electronic Protocols Application Software* (EPAS) comme alternative ISO 20022 aux différentes adaptation nationales de l'ISO 8583. Pour ceci EPAS propose la standardisation des protocoles :

- d'acquisition (*EPAS Acquirer protocol*) ;
- de paramétrage (*EPAS Terminal Management System protocol*) ;
- de caisse (*EPAS Retailer protocol*).

La publication en janvier 2014 de la version 7 du *SEPA Cards Standardisation Volume*, dont la mise en application est souhaitée d'ici 2017, semble entériner cette proposition par l'adoption de messages ISO 20022 *CArd Payments Exchanges* (CAPE) pour les terminaux et réseaux d'acquisition de la zone SEPA dans son livre 3 [23].

Enfin les messages au format ISO 20022 seront également applicables aux réseaux de routage des autorisations interbancaires avec l'adoption dans ce même livre des messages *Acquirer To Issuer CArd* (ATICA).

1.3.3 La sécurité du système monétique

La sécurité des systèmes monétiques a longtemps été laissée à la discrétion des établissements financiers ou des systèmes de paiement.

Néanmoins depuis 2004, le *Payment Card Industry* (PCI) *Security Standards Council* (SSC), initié par les systèmes de paiement internationaux, développe et diffuse plusieurs normes contraignantes relatives à la sécurité des systèmes et réseaux monétiques. Parmi celles-ci, on retrouve les trois plus importantes :

- la norme de sécurité des données (*Data Security Standard* - DSS) ;
- la norme de sécurité des données d'application de paiement (*Payment Application Data Security Standard* - PA-DSS) ;
- les besoins liés au service de saisie du numéro d'identification personnel – ou *Personal Identification Number* (PIN) – (*PIN Transaction Security* - PTS).

Initialement conçues pour endiguer les vols de numéros de cartes et de données de pistes magnétiques improprement stockées par les acteurs monétiques américains, les normes PCI

sont applicables à l'ensemble des acteurs internationaux. En effet, elles sont imposées sous forme de règles contractuelles par les deux plus grands systèmes de paiement internationaux *(Security Data Protection* chez MasterCard et *Account Information Security* chez Visa). Le PCI DSS est la norme phare du PCI SSC. Elle liste un ensemble de points de contrôles (tant techniques qu'organisationnels) relatifs aux systèmes d'information qui capturent, transportent, stockent et traitent des données de cartes bancaires.

Enfin une sécurité d'ensemble de son système d'information (pas seulement monétique) peut-être visée par un acteur monétique par la recherche d'une certification ISO 27001 « Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences ». Néanmoins cette certification n'est pas requise par les systèmes de paiement et ne reste donc qu'un gage de confiance supplémentaire.

2 La carte de paiement

2.1 Historique de la carte de paiement

2.1.1 Un demi siècle de carte de paiement

Les cartes de paiement remontent aux années 1950 où, sur présentation de sa carte Diners' Club (figure 2.1a), il était possible de payer repas, voyages et dépenses d'affaires dans les enseignes partenaires [58], d'abord aux États-Unis d'Amérique puis dans le monde entier.

(a) Carte Diners' Club

(b) Carte American Express

FIGURE 2.1 – Cartes de paiement des années 1950 - *source : www.creditcards.com*

La carte de paiement n'abandonne le support cartonné qu'en 1959 lors du lancement de la première carte plastique par Amercian Express (figure 2.1b).
Cependant ces cartes demeurent privatives et il faut attendre les années 1960 pour voir l'émergence de l'interbancarité avec la création de BankAmericard en 1958 (devenu Visa) et d'InterBank Card Association en 1966 (devenu MasterCard Worldwide) [67, 46].

L'embossage des cartes est effectif depuis 1959, permettant aux commerçants de réaliser des empreintes de cartes American Express (figure 2.2), facilitant la recopie et évitant les erreurs.

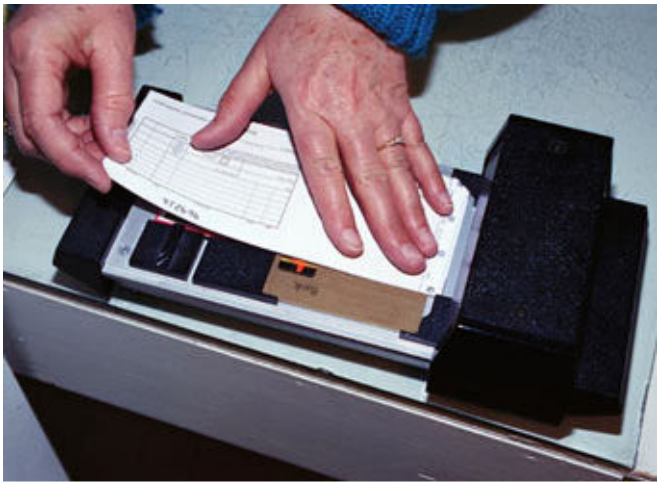


FIGURE 2.2 – Lecteur (sabot ou fer à repasser) d'embossage de carte de paiement - *source : fortune.com*

La piste magnétique est apparue sur les cartes de paiement dès 1970 avec la réalisation d'un pilote associant Americam Express, American Airlines et IBM. Néanmoins son adoption massive par les systèmes de paiement interbancaires internationaux ne se fit pas avant 1980.

2.1.2 La carte de paiement française

L'apparition de la carte bancaire en France est plus tardive puisqu'elle date de 1967 et ne permet initialement que de réaliser des opérations de retrait dans les distributeurs automatiques de billets de son établissement bancaire. Les cartes internationales, permettant des retraits et paiements en France et à l'étranger, apparaissent en 1973 avec l'arrivée de Visa.

La création en 1984 du Groupement des Cartes Bancaires signe le début de l'interbancarité. Dès lors, l'évolution des cartes de paiement françaises sera très rapide, embarquant dès 1986 un micro-contrôleur (ou « puce »). Généralisée en 1992, la carte à puce permet alors des paiements sécurisés par un code confidentiel à 4 chiffres.

Bien que précurseur, le modèle monétique français se conforme en 1998 à la norme internationale EMV (cf. 2.4.2) et abandonne définitivement, au début des années 2000, son format B4/B0', dont les dernières années ont été entachées par la fraude aux « *YesCard* ». Les cartes françaises permettent ensuite de s'adjoindre une marque commerciale avec les cartes dites « co-brandées » (2007) et adoptent des avancées technologiques internationales comme le paiement sans-contact (2011).

Afin de présenter le fonctionnement des cartes de paiement et de pouvoir en étudier la fraude, il est nécessaire d'introduire la notion d'interfaces d'interaction des cartes de paiement ; une interface étant un des moyens pour le terminal ou le commerçant d'interagir et dialoguer avec la carte.
Chaque carte peut ainsi être dotée, à l'heure actuelle, d'un maximum de quatre interfaces :

- l'interface visuelle ;
- l'interface magnétique ;
- l'interface puce à contacts ;
- l'interface puce sans contact.

2.2 Interface visuelle

La forme et le visuel de la carte de paiement répondent à des normes internationales, dont :

- l'ISO 7810 qui définit sa taille ;
- l'ISO 7811-1 qui définit la position de la ligne du numéro porteur, de la zone de nom et adresse ainsi que les caractéristiques des caractères lisibles ;
- l'ISO 7811-2 qui définit la position des pistes magnétiques ;
- l'ISO 7812-1 qui définit le format du numéro porteur ;
- l'ISO 7816-2 qui définit la position des contacts.

FIGURE 2.3 – Visuels recto/verso d'une carte de paiement

L'identité visuelle d'une carte de paiement peut ainsi être caractérisée par les éléments présents sur la figure 2.3 :

1. numéro porteur (*Primary Account Number* (PAN)) ;
2. nom du porteur ;
3. date d'expiration ;
4. logo(s) du(des) système(s) de paiement ;
5. code de vérification (CVV2/CVC2) pour paiement distant ;

6. numéro de série (ou masque) du fabriquant ;
7. signature du porteur ;
8. hologrammes et UV de sécurité.

2.3 Interface magnétique

La quasi-totalité des cartes de paiement en circulation possède une bande magnétique. Celle-ci est composée de trois pistes magnétiques. Les deux premières, appelées « piste 1 » et « piste 2 », sont les plus utilisées pour les opérations de paiement. Leurs positions et encodages sont définis par la norme ISO 7811.

La norme ISO 7813 décrit les données écrites (ou encodées) sur les pistes 1 et 2 des cartes de paiement. La principale différence technique entre ces deux pistes concerne la densité d'encodage. Chaque unité d'information (bit) est encodé plus finement sur la piste 1 (figure 2.4), ce qui permet d'écrire davantage d'information.

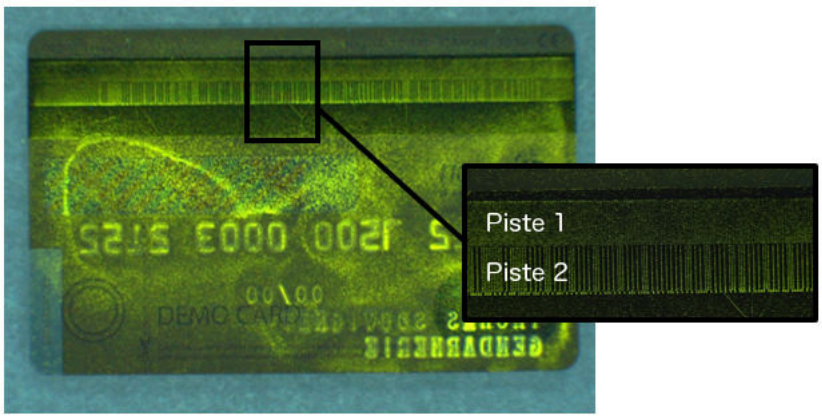


FIGURE 2.4 – Bande magnétique révélée chimiquement et par exposition UV

Sur la piste 1, il est possible de retrouver, entre autre, le numéro porteur, son nom, la date d'expiration et le code de service (figure 2.5). Ce code indique les droits d'utilisation de la carte (international, crédit) et si elle dispose d'une puce.

La piste 2 contient les mêmes informations à l'exception du nom du porteur qui n'est pas présent. Chacune de ces pistes disposent de mécanismes de sécurité permettant de s'assurer de l'intégrité des données présentes (code de Luhn, contrôle longitudinal de redondance (LRC)).

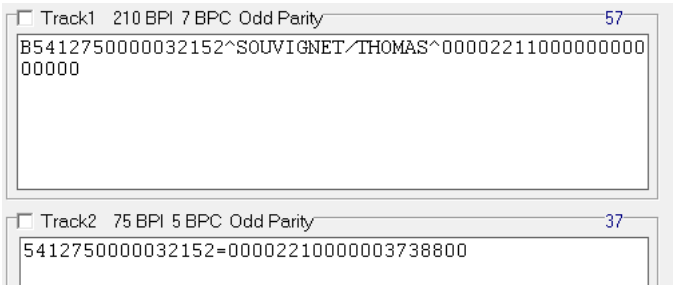


FIGURE 2.5 – Pistes 1 et 2 décodées

2.4 Interface puce à contacts

Les cartes de paiement à puce à contacts sont généralisées en Europe, en Amérique du Sud, au Canada et en Asie mais tardent à s'implanter aux États-Unis d'Amérique.

2.4.1 Présentation de la carte à puce

Une carte à puce se caractérise par la présence d'un micro-contrôleur à l'intérieur de celle-ci (figure 2.6 - gauche). La connexion entre le lecteur du terminal et le micro-contrôleur se fait par l'intermédiaire de contacts présents à la surface de la carte reliés à ce dernier (figure 2.6 - droite). La position et la nature de ces contacts sont définis par la norme ISO 7816-2.

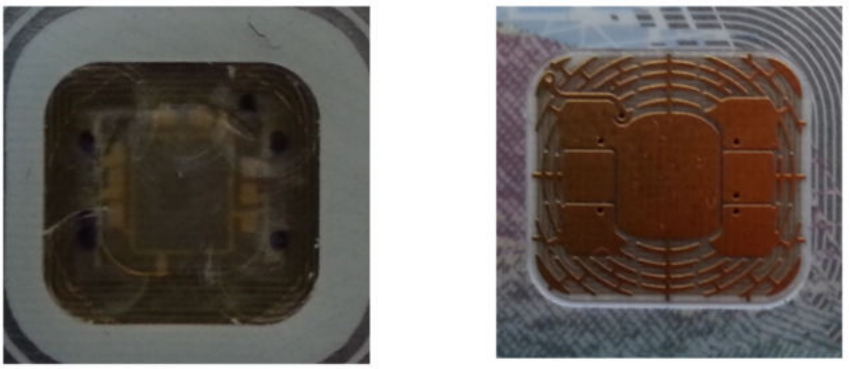


FIGURE 2.6 – Micro-contrôleur et contacts d'une carte à puce

Les niveaux des signaux électriques et les protocoles de transmission entre lecteur et carte sont définis par la norme ISO 7816-3.

Enfin, la norme 7816-4 définit les formats qu'ils utilisent pour s'échanger de l'information. Cette norme s'appuie sur un protocole commande/réponse. La puce est passive et ne fait que répondre aux commandes du terminal. Le nature de ces commandes/réponses est définie au niveau de l'application de paiement, la norme actuelle étant l'EMV.

2.4.2 Présentation de l'EMV

Europay-Mastercard-Visa (EMV) est un protocole applicatif de paiement et de retrait initialement défini en 1996 par les systèmes de paiement dont il porte le nom. Depuis, il s'est imposé comme standard international et est géré par l'organisme EMVCo.

Les spécifications EMV sont aujourd'hui à leur version 4.1 et se déclinent autour de quatre livres :

- livre 1 : interface entre la carte et le terminal, indépendante de l'application ;
- livre 2 : sécurité et gestion des clés ;
- livre 3 : spécification de l'application ;
- livre 4 : interface du porteur de carte, du commerçant et de l'acheteur.

Le livre 3 d'EMV définit la nature des échanges entre la carte et le terminal sous forme d'*Applicative Protocol Data Units* (APDU), conformément à la norme l'ISO 7816-4. Les commandes sont ainsi dénommées C-APDU et les réponses R-APDU.
Les réponses contiennent un indicateur d'état (*status word*) et des données optionnelles. Cet indicateur d'état dépend de l'état de la carte mais l'EMV impose qu'il soit égal à NORMAL (0x9000) quand une opération a été effectuée avec succès.

La première étape d'une transaction EMV consiste à choisir une application de paiement. En effet, une carte à puce peut contenir plusieurs applications. C'est par exemple le cas avec les cartes « co-badgées » où une application de paiement domestique (ex. Cartes Bancaires) est présente à côté d'une application de paiement internationale (ex. Visa/Mastercard). C'est encore le cas avec les cartes qui embarquent une application de porte monnaie virtuel (ex. Monéo).
Cette opération est effectuée à l'aide de la commande « SELECT » associée à l'identifiant de l'application souhaitée (ex. 421010 pour Cartes Bancaires, 031010 pour Visa ou encore 041010 pour Mastercard). En cas de présence de l'application la carte sélectionne (« entre dans ») l'application choisit et renvoie l'indicateur d'état 0x9000. Dans le cas contraire un état d'erreur est renvoyé.

Les opérations suivantes se déroulant de la même façon (par émission de commandes/réponses), une transaction de paiement nécessite typiquement les étapes suivantes [19] :

1. sélection d'une application de paiement ;
2. lecture des données de l'application ;
3. authentification des données (vérification de l'intégrité des données) ;
4. analyse des restrictions (plafonds, paiement *offline*, etc.) ;
5. vérification du porteur (signature ou code personnel - PIN) ;
6. analyse de la demande de paiement par la carte et le terminal ;
7. décision d'acceptation, de refus ou d'interrogation de l'émetteur (paiement *online*).

2.4.3 Les différentes authentifications d'EMV

A la différence des paiements et retraits effectués à partir de la piste magnétique, un paiement effectué à partir de la puce peut être *offline* (sans contact avec la banque émettrice). Il est donc primordial que l'intégrité de la carte puisse être vérifiée par le terminal afin que celle-ci ne puisse pas être modifiée afin d'accepter toutes les demandes de paiement que lui présenterait un terminal (principe de *YesCard*).

A ces fins, l'EMV propose trois techniques différentes d'authentification des données présentes sur la carte [18, 19] :

- une authentification statique des données (SDA) ;
- une authentification dynamique des données (DDA) ;
- une authentification combinée des données (CDA).

Basée sur une signature statique des données, la méthode d'authentification statique des données (SDA) est actuellement dépréciée car, elle peut faire l'objet d'une attaque par rejeu.
Basée sur une signature dynamique des données à partir de clés publiques/privées propres à chaque carte, la méthode d'authentification dynamique des données (DDA), permet une authentification acceptable des données et le chiffrement du code personnel échangé avec le terminal.
La méthode d'authentification combinée des données, formellement nommée *Combined DDA/Application Cryptogram Generation* (CDA), est basée sur DDA. Elle ajoute une sécurité supplémentaire en authentifiant les données échangées avec le terminal lors de l'émission de la demande de paiement.

2.5 Interface puce sans contact

Dans ses prévisions 2014, Eurosmart estime que plus de la moitié des cartes sans contact sera émise par l'industrie bancaire [26], démontrant l'intérêt porté au paiement sans contact par les institutions bancaires.

L'interface sans contact de la carte est définie dans les spécifications *EMV Contactless Specifications for Payment Systems*. Elles se décomposent en quatre livres (actuellement en version 2.4) :

- livre A : architecture et exigences générales ;
- livre B : point d'entrée ;
- livre C : spécification du noyau ;
- livre D : protocole de communication sans contact.

Plusieurs différences existent entre l'accès via l'interface contacts et l'interface sans contact.

La première réside dans le protocole de communication en champ proche – ou *Near Field Communication* (NFC) – utilisé, l'interface sans contact étant basée sur l'ISO 14443, norme internationale spécifiant les caractéristiques de communication avec les cartes de proximité. Le livre D spécifie une distance de fonctionnement pouvant aller jusqu'à 4 cm.
Une seconde différence réside au niveau des informations et fonctionnalités disponibles à travers l'interface sans contact. Ainsi, pour accélérer les paiements, la vérification du porteur n'est pas demandée et, pour en limiter les abus, les plafonds de paiement sont limités (eg. 20 €). De même, pour des raisons de confidentialité, le nom du porteur ne doit pas être présenté sur cette interface.

3 Les terminaux

3.1 Évolution des terminaux

Les terminaux ont suivi l'évolution des cartes. Les premiers terminaux étaient mécaniques, tel que celui présenté en figure 2.2. Les premières traces d'un terminal électronique (figure 3.1) remonte à 1969 avec le brevet déposé par John L. Gropper [31] concomitamment à l'émission des premières cartes magnétiques.

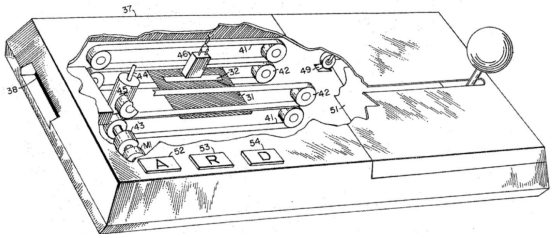


FIGURE 3.1 – Terminal de vérification de crédit (1969) - *source : [31]*

Ce premier terminal transmet par téléphone le signal brut de la piste magnétique à l'établissement émetteur et reçoit en retour un signal illuminant les voyants indiquant si le solde du client est suffisant.

Les premières traces d'automates de retrait remontent à 1978 avec un brevet déposé par Hitachi [36] (figure 3.2). On retrouve dans celui-ci tous les éléments des automates bancaires actuels : vérification de solde, émission de billets, délivrance de ticket, dépôt d'argent, etc.

Au tournant des années 1980, les terminaux effectuent leurs premières opérations de paiement (figure 3.3) et disposent déjà des fonctionnalités des terminaux actuels (lecture de cartes, saisie clavier, impression de reçu).
D'abord réservés aux grandes enseignes, l'essor de la télématique et des réseaux numériques permet de démocratiser les terminaux qui deviennent accessibles aux petits commerçants (figure 3.4).

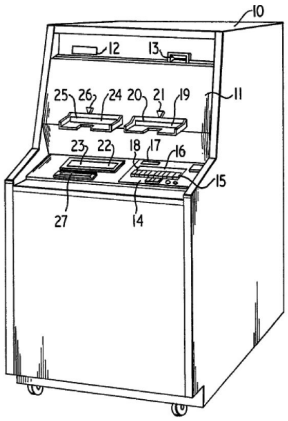


FIGURE 3.2 – Automate bancaire (1978) - *source : [36]*

(a) Terminal de Visa (1979)

(b) Monic 1800 d'Ingenico (1981)

FIGURE 3.3 – Premiers terminaux de paiement

FIGURE 3.4 – Terminal de paiement pour minitel - *source : Ingenico*

Les années 2000 correspondent à l'avènement des terminaux que nous utilisons actuellement et leur généralisation dans les commerces de proximité.

Enfin les années 2010 marquent un tournant dans l'évolution des terminaux. Ceux-ci deviennent tactiles, sans-contact, connectés et multimédia (figure 3.5) afin d'offrir au commerçant la possibilité de créer une véritable interface client et de supprimer les frontières entre ses boutiques physiques et sa présence en ligne.

FIGURE 3.5 – Terminal iSC Touch - *source : Ingenico*

3.2 Typologie des terminaux

Préalablement à toute étude, la diversité actuelle des terminaux nécessite de les regrouper en grandes familles ayant des caractéristiques communes (physiques ou d'usage).

La typologie des terminaux basée sur la segmentation commerciale des fabricants[1] est proposée comme suit :

- Terminaux de paiement physiques :
  - terminaux point de vente fixes ;
  - terminaux point de vente portables ;
  - terminaux portables et mobiles.
- Terminaux de paiement virtuels :
  - terminal de réservation connecté à une centrale de paiement ;
  - terminal de paiement virtuel (paiement en ligne).
- Automates de paiement et de retrait :
  - automates de paiement ;
  - automates de retrait ;
  - automates de libre service.
- Périphériques de caisse et accessoires :
  - claviers de saisie du code personnel (PIN Pad) ;
  - périphériques de signature ;
  - accessoires de paiement sans contact.

1. Ingenico, Verifone, Wincor Nixdorf, NCR

On retrouve ainsi trois grands types de terminaux : ceux de paiement physique, les virtuels et les automates (de paiement et de retrait). Un quatrième type est lié à la monétique intégrée où une partie du traitement du paiement est déporté sur un terminal ou un système d'acceptation centralisé.

3.2.1 Terminaux de paiement physiques

Les terminaux de paiement commercialisés aujourd'hui proposent plus qu'un simple paiement par piste ou puce.

En terme de technologie, ceux-ci peuvent proposer des paiements sans contact ou encore par biométrie. Mais c'est en terme d'intégration avec le système d'information du commerçant que les évolutions sont les plus importantes. Tout d'abord, les terminaux mobiles (ex. figure 3.6) permettent une fluidité des paiements en intégrant l'étape de paiement dans le processus de commande du commerçant.

FIGURE 3.6 – Exemple de terminal mobile adossé à un iPhone - *source : ingenico.com*

De plus, l'avènement des écrans couleurs et tactiles permet d'imaginer l'intégration d'une partie du processus de commande directement dans le terminal lui-même.

Enfin une évolution d'usage est peut-être en cours avec l'intégration de solutions de paiement directement dans les téléphones portables de dernière génération. Si les premières solutions, à base de simples lecteurs à pistes magnétiques branchés sur la prise audio, n'étaient pas sans poser des questions de sécurité, les solutions actuelles, basées sur des environnements d'exécution sécurisés (TEE) et des systèmes d'acceptation distants, pourraient permettre au commerçant une intégration toujours plus grande et à moindre frais.

3.2.2 Terminaux de paiement virtuels

Les terminaux de paiements virtuels correspondent aux plateformes de paiement utilisées lors de paiement sur Internet, par services vocaux ou par les opérateurs de vente à distance.

Ces terminaux ont longtemps fait reposer la vérification de la carte de paiement sur la saisie d'éléments présents sur son interface visuelle : numéro de la carte de paiement, date d'expiration et code de vérification (CVV2/CVC2) pour les paiements distants.

Face à l'augmentation des fraudes sur la vente à distance, les acteurs de la monétique ont mis en place une authentification renforcée du porteur. Cette authentification, rendue possible par le protocole 3D-Secure[2], est parfois assurée par « ce que sait le porteur » (mot de passe, date de naissance) ou « ce qu'il possède » (carte contenant des codes d'identification, équipement d'authentification – *token* – ou en encore téléphone portable[3]).

3.2.3 Automates

Les automates ou terminaux de borne se distinguent par leur caractère autonome et sans surveillance du commerçant (« *unattended* »).

Les plus répandus sont sans doute les automates de retrait avec 58 624 Distributeurs Automatiques de Billets (DAB) et Guichets Automatiques Bancaires (GAB) à la fin 2013 sur le territoire français [27].
Néanmoins, d'autres automates sont également largement répandus comme les Distributeurs Automatiques de Carburant (DAC) ou les automates des sociétés de transport en commun (SNCF, RATP, Air France, etc.) ou de restauration rapide.

La caractéristique « non surveillés » de ces terminaux requière une sureté de fonctionnement et une sécurité accrue.

3.3 Normes

Les normes de sécurité sont les principales normes s'appliquant à la conception et la mise en place d'un terminal, même si des initiatives tentent actuellement d'en normaliser la structure.

2. Également désignée par les appellations commerciales Verified By Visa et MasterCard SecureCode.
3. Il s'agit là d'une vérification par code de sécurité envoyé sur le téléphone du porteur par SMS.

3.3.1 La sécurité des terminaux

En dehors des normes de sécurité applicables à l'ensemble du système monétique décrites précédemment (1.3.3), les terminaux doivent également répondre aux exigences PCI PTS (PCI PIN Entry Devices avant 2010) du PCI SSC.

Ces exigences de sécurité se déclinent au travers de quatre documents :

- exigences de sécurité des codes personnels (*PIN Security Requirements*) ;
- module matériel de sécurité (*Hardware Security Module* (HSM)) ;
- exigences de sécurité modulaires des points d'interaction (*Point of Interaction* (POI) *Modular Security Requirements*) ;
- exigences de sécurité des automates de paiement (*Unattended Payment Terminal* (UPT) *Security Requirements*).

Comme pour les normes PCI relatives à la sécurité des données, ces exigences sont imposées à tout terminal pouvant être commercialisé ou utilisé. Ces exigences se présentent sous la forme d'une liste de bonnes pratiques à mettre en œuvre.
Les 32 exigences de sécurité de PCI PTS en matière de sécurité des codes personnels [53] peuvent se résumer par les points suivants :

- chiffrement des codes personnels qui ne doivent jamais apparaître en clair ;
- cycle de vie sécurisé et documenté des clés de chiffrement ;
- protection mécanique à l'ouverture ou à la compromission, entraînant la suppression des codes stockés et des clés de chiffrement.

3.3.2 Une normalisation en cours

Jusqu'à présent, la structure des terminaux n'est pas encadrée, sa conception devant uniquement répondre à des standards de sécurité et d'interopérabilité (ex. EMV, CB2A, PCI). Néanmoins, des projets de normalisation de terminaux tentent actuellement de s'imposer sur le marché européen.

Ainsi le groupe de travail technique du *« Common Implementation Recommendations »* (CIR) propose un premier standard pour les terminaux de paiement et de retrait, le « *Financial Application Specification for SCS Volume Compliant EMV Terminals* » (SEPA-FAST).
L'objectif de ce standard est d'offrir au consommateur une expérience uniforme, de réduire les risques d'obstacle à l'interopérabilité entre applications et de permettre un marché ouvert de composants basés sur l'EMV.

Il est à noter le caractère opérationnel de ce projet normatif puisqu'une preuve de concept,

le projet OSCAR [4], implémente avec succès SEPA-FAST conjointement avec EPAS (abordé en 1.3.2).

4. http://www.oscar-project.eu/

Première partie

Les fraudes, état de l'art

4 Taxonomie des fraudes au système monétique

4.1 Présentation de l'approche adoptée

Dès 1993, Ross Anderson, chercheur à l'université de Cambridge, référençait les faiblesses et les fraudes au système monétique [1] à travers une impressionnante liste d'erreurs et vulnérabilités présentes sur les distributeurs automatiques de billets.

Depuis cette date, différents travaux de recherche se sont focalisés sur les attaques pouvant être réalisées sur les composants du système monétique afin de s'en prémunir ou d'en réduire la portée. L'originalité de ce travail de thèse est d'aborder la problématique sous un angle différent, en se focalisant sur les fraudes constatées et non hypothétiques.

En effet, une connaissance actualisée des fraudes au système monétique permet aux acteurs luttant contre celles-ci d'orienter leurs actions et ainsi d'accroitre leur efficacité.

Il est ainsi possible de classer les fraudes actuelles en fonction des éléments du système monétique sur lesquelles elles s'appuient :

- la carte ;
- le terminal ;
- le système de traitement monétique.

4.2 Fraudes basées sur la carte

Les fraudes basées sur les cartes de paiement sont sans doute les plus connues puisque les plus anciennes et les plus médiatisées.

La plus simple des fraudes, et donc l'une des plus répandues, consiste à collecter les données présentes sur les pistes magnétiques d'une carte de paiement. Ces données peuvent permettre de réaliser des opérations de retrait ou de paiement.

La dotation en « puces » des cartes de paiement, qui a pour objectif de réduire ce type de fraude, a eu pour conséquence de transférer une partie de l'intérêt des fraudeurs sur cette technologie. A ce jour, seules deux fraudes ciblant les microprocesseurs sont recensées : la première visant l'espionnage des échanges entre la carte et le terminal, la seconde vise à modifier le comportement observé de la carte. Toutes deux sont basées sur l'attaque de l'homme du milieu décrite au paragraphe 4.2.2.

4.2.1 Fraude par mouchard

4.2.1.1 Présentation

La fraude par mouchard, plus connue sous le terme de *skimming*, consiste à capturer, à l'insu du porteur, des données de la carte de paiement.

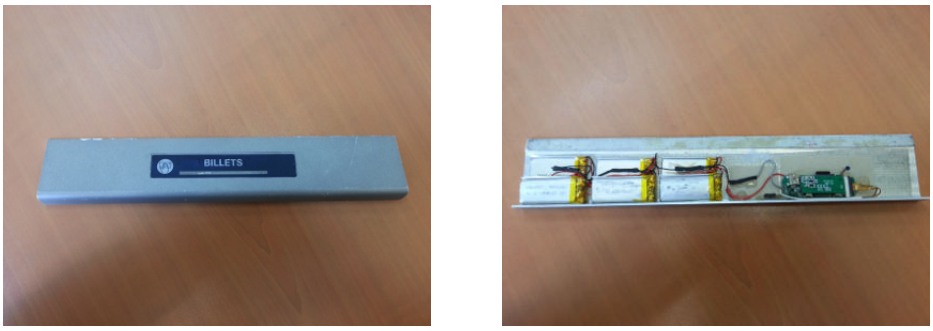
En théorie la collecte peut être réalisée à partir de l'ensemble des interfaces de la carte : l'embossage/les données sérigraphiées, la bande magnétique, la puce et l'interface sans contact. Toutefois, en raison du faible niveau de sécurité qu'elle présente, la bande magnétique est le plus souvent la cible du dispositif de capture des données bancaires (figure 4.1).

(a) Recto (b) Verso

FIGURE 4.1 – Exemple de mouchard ou *skimmer* à pistes magnétiques

Afin d'être complète et de permettre une opération de retrait ou de paiement, la collecte des données de paiement est souvent accompagnée d'une collecte du code confidentiel (figure 4.2).

Une fois ces données capturées, elles peuvent être revendues afin de réaliser des cartes contrefaites ou des paiements sur Internet (données de l'interface visuelle). Cette opération est communément appelée « *carding* ».
Une carte contrefaite peut aisément être réalisée en récrivant des données récupérées sur une autre carte à pistes magnétiques. Seule la détention d'une encodeuse de pistes magnétiques est nécessaire (environ 200 €).



(a) Recto) (b) Verso

FIGURE 4.2 – Exemple de dispositif de capture du code confidentiel

4.2.1.2 Évolution de la fraude par mouchard

Bien qu'il en soit difficile de déterminer à quelle date remonte la première fraude par mouchard, il est vraisemblable qu'elle remonte aux premières cartes de paiement émises, avec une interception manuelle des données imprimées sur celles-ci.

Depuis quelques années, cette fraude s'est très largement répandue et de nombreux organismes (*European ATM Security Team* (EAST), Observatoire de Sécurité des Cartes de Paiement (OSCP), *Financial Fraud Action UK* (FFA UK), etc.) s'appliquent à la surveiller. Ainsi, il possible d'en dessiner assez fidèlement l'évolution sur les dix dernières années [63].

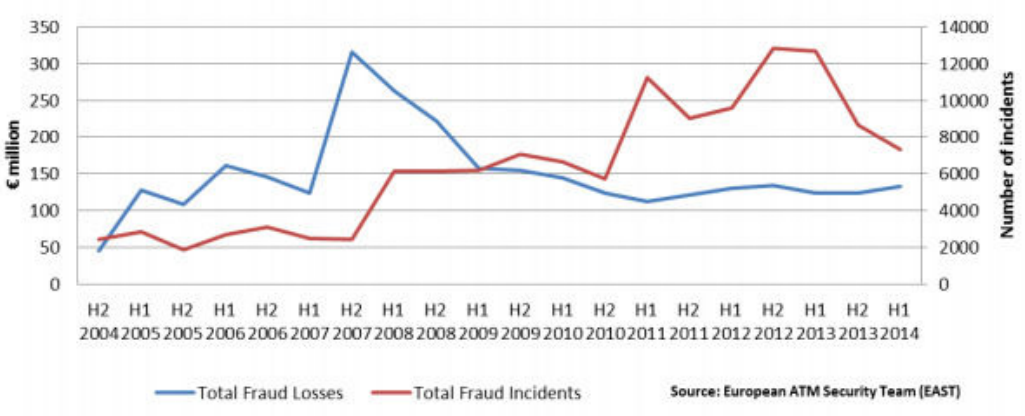


FIGURE 4.3 – Évolution de la fraude par mouchard au cours des dix dernières années - *source : EAST [63]*

On peut observer la constante évolution de cette fraude en terme de faits constatés jusqu'en 2013 (tracé rouge sur figure 4.3). Cette croissance s'observe moins en terme de volume de montant fraudé (tracé bleu sur figure 4.3) dont le volume est stagnant.

Si l'évolution de la fraude constatée est enrichissante, l'évolution des techniques et technologies employées l'est tout autant. La rareté des articles scientifiques sur le sujet [47, 34] ne permet toutefois pas d'obtenir une base de référence suffisante sur le sujet, et seul le ressenti des spécialistes du domaine permet d'apprécier l'évolution des techniques employées.
Il en ressort une forte adaptation des mouchards à leur environnement et à la recherche d'une efficacité et autonomie toujours plus grande. Ainsi la collecte des informations est passée d'une collecte manuelle des données embossées sur la carte, à une collecte des données de la piste à partir d'un lecteur de bureau, puis d'un lecteur portable autonome, d'un lecteur caché dans une fente d'insertion de carte, dissimulé dans une fente d'accès à un sas sécurité, pour enfin s'intéresser aux données échangées par la puce.

4.2.1.3 Taxonomie des mouchards actuels

De nombreux modèles différents de mouchard coexistent de nos jours. Bien qu'il soit possible de les classer en fonction du support sur lesquels ils sont retrouvés (terminal de paiement, de retrait, lecteur portable ou encore autonome), un classement en fonction de leurs propriétés intrinsèques en permet une identification plus fidèle.

En prenant en considération l'interface de la carte que le mouchard cible pour la collecte des données, une première classification peut être effectuée entre les mouchards de pistes magnétiques et ceux de cartes à puce à contacts. A ce jour, aucun mouchard visuel ou sans contact n'a été utilisé concrètement lors d'une fraude.

Une fois cette première grande distinction réalisée, les dispositifs de capture de données de carte peuvent être triés en fonction des technologies employées par chacune des quatre composantes d'un mouchard (figure 4.4) :

- l'acquisition du signal de pistes magnétiques. Elle peut demeurer analogique ou être numérisée. L'emploi d'un amplificateur opérationnel ou d'un circuit de décodage du signal modulé (décodeur F2F - fréquence/double fréquence) se révèle donc être un premier élément de classification qui peut être complété par la référence du ou des composants employés ;
- le traitement des données collectées. Une classification peut être réalisée en fonction des composants employés pour réaliser cette tâche (eg. micro-contrôleur) ;
- le stockage des données collectées. Une classification par les composants utilisés (eg. mémoire Flash) peut également être réalisée ;
- l'interface de communication. Elle se révèle également être un élément de classification pertinent. Quelle que soit sa nature (2 broches, 3 broches, 4 broches, Bluetooth ou encore GSM), la présence d'une interface de communication est en effet indispensable pour que l'utilisateur récupère les données collectées.

Cette proposition de classification a été adoptée par l'*Europol CyberCrime Center* (EC3) au sein de sa plateforme destinée à ses experts du domaine, l'*European Plateform for Expert.*

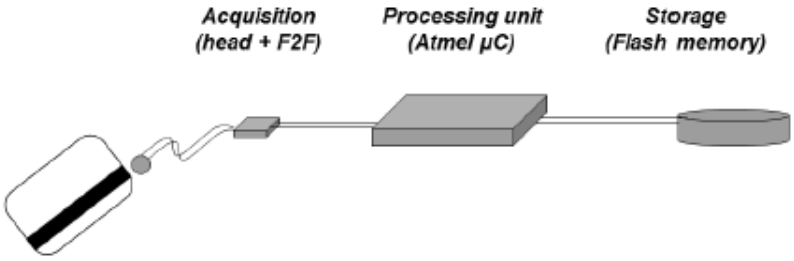


FIGURE 4.4 – Schéma de décomposition d'un mouchard de carte de paiement (hors interface de communication) - *source : Souvignet et Frinken [62]*

4.2.2 Fraude par attaque de l'homme du milieu

4.2.2.1 Présentation

Une attaque de l'homme de milieu, ou *man in the middle attack*, consiste à s'insérer dans un canal de communication entre deux entités pour intercepter voire modifier les échanges entre ces parties. Une telle attaque a récemment été démontrée sur des cartes à puce EMV par l'équipe sécurité de l'université de Cambridge [48].

L'attaque proposée consiste à insérer un dispositif électronique entre la puce d'une carte et ses contacts. Au cours d'une transaction de paiement, ce dispositif indique à la carte que l'utilisateur est authentifié par signature du porteur, et au terminal (en contact avec la carte) qu'il est authentifié par vérification du code PIN.

La miniaturisation de cette attaque, démontrée sur une publication plus récente de cette même équipe [6] (figure 4.5), rend cette attaque furtive et donc exploitable par un fraudeur. L'existence d'une fraude liée à ce type d'attaque a été rendue publique début 2013 [43]. Bien qu'elle soit difficile à mettre en œuvre, le retour sur investissement (plus de 500000 € de préjudice pour une dizaine de cartes falsifiées) semble être suffisamment important pour intéresser les fraudeurs et entrevoir une généralisation de la fraude.

4.2.2.2 Évolution et dispositif de lutte contre la fraude

Dans son rapport annuel 2013 sur la fraude 2012 [50], l'OSCP souligne la complexité de mise en œuvre de cette fraude et sa portée limitée uniquement aux paiements *offline*, donc de montants faibles (en France inférieurs à 100 euros). Il reste donc optimiste quant à une

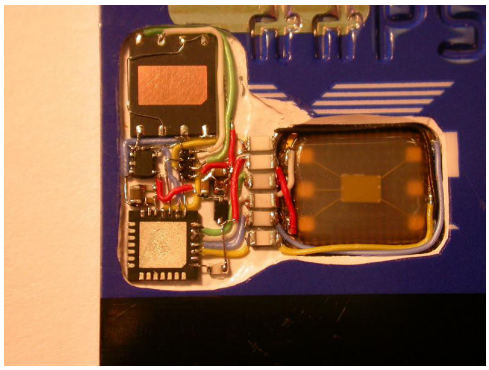


FIGURE 4.5 – Carte modifiée pour attaque de l'homme du milieu - *source : lightbluetouch-paper.org / Mike Bond*

évolution limitée de cette fraude.

Dans ce même rapport, l'OSCP indique que deux solutions permettant de lutter contre cette fraude : une systématisation du paiement *online* ou une migration accélérée vers une authentification CDA (cf. 2.4.3).

La première solution s'avère difficilement envisageable (mise à jour du parc hétérogène) et ôterait tout intérêt au paiement par carte à puce dont l'une des principales forces réside dans un paiement *offline* sécurisé. Par ailleurs, cette solution sous-entend que les établissements aient mis en place une solution remontant de manière systématique le mode d'authentification du porteur utilisé, le résultat obtenu et qu'ils en vérifient l'adéquation avec le système de paiement utilisé.

La seconde proposition apporte une solution à long terme qui pourrait par ailleurs être réglée par une personnalisation adaptée, interdisant toute authentification par défaut ou basée sur la signature du porteur.

4.3 Fraudes basées sur les terminaux

Les fraudes basées sur les terminaux correspondent aux fraudes dont la cible principale est un terminal, quelle que soit sa nature : terminal de paiement physique, terminal virtuel, automate, etc.

Les attaques sous-jacentes peuvent se caractériser sous deux formes : celles visant à modifier le comportement du terminal pour y ajouter des dispositifs malicieux et celles visant à exploiter des défauts de conception du terminal pour en retirer un bénéfice.

4.3.1 Fraudes aux terminaux compromis

Même s'il sont conçus pour être inviolables (notamment en chiffrant leurs communications et en se désactivant s'ils sont ouverts - cf. 3.3.1), les terminaux monétiques ont une durée de vie importante (pouvant atteindre une dizaine d'année) et sont donc sujets aux avancées technologiques dont peuvent profiter les fraudeurs.

4.3.1.1 Terminaux de paiement infectés

Une des cibles les plus simples à compromettre semble être les terminaux de réservation disposant d'un terminal de paiement léger ou une solution monétique intégrée. Une telle configuration permet au fraudeur disposant d'un accès physique à l'ordinateur d'installer un dispositif physique (*keylogger*, etc.) ou logique (logiciel malveillant, *keylogger* logiciel, etc.) permettant la capture des données de paiement.

Bien que cette fraude semble des plus aisées puisqu'un accès à ces terminaux de réservation est par nature indispensable dans les services de proximité, très peu de cas de fraude étaient connus jusqu'à peu.
Le logiciel malveillant « Dexter » a toutefois largement contribué à la connaissance de cette fraude par le grand public. Début 2012, de nombreux médias ont en effet relayé les découvertes de la société Seculert. Ce logiciel malveillant consiste à parcourir la mémoire d'applications de réservation et paiement à la recherche des données de pistes magnétiques (pistes 1 et 2) [56]. Il vise donc essentiellement les terminaux qui ne répondent pas aux exigences de sécurité détaillées en 1.3.3 et les systèmes de caisses reliés à des terminaux légers n'implémentant pas l'EMV (puisque visant l'utilisation de la piste).
Les fraudes par infection des terminaux de paiement semblent être en pleine expansion comme le montre les dernières attaques des chaines nord-américaines Target en 2013 et Home Depot en 2014 [41]. La compromission des automates de caisses de cette dernière chaîne (figure 4.6) a rendu possible la collecte des données de 56 millions de cartes de paiement (contre 40 millions pour Target).
Ces deux récentes infections seraient la conséquence de l'injection du *malware* « BlackPOS » [65]. D'autres *malware* visant les caisses reliées à des terminaux sont également identifiés, tels que BrutPOS ou Backoff POS (CERT-IN).

Enfin, si des travaux de recherche [49] tendent à prouver qu'une infection d'un terminal de paiement électronique par les interfaces légitimes serait possible, aucune fraude liée à une telle attaque n'a encore été observée.

4.3.1.2 Terminaux de retrait infectés

L'infection de terminaux de retrait est beaucoup plus difficile à mettre en œuvre puisque les accès physiques et logiques aux automates distributeurs de billets sont contrôlés et

FIGURE 4.6 – Automate de caisse de Home Depot - *source : lightbluetouchpaper.org / http://krebsonsecurity.com*

cloisonnés.

Jusqu'en 2014, seuls quelques cas de fraudes étaient connus notamment en Europe de l'est et en Amérique du Sud (sans publication). Dans les deux cas, une complicité interne semble avoir été mise en œuvre afin de modifier le système d'exploitation du distributeur de billets afin d'y insérer une porte dérobée (figure 4.7) permettant de vider les cassettes de billets [42].

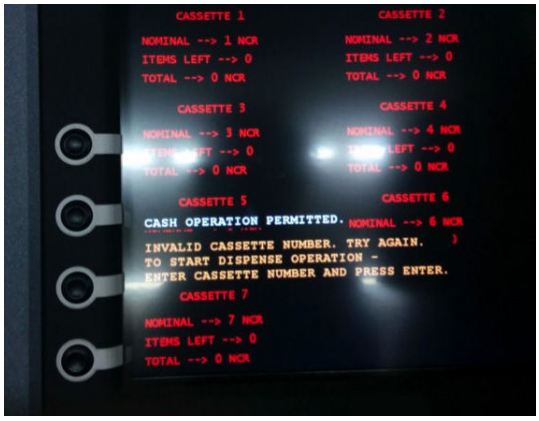


FIGURE 4.7 – Portée dérobée installée sur distributeur de billets - *source : [42]*

La seule affaire d'infection de terminaux sans complicité interne a avoir été rendue publique est très récente (mai 2014). La police de Macau (Chine) a arrêté un groupe criminel qui utilise un long dispositif électronique (figure 4.8) pour injecter un virus dans des

distributeurs de billets à travers l'interface carte à puce [64].

FIGURE 4.8 – Dispositif inséré dans le distributeur de billet afin d'injecter un virus - *source : http://orientaldaily.on.cc*

Ce virus est alors en charge de récolter les données de paiement et de les restituer via la même interface.

L'évolution des logiciels malveillants sur terminaux de retrait est inquiétante puisqu'en l'espace de quelques mois, elle est passée de quelques cas isolés à des dizaines de cas par mois (figure 4.9). Cette évolution subite s'explique notamment par le fait que la complicité interne n'est plus de rigueur mais que des accès sont rendus possibles sur les terminaux de retrait présents sous la forme de bornes isolées (non fixées au bâti) [42].

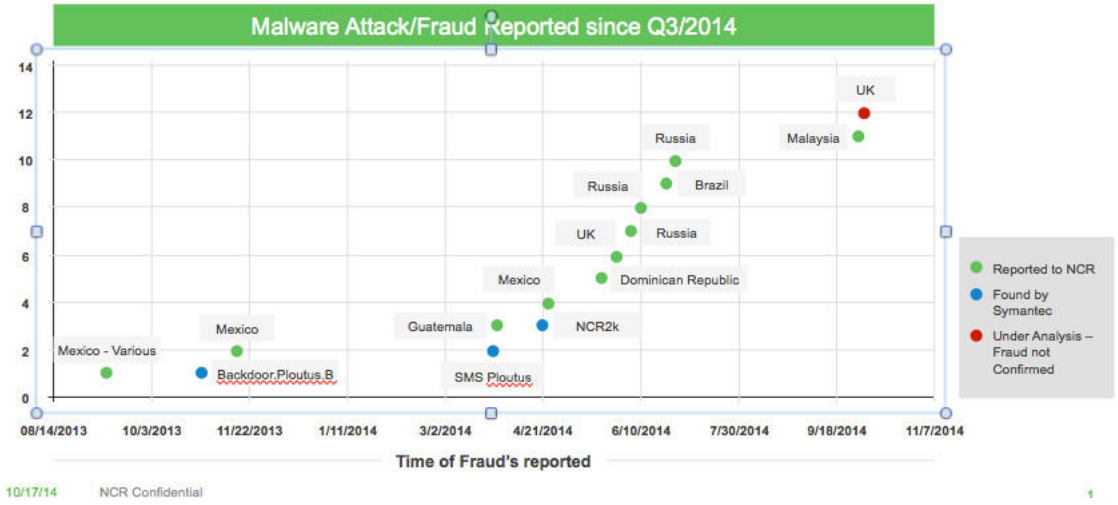


FIGURE 4.9 – Fraudes par logiciels malveillants sur terminaux de retrait depuis mi-2013- *source : [42] (recadrée)*

4.3.1.3 Terminaux de paiement reprogrammés

Une dernière fraude consiste à compromettre un Terminal de Paiement Électronique (TPE) en le reprogrammant totalement. Une fois reprogrammé, le TPE se comporte comme

un terminal légitime à la différence qu'il impose au porteur de passer sa carte dans le lecteur à piste magnétique, prétextant un échec puce. A l'issue de l'opération de paiement systématiquement acceptée, imprimant un ticket vraisemblable et personnalisable (figure 4.10), le TPE dispose en mémoire du contenu de la piste magnétique et du code personnel du porteur.

FIGURE 4.10 – Ticket client personnalisé imprimé par un TPE reprogrammé

Cette fraude, dont des signes de diffusion sont pourtant largement présents sur Internet, est pour le moment très peu identifiée. En effet, les transactions effectuées ne sont pas mises en paiement et aucun point de compromission ne peut donc être décelé. Il est donc impossible de savoir que le vol de ces données de paiement provient de cette fraude ou d'une lecture « sauvage » de ces données, à moins d'interroger chaque porteur sur l'ensemble de ses paiements. C'est la raison pour laquelle ce type de fraude est surnommée « fraude aux TPE fantômes ».

4.3.2 Fraudes par rétro-ingénierie du terminal

Si la compromission d'un terminal permet de collecter de façon massive des données de paiement, d'autres fraudes ciblent également les terminaux, de façon beaucoup plus individualisée mais avec un gain beaucoup plus immédiat.

Ces fraudes s'appuient sur une étude poussée du fonctionnement du terminal à la recherche de failles pouvant être exploitées.

4.3.2.1 Fraude par *cash trapping*

La fraudes par rétro-analyse du terminal la plus répandue est la fraude par « *cash trapping* ». Cette fraude vise à subtiliser les billets de banques distribués, à l'insu du porteur de la carte et de l'établissement bancaire propriétaire du distributeur de billets. Cette fraude se concrétise sous deux formes majeures, en fonction du dispositif utilisé pour subtiliser les billets : une réglette adhésive ou une « fourchette ».

La fraude par *cash trapping* à la réglette s'appuie sur une simple observation du terminal de retrait : si les billets ne sont pas retirés par l'utilisateur de l'automate, ceux-ci sont ravalés quelques secondes après que l'utilisateur ait été invité à reprendre sa carte de retrait et l'automate revient à son écran d'accueil. La fraude consiste donc à mettre en place une réglette disposant d'un adhésif puissant devant la fente de distribution des billets (figure 4.11). L'utilisateur a ainsi l'impression que le distributeur ne fonctionne pas (billets non délivrés et carte restituée) et le fraudeur n'a plus qu'à attendre son départ pour récupérer sa réglette et les billets collés dessus.

FIGURE 4.11 – *Cash trapping* à la réglette - *source : Lyon Mag*

La fraude de *reversal cash trapping* à la « fourchette » s'appuie sur une analyse un peu plus avancée du terminal de retrait. En effet, la plupart des terminaux de retrait préparent les billets demandés quelques secondes avant de les distribuer. Si l'opération est annulée après cette préparation, les billets ainsi préparés vont alors dans une caissette dédiée. Cette fraude consiste donc à annuler l'opération de retrait juste après que les billets aient été préparés et à empêcher qu'ils ne soient renvoyés dans la caissette sécurisée. Pour cela, les fraudeurs annulent l'opération (via le bouton dédié ou en empêchant le rejet de la carte) et récupérent les billets en attente présents derrière la fente de distribution de l'automate à l'aide d'une « fourchette » préalablement placée dans celle-ci (figure 4.12).

L'opération ayant été annulée, le cumul des retraits effectués n'est pas modifié et le plafond de retrait autorisé pour la carte jamais atteint.

FIGURE 4.12 – *Cash trapping* à la fourchette - *source : Quotidiano Piemontese*

Ce type de fraude est en constante évolution depuis quelques années [63]. Souvent perçue comme une fraude à basse technicité en raison du faible niveau de technicité nécessaire à sa mise en œuvre et non pour la concevoir, elle permet un important gain immédiat en prenant un minimum de risque. Si le distributeur ne dispose d'aucune contremesure et de système d'alerte, il est en effet possible à un fraudeur à la fourchette de vider le contenu d'un distributeur en quelques dizaines de minutes.

4.3.2.2 Fraude par forçage du terminal

La fraude par rétro-ingénierie du terminal ne vise pas uniquement les terminaux de retrait. La connaissance du fonctionnement d'un terminal de paiement et de ses spécificités est également la source de quelques escroqueries. L'une des plus efficaces repose sur le principe de forçage d'une opération de paiement.

Pour éviter toute interruption de service dès lors qu'une interrogation d'un serveur d'autorisation de paiement n'est pas possible (pas d'accès au réseau de demande d'autorisation ou serveur hors service), il est prévu de pouvoir obtenir une autorisation par téléphone (appel phonie). Pour cela le commerçant est censé contacter un numéro dédié et transmettre les informations sur le paiement afin d'obtenir un code de forçage (numéro d'autorisation). Une fois obtenu, le commerçant n'a plus qu'à rentrer dans un mode dédié de son terminal afin d'entrer le code obtenu et ainsi forcer manuellement la transaction (certains terminaux demandant également la présence de la « carte commerçant »). La validité de l'autorisation ne sera vérifiée que lors de la mise en compensation des transactions.

La connaissance et l'analyse de ce fonctionnement a permis la mise en place d'une escroquerie lors d'un paiement très important. Elle vise à détourner l'attention du commerçant, à rentrer dans le menu dédié et à forcer la transaction sans l'autorisation par téléphone et sans insérer la « carte commerçant ». Bien que le forçage soit mentionné sur le ticket commerçant, le commerçant distrait pense que le paiement a été effectué avec succès et remet la marchandise aux clients.

Cette fraude par forçage du terminal reste très limitée en terme de volume. Toutefois elle reste très intéressante pour les fraudeurs au regard des montants concernés par opération. Cette fraude devrait toutefois être en voie d'extinction en France puisque le bulletin de sécurité CBEMV 13, devant être appliqué depuis le 1er juillet 2013, impose l'insertion de la carte commerçant lors des forçages [54].

4.4 Fraudes basées sur le système de traitement monétique

Les fraudes précédentes s'appuient sur un accès physique à un des éléments du système monétique. Les fraudes basées sur le système de traitement monétique s'appuient sur un accès logique soit au niveau du client (ordinateur d'un client de vente à distance), soit au niveau du serveur (serveur de e-commerce ou serveur d'acceptation).

4.4.1 Fraudes côté client

L'ordinateur ou le téléphone mobile du client sont souvent exclus du périmètre du système monétique, notamment lorsque l'on considère les évaluations sécuritaires. Les responsables de systèmes d'information monétiques n'ont en effet aucune emprise sur le poste de leurs clients.
Lorsque l'on considère la fraude, il devient toutefois important de considérer le poste client comme part entière du système d'information monétique, puisqu'une part importante de la fraude semble en être issue.

4.4.1.1 Fraude par hameçonnage

La fraude par hameçonnage, ou *phishing*, semble la plus connue du grand public puisque tout usager d'Internet fait au moins une fois l'expérience d'une tentative d'hameçonnage. Cette fraude consiste à envoyer un courriel en masse (spam), poster un message sur un forum ou afficher un encart publicitaire usurpant l'identité d'une banque émettrice ou d'un site commerçant, invitant son client à se rendre sur un site Internet afin d'y indiquer des éléments d'authentification ou de paiement. Un client non averti va donc se connecter sur le site indiqué, reprenant les éléments visuels du site légitime, et renseigner les éléments

demandés. Ces données sont ensuite stockées puis récupérées par le fraudeur.

Cette technique a certes un très faible taux d'adhésion (clients renseignant les données demandées) mais le très faible coût d'envoi de courriels en masse rend l'opération très lucrative. La complétude des données récupérées (numéro de carte, date expiration, cryptogramme visuel, nom du porteur, numéro de client bancaire, date de naissance, numéro de téléphone...) peut même permettre de contourner certains systèmes d'authentification non-rejouable. Les authentifications fortes basées sur une date de naissance ou la réception de SMS sont ainsi tout particulièrement fragilisées, le fraudeur pouvant renseigner la date préalablement communiquée ou faire procéder au changement du numéro de téléphone portable du client (sur le site internet de la banque ou en contactant l'agence bancaire).
Dans son rapport sur cette menace [37], le laboratoire de l'éditeur de logiciels anti-virus Kaspersky estime la progression du phénomène à +86% entre 2011/2012 et 2012/2013 pour finalement atteindre plus de 37 millions de victimes. Toujours d'après ce rapport, l'hameçonnage bancaire représente la majorité de cette fraude avec 20% des sites visés.
L'analyse de l'évolution du spam d'origine criminelle réalisée par l'initiative française Signal Spam (figure 4.13) va dans le même sens avec une constante évolution de l'importance du *phishing* par rapport au volume total de spam [59].

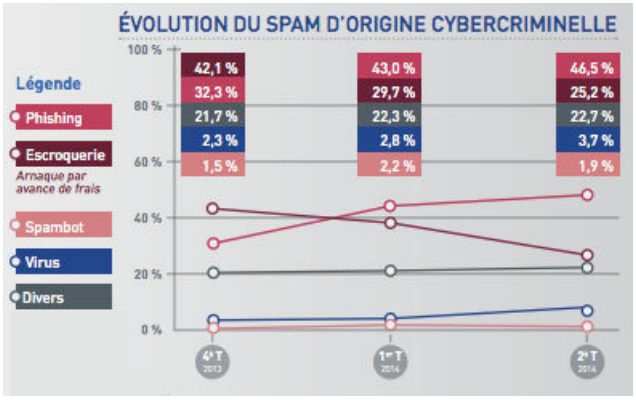


FIGURE 4.13 – Evolution du spam d'origine criminelle - *source : Signal Spam*

4.4.1.2 Fraude par logiciel espion

Une seconde fraude visant également le poste client est la fraude par logiciel espion. Cette fraude ne s'appuie pas sur une technique d'ingénierie sociale comme la précédente mais sur un défaut de sécurisation de l'ordinateur ou du téléphone du client.

La technique sous-jacente s'appuie sur l'injection d'un logiciel malveillant dans l'ordinateur ou l'équipement mobile de la victime qui s'emploie à capturer les éléments d'authentification et de paiement lors de leur saisie (par captation des touches, enregistrement de l'écran,

enregistrement des flux...).
L'un des principaux avantages de cette technique consiste à infecter un équipement mobile. Dans un tel cas, les systèmes d'authentification non-rejouables basés sur SMS seront sans effet puisque le logiciel malveillant est en mesure d'intercepter le code transmis par SMS et d'en cacher l'arrivée au propriétaire du téléphone.

De nombreux logiciels espions de type bancaire sont référencés dont Anserin, Citmo ou encore Sinowal [7]. Si la plupart se contente de récupérer des identifiants de connexion aux sites de banque en ligne, certains récupèrent également les numéros de cartes de paiement frappés au clavier ou permettent de déjouer les paiements à authentification renforcée. Pour chacun d'entre eux, il est difficile d'en connaître le volume diffusé et le nombre de numéros de carte interceptés. La société de sécurité informatique RSA estime néanmoins que le *malware* Sinowal aurait conduit à la compromission de 240000 cartes de paiement [9].

4.4.1.3 Fraude par force brute

Dans son rapport 2012 [50], l'OSCP confirme que les fraudes par force brute sont toujours d'actualité. Cette technique de fraude consiste à générer des numéros de cartes de paiement par« moulinage », et à essayer les différentes combinaisons possible de date d'expiration, voire de cryptogramme visuel, sur des sites marchands. Une fois qu'une combinaison acceptée a été obtenue, des achats plus importants peuvent être rapidement effectués par le fraudeur.

Cette fraude s'appuie essentiellement sur l'absence de détection et de contre-mesure au niveau des serveurs d'autorisation de la banque émettrice et peut donc cibler certains établissements bancaires plutôt que d'autres.
Si elle ne constitue pas une importante menace pour un émetteur correctement équipé, elle peut toutefois générer un bruit de fond qui pourrait profiter à d'autres fraudes.

4.4.2 Fraudes côté serveur

Le poste client n'est pas le seul à être visé par des attaques. Les serveurs de paiement, au cœur du système de traitement monétique, sont également pris pour cibles.

4.4.2.1 Fraude sur serveur commerçant

Certains commerçants ou fournisseurs de service n'utilisent pas les services des plateformes de paiement et se chargent eux-même de collecter et stocker les informations des cartes de paiement de leurs clients. Il leur incombe alors de mettre en œuvre les exigences de sécurité imposées par les normes en vigueur (voir 1.3.3).

Une attaque contre leurs serveurs constitue donc, pour les fraudeurs, un moyen d'obtenir un volume de cartes de paiement proportionnel à la fréquentation du site visé.
Ainsi l'attaque en 2011 contre les serveurs du réseau PlayStation de Sony aura permis le vol des données de l'ensemble des 77 millions d'utilisateurs dont 12,3 millions porteurs de numéros de carte de paiement [60]. Dans ce cas particulier, Sony déclare avoir mis en œuvre les exigences de PCI DSS en chiffrant les numéros de cartes conservées. Néanmoins c'est sur le délai de notification aux systèmes de paiement que Sony est critiqué car l'incident n'a été notifié que cinq jours après sa découverte alors que la quasi-totalité des systèmes de paiement exigent une notification immédiate [55].

4.4.2.2 Fraude sur serveur monétique

Les acquéreurs peuvent également faire l'objet d'attaques sur leurs systèmes d'information. Bien que particulièrement protégés, les serveurs d'acquisition sont une cible de choix pour les fraudeurs qui peuvent espérer compromettre un nombre important de cartes de paiement.

Ainsi l'une des plus importantes compromissions (en volume) a eu lieu en 2008, sur les serveurs de l'acquéreur américain *Heartland Payment Systems*.
Alerté par Visa et Mastercard début 2009, Heartland a identifié une intrusion sur ses systèmes remontant à fin 2007 et la mise en place d'un logiciel espion chargé d'exfiltrer les données de cartes véhiculées sur le réseau interne de l'acquéreur [66, 16].
L'attaque contre ses serveurs a conduit à la capture des données de 130 millions de cartes de paiement et au retrait temporaire de son agrément Visa [35].

Cet incident n'est pas isolé : l'acquéreur *Global Payments Inc.* a aussi fait l'objet d'une attaque sur son système d'information entre 2011 et mi-2012 ayant exposé 7 millions de cartes [38].

5 La fraude en chiffre

5.1 La fraude actuelle

Les chiffres de la fraude monétique sont rapportés de manières différentes en fonction de l'organisme qui les fournit. Pour les organismes bancaires (Banque Centrale Européenne (BCE), OSCP, FFA UK, etc.), les chiffres de la fraude s'entendent essentiellement en volume de pertes et nombre de points de compromission. Pour la justice et les forces de l'ordre, ils sont rapportés en nombre de faits constatés (crimes ou délits).

5.1.1 La fraude en volume de perte

Sujet sensible pour l'industrie bancaire qui craint une perte de confiance dans cet instrument de paiement, les chiffres de la fraude à la carte de paiement restent souvent confidentiels.

Néanmoins, si les principaux systèmes de paiement ne publient pas de chiffres annuels de la fraude, des systèmes nationaux, associations ou banques nationales publient des données statistiques permettant de régulièrement évaluer l'ampleur et l'évolution de la fraude à la carte de paiement.

Ainsi, depuis 2012, la BCE s'attache à analyser et publier annuellement les chiffres relatifs à la fraude à la carte de paiement des différents pays de la zone SEPA à partir de données fournies par les systèmes de paiement. Dans son rapport publié en 2014 sur la fraude constatée en 2012 [22], la BCE estime la fraude totale supportée par les émetteurs de cartes de la zone SEPA à 1,33 milliard d'euros, en augmentation de 14,8% par rapport à l'année précédente.
L'exercice de macro-vision effectué par la BCE permet d'avoir un éclairage sur les différentes pratiques européennes en matière de carte de paiement, tel que son taux d'adoption allant de 0,6 carte par habitant en Roumanie jusqu'à 3,7 cartes par habitant au Luxembourg. Il est toutefois surprenant de constater (figure 5.1) un taux de fraude allant du simple au triple entre des pays ayant des développements économiques et culturels comparables (Allemagne, Italie contre Royaume-Uni, France). Ces écarts peuvent s'expliquer par une réelle différence des cas de fraude mais également par une remontée

statistique différente. Les pays les plus exposés (France et Royaume-Uni) sont en effet ceux qui ont mis en place depuis des années des observatoires de surveillance (OSCP et FFA UK) fournissant annuellement des chiffres complets en matière de fraude à la carte de paiement.

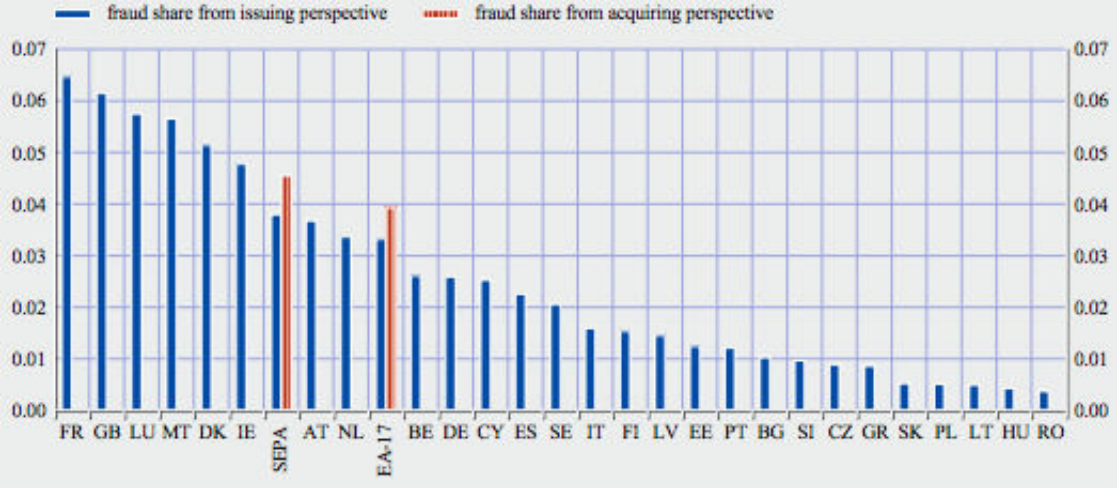


FIGURE 5.1 – Taux de fraude en pourcentage du volume total des transactions des cartes émises par pays (en bleu) et des paiements enregistrés dans la zone SEPA (en rouge) - *source : ECB [22]*

L'impact non négligeable de la collecte statistique semble se confirmer lorsque l'on considère la distribution de la fraude en fonction du canal d'acquisition (figure 5.2). Si l'importance de la fraude à distance (*Card Not Present* (CNP)) est unanimement mise en avant, il est surprenant de constater les écarts entre différents pays. Par exemple, la fraude sur distributeurs de billets (*Automatic Teller Machine* (ATM)) ne représenterait que 6% de la fraude totale du Royaume-Uni contre 52% de celle des Pays-Bas.
Ces différences peuvent notamment s'expliquer si un pays considère la fraude brute tandis que l'autre considère la fraude nette. En effet, les volumes de fraude s'entendent souvent bruts, c'est-à-dire aux montants payés par l'émetteur de la carte suite à une opération frauduleuse. Néanmoins, notamment lors de paiement à distance, l'émetteur a la possibilité de se retourner vers l'acquéreur lorsque les mécanismes minimums de sécurité prescrits par les systèmes de paiement n'ont pas été mis en œuvre. Par transfert de responsabilité, les montants frauduleux sont alors remboursés à l'émetteur par l'acquéreur défaillant. Après opération, le montant de fraude restant à la charge de l'émetteur correspond à la fraude nette. La marge entre fraude brute et nette peut être très importante, notamment lors de paiement frauduleux à distance sur des sites ne vérifiant pas le code de vérification visuel (CVV2 ou CVC2) ou ne mettant pas en œuvre de système d'authentification renforcée du porteur (3D-Secure). Dans le cas des Pays-Bas sur la figure 5.2, considérer les chiffres fournis à la BCE comme ceux de la fraude nette pourrait expliquer la part de fraude à

distance relativement faible comparée à celle des distributeurs de billets et du paiement de proximité (*Point Of Sale* (POS)).

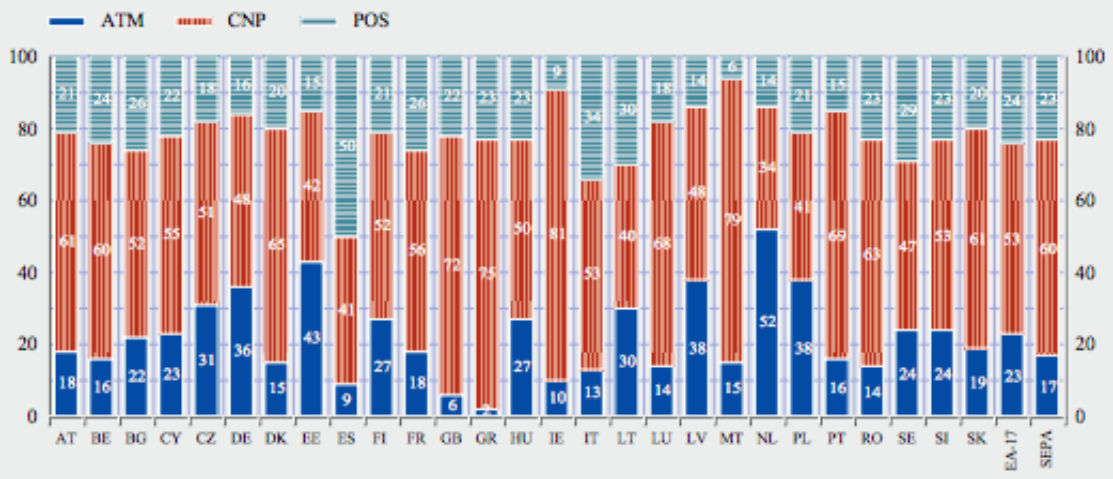
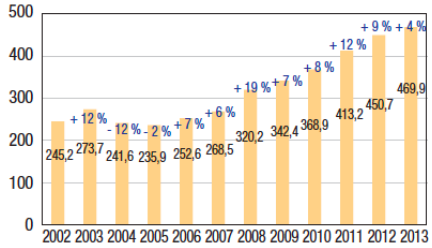
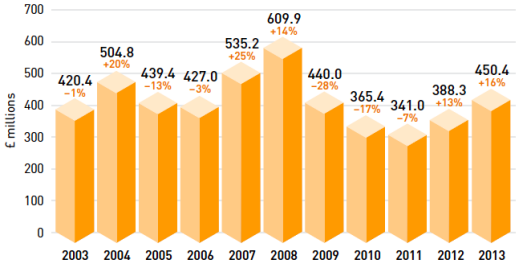


FIGURE 5.2 – Distribution géographique des montants de la fraude à la carte en fonction du canal d'acquisition, d'un point de vue émetteur - *source : ECB [22]*

Pour une analyse consolidée de l'évolution de la fraude, il convient donc de se tourner vers les chiffres fournis par des organismes établis de longue date. Les statistiques des rapports 2014 de l'OSCP [51] et de la FFA UK [28] permettent ainsi d'en remarquer une constante évolution (figure 5.3).



(a) en France (en millions d'euros)



(b) au Royaume-Uni (en millions de Livres)

FIGURE 5.3 – Montant total de la fraude à la carte de paiement - *source : OSCP [51] et FFA UK [28]*

Il est intéressant de constater comment le passage à EMV aura permis, dans les deux pays, de réduire temporairement le montant de la fraude : dès 2003 en France en réponse à la

problématique de « YesCard » affectant les cartes à puce de génération précédente, dès 2008 au Royaume-Uni faisant s'effondrer le montant de fraudes par carte contrefaite de 170 à 81 millions de Livres Sterling en une seule année.

5.1.2 La fraude en nombre de faits constatés

Un autre angle de vue consiste à ne plus voir la fraude sous l'angle des pertes réalisées mais sous celui des actes délictueux ou criminels identifiés. C'est l'angle de vision régulièrement adopté par la Justice et les forces de police.

Les statistiques de crimes et délits sont plus facilement rendus publiques par les différents gouvernements mais souffrent de limitations quant à leur précision et leur complétude.

De nombreux pays, dans un but de transparence, publient au moins annuellement les chiffres de la délinquance. C'est le cas en France où l'Observatoire National de la Délinquance et des Réponses Pénales (ONDRP), département de l'Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ), publie annuellement les faits constatés par les unités de police et gendarmerie [1].
La consultation des chiffres fournis par l'ONDRP [2] permet dans un premier temps d'identifier qu'un index (numéro 90) est dédié à la « falsification et [aux] usages de cartes de crédit ». Néanmoins, une part non négligeable des faits peut également être classée sous l'index (numéro 91) « escroqueries et abus de confiances » lors du dépôt de plainte (notamment lorsqu'il s'agit d'une fraude par hameçonnage ou par *cash trapping*).

Au cours de l'année 2013, 41951 faits relatifs à un usage frauduleux de cartes de crédits (index 90) ont ainsi été recensés. Par ailleurs, 183216 faits d'escroquerie (index 91) ont été portés à la connaissance de la Justice, sans pour autant en connaître le pourcentage lié à la fraude à la carte de paiement.

L'étude de l'évolution de ces faits sur les 17 dernières années (figure 5.4) permet d'en noter l'augmentation régulière et de confirmer une corrélation entre ces deux index.

Ces chiffres sont toutefois à nuancer par le chiffre gris de la délinquance (faits portés à la connaissance des institutions pénales mais non comptabilisés) qui est ici amplifié par des consignes locales émises depuis 2009, confirmées par une dépêche de 2011 provenant de la Direction des Affaires Criminelles et des Grâces (DACG) [14]. Cette dernière indique aux Procureurs Généraux près des Cours d'Appel que seules les banques, victimes, sont en mesure de porter plainte concernant les usages frauduleux de cartes bancaires et invite les

1. Carte de la criminalité disponible sur www.cartocrime.net.
2. Données brutes disponibles sur www.data.gouv.fr.

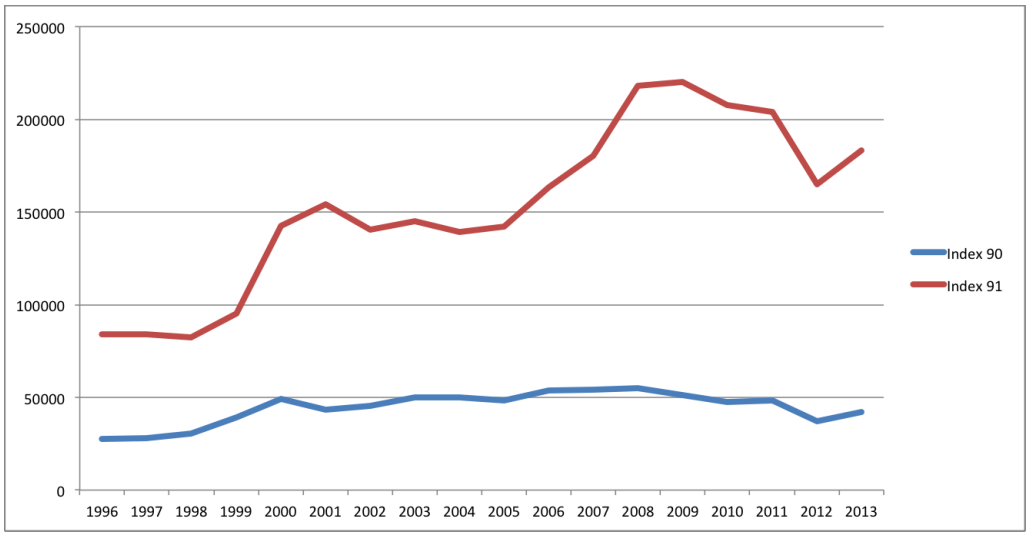


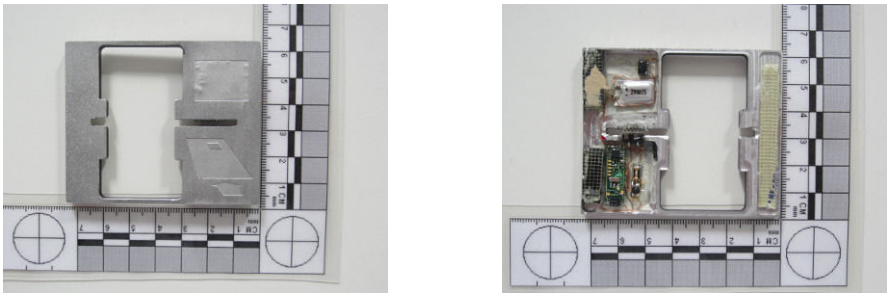
FIGURE 5.4 – Nombre de faits constatés pour les index 90 et 91 - *données cartocrime.net*

services de police et de gendarmerie à fournir une notice d'information aux porteurs qui souhaiteraient porter plainte.
Ainsi, jusqu'en 2009, les courbes des faits constatés présents sur la figure 5.4 sont en adéquation avec la courbe du volume des fraudes enregistré par les émetteurs sur la figure 5.3a, notamment avec les pics de fraudes enregistrés entre 1999 et 2002 suite aux paiements à distance possibles sans code de vérification visuel et aux fraudes à la « YesCard ». A partir de 2009, aucune adéquation ne peut être identifiées entre pertes enregistrées par les émetteurs et faits constatés.

5.2 Évolution prévisible

A court terme, et en l'absence d'avancée technologique pro ou anti-fraude majeure, les fraudes en ligne devraient continuer à croitre dans des proportions identiques à ces dernières années. La forte augmentation des paiement en ligne est en effet compensée par une adoption toujours plus importante des systèmes à authentification renforcée.
Concernant les fraudes physiques, même si aucune donnée statistique ne vient encore étayer cette hypothèse, il semble y avoir, au niveau européen, une cristallisation de la fraude autour de certains pays. En effet, l'adoption par quelques pays européens (Belgique, Pays-Bas, Suisse, Allemagne, etc.) de solutions visant à restreindre les paiements par pistes magnétique d'une carte dans son pays ou zone d'émission (solutions connues sur le nom de « *geoblocking* »), semble être la source d'un déplacement et d'une concentration des fraudes sur des pays n'ayant pas recours à ces solutions. Ainsi sur le territoire Français, les faits de fraude par mouchard semblent évoluer dans des proportions inhabituelles depuis le début de l'année 2014.

Toujours concernant les fraudes physiques, on observe également un mouvement global visant à délaisser les automates distributeurs de billets au profit de systèmes moins protégés contre ces attaques, tels que les automates distributeurs de carburant (figure 5.5) ou de paiement de stationnement, ou en ayant directement recours au vol de la carte par détournement de l'attention du porteur.



(a) Recto) (b) Verso

FIGURE 5.5 – Mouchard présent sur distributeur de carburant

A long terme, si la généralisation de la puce se confirme et que la piste magnétique vient à être retirée ou à avoir une portée limitée (par exemple via « *geoblocking* »), il devrait y avoir une forte évolution de la fraude physique.
Cette évolution est difficile à prédire puisqu'elle peut se concrétiser pour les fraudeurs par un abandon de la fraude physique (par exemple au profit de la fraude en ligne) ou une adaptation à la technologie puce. Dans ce dernier cas, l'adaptation peut se concrétiser par une modification de la technique de collecte utilisée (mise en œuvre d'attaques par relais, exploitation de failles à venir dans EMV, etc.) ou même en se tournant vers des modes opératoires technologiquement moins avancés, en ne visant plus le vol des données de paiement mais directement de la carte elle-même (« collet marseillais » - ou *Card Trapping* -, vol par ruse, etc.).

6 Les moyens de lutte actuels

De nombreux acteurs se mobilisent pour lutter contre toutes les formes que peut revêtir la fraude à la carte de paiement. Ces acteurs peuvent être étatiques, collaboratifs ou individuels.

6.1 Étatiques

En France, l'un des premiers acteurs institutionnels s'attachant à lutter contre cette fraude est la Banque de France qui a mis en place, depuis 2001, l'Observatoire de Sécurité des Cartes de Paiement (OSCP). Les attributions de cet observatoire, définies par l'article L. 141-4 du Code monétaire et financier, sont :

- le suivi des mesures de sécurisation entreprises par les émetteurs et les commerçants,
- l'établissement de statistiques de la fraude,
- une veille technologique en matière de cartes de paiement, avec pour objet de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement.

Plusieurs ministères sont membres de cet observatoire dont ceux de l'Économie et des Finances, de la Justice, de l'Intérieur et de la Défense. Parmi ceux-ci, peu sont ceux disposant de services dédiés à la lutte contre ces fraudes.

Ainsi, s'il n'existe pas de juridiction spécialisée au sein du ministère de la Justice, la création début septembre 2014 d'une section de lutte contre la cybercriminalité au sein de la nouvelle division économique, financière et commerciale du Parquet de Paris pourrait en être un signe préalable. La fraude monétique rentre intégralement dans les prérogatives de cette nouvelle section puisque le Procureur de Paris, François Molins, motive sa création par « l'explosion de la cybercriminalité : faux ordres de virement, escroquerie sur les sites de e-commerce, usage frauduleux de cartes bancaires ou encore atteinte aux systèmes de traitement automatisés des données » [61].

D'autres ministères disposent de services d'enquête spécialisés traitant de ce types de fraudes parmi lesquels le groupe « cartes » de l'Office Central de Lutte contre la Criminalité

liée aux Technologies de l'Information et de la Communication (OCLCTIC), la Brigade des Fraudes aux Moyens de Paiement (BFMP) ou encore le Département de lutte contre la délinquance Économique, Financière et Stupéfiant (DEFS) et la Division de Lutte Contre la Cybercriminalité (DLCC) du Service Technique de Recherches Judiciaires et de Documentation (STRJD).
Ces services d'enquête sont épaulés pour l'analyse technique des matériels saisis par des laboratoires criminalistiques disposant de capacités d'analyse en électronique tels que le département INformatique-éLectronique (INL) de l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN) ou le Service Central de l'Informatique et des Traces Technologiques (SCITT).

6.2 Collaboratifs

Des moyens de lutte collaboratifs sont également mis en place afin de lutter contre la fraude monétique au niveau international.

Ils sont d'abord mis en place par les États. Ainsi, pour l'ensemble des services d'enquête nationaux étant amené à travailler au niveau international sur ce type de fraude, le point de convergence « *Focal Point Terminal* » du Centre de lutte contre la Cybercriminalité d'Europol (EC3) constitue un point d'échange et de coordination pour les états membres d'Europol.

Les systèmes de paiement proposent également à leur membres ou clients des outils d'analyse de risque et de détection de fraude.
Ainsi Cartes Bancaires, Visa ou Mastercard proposent aux émetteurs l'évaluation (« scoring ») de chacune des demandes d'autorisation de paiement qu'ils relaient. Ces évaluations sont basées sur la réputation de sites marchands, la probabilité de présence géographique dans un laps de temps donné ou encore des analyses statistiques du porteur...
De la même manière, ils proposent aux banques partenaires des services de détection de point de compromission. Basés sur l'analyse de l'ensemble des flux qu'ils voient transiter et les cas de fraude déclarés, leur outils de détection s'attachent à identifier la source possible d'une capture de données (DAB ou plateforme de paiement en ligne compromis).

Enfin, des associations à but non lucratif s'attachent enfin à améliorer certaines parties du système monétique.
C'est par exemple le cas de l'association « SignalSpam » qui s'applique à limiter les courriels non sollicités et à identifier leurs auteurs. Ses actions permettent ainsi d'identifier et limiter les campagnes de courriels d'hameçonnage visant les établissements bancaires ou la récolte de numéro de cartes de paiement.

Au niveau européen, l'association EAST s'appuie sur ses membres provenant d'institutions bancaires, des fournisseurs de solutions matérielles ou d'organisations étatiques pour étudier et lutter contre les fraudes présentes sur les automates bancaires.

6.3 Individuels

Des acteurs individuels contribuent également à la lutte contre la fraude monétique.

Les banques émettrices ne pouvant pas entièrement déléguer leur gestion des risques aux systèmes de paiement, elles disposent de services de lutte contre la fraude. Ceux-ci sont chargés de détecter les attaques, d'en limiter la portée et de résoudre les éventuels incidents. La plupart des services de fraudes bancaires sont dissociés en deux entités : l'une luttant contre la fraude aux moyens de paiement et la seconde contre les attaques visant les systèmes d'information.
Les services émetteurs luttant contre la fraude aux moyens de paiement effectuent des opérations de détection et d'évaluation semblables à celles effectuées par les systèmes de paiement mais avec une vision limitée à leurs seuls porteurs. En plus de ces éléments de détection, ils doivent gérer les vérifications de fraudes potentielles, les mises en opposition, les demandes de renouvellements de carte anticipées associées et les demandes de transfert de responsabilités.
Les services des établissements émetteurs veillant à l'intégrité de leurs systèmes d'information sont en charge de sécuriser leurs serveurs monétiques, leurs services en ligne mais également de veiller à l'intégrité des postes de leurs clients. Ils suivent donc les campagnes d'hameçonnage et de logiciels malveillants afin de pouvoir répondre au plus tôt et limiter au mieux les incidents de sécurité. Bien que centrés sur leurs intérêts sécuritaires, ces services ne sont pas forcément isolés et certains n'hésitent pas à échanger avec leurs pairs comme par exemple certains établissements bancaires (Société Générale, Crédit Agricole, etc.) qui ont créé leur propre centre d'alerte et de réponse à incidents (CERT) afin de protéger leurs systèmes d'information de manière participative.

Enfin certains particuliers, par leur expertise et leur liberté d'expression, permettent également de faciliter la diffusion de l'information. L'un des experts le plus influant dans ce domaine est Brian Krebs, auteur du blog « krebsonsecurity.com », qui met au jour, en assurant la confidentialité de ses sources, de nombreux incidents de sécurité et techniques de fraude monétique.

Deuxième partie

Améliorer la lutte contre la fraude

7 Connaître la source de la fraude

La prévention d'une fraude nécessite souvent de mieux la connaître, d'en identifier les menaces et de mener des actions visant à en tarir les sources. La compréhension de la fraude monétique peut paraître complète et la fraude assez claire à la lecture des nombreux rapports l'analysant annuellement [51, 28, 22]. Néanmoins son analyse est incomplète et une partie nécessaire à sa prévention reste à être effectuée : l'analyse des sources d'acquisition.

7.1 Des chiffres basés sur la réutilisation

L'ensemble des rapports utilisés dans ce mémoire analyse la fraude à la monétique à partir de données relatives aux fraudes déclarées par les porteurs ou détectées par les établissements bancaires et les systèmes de paiement. Il ne s'applique ainsi qu'à la répartir en fonction de l'opération frauduleuse, en dissociant paiement et retrait, en précisant s'il s'agit d'un paiement de proximité ou un paiement en ligne, en détaillant si la carte était présente ou ne l'était pas, etc.

Ces différents rapports n'analysent que le produit de la fraude, c'est-à dire la réutilisation des données capturées. Ils invitent toutefois le lecteur, plus ou moins subtilement, à associer certaines réutilisations à certains modes de captures. Les paiements effectués alors que la carte n'est pas présente (paiements sur Internet, par téléphone, etc.) devraient ainsi être associés à la réutilisation de données capturées en ligne (hameçonnage, attaque d'un serveur de paiement, etc.). Or, à partir des données utilisées par ces organismes pour effectuer leurs études, rien ne permet vraiment d'en détecter les origines. Ainsi dans l'exemple précédent, les données pourraient également avoir été capturées par des mouchards, prélevés par des terminaux compromis, obtenues par essais successifs (force brute), etc.

Seul Europol, dans son rapport 2014 sur la criminalité organisée sur Internet [25], n'est pas aussi réducteur et présente les différentes formes de monétisation qui peuvent être faites des cartes ou données volées (figure 7.1). Ce rapport n'exclut pas par exemple que des données collectées par mouchards soient utilisées pour des paiements à distance.

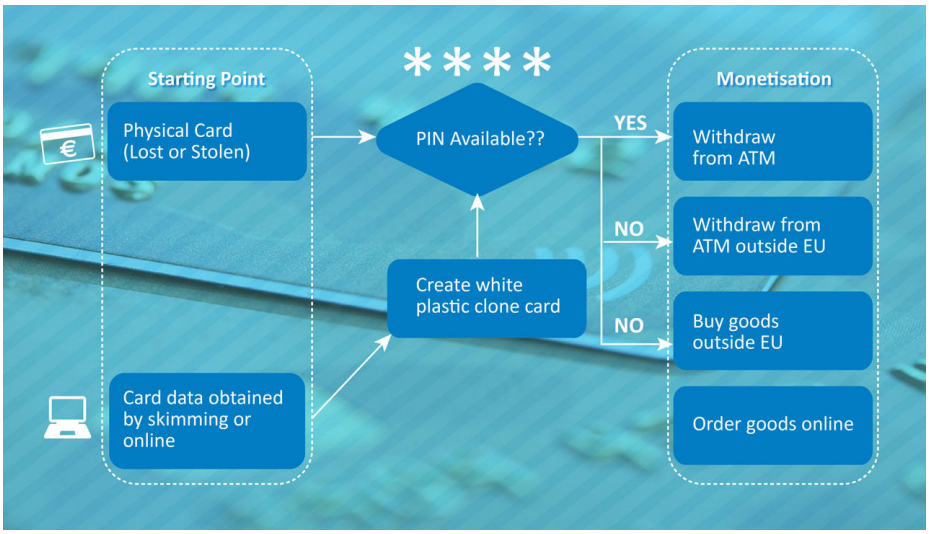


FIGURE 7.1 – Différentes options de monétisation des cartes ou données de cartes volées - *source : Europol [25]*

7.2 Des chiffres basés sur l'acquisition

Actuellement, il n'existe aucune source pouvant fournir des chiffres sur la répartition de la capture des données bancaires. Or c'est cette capture qu'il est nécessaire de combattre afin de prévenir la fraude préjudiciable.

Une expertise pourrait ainsi être développée afin d'étudier et de fournir des statistiques sur les sources d'acquisition des données utilisées pour commettre des paiements frauduleux. L'intérêt de produire de telles statistiques réside essentiellement dans l'établissement de stratégies de prévention de la fraude. En effet, tant pour les forces de l'ordre que pour l'industrie, c'est un outil de décision permettant de savoir où allouer les ressources nécessaires à la prévention de la fraude. Par exemple, si une telle étude venait à identifier que 60% de la fraude de la vente à distance provenait de logiciels malveillants bancaires, cela justifierait des actions visant à sécuriser les postes de leurs clients par les organismes bancaires et pourrait motiver la création ou le renfort de services d'enquête adaptés.

De telles données statistiques sont toutefois difficiles à produire. En effet, pour être exhaustif, il serait nécessaire de déterminer la source de compromission de chaque opération frauduleuse. Pour ceci, il pourrait être nécessaire de contacter les porteurs afin d'identifier la source précise de la capture de données dès lors qu'aucun point de compromission (physique ou en ligne) n'a pu être identifié. Cette démarche fastidieuse et intrusive reste le seul moyen de clairement identifier une capture des données par hameçonnage, logiciel malveillant ou mouchard mobile. Malgré la complexité de la démarche, cette étude statistique reste tout de même envisageable.

Sous l'impulsion de la présente réflexion, des travaux sont actuellement conduits par les groupes « veille technologique » et « statistique » de l'OSCP.

8 Améliorer l'expertise judiciaire

L'expertise judiciaire dans le domaine de la monétique peut être considérée comme marginale et peu lucrative, comparée à d'autres domaines comme celui de l'ADN. Elle intéresse donc que peu les laboratoires privés et semble méconnue du monde universitaire qui s'attache surtout à identifier les menaces et à améliorer la sécurité des systèmes monétiques.

L'amélioration des techniques employées par les experts judiciaires ne passe donc pas par une activité de recherche propre mais impose plutôt une captation du progrès scientifique.

8.1 L'expertise judiciaire des fraudes monétiques

8.1.1 Cadre légal

L'expertise judiciaire pénale, prévue par les articles 156 à 169-1 du Code de Procédure Pénale (CPP), est ordonnée par toute juridiction d'instruction ou de jugement (art. 156 du CPP).

Ces expertises sont strictement encadrées. Ainsi : « la mission des experts [...] ne peut avoir pour objet que l'examen de questions d'ordre technique » (art. 158 du CPP) et « les experts sont choisis parmi les personnes physiques ou morales qui figurent sur la liste nationale dressée par la Cour de cassation ou sur une des listes dressées par les cours d'appel » même si « à titre exceptionnel, les juridictions peuvent, par décision motivée, choisir des experts ne figurant sur aucune de ces listes » (art. 157 du CPP) .

Ces dernières dispositions sont également valables lors des enquêtes de crimes et délits flagrants ou d'enquêtes préliminaires puisque, respectivement, les articles 60 et 77-1 du CPP prévoient que « s'il y a lieu de procéder à des constatations ou à des examens techniques ou scientifiques », il est possible au procureur de la République, voire à l'officier de police judiciaire, d'avoir « recours à toutes personnes qualifiées ».

8.1.2 Méthodologie

Aucune méthodologie n'est présente dans la littérature quant à l'analyse technique de la fraude monétique. Il reste néanmoins possible d'appliquer les concepts liés à l'expertise judiciaire des équipements numériques.

Ainsi une analyse simple peut consister à suivre le cheminement suivant :

- prélèvement des indices ;
- identification des éléments en présence ;
- extraction des données ;
- interprétation des données ;
- réalisation d'un rapport.

8.1.2.1 Prélèvement

Avant toute analyse d'indices présents sur un système source ou victime d'une fraude, il convient de les identifier et de les prélever de leur environnement d'exécution.
Ainsi pour une fraude par mouchard sur distributeur de billet, il convient de retirer à la fois les équipements liés à la capture du code confidentiel et des données bancaires. Pour les fraudes en ligne, le prélèvement peut s'avérer plus complexe puisque les données liées à la commission de l'infraction ne sont pas, géographiquement, directement disponibles. De même, les opérations de prélèvement d'indices sur un système sécurisé suspecté d'être compromis, tel un distributeur de billet ou un terminal de paiement, doivent être réalisées de manière à ne pas entrainer leur disparition.

Les opérations de prélèvement sont le plus souvent réalisées par les victimes, les premiers intervenants ou les enquêteurs, rarement par des personnels formés aux technologies numériques. L'absence de prélèvement ou un acte mal réalisé pouvant être de nature à empêcher toute analyse ultérieure, il convient donc de sensibiliser ces potentiels acteurs sur les éléments importants et à les former à des actions simples.
Visa Europe a initié un tel travail de sensibilisation à travers l'Europe sur la problématique de la fraude par mouchard en distribuant des livrets de sensibilisation (figure 8.1) destinés aux unités élémentaires.

A l'issue de son prélèvement, un indice doit pouvoir garantir son intégrité par son conditionnement (scellé judiciaire) mais également, lorsque cela est possible, par son contenu (empreinte numérique pour les données copiées, etc.).

8.1.2.2 Identification des éléments en présence

L'étape suivante consiste à analyser les éléments collectés afin d'identifier les moyens mis en œuvre pour réaliser la fraude, objet de l'enquête.

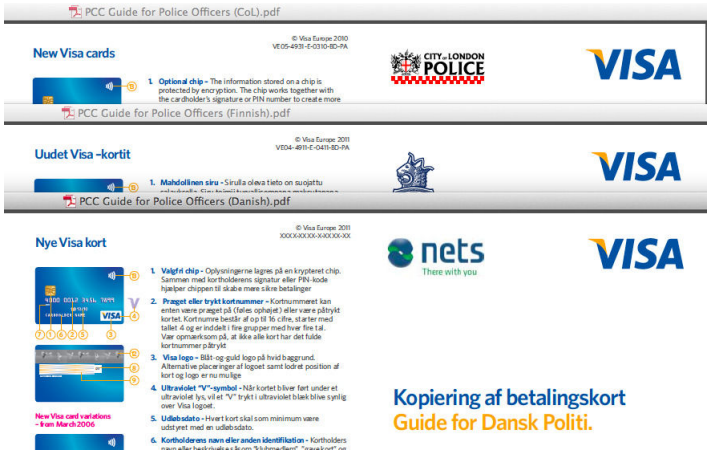


FIGURE 8.1 – Exemples (en danois, finlandais et anglais) de livrets de sensibilisation distribués par Visa Europe

La notion d'expertise prend alors tout son sens puisque l'expert désigné doit être en mesure d'identifier la nature de l'objet prélevé.
En effet, si l'on considère la fraude monétique dans son ensemble, les éléments prélevés peuvent être hétéroclites, de la capture d'un flux réseaux provenant d'un système d'acquisition au système électronique sans fil présent sur un automate de paiement.

8.1.2.3 Extraction de données

L'extraction des données est une opération préalable à leur interprétation afin d'accéder aux données éventuellement présentes dans les supports étudiés et d'en garantir l'intégrité.

Dans le plus simple des cas (supports de données standards : disques durs, cartes mémoire, etc.), cette opération consiste à brancher le support sur une machine de copie au moyen d'un dispositif empêchant la modification intempestive des données, d'en réaliser une copie intégrale et d'en garantir l'intégrité en calculant l'empreinte numérique des données lues.

Néanmoins cette opération devient plus complexe quand il s'agit de systèmes électroniques. L'extraction des données enregistrées et stockées par un mouchard bancaire, par exemple, peut se faire par plusieurs moyens.
La méthode la plus simple consiste à dessouder et lire le contenu du composant mémoire du mouchard. La difficulté réside uniquement à identifier le composant mémoire et à acquérir un lecteur compatible.
Une méthode plus complexe à développer, mais plus aisée à mettre en œuvre, consiste à utiliser le port de communication éventuellement présent sur le mouchard pour communiquer avec le composant mémoire pour en obtenir son contenu. Une analyse poussée

du système est néanmoins nécessaire puisqu'il faut à la fois identifier le type de port de communication (USB, 3 connecteurs, etc.) et le protocole de communication utilisé.

8.1.2.4 Interprétation des données

Une fois les données extraites, il convient de les interpréter. En matière de fraude monétique, les données recherchées sont le plus souvent des numéros de cartes de paiement provenant de pistes magnétiques capturées, de bases de données dérobées ou encore de flux de transactions capturés. Il peut également s'agir de mettre en évidence des défaillances dans la conception de systèmes (par exemple pour les fraudes par rétro-ingénierie du terminal exposées en 4.3.2).

Si l'on se réfère de nouveau à l'analyse d'un mouchard bancaire, l'interprétation des données vise à mettre en évidence les données de piste collectées. Le travail afférent consiste donc à rechercher des données bancaires encodées (comme présenté en 2.3), à les décoder puis à les vérifier.
Néanmoins si les données extraites s'avèrent codées avec des formats non standards ou chiffrées, il peut être nécessaire de désassembler le système afin d'identifier l'algorithme et/ou la clé de chiffrement.

8.1.2.5 Réalisation d'un rapport

Lorsque les opérations d'expertise sont terminées, un rapport doit être rédigé pour être remis au requérant.
Le contenu d'un rapport d'expertise n'est pas défini puisque l'article 166 du CPP prévoit uniquement que « les experts rédigent un rapport qui doit contenir la description desdites opérations ainsi que leurs conclusions ».

Les opérations d'expertise se voulant reproductibles, les descriptions des opérations doivent être suffisamment tracées et détaillées pour permettre la confirmation des résultats exposés lors d'une seconde expertise.

8.2 Exploiter le progrès scientifique

L'évolution des techniques de fraude n'implique pas systématiquement une adoption de technologies avancées. Néanmoins, les fraudeurs n'hésitent pas à employer si nécessaires les derniers standards et équipements dans la conception de leur dispositifs.
Dès lors, l'expert peut rapidement être dépassé s'il n'est pas en mesure de s'approprier les dernières avancées scientifiques permettant éventuellement de contourner les dispositifs

mis en place par les fraudeurs.

Afin d'illustrer concrètement ce concept de nécessaire captation de progrès scientifique, une partie de nos travaux se focalise sur l'expertise d'un mouchard, fréquemment installé sur des terminaux de retrait depuis début 2011, chiffrant les données collectées en s'appuyant sur un standard de chiffrement reconnu, *Advanced Encryption Standard* (AES).
A cause de ce chiffrement, ce mouchard a longtemps été considéré comme impossible à analyser par de nombreux experts européens.

8.2.1 Présentation de la fraude par mouchard chiffrant

Il existe de nombreux mouchards chiffrants (figure 8.2). Le mouchard étudié, modèle MSRv007 initialement vendu 2500 $ l'unité par la société CardReaderFactory.com [1], peut être considéré au travers du concept général des mouchards proposé en 4.2.1.3.

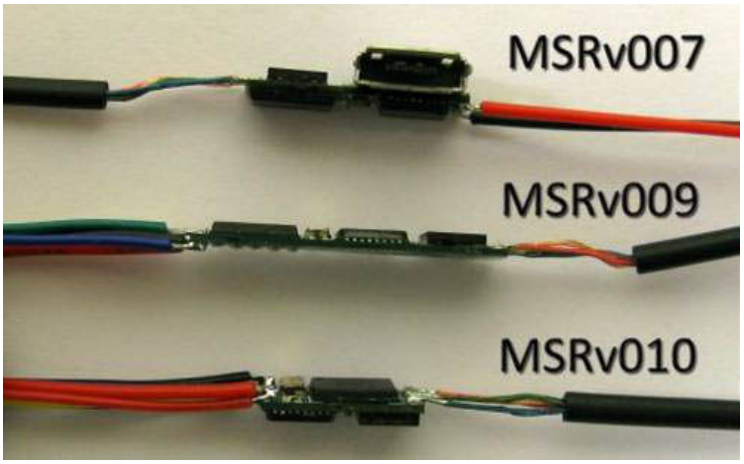


FIGURE 8.2 – Exemple de mouchards chiffrants commercialisés par CardReaderFactory - *source : CardReaderFactory.com*

Il s'agit ainsi d'un mouchard à piste magnétique, s'appuyant sur un pré-décodage du signal acquis par un composant F2F (MAGTEK), un traitement par microcontrolleur ATMEL (ATMEGA640P) et un stockage sur un composant mémoire ATMEL (AT45DB081D). La récupération des données par son utilisateur se fait via un connecteur 4 broches (USB).

La particularité de ce mouchard, outre sa taille très réduite qui peut lui permettre de ne pas être détecté par certains dispositifs anti-skimming, réside dans le chiffrement qui est opéré sur les données collectées par le micro-contrôleur avant de les stocker dans le composant mémoire. Il est alors indispensable de connaître la clé de chiffrement pour déchiffrer les

1. http://www.cardreaderfactory.com/shop/msrv007.html

données extraites du *skimmer*. Sans celle-ci, une personne retrouvée avec un tel dispositif ne pourra donc pas être inquiétée concernant la nature des données qu'il possède.

Le chiffrement qu'utilise ce *skimmer* est le standard américain AES dont la robustesse à de nombreuses attaques est internationalement reconnue. La clé de 128 bits utilisée protège par ailleurs les données de toute attaque par force brute.
Grâce à ses propriétés, ce mouchard résiste aux techniques classiques d'analyse utilisées par les experts judiciaires (recherche de présence d'encodage, de pseudo-chiffrement, identification du principe d'acquisition utilisé, etc.).

8.2.2 Le concept de captation de progrès scientifique appliqué à la fraude par mouchard chiffrant

A ce jour, seules deux solutions permettent à l'expert judiciaire de déchiffrer les données présentes dans ce type de *skimmer* s'il ne dispose pas initialement de la clé. L'une est mise en œuvre par la police judiciaire allemande – *Das Bundeskriminalamt* (BKA) – et la seconde a été développée dans le cadre de ces travaux ; toutes deux s'appuient sur des travaux de recherche datant d'une quinzaine années.

La première technique, mise en œuvre par le laboratoire de police scientifique du BKA, consiste à modifier physiquement le câblage interne d'un micro-contrôleur afin de changer l'état de « fusibles », rendant ainsi possible la lecture du programme présent dans ce micro-contrôleur [30]. La clé de chiffrement étant stockée dans ce programme, il devient alors possible de déchiffrer les données présentes dans la mémoire du mouchard.
Cette attaque physique, notamment développée dans le cadre de projets de recherche autour de la sécurité de la carte à puce, nécessite des moyens importants : sonde ionique focalisée (ou *Focused Ion Beam* (FIB)), nano-sondes... Cette méthode d'extraction de la clé AES constitue déjà un bon exemple de captation réussie du progrès scientifique.

Cette technique étant fastidieuse à mettre en œuvre et ne pouvant qu'être mise en place par des laboratoires possédant des matériels dont le coût dépasse le million d'euros, nous avons décidé de mettre en œuvre une autre attaque, non invasive, basée sur des avancées scientifiques différentes, les attaques par canaux cachés.

8.2.2.1 Attaques par canaux cachés

Les attaques par canaux cachés consistent à observer un processus en cours de traitement afin d'identifier des éléments autres que les données d'entrées et de sorties, qui varient au cours des différents essais. Il convient ensuite de vérifier si la variation des données dépend de la clé utilisée. Si tel est le cas, il devient alors possible de déterminer la clé d'un système

inconnu en n'observant que son fonctionnement (et éventuellement les données manipulées).

Un exemple médiatisé d'attaque par canal caché réside dans la détermination de la combinaison d'un coffre fort à l'aide d'un stéthoscope : l'attaquant observe l'émission sonore de la serrure et sait qu'il atteint la bonne combinaison lorsque le son de celle-ci devient inhabituel.

Il existe de nombreux éléments pouvant être observés dans le cadre d'attaques par canaux cachés : temps, émissions électromagnétiques, émissions sonores, consommation de courant, etc.

8.2.2.2 Analyse différentielle de la consommation

Afin de déterminer la clé de chiffrement utilisée dans le mouchard étudié, nous avons employé une attaque par canal caché basée sur l'observation de la consommation de courant d'un système électronique. Cette attaque dite d'analyse différentielle de la consommation (ou *Differential Power Analysis* (DPA)) a été initialement développée en 1998 par Paul Kocher, Joshua Jaffe, et Benjamin Jun [39, 40].

Elle est basée sur le fait que la consommation instantanée d'un équipement cryptographique dépend des données manipulées et des opérations effectuées [45].
La DPA consiste à mesurer la consommation électrique du contrôleur réalisant les calculs cryptographiques lors de différentes opérations de chiffrement pour lesquelles seules les données en entrée sont connues et varient. Il est ensuite nécessaire de rechercher une forte corrélation entre les données hypothétiques en un point donné de l'algorithme étudié (ici la sortie de la box S d'AES) et les mesures effectuées. Pour ceci, les données hypothétiques sont calculées à partir des données en entrées (connues) et une partie hypothétique de la clé. Les mesures effectuées sont quant à elles modélisées en utilisant un modèle adéquate (poids de Hamming, distance de Hamming, etc.).

Bien que cette attaque soit connue et employée dans le monde universitaire et industriel depuis plus d'une décennie, aucune publication d'utilisation à des fins criminalistiques n'a été identifiée à ce jour.

8.2.2.3 Mise en œuvre

Une mise en œuvre de cette attaque à des fins criminalistiques a donc été réalisée sur le mouchard chiffrant MSRv007.

Ces travaux, ayant fait l'objet d'un article publié dans *Forensic Science International* et

disponible dans son intégralité en annexe A, ont été conduits en boite blanche [2]. En effet, un accès au code assembleur de ces mouchards permet d'identifier, sur les mesures effectuées, les zones où le chiffrement a lieu. Ceci permet, dans un premier temps, de confirmer les « fuites » (variations de consommation électrique) lorsqu'une opération de chiffrement a lieu (figure 8.3).

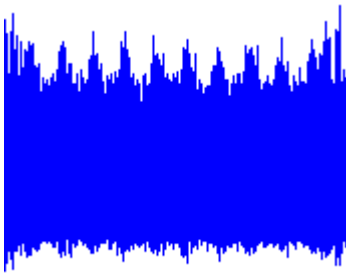
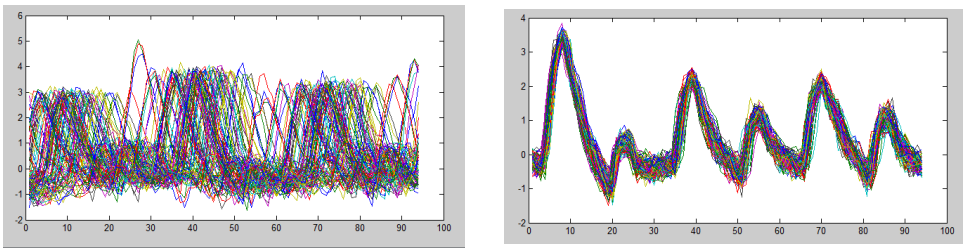


FIGURE 8.3 – Variation de la consommation électrique observée lors du chiffrement AES

L'identification de la zone d'attaque ayant été déterminée, les mesures sont alors possibles. La génération des données d'entrée est assurée par un système embarqué (Arduino) simulant le passage de cartes de paiement dans le mouchard.
L'absence d'oscillateur externe dans la conception du mouchard est toutefois la source d'un déphasage entre les différentes mesures. Il est alors nécessaire de réaligner les mesures effectuées (figure 8.4).



(a) (b)

FIGURE 8.4 – 100 mesures de consommation électrique avant alignement (a) et après alignement (b)

Dès lors, l'attaque par analyse différentielle peut être conduite en générant des tracés de corrélation pour chacune des 256 valeurs possibles de la partie de la clé attaquée (chaque attaque portant sur $\frac{1}{16}$ de la clé recherchée). La valeur résultante de l'attaque est celle possédant une corrélation maximale (désignée par la flêche rouge sur la figure 8.5).

2. En ayant connaissance du fonctionnement interne du système analysé.

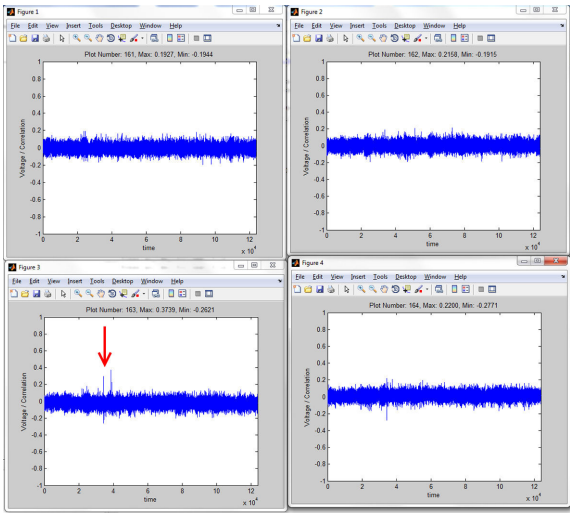


FIGURE 8.5 – Tracés de corrélation pour quatre valeurs possibles d'un octet de la clé AES recherchée

L'attaque doit ensuite être répétée quinze fois afin d'obtenir l'ensemble de la clé AES recherchée.

8.2.3 Résultats obtenus et extrapolation

Les résultats obtenus, détaillés en annexe A, ont d'abord permis de confirmer le potentiel des attaques par canaux cachés pour répondre à des besoins criminalistiques.

La solution développée répond ainsi aux exigences initiales puisqu'elle constitue une solution non invasive, à moindre coût (quelques milliers d'euros d'équipements) et rapide (environ deux heures pour une attaque complète) pour extraire les clés AES des mouchards chiffrants.

Enfin cet exemple illustre la manière dont la captation du progrès scientifique peut sensiblement améliorer l'expertise judiciaire.

9 Diffuser l'information et les outils d'analyse

La captation du progrès scientifique par l'expert judiciaire peut donc s'avérer indispensable s'il souhaite conduire à son terme les analyses de systèmes récents. Néanmoins une capitalisation des connaissances sur ces seuls experts peut générer d'autres problèmes dans le système judiciaire tels que la création d'une dépendance et d'un goulet d'étranglement lors de leur sollicitation par les magistrats ou les enquêteurs.

Afin d'éviter cette dépendance des enquêteurs vis-à-vis d'experts judiciaires dans le domaine du numérique, les services d'enquêtes de nombreux pays se sont rapidement dotés d'enquêteurs spécialisés, capables d'analyser différents objets numériques. Ainsi, en France, la gendarmerie nationale s'est appliquée à former, dès 2001, 260 enquêteurs en technologies numériques (NTechs). La police nationale dispose de 366 investigateurs en cybercriminalité (ICC) depuis 1999 et les services douaniers seulement de quelques fonctionnaires affectés à la Cyberdouane [32].

Pour ne pas être surchargé, d'être en mesure d'évoluer et de continuer à capter l'évolution du progrès scientifique, il devient également nécessaire pour l'expert de savoir transmettre ses acquis aux enquêteurs spécialisés. Dans le domaine de l'expertise de la fraude monétique cette transmission des compétences n'est que très peu présente, aussi bien en France qu'au niveau européen.

Afin de matérialiser cette possible décentralisation des savoirs et des outils en matière d'analyse monétique, nous proposons de réaliser un outil permettant aux enquêteurs spécialisés d'analyser simplement l'un des éléments les plus importants et communs du système monétique, la carte de paiement [1].

1. Ces travaux font l'objet d'un article publié dans *Digital Investigation*, disponible dans son intégralité en annexe B.

9.1 Présentation du projet *Forensic Payment Card Analyzer*

L'analyse d'une carte par un enquêteur peut s'avérer nécessaire assez régulièrement, que se soit pour lire les données d'une carte blanche, pour vérifier l'intégrité d'une carte de paiement que l'on suspecte d'être modifiée ou encore pour retrouver les historiques de paiement qu'elle pourrait contenir.

9.1.1 Mise en évidence d'une carte falsifiée

La technique utilisée jusqu'alors consiste à lire les données présentes sur la piste magnétique de la carte, d'en extraire les données de paiement et de les comparer avec les données embossées ou sérigraphiées sur la carte.
Conceptuellement, cela correspond à la lecture des données de paiement présente sur l'interface magnétique de la carte et à leur comparaison avec celles présentes sur l'interface visuelle. Si les numéros du porteur et dates d'expiration correspondent la carte peut être considérée comme cohérente, sinon comme contrefaite.

Bien que simple, cette analyse n'est pas réalisée par les enquêteurs spécialisés, faute de connaissance ou de lecteur de piste magnétique. Une version dégradée, mais pas du tout forensique, consiste à effectuer un micro-paiement en utilisant la piste magnétique chez un commerçant pour récupérer les données présentes sur son ticket commerçant.

9.1.2 Outil proposé

Afin de faciliter le transfert de ces compétences détenues par les experts du domaine, nous avons conçu un outil d'analyse de carte de paiement, basé sur la lecture de l'ensemble des interfaces disponibles de la carte. En effet, comme cela est expliqué au chapitre 2, la carte possède de nombreuses interfaces : visuelle, magnétique, à contact et sans contact. L'altération des données accessibles par l'une de ces interfaces doit conduire à déclarer la carte comme falsifiée. Ainsi une carte dont les pistes magnétiques ont été réencodées est déclarée modifiée, tout comme une carte ayant fait l'objet d'une manipulation de son interface « puce à contact » en vue d'une fraude par l'homme du milieu (cf. 4.2.2).

L'outil proposé se base donc sur une lecture des données de l'ensemble des quatre interfaces possibles d'une carte à l'aide de lecteurs adéquats. Si l'interface visuelle (données embossées ou sérigraphiées) peut être lue à l'oeil nu, les interfaces magnétiques et à contact/sans contact nécessitent l'emploi de lecteurs dédiés. L'objectif du projet étant de mettre en œuvre un outil à bas coût, nous avons sélectionné un lecteur de pistes magnétiques le moins cher possible (MSR90, environ 20 €) et conçu le logiciel autour de l'emploi du protocole de communication « PC/SC » pour la lecture des données puce (avec ou sans

contact). Ceci permet en effet aux unités disposant déjà de lecteurs appropriés (notamment pour la lecture des cartes SIM) de ne pas avoir à racheter un lecteur dédié. Enfin nous avons identifié un lecteur tout-en-un, compatible avec nos développements et à moins de 100 € (Poshmfg MX53-SC), permettant de lire les données présentes sur ces trois dernières interfaces.

Une fois les données de toutes les interfaces disponibles lues, l'outil présente à son utilisateur les données qui devraient être communes à ces interfaces, à savoir : le numéro de la carte, la date d'expiration et le nom du porteur[2]. L'utilisateur n'a alors plus qu'à vérifier la cohérence des données et à déclarer la carte comme originale ou falsifiée/contrefaite.
Des actions parallèles à la simple lecture des données du porteur sont également effectuées afin de détecter certaines manipulations de la carte (fraude de l'homme du milieu, etc.) et d'extraire des données pouvant intéresser l'enquêteur (journaux de paiement).

9.2 Réalisation et résultats

9.2.1 Développement

Le développement d'une version bureau de l'outil a été réalisé par deux étudiants (Fabrice Maqua[3] et Romain Hormière[4]) au sein de l'IRCGN en reprenant les spécifications préconisées ci-dessus.

L'outil *Forensic Payment Card Analyzer* (nom officiel de l'outil) est actuellement en version beta. Des tests sont en cours auprès de différents utilisateurs potentiels, français et européens, afin de vérifier que l'outil répond à leur besoin et dispose d'une interface conviviale. L'interface (figure 9.1) se veut très simple en proposant seulement trois zones :

- une zone de menu permettant la configuration du logiciels et des lecteurs ;
- une zone de gestion du dossier (en proposant un structure scellé - objet d'essai) ;
- une zone dédiée à l'analyse présentant l'ensemble des éléments extraits.

Une version plus complète, réservée à un utilisateur averti, est également proposée dans un mode « expert ».

L'objectif de l'outil est également de fournir un rapport immédiatement exploitable par les enquêteurs et à forte valeur ajoutée. Le rapport généré (extrait en figure 9.2) fourni pour chaque carte :

2. Le nom du porteur ne devrait plus être disponible sur l'interface sans contact suite aux préconisations des différents systèmes de paiement
3. Institut de Recherche de la Gendarmerie Nationale /Licence professionnelle Enquêteur Technologies Numériques de l'Université de Technologie de Troyes
4. 2ème année du cycle d'ingénieur de l'INSA de Lyon

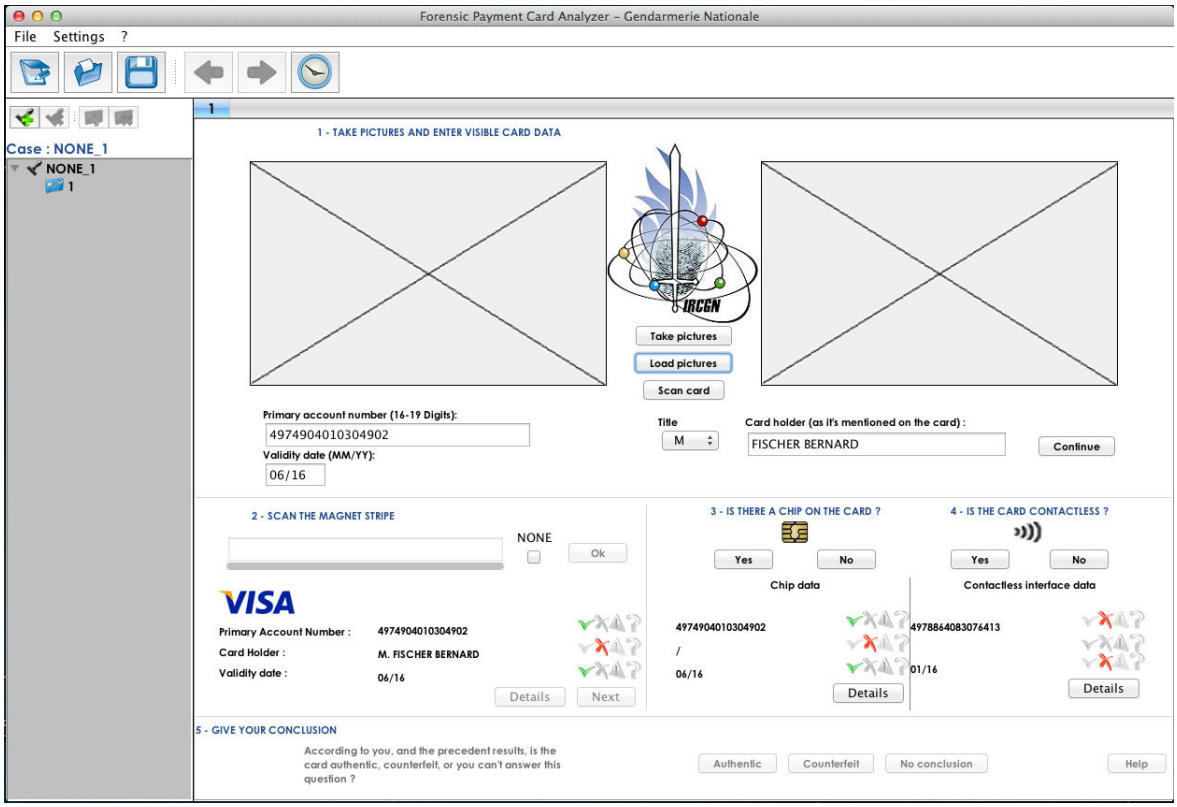


FIGURE 9.1 – Interface graphique de *Forensic Payment Card Analyzer*

- les données de la carte (nom du porteur, numéro de carte, date d'expiration) pour chacune des interfaces ;
- le journal, s'il est présent, de l'ensemble des transactions stockées dans la puce ;
- la conclusion de l'utilisateur quant à la nature (originale ou falsifiée) de la carte ;
- les coordonnées du(des) service(s) fraude de(s) l'émetteur(s) des numéros de carte identifiés.

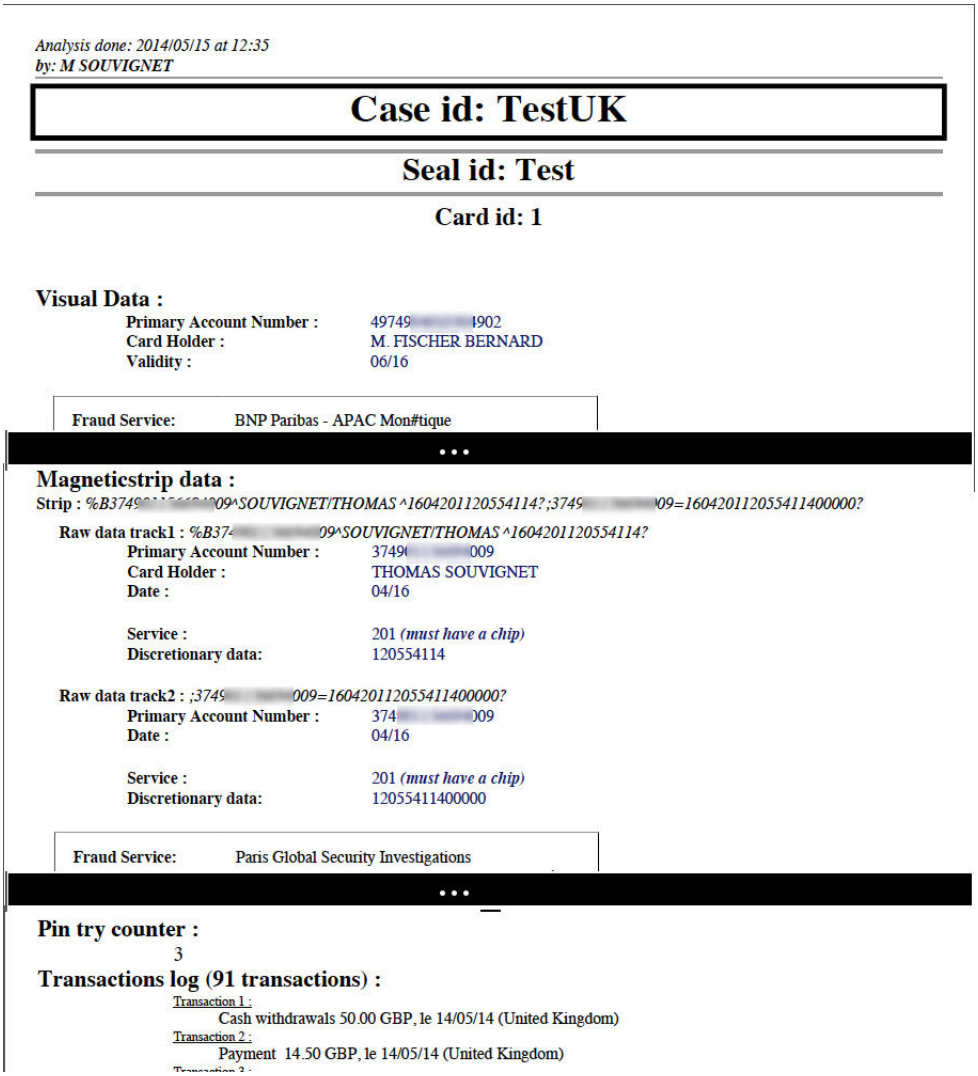


FIGURE 9.2 – Extraits d'un rapport généré par *Forensic Payment Card Analyzer*

Cette dernière fonctionnalité a pu être obtenue par la mise en place de partenariats avec les différents systèmes de paiement. Elle permet aux enquêteurs de ne pas perdre de temps avec des réquisitions inutiles pour obtenir l'identité de la banque émettrice à partir d'un numéro de carte.

Un prototype de version mobile (Android) a également été développé par trois étudiants (Julien Hatin, Damien Tesniere et Pierre Léger) de l'école nationale supérieure d'ingénieurs de Caen (ENSICAEN). Cette application reprend les mêmes fonctionnalités que la version bureau en utilisant toutefois des lecteurs magnétiques propres à cette plateforme (figure 9.3).

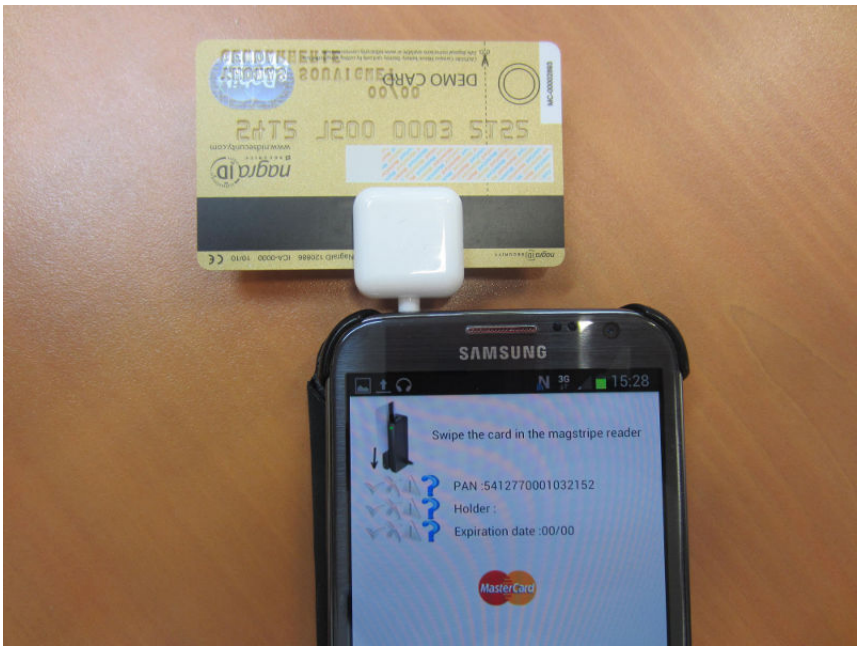


FIGURE 9.3 – Version mobile de *Forensic Payment Card Analyzer*

9.2.2 Distribution

La distribution de l'outil devrait être gratuite et en sources ouvertes. Ces deux conditions doivent permettre à l'outil d'obtenir une adoption massive par les enquêteurs spécialisés et une maintenance régulière du code.

Certains fonctionnalités (comme la détection possible d'une fraude en cours) peuvent toutefois nécessiter un hébergement du code source à accès limité. Des solutions sont actuellement recherchées auprès de l'EC3.

Enfin, une des vocations de cet outil étant d'être gratuit, le financement de lecteurs de pistes magnétiques compatibles par les services de lutte contre la fraude des principaux systèmes de paiement est actuellement acquis et la distribution aux enquêteurs NTechs en cours.

10 Dynamiser les méthodes d'enquête

Nous avons vu dans les chapitres précédents comment l'expert monétique peut améliorer ses réponses aux demandes d'analyses que lui soumettent enquêteurs et magistrats en captant le progrès scientifique et en transférant une partie de ses connaissance.
Néanmoins le soutien fourni par l'expert d'un domaine pourrait ne pas se limiter à la simple analyse d'objets prélevés mais arriver bien en amont de cet acte technique, c'est-à-dire au moment de la commission de l'infraction.

10.1 Méthodes réactives

Dans le domaine de la sécurité informatique, le concept de réactivité consiste à apprendre des attaques passées afin d'améliorer ses processus sécuritaires. Si ce principe est transposé au domaine de la fraude monétique, l'expert apparaît comme le meilleur atout pour connaître les détails des fraudes actuelles et ainsi améliorer les méthodes de lutte.

L'expert doit donc avoir un rôle actif, au plus près de l'infraction, en soutien aux enquêteurs. L'objectif est alors de répondre à un besoin des enquêteurs, exprimé ou non, en développant de nouveaux outils (stratégiques ou techniques) d'aide à l'enquête.
A la différence de l'outil d'analyse de cartes de paiement présenté précédemment, qui permet d'intervenir sur une infraction déjà commise, la réactivité présentée ici implique de développer des outils permettant de détecter la réalisation en direct d'un acte frauduleux.

10.2 Cas concret : fraude aux TPE modifiés

Afin d'illustrer ce concept, nous avons réalisé, dans le cadre de nos travaux de recherche[1], différents outils permettant aux enquêteurs de mieux appréhender une fraude récemment apparue sur des TPE.

1. Ces travaux ont l'objet d'un article publié dans *Digital Investigation*, disponible dans son intégralité en annexe C.

10.2.1 Présentation de la fraude actuelle aux TPE modifés

Cette fraude, récemment rendue publique par la presse écrite [57, 52, 44], est une fraude mixte consistant à installer un mouchard sur un terminal compromis. Le premier travail réalisé par le fraudeur consiste à compromettre le terminal en désactivant l'ensemble de ses sécurités à l'ouverture, à modifier la fente d'insertion du terminal puis à y installer un mouchard interrogeable à distance (figure 10.1).

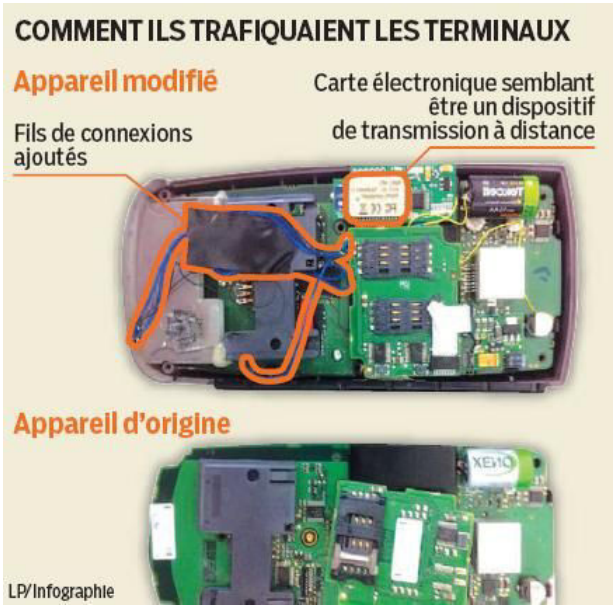


FIGURE 10.1 – TPE modifié - *source : Le Parisien*

L'énorme avantage de cette fraude par rapport à une fraude par mouchard classique réside sur le fait que le dispositif est visuellement indétectable, interrogeable à distance et auto-alimenté par le terminal. Le système peut ainsi être installé pendant des mois sans que son utilisateur n'ait besoin de le manipuler pour récupérer les donnés capturées.

Ceci n'est pas sans poser quelques problèmes aux enquêteurs devant faire face à une telle fraude. Plusieurs problématiques se posent : comment fonctionne cette fraude ? Où ces terminaux sont-ils installés ? Si un terminal compromis est découvert, comment en identifier son utilisateur ? Y'a-t-il un ou plusieurs utilisateurs ?

Si l'expertise classique d'un terminal modifié peut répondre à la première question relative aux détails de cette fraude, les pratiques habituelles des enquêteurs et experts ne peuvent pas répondre aux autres. La détection des terminaux de paiement compromis n'est pas aisément possible par le commerçant ou par un système de veille au niveau du système d'information monétique comme c'est le cas pour les mouchards installés sur les terminaux de retrait. De plus, même si un terminal compromis est identifié, il est impossible de mettre

en place une surveillance du dispositif afin d'identifier son utilisateur lors de la collecte des données. En effet, à la différence des mouchards installés sur DAB, où la collecte de données est quotidienne (principalement en raison de l'autonomie du dispositif), la collecte des mouchards TPE peut s'effectuer à tout moment et à distance !

10.2.2 Outils réactifs proposés

Afin de répondre à ces problématiques majeures dépassant le cadre classique de l'expertise judiciaire du terminal, nous avons développé et mis en œuvre deux outils à destination des enquêteurs. De manière réactive, en analysant un terminal saisi après commission de l'infraction, nous avons déterminé le fonctionnement du mouchard et réalisé des dispositifs permettant de détecter la commission d'une infraction.

10.2.2.1 Outil de détection d'un TPE modifié

Le premier dispositif réalisé est un outil destiné à répondre à la problématique « où les TPE compromis sont-ils installés », ce qui revient à déterminer les lieux où les infractions sont actuellement en cours de commission.

L'expertise du terminal a rapidement permis d'identifier un moyen mécanique de déterminer si un terminal est compromis ou non. Cette fraude nécessite en effet la modification de la fente d'insertion du terminal et son allongement afin de capturer l'ensemble de la piste magnétique des cartes de paiement. Il devient alors aisé de concevoir une carte étalon en marquant une carte quelconque (fidélité, etc.) sur un terminal valide et de vérifier ensuite sur les autres terminaux si elle ne s'enfonce pas davantage.
Néanmoins cette technique est difficilement exploitable par les enquêteurs qui doivent faire face à une multitude de terminaux à tester, un par un, et au caractère intrusif de cette détection, qui nécessite un accès physique au terminal (et donc un échange avec le commerçant).

Nous avons donc développé un outil permettant une détection de masse et sans caractère intrusif : l'application Android « 4n6 Bluetooth Scanner ».
Comme son nom l'indique, cet outil est basé sur la détection de l'émission Bluetooth du mouchard mis en place par le fraudeur dans le terminal. En raison de la qualité professionnelle du mouchard présenté sur la figure 10.1 (qui laisse présager une production en série) et en se basant sur l'analyse du module Bluetooth utilisé (RN41 de la société Roving Networks), il devient alors envisageable de déterminer une signature de l'émission radio de ces mouchards. L'application se contente donc d'afficher l'ensemble des émissions Bluetooth émises par les équipements avoisinants et filtre celles qui pourraient être en relation avec la fraude étudiée.
Le choix d'une application mobile (Android) a été guidé par le caractère national, voire international, que peut revêtir cette fraude. De plus, il était nécessaire de distribuer l'outil

le plus rapidement possible à un maximum d'enquêteurs sans limitation géographique. L'application a donc été déposée en toute discrétion début 2013 (présentée comme un banal outil de détection d'émissions Bluetooth) sur Google Play. Une limitation a depuis été mise en place pour restreindre l'accès à certaines fonctionnalités aux seuls enquêteurs identifiés.

L'application se veut très simple en ne présentant qu'une seule interface (figure 10.2) et en activant automatiquement l'équipement Bluetooth du périphérique mobile si celui-ci est éteint. L'unique bouton de l'interface permet de lancer et arrêter la détection. Les équipements détectés sont alors affichés et ceux répondant à la signature pré-déterminée (potentiels mouchards) sont mis en évidence par un fond rouge, une alerte sonore et sensorielle (vibreur).

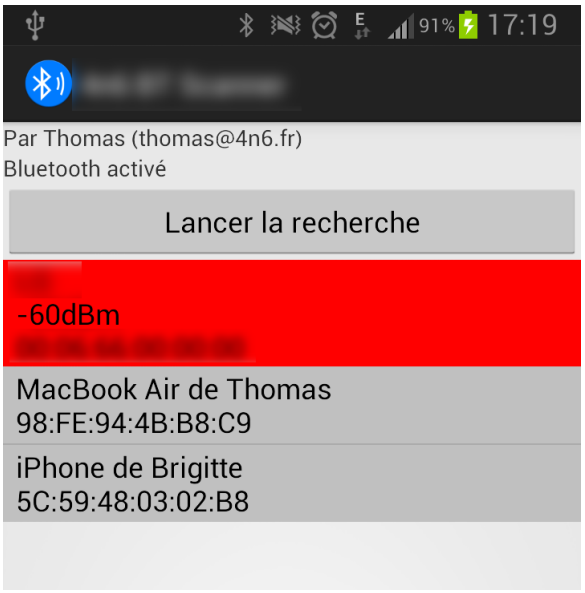


FIGURE 10.2 – Interface de l'application 4n6 Bluetooth Scanner

Un menu d'option est toutefois disponible afin d'activer une détection permanente (afin de pouvoir par exemple parcourir tout un centre commercial) et de régler les différentes alertes en cas de détection.

Cette application permet donc de mener de longues opérations de contrôle des émissions Bluetooth à portée, d'en filtrer celles pouvant avoir été générées par un mouchard et d'alerter l'utilisateur en cas de résultat positif. L'emploi de cette application par un enquêteur lui permet ainsi d'identifier, par un simple parcours de commerce en commerce, tous les terminaux de paiement modifiés d'une zone commerciale.

10.2.2.2 Dispositif d'assistance à l'identification de l'auteur

Une fois l'infraction matérialisée, il reste néanmoins nécessaire pour l'enquêteur d'en identifier son auteur. Cependant, l'utilisation de techniques traditionnelles impliquerait la mise en place d'une surveillance permanente sur une durée indéterminée, sans même connaître le profil (l'équipement) de la personne venant récolter les données collectées par le mouchard.

Toujours sur le principe de réactivité, les informations recueillies par l'expert judiciaire lors d'une précédente analyse peuvent lui permettre d'élaborer un outil d'aide à l'enquête visant à détecter la présence d'un utilisateur du mouchard.
Il serait donc possible d'intercepter les communications Bluetooth à destination du mouchard et d'alerter l'enquêteur en cas de communication active. Néanmoins cette solution pose plusieurs problèmes. Le premier est d'ordre légal puisque, suivant les interprétations qui peuvent être faites du CPP et du Code Pénal (CP), ces interceptions peuvent rentrer dans le cadre des articles 100 et suivants du CPP : « interceptions de correspondances émises par la voie des télécommunications ». Dans ce cas, et conformément à l'article R. 226-3 du CP, le matériel développé pourrait nécessiter l'agrément de la commission consultative mentionnée à l'article R. 226-2 du CP. Cette solution implique également le maintien sur place du mouchard, laissant ainsi courir la captation des données de paiement et leur potentielle réutilisation. Enfin, elle implique une très grande réactivité du système et des enquêteurs puisque la collecte ne dure que quelques secondes.
Aussi, la solution proposée dans le cadre de ces travaux de recherche s'appuie, non pas sur une interception des communications des données d'un mouchard, mais sur l'émulation de son fonctionnement.

Nous avons donc réalisé un dispositif électronique émulant le fonctionnant de la partie collecte des données du mouchard en associant un dongle Bluetooth USB à une plateforme de développement Arduino ADK. Cette association permet un contrôle bas niveau du module Bluetooth et ainsi d'en modifier les paramètres ou de détecter les tentatives de connexion. Dès lors il est possible de simuler le signalement électromagnétique du mouchard en émettant un signal Bluetooth avec la même adresse, la même classe, le même nom et le même code PIN (si connu). Afin d'aller plus loin dans l'émulation du mouchard, nous émulons également le menu interactif constaté sur un mouchard expertisé. Seule la transmission des données via le protocole dédié n'est pas émulée.
Nous disposons dès lors d'un dispositif dont la présence radioélectrique est semblable à celle des mouchards déposés par les fraudeurs. Afin d'alerter les enquêteurs de toute tentative de connexion d'un fraudeur, pensant se connecter sur son mouchard, nous ajoutons un module GSM permettant l'envoi de SMS.

Le dispositif ainsi obtenu (figure 10.3) émet donc un signal semblable à un mouchard de TPE qui envoie un SMS aux enquêteurs dès qu'une tentative d'appairage a lieu.

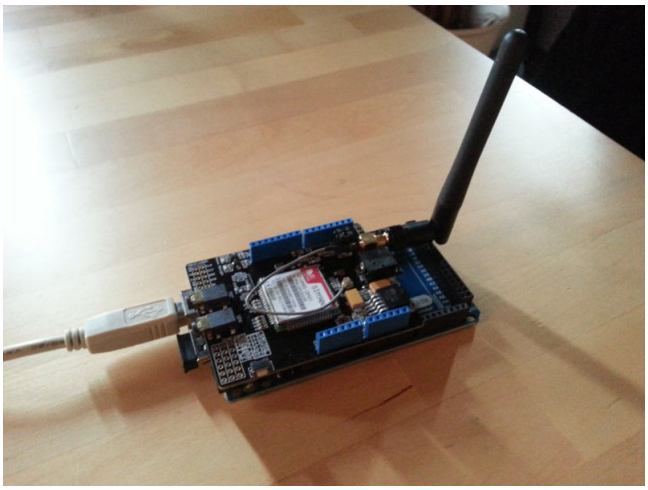


FIGURE 10.3 – Dispositif électronique de détection de présence d'un utilisateur de mouchards

Ce dispositif répond donc à une problématique majeure des enquêteurs puisqu'il participe à l'identification des auteurs. L'alerte émise lors d'une tentative de connexion permet ainsi au service d'enquête de visualiser les éventuels enregistrements de vidéo-protection à postériori ou, s'il est assez réactif, d'appréhender les suspects en flagrant délit.

Afin de permettre une identification toujours plus fine des suspects, nous fournissons sur le SMS envoyé aux enquêteurs les éléments techniques, présumés uniques, que sont le nom déclaré et l'adresse matérielle Bluetooth du téléphone ou de l'ordinateur utilisé pour la tentative de connexion (figure 10.4).

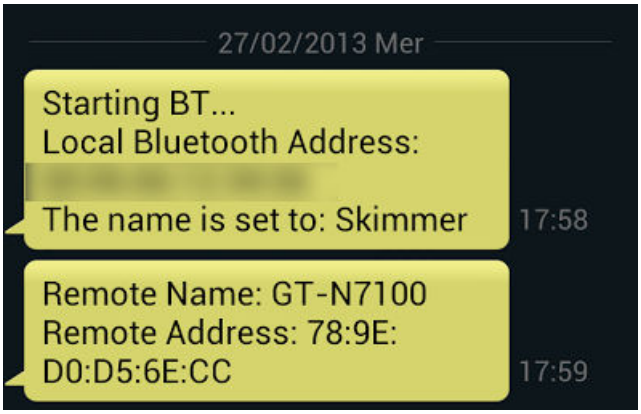


FIGURE 10.4 – Exemple de SMS envoyés par le dispositif proposé

10.2.3 Résultats obtenus

L'un des premiers résultats obtenus concerne l'adoption de l'outil de détection de TPE modifiés avec à ce jour plus de mille installations effectives (non supprimées) de l'application sur des terminaux Android. Les deux tiers sont installés en France et le tiers restant essentiellement en Allemagne, où une fraude identique est observée.
Plus que son utilisation, son efficacité est également avérée puisque que pas moins de sept terminaux modifiés, en trois lieux distincts, ont été découverts pendant la phase de conception et développement de l'application (avant même sa diffusion).

Le dispositif d'identification des auteurs a lui aussi fait la preuve de son efficacité puisqu'il a permis l'identification de nombreux utilisateurs ainsi que l'interpellation de trois individus [57].
L'alerte donnée par le dispositif couplée avec la réactivité des services de sécurité et de police a en effet permis d'identifier et interpeller les utilisateurs d'un mouchard de TPE en flagrant délit.

D'une manière globale les cas concrets de mise en application du concept d'expert réactif proposés ici ont reçu l'entière satisfaction [2] des services d'enquêtes ainsi que des organismes bancaires.

10.3 Développer des méthodes prédictives

Le rôle réactif de l'expert ne doit pas uniquement se limiter à l'assistance à détection de la fraude sur place mais peut également s'étendre à une prédiction des lieux de commission d'infraction ou l'assistance à identification d'auteurs d'infraction sur Internet.

10.3.1 Prévision des faits sériels

Une connaissance complète de la chaîne monétique, des solutions anti-fraude et des techniques de fraude pourrait permettre dès lors qu'une fraude est connue d'en prévoir les possibles faits sériels qui pourraient suivre. Il semble en effet que les fraudeurs ne se limitent pas à une action locale mais opèrent en série, avec une mobilité réduite à un court terme et un mode opératoire prévisible [17].

Une plateforme d'échange d'information, regroupant acteurs monétiques (émetteurs, acquéreurs, systèmes de paiement, fabriquants de matériel), forces de l'ordre et citoyens,

2. L'auteur a en effet reçu des témoignages de satisfaction écrits de la Préfecture de Police de Paris, du BKA ainsi que du GIE Cartes Bancaires

pourrait permettre la prévision des faits sériels relatifs aux attaques physiques (fraudes basées sur la carte, sur les terminaux, etc.).

En effet, la lutte contre les fraudes monétiques physiques souffre du manque de communication entre les acteurs. Ainsi une banque ne communiquera pas forcément aux forces de police une fraude par *card trapping* dont elle fera l'objet et les forces de l'ordre ne communiqueront pas forcément à l'ensemble des stations essence d'une zone donnée qu'une fraude a eu lieu chez un concurrent, etc.

La plateforme ici proposée se veut donc, à la manière de la plateforme « signal spam », une plateforme de recueil des alertes et d'analyse.

La signalisation pourrait émaner de n'importe quel acteur :

- un citoyen qui découvrirait un terminal compromis et qui créerait une alerte à partir d'une application mobile ou par appel d'un numéro dédié ;
- un établissement émetteur ou acquéreur qui constaterait visuellement ou par analyse des demandes d'autorisation qu'un terminal est compromis ;
- un équipementier qui aurait connaissance d'un terminal compromis par télémaintenance ou service de réparation ;
- un service de police informé d'un point de compromission.

Dès lors, le travail d'analyse de la plateforme consisterait à :

- automatiquement prévenir les acteurs concernés de la fraude constatée (accepteur et service de police locaux) ;
- rechercher les faits similaires (matériel identique dans un espace/temps donné) et proposer à un opérateur un cheminement possible des fraudeurs ;
- identifier les matériels ayant les mêmes caractéristiques dans la continuité du cheminement proposé afin de pré-alerter leur propriétaire et les services de police compétents d'une possible fraude à venir.

La réalisation de cette plateforme n'a pu être réalisée faute de temps et de coopération des différents acteurs. En effet, si l'ensemble des acteurs interrogés semble convaincu de l'intérêt d'une telle plateforme, tous sont réticents pour partager l'information détenue par chacun.

Ainsi, à partir d'un profil d'équipements visés provenant de fraudes relevées, il semble théoriquement réalisable de déterminer les cibles potentielles dans un périmètre établi. Ceci implique néanmoins une connaissance approfondie du parc des terminaux monétiques, tant au niveau matériel que géographique. Le partage de ces éléments fait l'objet d'une forte réticence des institutions bancaires pour lesquelles il s'agit de données concurrentielles sensibles.

10.3.2 Études des logiciels malveillants bancaires

De la même façon, l'étude approfondie des « logiciels malveillants bancaires » et des campagnes d'hameçonnage pourrait permettre d'identifier les nouvelles diffusions et de proposer des mesures réactives efficaces aux services d'enquêtes, souvent démunis.

Les travaux de recherche d'Eric Freyssinet vont en ce sens en proposant une classification de logiciels malveillants (www.botnets.fr) avec pour objectif d'établir un système automatisé de surveillance et une méthodologie d'enquête sur des faits liés à cette problématique [29].

11 Faciliter d'avance les futures expertises et enquêtes

La prévention de la fraude passe enfin par l'amélioration des standards existants mais également par la mise en place de nouveaux standards. Souvent absents des groupes en charge de l'élaboration de ces standards, dépassés par le niveau de technicité, les forces de l'ordre pourraient toutefois être intégrés à ces organisations, afin de mettre en place les mécanismes nécessaires à l'identification des fraudeurs.

11.1 Intégrer les besoins d'enquête dans les normes

Comme nous avons pu le voir dans les chapitres précédents, une importante partie des dispositifs de sécurité et des dispositifs de lutte contre la fraude repose sur différents standards. Ceux-ci sont en constante évolution, par leur mise à jour ou par le remplacement par de nouveaux standards.

Les créations et modifications de standards (et normes) sont toutefois le résultat d'une réflexion de groupes souvent fermés (au moins en terme de nombre). Ces groupes de travail sont presque exclusivement composés par des acteurs de l'industrie de la monétique et du monde bancaire, souvent réunis en consortium afin de promouvoir une technologie et entre experts pour sa mise à jour. Si le monde universitaire peut trouver une place dans ces groupes de standardisation, les forces de l'ordre n'y sont que rarement représentés. Ainsi aucune force de police n'est représentée dans les différents groupes de réflexion ayant conduit à la version 4.3 du standard EMV [1], ni même dans les groupes relais comme le groupe de travail technique du CIR [2].

Cette absence peut s'expliquer par la réticence de groupes de normalisation à intégrer des services d'enquête mais également par le manque d'intérêt et de connaissance de ces services vis-à-vis des différents standards monétiques. Il devient alors difficile pour les

1. http://www.emvco.com/about_emvco.aspx?id=55
2. http://www.cir-twg.org/index.html

services luttant contre la fraude monétique d'imposer ou même de faire transmettre des mécanismes pouvant prévenir une fraude ou aider les enquêteurs dans leurs enquêtes.
Un rôle proactif de l'expert judiciaire consisterait alors à faire l'interface entre besoins des services enquêteurs et réalité technique, tout comme il le fait dans le processus d'enquête, en intégrant certains groupes de standardisation en leur nom.

Des exemples concernant l'intégration de besoins d'enquêtes dans des normes internationales existent toutefois dans d'autres secteurs. L'*European Telecommunications Standards Institute* (ETSI) a ainsi pu pousser à l'intégration des besoins d'interceptions légales et de rétention de l'information lors de l'élaboration des standards des réseaux de téléphonie mobile de 3ème génération (3GPP) [24] [10]. De tels mécanismes d'assistance aux enquêteurs pourraient également être définis et intégrés dans les nouveaux terminaux de paiements ou les réseaux monétiques. Il est ainsi possible d'imaginer un mécanisme permettant la mise sous surveillance renforcée de certaines cartes qui nécessiteraient obligatoirement une vérification en ligne et/ou qui déclencherait une alerte auprès du service d'enquête requérant.

11.2 Favoriser l'adoption de ces fonctionnalités

La difficulté réside alors dans la nécessité de faire évoluer les usages et à faire adhérer ou imposer les requêtes des services judiciaires dans la conception et la mise à jour des standards.

Interrogé sur la faisabilité d'une intégration d'une force de police dans le processus de standardisation, l'un des acteurs de la standardisation EPAS (voir 1.3.2) nous a déclaré qu'elle pouvait être envisageable, notamment en raison de l'intérêt concurrentiel que l'implémentation obligatoire des exigences judiciaires pourrait constituer.

Néanmoins les fonctionnalités recherchées (traçabilité accrue, mise sous surveillance) pourraient venir d'exigences administratives plutôt que judiciaires.
De plus en plus d'États considèrent que les paiements électroniques sont un moyen de lutte contre l'évasion fiscale. C'est le cas de la Turquie qui impose désormais que les terminaux de paiement embarquent des fonctionnalités de « borne de paiement, de caisse enregistreuse et de mémoire fiscale » [3]. Ces fonctionnalités permettent aux services fiscaux turcs de lutter contre la fraude à la Taxe sur la Valeur Ajoutée (TVA) et contre le travail dissimulé.

3. http://www.capital.fr/bourse/actualites/ingenico-lance-un-nouveau-terminal-multifonctions-en-turquie-901408

Troisième partie

Discussion

12 L'aspect économique de l'expertise monétique

L'un des moyens de lutte contre la fraude monétique que nous proposons consiste à améliorer l'expertise monétique en réalisant notamment une captation sélective du progrès scientifique. Ceci s'avère indispensable quand il s'agit de contourner les mécanismes de protection employés par certains fraudeurs monétiques ou même ceux légitimes lorsqu'il s'agit d'analyser un terminal suspecté d'être compromis.

Ce travail d'appropriation de l'état de l'art est toutefois difficile puisqu'il nécessite à la fois une veille et une mise en œuvre des avancées universitaires et industrielles.

12.1 Difficultés rencontrées

12.1.1 Veille

La connaissance du progrès scientifique implique un suivi régulier des publications ainsi que de l'évolution des produits et techniques industriels.

La majeure partie des experts judiciaires en technologies numériques sont des personnes isolées. Il est alors difficile pour eux de réaliser cette veille, coûteuse en temps, alors qu'ils doivent déjà allier temps professionnel et temps de réalisation des expertises judiciaires.
Les solutions pour les personnes isolées peuvent alors consister à se regrouper dans des structures, aux formes juridiques variables, afin de partager le coût de cette veille. Ce regroupement peut se faire sous forme de sociétés civiles comme certains experts le font pour partager les frais administratifs et obtenir une meilleure visibilité. Ce travail collaboratif peut également être réalisé au sein de sociétés scientifiques ou d'association d'experts. Ainsi des associations telles que l'Association Francophone des Spécialistes de l'Investigation Numérique (AFSIN) ont pour champ d'action la prospective et la veille qu'elles partagent lors de réunions annuelles [2].

Les capacités de ces experts isolés restant limitées, même regroupées, il devient alors

indispensable pour les laboratoires publics d'assurer cette veille et de la transférer. Cependant cette captation du progrès scientifique reste difficile et coûteuse, même pour les laboratoires nationaux, moins sujets aux problématiques de rentabilité financière. Ils se regroupent donc également pour échanger sur le sujet, en participant à des conférences scientifiques ou à des réunions régulières de groupes constitués, tels que l'*European Network of Forensic Science Institutes* (ENFSI).

12.1.2 Mise en œuvre

Une fois qu'une évolution intéressante du progrès scientifique a été identifiée, il reste nécessaire de l'exploiter. Pour ceci, il faut concevoir et mettre en œuvre une méthode d'analyse basée sur cette évolution.

La conception et la mise en œuvre des dernières avancées techniques demeurent onéreuses en raison de l'investissement en personnel et matériel souvent requis. Ainsi les dernières attaques par injections de fautes ou canaux cachés nécessitent laser et FIB, équipements difficiles à maitriser et dont l'acquisition nécessite plusieurs centaines de milliers d'euros. Si de tels investissement sont inenvisageables pour des personnes isolées, ils le sont tout aussi difficilement pour des laboratoires étatiques en dehors d'importants programmes d'équipement. Une solution réside donc dans la coopération internationale et universitaire. Un premier projet majeur dans le domaine a été le projet *Cybercrime Centres of Excellence Network for Training Research and Education* (2CENTRE) [1] visant à développer les échanges européens en matière de recherche et de formation. Ce projet visait toutefois davantage l'échange en matière de formation et le développement de nouveaux outils que la recherche de mise en application du progrès scientifique en criminalistique numérique. De même le groupe de travail en criminalistique numérique de l'ENFSI n'est guère propice à ce genre de développements qui nécessitent des échanges réguliers.

Il reste donc à créer de tels groupes de laboratoires étatiques, disposant d'un minimum de ressources et intéressés par le partage afin de mutualiser leurs efforts pour atteindre un objectif commun. Des démarches sont actuellement menées pour créer un tel groupe et l'héberger au sein de l'entité R&D d'EC3.

12.2 Le *crowdsourcing* comme solution ?

Face au manque de ressources (humaines et financières) de la Justice, le *crowdsourcing*, « externalisation ouverte » ou « production participative », pourrait être une partie de la réponse.

1. http://www.2centre.eu

L'action judiciaire en matière de lutte contre la fraude monétique pourrait en effet s'appuyer davantage sur des productions participatives et, pour des cas précis, faire appel à des experts citoyens.

12.2.1 Les productions participatives

Comme nous l'avons vu en 6.2, des moyens de lutte collaboratifs existent déjà, l'association « signal spam » en est l'un des meilleurs exemples.

Néanmoins ce partenariat public/privé, datant de 2005, fait figure d'exception dans le paysage français de lutte contre la cybercriminalité. De plus, comme exposé en 10.3.1, une initiative similaire proposée dans le cadre de ce travail de recherche se heurte au protectionnisme des acteurs industriels.

Il semble manquer une entité porteuse de ces projets participatifs, qui serait garante de la qualité des projets et serait en mesure de faire contrepoids et interface entre les différentes parties prenantes (étatiques, industrielles, citoyennes, etc.).

Le Centre Expert contre la Cybercriminalité Français (CECyF) essaie actuellement d'être cette entité. Cette association, issue du centre d'excellence français du projet européen 2CENTRE, permet « aux services chargés de l'application de la loi, aux chercheurs de toutes origines (académiques, industriels, indépendants) et aux établissements d'enseignement de se rencontrer et d'échanger pour créer des projets qui contribuent à la formation, l'éducation et la recherche contre la cybercriminalité ».
Pour répondre à l'absence de certains outils criminalistiques, cette association dispose en son sein de la Communauté Francophone OpenSource pour l'Investigation Numérique (CoFrOSIN). Cette dernière a pour ambition d'« approcher les personnes souhaitant réaliser des développements de solutions logicielles ou matérielles en source ouverte au profit de l'investigation numérique avec ceux qui les utilisent au quotidien et expriment des besoins ». Une sollicitation a d'ailleurs été émise [2] à cette communauté concernant le développement de l'outil *Forensic Payment Card Analyzer* décrit au chapitre 9.1.

12.2.2 Experts citoyens en support à l'enquête

Un autre moyen de lutte contre la fraude monétique que nous proposons consiste à confier un rôle réactif à l'expert technique en l'associant au plus près de l'enquête. Les premiers résultats obtenus sont très encourageants puisqu'ils ont permis d'assister les enquêteurs et d'interpeller des fraudeurs.

2. Proposition restée sans réponse, sans doute en raison de la jeunesse et de l'absence de visibilité d'alors.

Néanmoins le passage à plus grande échelle peut s'avérer complexe, cette activité étant à priori peu lucrative. Seuls les experts des laboratoires nationaux semblent pouvoir s'attacher à un tel rôle. Afin de palier cette vision pessimiste, il pourrait être possible de développer la notion d'expert citoyen.

12.2.2.1 Le concept d'expert citoyen

Face aux évolutions toujours plus nombreuses et rapides des délinquants, une solution consisterait donc à maximiser les experts réactifs et à faire appel aux experts du domaine universitaire et de l'industrie afin d'assister les enquêteurs.

Il est toutefois difficile d'intégrer ces experts dans un processus d'enquête qui doit garantir une confidentialité vis-à-vis de l'extérieur. Par ailleurs, il peut paraitre difficile de pouvoir réunir rapidement et en un minium de démarches administratives et financières des experts d'un domaine particulier.

Le concept d'expert citoyen pourrait néanmoins répondre à cette problématique. Ce concept repose sur la volonté de nombreux citoyens à aider la police à résoudre les crimes et délits. En contrepartie, ils peuvent s'attendre à une gratification financière ou honorifique. Parmi ces citoyens, certains disposent de connaissances et d'expériences pouvant être mis à profit de l'enquête.
Le concept proposé peut être à rapprocher de celui des « chapeaux blancs » (*white hats*) dans le domaine de la sécurité informatique qui cherchent à améliorer la sécurité des systèmes en recherchant leurs vulnérabilités mais en ne publiant pas leur trouvailles avant qu'elles ne soient complètement corrigées et les correctifs déployés.

12.2.2.2 Formes possibles

Afin de pouvoir tirer le meilleur partie du civisme de ces experts, il est nécessaire de les fédérer sous une entité qui doit être attractive et réactive.

Une solution consisterait à la mise en place d'un centre d'expert citoyen. Ce centre regrouperait un ensemble d'experts monétiques (parmi d'autres spécialités) auxquels les problématiques d'enquêteurs seraient soumises afin de trouver des solutions. L'attractivité d'une telle structure résiderait dans l'aspect honorifique qui serait attribué à chaque participant en lui attribuant le statut de réserviste citoyen. Ce statut peut en effet être confié par les forces de police françaises de part la réserve citoyenne de la gendarmerie nationale (prévue par l'article L. 4241-2 du Code de la Défense) et la réserve civile de la police nationale (prévue par la Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure).

Ce concept de centre d'experts (réservistes) citoyens se heurte toutefois à la relative complexité d'accès aux réserves citoyennes et à la restriction, de fait, de celles-ci à des fonctions de prospective et d'encadrement. L'emploi des réservistes citoyens se fait par ailleurs de façon programmée, ce qui va à l'encontre même du principe de réactivité visé.

13 Les défis de demain

Au delà de la problématique de passage à l'échelle ou de concrétisation des solutions proposées, les défis de demain pourraient davantage concerner l'adaptation nécessaire des services anti-fraude à l'évolution de celle-ci mais également à l'évolution de la monétique elle-même.

13.1 Évolution de la monétique

Le secteur de la monétique a évolué de façon exponentielle ces dernières années, notamment avec des terminaux toujours plus connectés et intelligents mais également avec une évolution dans les usages.

L'un des principaux changements d'usage concerne l'évolution du système monétique présenté. En effet, cette présentation traditionnelle à cinq acteurs doit faire face, depuis quelques années, à l'apparition d'un sixième acteur : le porte monnaie virtuel. Ceux-ci avaient initialement pour vocation d'être des tiers de confiance. A l'heure où les plateformes des cybermarchands de paiement n'étaient pas suffisamment sécurisées, ces portes monnaie garantissaient des paiements simples et sécurisés où les détails de la carte n'étaient pas communiqués au commerçants.
Depuis, les plateformes de paiement des cybermarchands se sont sécurisées (notamment sous l'impulsion des standards détaillés en 1.3.3) mais forts de leurs utilisateurs fidélisés, ces portes monnaies ont évolués et se positionnent aujourd'hui comme des accessoires de paiement à part entière. Ils poussent leurs utilisateurs à se passer de la carte de paiement en prélevant (à moindre frais) les paiements directement sur leurs comptes bancaires. Ensuite, ils se positionnent comme émetteurs en distribuant leur propres cartes (souvent prépayés) et, depuis peu, proposent des paiements mobile avec téléphones dotés de la technologie NFC ou par codes barres à deux dimensions (codes QR).
Les nouveaux acteurs se bousculent derrière les portes monnaie historiques (comme Paypal créé en 2002) ou des systèmes de paiement classiques (V.me de Visa et MasterPass de Mastercard) [15]. Ainsi les géants de l'Internet comme Google, Amazon et Apple, forts des coordonnées bancaires de leur clients (magasins en ligne ou d'applications), tentent de s'imposer sur ce marché prometteur. Forts de leur positionnement sur le marché de

la téléphonie mobile, Google et, plus récemment, Apple ont même réussi une intégration complète de leur solution de paiement mobile NFC Google Wallet et Apple Pay, toutes deux conformes aux exigences de sécurités décrites en 3.3.1.

13.2 Évolution de la fraude

Comme évoqué précédemment, la répartition de la fraude monétique pourrait évoluer en fonction des avancées technologiques (ex. désactivation de la piste magnétique) ou en fonction de la profitabilité des différentes attaques (migration de la fraude de proximité vers la fraude en ligne).

Les émetteurs doivent d'ailleurs faire face à une réelle gestion du risque. Dans certains cas, endosser une fraude peut s'avérer plus profitable que d'essayer de la réduire à tous prix, le rapport coût sécuritaire/risque de fraude étant peu élevé. Bien que cette gestion de risque reste difficilement acceptable pour les services étatiques s'employant à démanteler les organismes criminels à l'origine de ces fraudes, elle demeure tout à fait compréhensible d'un point de vue financier et en terme d'image.

Ainsi, suite aux différentes solutions sécuritaires mises en œuvre pour sécuriser leurs agences, les établissements bancaires doivent faire face, depuis 2011, à de nombreuses attaques de distributeurs bancaires au gaz. Ces attaques ont des conséquences financières importantes suite aux dégâts générés par ces explosions (figure 13.1).

FIGURE 13.1 – Dégâts générés dans une agence bancaire suite attaque distributeur automatique de billet au gaz - *source : Europe 1 / Gendarmerie nationale*

Si une attaque au gaz peut être considérée comme préférable à un vol à main armée, les

impacts moraux étant bien moindres et les dégâts matériels réparables, il est raisonnable de craindre qu'une sécurisation complète du système monétique ait des effets similaires. Le porteur, détenteur de la carte et du code confidentiel, resterait en effet le maillon faible et ne pourrait résister à la violence d'un agression physique pour les obtenir.

13.3 Une adaptation des moyens de lutte nécessaire

Face à la mutation de l'écosystème monétique et l'évolution probable de la fraude, les moyens de lutte doivent évoluer.

Un renforcement des échanges entre les différents acteurs de cette lutte semble inévitable. Ces échanges pourraient en effet conduire à l'avènement de solutions mutualisées et prédictives telle que celle proposée dans cette étude.

Dans l'attente de l'avènement de cette coopération renforcée, des travaux de recherche actuellement menés au sein de l'École des Sciences Criminelles de l'Université de Lausanne permettent d'entrevoir la conception de moyens de lutte alternatifs basés sur le renseignement criminel. En effet, Mélanie Eudes [1] emploie des techniques d'analyse criminelle pour mieux comprendre les modes opératoires des cybercriminels et appréhender le phénomène du *carding* dans sa globalité. L'analyse qu'elle a réalisée [20] à partir d'artefacts provenant d'affranchissements postaux émanant de mules [2] permet en effet de clairement identifier, parmi le flot des livraisons, un membre clé du réseau.

1. Assistante-Doctorante à l'Institut de Police Scientifique de l'École des Sciences Criminelles, l'Université de Lausanne.
2. Intermédiaires d'opérations criminelles. Ici, recel de biens provenant d'achats réalisés à partir de cartes de paiement provenant d'un forum de *carding*.

Conclusion

La carte de paiement, présentée en introduction comme un « simple morceau de plastique âgé d'une cinquantaine d'année », est loin d'être aussi simpliste et ne constitue qu'une petite partie de son écosystème que représente la monétique.
Embarquant, à l'instar des autres éléments de la monétique, des technologies permettant des transactions sécurisées (certificats, aléas, chiffrement de données, etc.), la carte bancaire fait l'objet de nombreuses fraudes notamment en raison de sa rétro-compatibilité avec des systèmes à pistes magnétiques ou des possibilité de paiement à distance sans authentification.

L'étude des fraudes monétiques, qui dépassent celles uniquement liées à la carte, nous a permis de mettre en évidence leur ampleur, leur évolution mais surtout leur diversité. Il en ressort une multitude de fraudes différentes contre lesquelles luttent en premier lieu les acteurs de la monétiques.
Porteurs, émetteurs, accepteurs, acquéreurs et systèmes de paiement veillent ainsi, chacun à leur niveau, à protéger l'intégrité du système monétique. Néanmoins les derniers chiffres (1,33 milliard d'euros de paiement frauduleux pour l'année 2012) et les dernières publications (des millions de numéros de carte dérobés par des logiciels malveillants aux États-Unis d'Amérique) montrent les limites des dispositions sécuritaires monétiques.
La fraude réalisée, l'infraction étant commise, plusieurs nouveaux acteurs interviennent pour identifier les auteurs et mettre fin au vol ou à la réutilisation des données. La Justice, pour mener ses enquêtes, doit alors travailler de consort avec les institutions financières victimes ou témoins. Elle fait également appel aux services d'enquêtes, pas toujours spécialisés ou équipés, et dans certains cas aux experts judiciaires, trop rares et pas toujours compétents dans ce domaine spécialisé.

Pour améliorer la lutte contre la fraude, nous avons proposé différentes actions qu'elles soient passives, réactives ou proactives. Alors que certaines dispositions sont encore à l'état de proposition, d'autres ont été mises en œuvre avec succès.

Les actions qui n'ont pas été mises en pratique sont celles nécessitant la coopération d'un grand nombre d'acteurs. Ainsi l'amélioration statistique, ayant pour objectif de connaître la source des données de la fraude (et plus seulement son lieu de réutilisation) commence seulement à être débattue au sein de groupes de travail de l'OSCP. La proposition consistant à faciliter d'avance les futures expertises est quant-à-elle restée au stade de concept même si des signes de faisabilité et des travaux de recherche sont actuellement en cours.

Plus encourageant, l'amélioration de l'expertise judiciaire proposée a été illustrée, par captation du progrès scientifique, en réalisant un outil criminalistique de récupération

de clés de chiffrement AES, basé sur une attaque DPA. De même, la diffusion de l'information et des outils d'analyse a été concrétisée par la conception, le développement et la diffusion gratuite d'un outil d'analyse de carte de paiement. Enfin, des méthodes d'enquête monétique ont été dynamisées par la conception d'une application mobile et d'un système embarqué ayant permis la découverte de nombreux lieux d'infraction ainsi que l'identification et l'arrestation d'auteurs présumés.

Il ressort de ces travaux l'importance de l'expertise et l'impact que peuvent avoir des actions, principalement techniques, dans la lutte contre la fraude monétique. Il n'en reste pas moins que les acteurs de cette lutte devront faire face à l'importante mutation que connait actuellement le monde monétique et à la possible évolution de la fraude afférente. Des solutions à ces évolutions, notamment participatives, ont d'ailleurs été discutées et pourraient constituer une arme supplémentaire contre cette criminalité constituant une part importante de la cybercriminalité.

Table des figures

Index

Annexes

A Differential Power Analysis as a digital forensic tool

Forensic Science International 230 (2013) 127–136

Contents lists available at SciVerse ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

Differential Power Analysis as a digital forensic tool☆

T. Souvignet [a,b,*], J. Frinken [c]

[a] French Gendarmerie National Forensics Lab (IRCGN), Digital Forensics Department (INL), 1 boulevard Théophile Sueur, 93110 Rosny-Sous-Bois, France
[b] PRES Sorbonne Universités – Université Panthéon-Assas Paris II, 12 place de Panthéon, 75005 Paris Cedex 05, France
[c] Kriminaltechnisches Institut (KTI) des Bundeskriminalamtes (BKA), Äppelallee 45, 65173 Wiesbaden, Germany

ARTICLE INFO

Article history:
Available online 24 April 2013

Keywords:
Digital forensic tool
Skimmer
Advanced Encryption Standard (AES)
Power Analysis Attack (PAA)
Differential Power Analysis (DPA)
Side Channel Attack (SCA)

ABSTRACT

Electronic payment fraud is considered a serious international crime by Europol. An important part of this fraud comes from payment card data skimming. This type of fraud consists of an illegal acquisition of payment card details when a user is withdrawing cash at an automated teller machine (ATM) or paying at a point of sale (POS).

Modern skimming devices, also known as skimmers, use secure crypto-algorithms (*e.g.* Advanced Encryption Standard (AES)) to protect skimmed data stored within their memory. In order to provide digital evidence in criminal cases involving skimmers, law enforcement agencies (LEAs) must retrieve the plaintext skimmed data, generally without having knowledge of the secret key.

This article proposes an alternative to the current solution at the Bundeskriminalamt (BKA) to reveal the secret key. The proposed solution is non-invasive, based on Power Analysis Attack (PAA). This article first describes the structure and the behaviour of an AES skimmer, followed by the proposal of the full operational PAA process, from power measurements to attack computation. Finally, it presents results obtained in several cases, explaining the latest improvements and providing some ideas for further developments.

© 2013 Elsevier Ireland Ltd. All rights reserved.

1. Introduction

1.1. Payment fraud and skimming

Despite attempts by the banking industry to improve the integrity of payment card systems, recent 2009 Europol statistics indicate that "organised crime groups derived more than 1.5 billion euros from payment card fraud in the EU" [1].

In France alone, payment card fraud in 2011 reached 413.2 million euros [2]. The domestic component of this fraud is orchestrated, from greatest losses to least, via Internet payments, local and automated payments, mail and phone payments and cash withdrawals. Retail payment and withdrawal fraud play a much more important part when considering international transactions.

As seen in Fig. 1, fraud is perpetrated from [3] (sorted from light to dark blue):

- lost or stolen cards;
- intercepted cards during delivery;
- forged or modified cards;
- illegally acquired card numbers;
- other types of fraud such as false identity based opened account.

In its 2010 annual report [3], the French Observatory for Payment Cards Security underlines the increasing prevalence of illegally acquired card number fraud.

This illegal acquisition of card numbers is usually linked to skimming. Payment card skimming is the concept of copying payment card data during normal usage (payment, cash withdrawal, bank door identification, *etc.*). This illegally acquired data is then used to forge cards or process online payments.

Skimming operations are based on "skimmers" which collect card data and gather the Personal Identification Number (PIN) information.

The two main targets for skimmers are automated teller machines (ATMs) and point of sale (POS) terminals.

Despite the wide use of anti skimming techniques, the skimming phenomenon is still increasing (Fig. 2).

To combat this fraud, secured payment protocols have been developed. Currently, Eurocard–Mastercard–Visa (EMV) chip based payment protocol is well deployed throughout Europe (Fig. 3) and online secure solutions (like Verified by Visa, 3D secure, MasterCard SecureCode) are available.

However, to maintain international compatibility, EMV cards still have an operational magnetic stripe. This magnetic stripe is

☆ This paper is part of the special issue entitled: 6th European Academy of Forensic Science Conference (EAFS 2012), Guest-edited by Didier Meuwly.

* Corresponding author at: French Gendarmerie National Forensics Lab (IRCGN), Digital Forensics Department (INL), 1 boulevard Théophile Sueur, 93110 Rosny-Sous-Bois, France. Tel.: +33 158665843.
E-mail addresses: thomas.souvignet@gendarmerie.interieur.gouv.fr (T. Souvignet), juergen.frinken@bka.bund.de (J. Frinken).

0379-0738/$ – see front matter © 2013 Elsevier Ireland Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.forsciint.2013.03.040

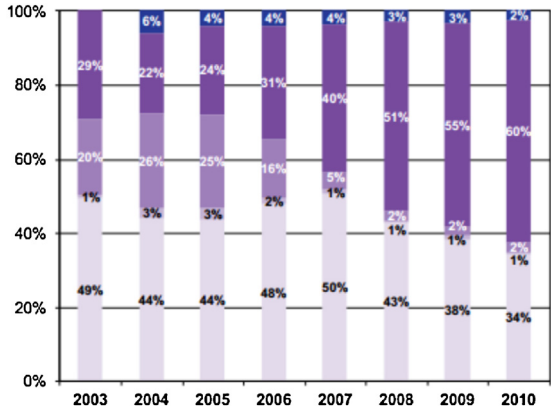


Fig. 1. Breakdown of domestic payment fraud by fraud type. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)
Source: French Observatory for Payment Cards Security.

freely readable and remains an easy way to illegally acquire card data.

Although several stakeholders (Eurosystem [4], Europol [1], European Payment Council (EPC) [5]) are attempting to promote magnetic stripe free EMV cards, skimming will continue to be a fraud phenomenon that law enforcement agencies (LEAs) will have to face due to the requirement by some non-European payment systems for magnetic stripe usage.

1.2. Skimmer analysis

Skimmer analysis is the technique of analysing a skimmer which has been seized at a public location such as an ATM, a hotel room or a retail store. As it is not obvious if the skimmer has already collected some data or if it is a functioning device, it is necessary for LEAs to analyse the skimmer to obtain possible evidence of the crime.

Understanding the way a skimmer works is necessary to be able to proceed with its analysis. Even if different skimmers function in a variety of ways, a general working structure can be drawn:

- card data acquisition;
- card data processing/conversion;
- card data storage;
- PIN acquisition;
- PIN storage;
- card data/PIN serial transfer (post acquisition).

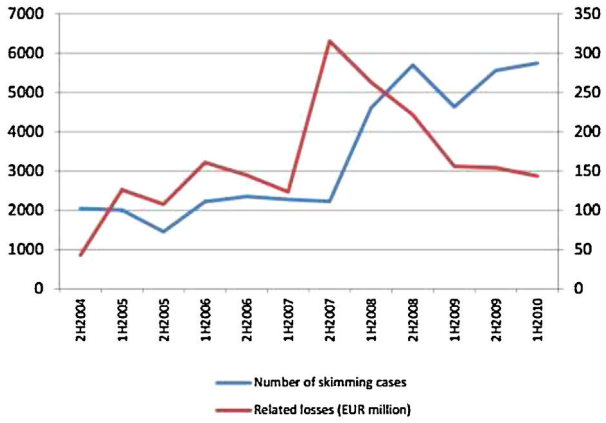


Fig. 2. Evolution of skimming cases and related loss.
Source: French Observatory for Payment Cards Security based on data from EAST.

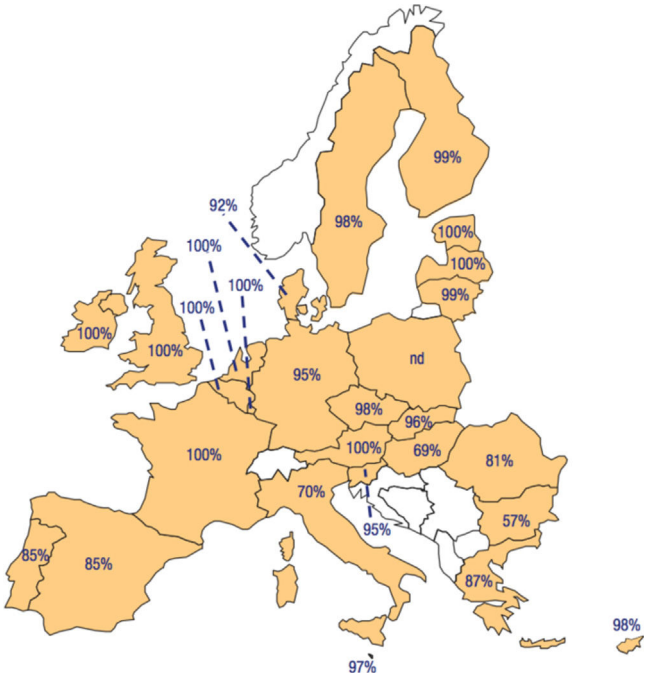


Fig. 3. EMV card deployment – march 2012.
Source: French Observatory for Payment Cards Security based on data from European Payments Council.

This processing structure is common to the hardware design of most skimmers, resulting in PIN acquisition and card data acquisition boards often being split (Fig. 4).

Moreover, the card data acquisition board can be functionally broken down as follows. The magnetic head and its preprocessing chip (*e.g.* magnetic stripe decoder chip – hereafter "Frequency – Double Frequency (F2F) decoder" – or amplifier) carry out the data acquisition. The skimmer microcontroller handles data processing and conversion. The memory chip (*e.g.* EEPROM or Flash memory) is dedicated to data storage.

The magnetic stripe stores the card holder and payment card details within 3 tracks. The first track, encoded using 7 bits per character, contains the card holder's details. Tracks 2 and 3, encoded using 5 bits per character, contain some payment card details.

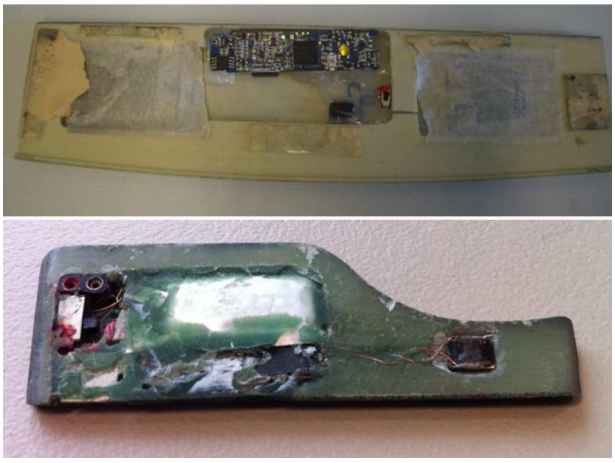


Fig. 4. At top, a PIN acquisition board (based on a mp4 recorder) and a card data acquisition board at bottom.

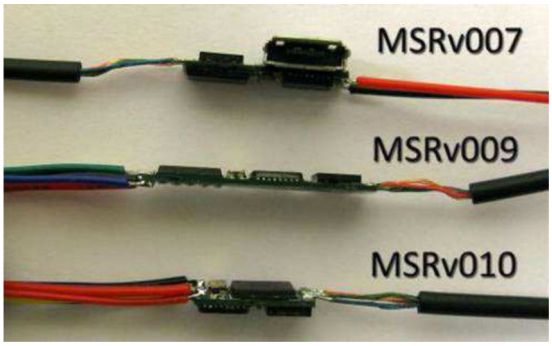


Fig. 5. MSR skimmers.

However only track 2, 37 bytes long and fully detailed by Padilla [6], is compulsory to forge a payment card. For efficiency, this track is often the only one recorded by skimmers.

To prevent stolen data from being processed by the local installer, who is generally different from the skimmer's owner, or by the police (as described by Master et al. [7]), tracks are often encoded or encrypted prior to being stored within the memory. Hiding techniques have evolved from simple shifting or XOR operation to advanced usage of cryptographic algorithms.

For example, Advanced Encryption Standard (AES), the standard symmetric cryptosystem chosen by US government in 2001 as FIPS 197 [8], is used by several Magnetic Swipe Reader (MSR) based skimmers to encrypt stolen data (Fig. 5).

Recorded tracks are then available via a communications serial interface and dedicated software. However, it is required to provide the AES key which was used to encrypt the stored data to access this protected information. This key is stored internally within the skimmer firmware programme.

For law enforcement investigations, the desired data on skimmers is the magnetic stripe data which has been stolen and stored within the device. Even more relevant data is that which permits the identification of victims in order to support the investigation.

AES skimmer cases were first encountered in early 2010. Due to the difficulty of handling such cases, requests to process them at the Bundeskriminalamt (BKA) have come from all over Germany and abroad (Switzerland, Canada, *etc.*).

The current analysis method consists of extracting the key from the microcontroller's assembly code. However, as the skimmer's microcontrollers are often protected against reading, it is necessary to use an invasive process to hack the chip in order to gain access to the skimmer code. This method [9] is expensive in terms of materials and equipments, as well as being very time consuming. After developing a basic method, each evidential skimmer must be processed individually over the course of a two or three day procedure.

1.3. Power Analysis Attack

Power Analysis Attacks (PAAs) were formally introduced in 1998 by Kocher et al. [10]. According to this research [11, Foreword], power analysis activities were developed to conduct affordable physical attacks by answering the question: "what information is available to attackers but is not assumed in the cryptographic protocols?".

In fact, even if a cryptographic algorithm is assumed to be secure, its physical implementation can suffer from some design problems. For example, information leakage could be produced by cryptographic implementations while executing the encryption process. PAA relies on such information leakage issues.

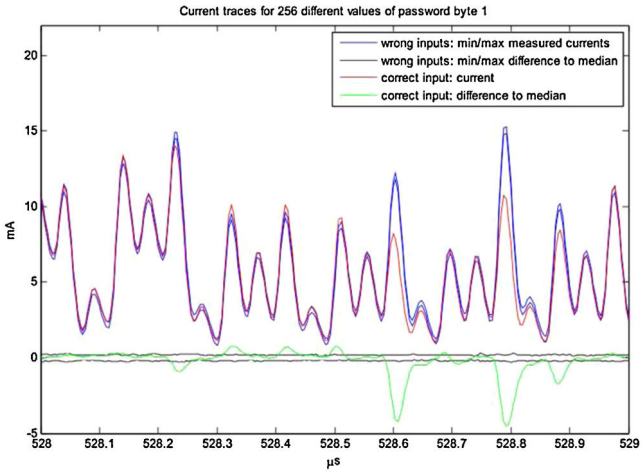


Fig. 6. SPA traces.
Source: BKA / [12].

Modern day microcontrollers are based on millions of basic electronic parts, called transistors. Field effect transistors are voltage-controlled gates. When voltage is applied to the gate, current flows across the doped substrate allowing charge to flow to additional circuitry [10]. Current consumption of transistors depends mainly on their switching activity. Also, when a full system is under operation, a general switching noise is produced on the power line depending on the current activity.

This switching noise is an information leakage that can be used by Simple Power Analysis and Differential Power Analysis to conduct an attack on cryptographic hardware implementations.

The Simple Power Analysis (SPA) consists of several individual trace analyses. The principle of SPA is to search for a characteristic pattern within the power trace to detect consecutive states of the examined microcontroller and thus determine the followed path within an algorithm.

Several SPA projects have already been conducted by or for the BKA. Skorobogatov et al. also demonstrated how SPA can be used to find the correct inputs to unlock a password protected programme running on Motorola MC68HC908AZ60A microcontroller [12].

In that work, inspection of individual power consumption traces permitted the identification of a different behaviour when the correct input (password character) was sent to the microcontroller (Fig. 6).

As SPA's main goal is to detect conditional jumps, SPA is unsuitable for AES analysis, because AES steps are not data dependent.

Differential Power Analysis (DPA) [13] consists in the statistical analysis of many traces. The principle of DPA is to compare hypothetical values (from the different possible key parts) against measured values, thus getting a correlation coefficient for each possible key part.

Mangard et al. [11] propose a general DPA process with 5 main steps:

1. Choose an intermediate result of the examined algorithm.
2. Measure the power consumption.
3. Compute hypothetical intermediate values.
4. Map hypothetical intermediate value to hypothetical power consumption value.
5. Compare the hypothetical power consumption value with real power traces and compute correlation traces (Fig. 7).

For DPA conducted on AES, the output of the SubBytes function in the first round is especially suitable for intermediate results. In

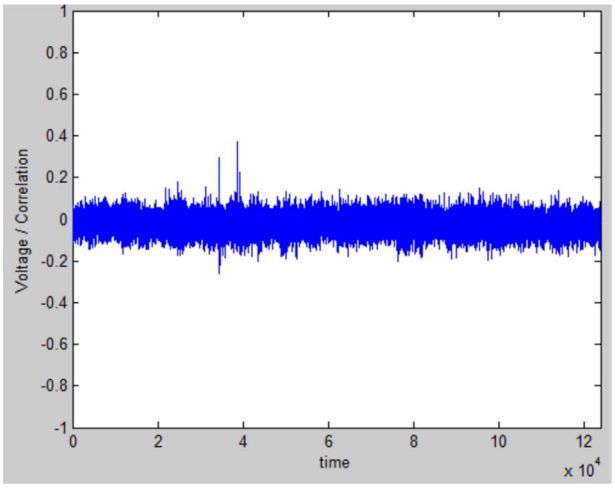


Fig. 7. Example of correlation trace (peaks imply high correlation between hypothetical and measured power consumption).

the same way, Mangard et al. [11] and some laboratory tests (data not shown) reveal that Hamming-Weight model is efficient enough to map hypothetical intermediate values to hypothetical power consumption values.

1.4. Differential Power Analysis as a forensic tool

The aim of our research was to design and run an alternative analysis method to handle AES skimmer cases based on non-invasive PAAs.

DPA was also be repurposed from its usual hacking and security analysis purposes to be used as a forensic tool to extract an encryption key.

2. Methods

Prior to processing a PAA on the AES skimmer microcontroller, a deep analysis of its structure and behaviour turned out to be necessary.

2.1. Skimmer black box analysis

Board design and communication observations (black box analysis) need to be conducted on a reference skimmer to get an overall idea of the skimmer mechanisms, prior to handling a case exhibit.

The design analysis relies on a visual examination of skimmer board lines and a connectivity check of the different pins.

Visual and connectivity examinations of the two layers were necessary to draw a connectivity schematic between the different pins (Fig. 8).

The external observation of the communications between the skimmer microcontroller and its environment permitted the development of a general idea of its behaviour. It was especially interesting when observing communications generated while the skimmer was recording swiped cards.

Thus, a logic analyser was connected to the data and the strobe lines of the "F2F decoder" and to the Serial Input (SI), Serial Output (SO) and Serial Clock (SCK) pins of the external serial flash memory.

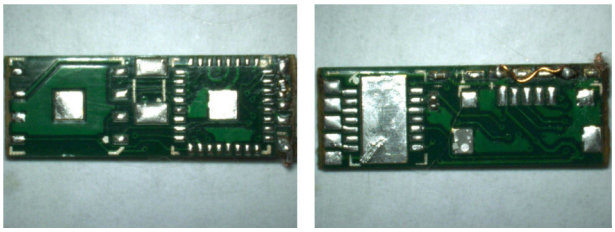


Fig. 8. Front and back of the skimmer board with all electronic components removed.

2.2. Skimmer white box analysis

Understanding the skimmer data encoding encryption could only be done by analysing its code (white box analysis).

To conduct this deep analysis, it was necessary to get access to the protected content of the skimmer. An invasive chip hacking method was performed on a reference chip to retrieve the bytecode of the microcontroller to analyse it later.

The method used to extract the content of the reference skimmer, called "lock bits attack", is an invasive method developed and used by the BKA for several years [9].

Once the bytecode is read, it was then possible to perform reverse-engineering to retrieve some source instructions. In the present research, the bytecode referred to AVR assembly instructions provided by the general AVR instructions list and the ATMega328P datasheet.

2.3. Power consumption measurements

To conduct a PAA, it was first necessary to get power measurements of the system under analysis during several comparable controlled operations.

The aim was to measure the power consumption of the skimmer microcontroller while encryption was performed for each card swiped. To conduct an attack, several different cards were provided during the measurement process.

As the environment needs to be fully under control, and for efficiency, data generation (result of card swiping) and data storage (result of encryption) were monitored during the power measurement process.

The data generation resulted, on the original skimmer, from the data acquisition process (see 1.2). To get a full control over the microcontroller's input, its behaviour was emulated using an external board.

Data generation was emulated using an Arduino Uno board. The choice of Arduino development board was made due to the fact that it was user friendly, of easy maintenance and very low cost. The so designed Arduino sketch (official name for Arduino program) was intended to emulate the data provided by the F2F Application-Specific Integrated Circuit (ASIC) to the microcontroller. It also had to react like the ASIC while a card was inserted and read, while the controller requested for read data.

In a similar way, the data storage was controlled using an Arduino ATmega2560 board (due to ease of availability). An Arduino Uno board could also have been used.

For efficiency and adaptability reasons, interaction with the on-board flash memory was preferred rather than emulating the memory behaviour. Hardware implementation consisted of connecting memory pins to those of the Arduino ATmega ones.

Initial software implementation consisted in implementing standard commands. Thus reset, read status and erase full memory functions could easily be implemented according to the codes provided within the relevant datasheet. These commands allowed the memory to be set to an initial state which was suitable for obtaining a comparable state for different measurements.

To proceed with power consumption measurements, the set up measurement protocol was based on measurement equipment, trigger and measurement set choices.

The measurement set up was made using previously developed boards and active measurement equipment. A digital oscilloscope with 1 GHz bandwidth and active probes were sufficient to handle the measurements (tests were conducted with an Tektronic TDS7404 and some P6245 – 1.5 GHz bandwidth – active probes).

The main probe measured the power consumption which was obtained from the voltage measured across a small resistor (*e.g.* 10 Ω) inserted in serial on the skimmer board. However, without differential probes, it was necessary to measure voltage from the ground. Thus a measurement point was added to the microcontroller's ground pin.

Other probes were necessary for trigger purposes and were located depending on trigger settings.

One of the most important parameters in measurement settings was the trigger point, especially in the DPA context where measurements had to be aligned. This point was a characteristic element, close to the interesting (encryption) area.

The encryption area was determined by modifying the reference skimmer's assembly code. The pin status of an unused pin was switched to a high level when the encryption subroutine was under progress. As shown in Fig. 9, minor changes were necessary.

A suitable trigger setting could then be set up to process measurements over this area on any (unmodified) exhibit.

As all necessary components were available, it was possible to process power consumption measurements. Measurements were then conducted by a Matlab script that controlled Arduino boards over serial (USB) communication ports and the oscilloscope over the Matlab Instrument Control Toolbox via Ethernet.

The acquisition script's algorithm was:

- erase the whole Flash memory
- reset and set oscilloscope parameters
- loop (until all measurements are done):
  - erase the Flash memory's first pages
  - send some card data to the data generation board that emulates a card swipe

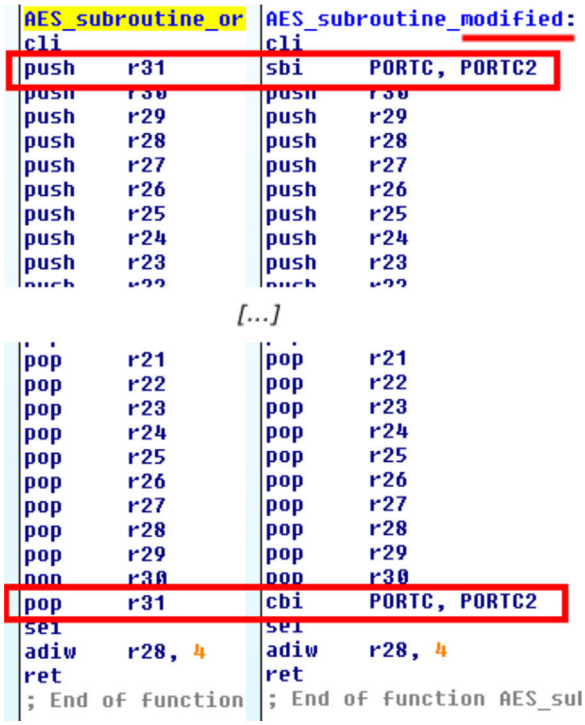


Fig. 9. AES encryption subroutine before/after modification.

- start microcontroller of the skimmer
- wait for emulated card swiped data to be computed by microcontroller of the skimmer
- stop microcontroller of the skimmer
- read and store oscilloscope measurement and encrypted data stored on the skimmer Flash memory

• end loop

2.4. Power Analysis Attack

Running a power analysis on the measurements required some pre-processing operations.

To prevent faulty records caused by noise generated by connection wires, as well as other sources, three different measurements were performed per input value in the extraction process. A cleaning matlab script removed entries whose outputs did not match any other from the same input data.

Perfectly aligned measurements had to be computed to perform a DPA. As the studied skimmer used an internal oscillator, measurements were not aligned enough to meet requirements. To solve this issue, a pre-processing Matlab script split the measurements on a clock cycle basis and aligned each of them, following this pseudo-algorithm:

- detect clock cycle rate
- go to trigger point (trigger point is after AES encryption)
- loop (backward cycle iteration)
  - set right boundary to current position
  - set left boundary to previous clock cycle limit (=current position − detected cycle rate)
  - detect max of the current cycle
  - copy current cycle to the aligned cycles matrix
  - go to the detected max position – 5 points (in order to be positioned at the end of the previous waveform – value may vary depending on waveform characteristics, sampling rate, *etc.*)
- end loop

The first step of DPA is the hypothetical values matrix generation. The predictive matrix contained values that should be retrieved depending on the AES key byte.

As it was a result of a non-linear substitution and only the result of the key and plaintext same byte computation, SBox output was said, by Mangard et al., to be an excellent choice for matrix generation [11].

To compute these hypothetical values, the following Matlab code was used within a PAA script.

```
1  key=[0:255];
2  after_sbox=zeros(mesurements_to_analyse,256);
3  for i=1:mesurements_to_analyse
4    after_sbox(i,:)= SubBytes(bitxor(input_final(i,byte_to_
       analyse),key)+1);
5  end
```

This part of the code generated an "after_sbox" matrix which contained all hypothetical intermediate values (computed from AES inputs and the key) for all recorded measurements.

Next, it was necessary to map hypothetical intermediate values to hypothetical power consumption ones. Mangard et al. and some laboratory tests (data not shown) indicated that Hamming Weight was a suitable mapping model [11]. The following code was used to generate the hypothetical power consumption matrix:

```
1  power_consumption= byte_Hamming_weight(after_sbox+1);
```

The "power_consumption" matrix contained all hypothetical power consumption values (from 0 to 8) for each recorded measurement.

Next, the hypothetical power consumption values were compared with the real power traces. A correlation trace was then generated for each possible value of the key (from 0x00 to 0xFF), using the code below (based on [11] online script):

```
1  chunksize=31;
2  for i=1:256
3    for j=1:cycles_to_analyse
4      cmatrix=corrcoef([T_final(:,1+(j-1)*chunksize:j*chunksize)
         power_consumption(:,i)]);
5      key_trace(i,1+(j-1)*chunksize:j*chunksize)=
         cmatrix(chunksize+1,1:chunksize);
6    end
7  end
```

This code split measured power traces into *cycles_to_analyse* "chunks" which were then compared to the previously generated hypothetical power consumption matrix. The resulting correlation coefficients were then stored within a correlation matrix "cmatrix". The visualisation of this matrix was a correlation trace.

Finally all correlation matrices (one per possible value of a key byte, *e.g.* 256) were stored within the global "key_trace" matrix.

The attacked key byte could then be obtained from a visual inspection of the 256 correlation traces, looking for correlation peaks.

Correlation peaks refers to high correlation values within the correlation matrices. An automated detection could be provided by looking for higher values within these matrices, as implemented in a display results script to automatically detect possible key byte.

However, as it is only based on one correlation peak, this solution was strongly subjective to false-positive detection.

To retrieve the full key, the DPA process was repeated on the same power traces (from hypothetical values matrix generation to correlation traces inspection) as many times as the number of key bytes. In this work, 16 PAA were performed to retrieve the full AES key.

3. Results

3.1. Skimmer black box analysis results

As a result of the visual and connectivity examinations, a testing board (hereafter named "analysis board") was designed to enable measurements on a more convenient platform. This board manufactured by BKA staff intended to recreate the initial board's connectivity (Fig. 10).

An overview of the communications between the microcontroller and its environment is shown in Fig. 11. Two different times were clearly distinguishable:

- the F2F decoder initialisation and communication time (rectangle);
- the memory communication time (circle).

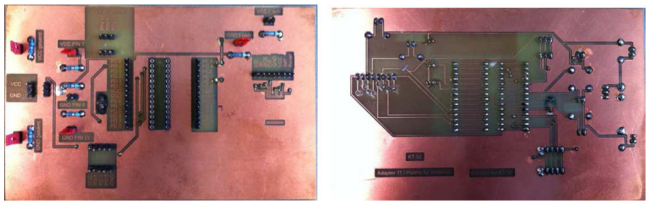


Fig. 10. BKA analysis board.

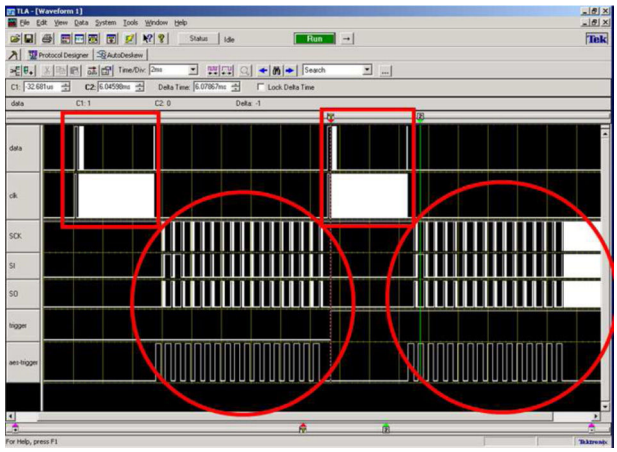


Fig. 11. Whole communications operated during the card data storage.

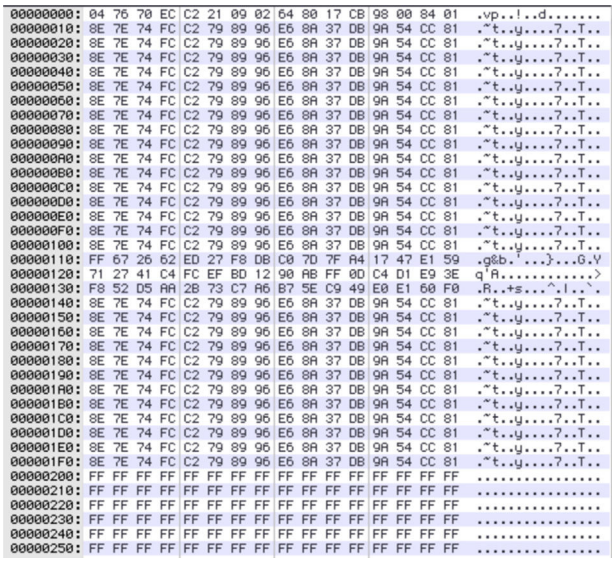


Fig. 12. Ciphertext stored within the Flash memory.

The F2F decoder communications, operated between the F2F decoder chip (*e.g.* Magtek 99875337) and the microcontroller, were performed according to the "Triple Track Delta Application Specific Integrated Circuit (ASIC)" datasheet.

Card data was sent to the microcontroller as read on the card (*i.e.* 5 bits encoded) except zero-bits that preceded the first one-bit which is not stored.

The communication with the external flash memory was performed as per the AT45DB161D datasheet.

As shown in Fig. 11, data was sent 16 bytes by 16 bytes and a large delay was present between each 16 bytes transmission.

A quick look at the ciphertext, after several card swipes, clearly showed that AES encryption was done using an Electronic CodeBook (ECB) mode (Fig. 12). This revealed that the 16 bytes encryption result did not depend on any previous results.

A closer look at the correlated plaintext (obtained using the known AES key of a reference device) revealed a storage format: for each stored card, a header was present, followed by the card data.

It also appeared that the 16 byte header did not always start with a new line and could be split between 2 different lines. Further tests revealed that even if the sent data length was always the same, records were stored with different lengths in the memory.

In fact, advanced tests revealed that, when all the 264 possible bits of the track of the first card were transmitted, only the 16 first bytes of the second swiped card were always encrypted together and stored in the same area (offset 0x120).

3.2. Skimmer white box analysis results

The assembly analysis, conducted with IDA Pro Disassembler, was performed on several interesting code parts. The more relevant ones referred to primordial routines in the skimmer microcontroller operation.

The skimmer initialization part provided important information on required elements for the skimmer to start.

In fact, at offset 0x0B7D and above, the microcontroller code received the status (with command 0x57) and the manufacturer/device IDs (command 0x9F) from the external memory.

Then it checked if the answers met the Atmel 16-Mbit DataFlash identifiers.

The F2F data transfer part also provided information on the way data was received by the skimmer.

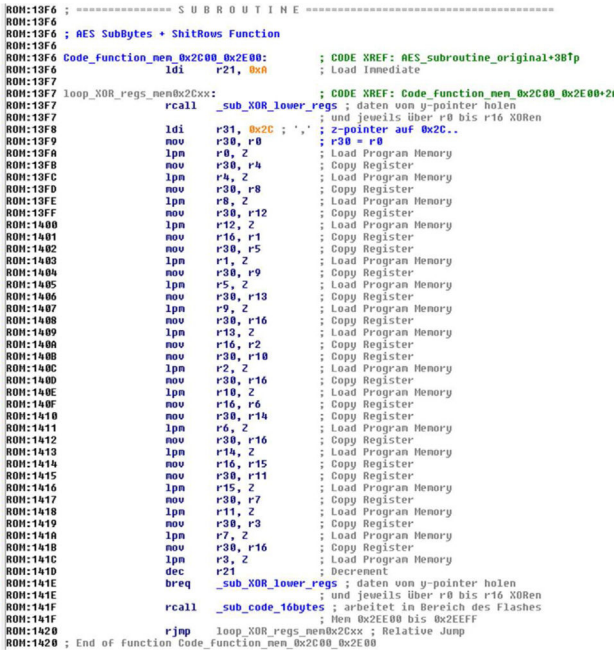
The subroutine located at offset 0x1F20 dealt with receiving data from the F2F decoder. Data exchange was processed with the code starting at offset 0x1FFA. F2F communication was handled by pulsing the clock line and reading the data line state after each pulse. Besides that, at offset 0x20C8, the full byte result was XORed with 0xFF.

Data sent from the F2F decoder was read as big-endian and inverted: if input data was little-endian, sent byte were first reversed and then inverted. For example, if byte 10110001 (0xB1) is sent, it was reversed to 10001101 and finally inverted to 01110010 (0x72).

Finally, the AES encryption part provided information on how and when encryption took place.

The AES encryption subroutine could be located at offset 0x270A, with encrypted plaintext first prepared at offset 0x1DCC and below. At the end, card data was stored using an "SCR" header.

The AES encryption subroutine code analysis showed that the SubBytes and ShiftRows AES functions ran at the same time (Fig. 13).



```
ROM:13F6 ; =============== S U B R O U T I N E =======================================
ROM:13F6
ROM:13F6 ; AES SubBytes + ShitRows Function
ROM:13F6
ROM:13F6 Code_Function_mem_0x2C00_0x2E00:        ; CODE XREF: AES_subroutine_original+38↑p
ROM:13F6                ldi     r21, 0xA         ; Load Immediate
ROM:13F7
ROM:13F7 loop_XOR_regs_mem0x2Cxx:                ; CODE XREF: Code_Function_mem_0x2C00_0x2E00+2A↓j
ROM:13F7                rcall   _sub_XOR_lower_regs ; daten vom y-pointer holen
ROM:13F7                                         ; und jeweils über r0 bis r16 XORen
ROM:13F8                ldi     r31, 0x2C ; ',' ; z-pointer auf 0x2C..
ROM:13F9                mov     r30, r0          ; r30 = r0
ROM:13FA                lpm     r0, Z            ; Load Program Memory
ROM:13FB                mov     r30, r4          ; Copy Register
ROM:13FC                lpm     r4, Z            ; Load Program Memory
ROM:13FD                mov     r30, r8          ; Copy Register
ROM:13FE                lpm     r8, Z            ; Load Program Memory
ROM:13FF                mov     r30, r12         ; Copy Register
ROM:1400                lpm     r12, Z           ; Load Program Memory
ROM:1401                mov     r16, r1          ; Copy Register
ROM:1402                mov     r30, r5          ; Copy Register
ROM:1403                lpm     r1, Z            ; Load Program Memory
ROM:1404                mov     r30, r9          ; Copy Register
ROM:1405                lpm     r5, Z            ; Load Program Memory
ROM:1406                mov     r30, r13         ; Copy Register
ROM:1407                lpm     r9, Z            ; Load Program Memory
ROM:1408                mov     r30, r16         ; Copy Register
ROM:1409                lpm     r13, Z           ; Load Program Memory
ROM:140A                mov     r16, r2          ; Copy Register
ROM:140B                mov     r30, r10         ; Copy Register
ROM:140C                lpm     r2, Z            ; Load Program Memory
ROM:140D                mov     r30, r16         ; Copy Register
ROM:140E                lpm     r10, Z           ; Load Program Memory
ROM:140F                mov     r16, r6          ; Copy Register
ROM:1410                mov     r30, r14         ; Copy Register
ROM:1411                lpm     r6, Z            ; Load Program Memory
ROM:1412                mov     r30, r16         ; Copy Register
ROM:1413                lpm     r14, Z           ; Load Program Memory
ROM:1414                mov     r16, r15         ; Copy Register
ROM:1415                mov     r30, r11         ; Copy Register
ROM:1416                lpm     r15, Z           ; Load Program Memory
ROM:1417                mov     r30, r7          ; Copy Register
ROM:1418                lpm     r11, Z           ; Load Program Memory
ROM:1419                mov     r30, r3          ; Copy Register
ROM:141A                lpm     r7, Z            ; Load Program Memory
ROM:141B                mov     r30, r16         ; Copy Register
ROM:141C                lpm     r3, Z            ; Load Program Memory
ROM:141D                dec     r21              ; Decrement
ROM:141E                breq    _sub_XOR_lower_regs ; daten vom y-pointer holen
ROM:141E                                         ; und jeweils über r0 bis r16 XORen
ROM:141F                rcall   _sub_code_16bytes ; arbeitet in Bereich des Flashes
ROM:141F                                         ; Wen 0x2EE00 bis 0x2EEFF
ROM:1420                rjmp    loop_XOR_regs_mem0x2Cxx ; Relative Jump
ROM:1420 ; End of function Code_Function_mem_0x2C00_0x2E00
```

Fig. 13. AES assembly code: SubBytes and ShiftRows done at the same time.

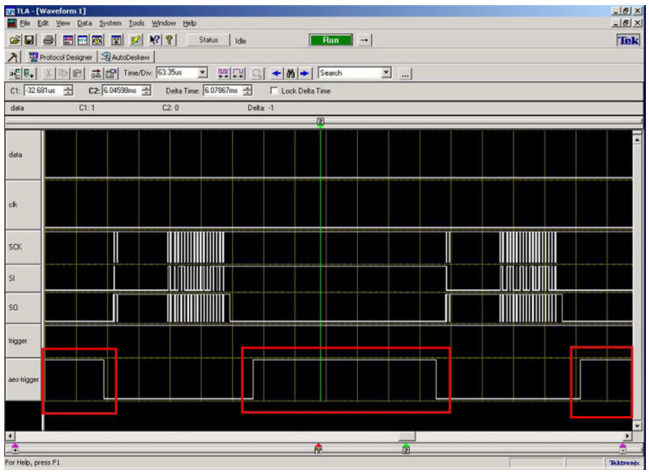


Fig. 14. Logic analyser encryption process visualisation.

3.3. Measurements results

The code modification provided within the measurement method permitted the identification of the encryption area. As shown in Fig. 14, the encryption of each 16 bytes plaintext was performed immediately before the resulting 16 bytes cyphertext was sent to the memory.

A trigger was set on a point in time where 16 consecutive bytes are always encrypted in the same way in order to measure the encryption area.

As offset 0x120 seemed to be only constant non-split 16 bytes encryption resulting position over the writing tests (see last paragraph of Section 3.1), the corresponding encryption area appeared to be appropriated. Thus an adequate trigger setting was set on the point in time when the writing command communication relative to this offset started between the microcontroller and the Flash memory.

Running the acquisition script described in the measurements method (see Section 2.3) provided a set of power consumption measurements for which DPA could be conducted.

Expected measurements were power consumption waveforms as shown in Fig. 15 which were computed from sample measurement sets provided by [11]. The characteristic aspects of suitable waveforms were smoothness (no noise), cyclic pattern and alignment.

Individual inspection of our measurement process results tended to indicate that waveforms conformed to expectation. A cyclic pattern could be observed and obvious noises was not present.

Visual inspection of several superposed waveforms around the trigger point also provided expected results.

However, the same traces, after some power cycles, revealed an alignment problem (Fig. 16) due to internal oscillator use.

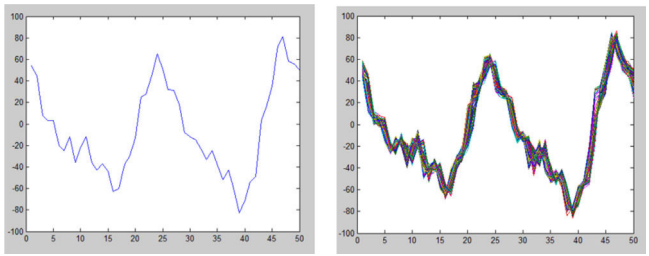


Fig. 15. Waveform examples: left 1 waveform, right waveforms from 100 measurements.

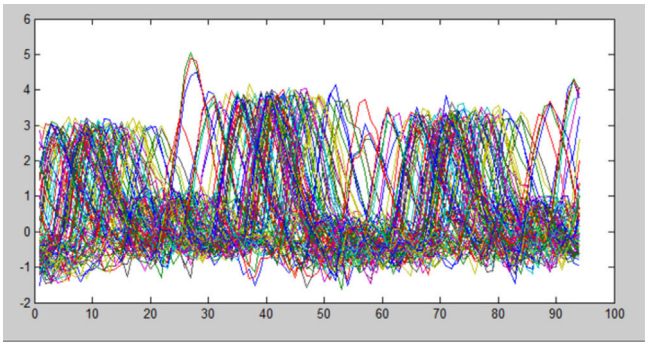


Fig. 16. Measurement process results: waveforms from 100 measurements 300 cycles before trigger point.

3.4. Power Analysis Attack results

As aligned measurements had to be computed to perform a DPA, the pre-processing script designed in Section 2.3 was ran to align measurements (Fig. 17).

Even though waveforms were not perfectly aligned due to acquisition resolution and some noise, alignments were good enough to run a DPA.

To validate the measurement and the correlation processes, a first analysis was conducted on the examined microcontroller using the plaintext as hypothetical intermediate values. In fact, running the DPA process with the plaintext as hypothetical values should have provided high correlation peaks when plaintext is manipulated on every possible key value (as plaintext does not depend on the encryption key).

The first set of measurements (Fig. 18) confirmed that the measurement and the correlation processes were functioning well, as correlation traces, since at some point, they contained high correlation (independent of the tested key).

To validate the whole process (measurements and data analysis), correlation between same measurements and suitable S-Box output (1st byte of the AES key as previously described in Section 2.4) were computed.

A visualisation of results (correlation coefficient traces) for every possible key byte values revealed some interesting correlation peaks on a few traces. As value 0xA2 related trace (plot 163 in Fig. 19) had an important correlation coefficient peak, 0xA2 appeared to be the 1st byte of the AES key.

The same process was repeated for the 15 other bytes, revealing the key: A27292925ae2a33ef452045c6030d502.

The guessed key almost matched the assembly code one (5th and 9th bytes were badly detected). The right key was guessed by a deeper examination. The full process was thus validated.

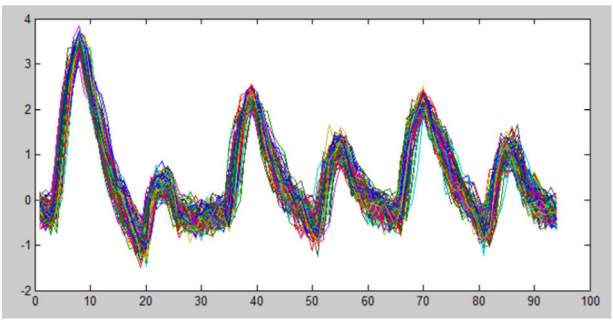


Fig. 17. Measurement and alignment processes results: waveforms from 100 aligned measurements 300 cycles before trigger point.

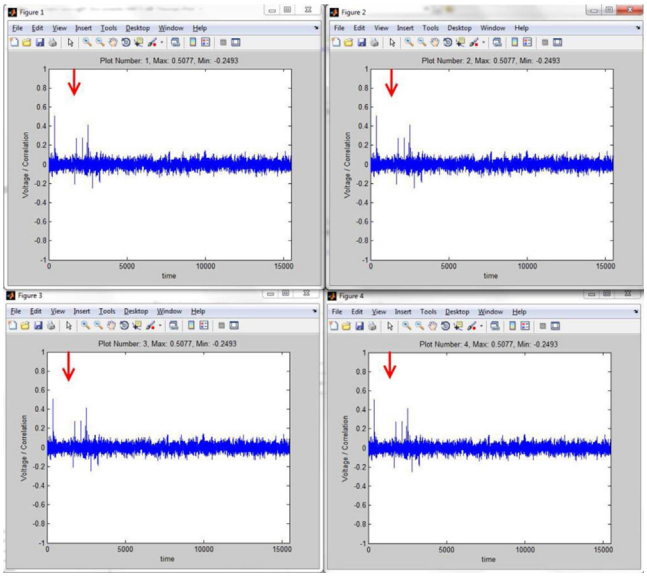


Fig. 18. Correlation coefficient on plaintext traces for 1st AES key byte. Displayed values from 0x00 to 0x03.

To confirm that results were not code-dependent and ensure repeatability of the results, blind tests were applied to different code versions (different firmware versions already extracted using the invasive method).

Thus, several firmware versions of MSR skimmers were:

- 6e (3 different skimmers);
- 6.1b (3 different skimmers);
- 6.1f (1 skimmer).

It appeared that some modifications were necessary on the data generation Arduino board's original sketch and on the analysis board connectivity.

After these modifications, all versions passed the tests: keys were successfully retrieved.

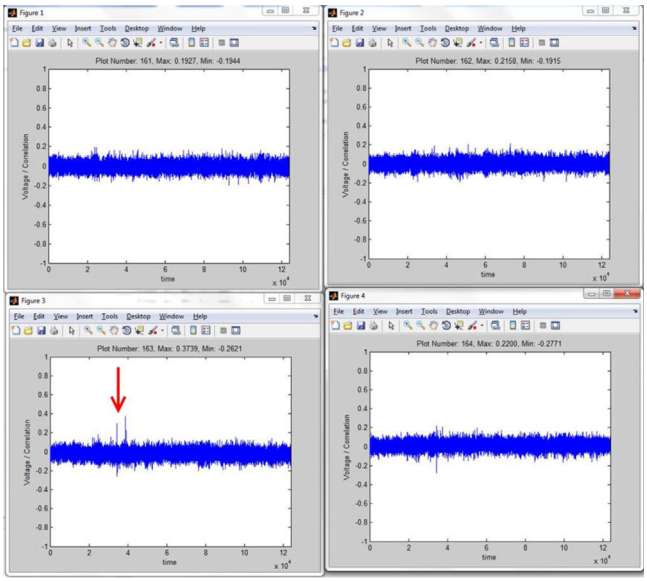


Fig. 19. Correlation coefficient of SBox output traces for 1st AES key byte value 0xA0 to 0xA3.

3.5. Case processing

Once the process passed quality tests, it was possible to apply it on real cases and measure its efficiency: 8 cases were successfully processed by this tool within 3 days.

Main feedbacks came from the power analysis process which was time consuming (2 h 15 min on first tests) and humanly demanding (key detection).

To reduce processing time, the encryption's location was refined to focus only on the first AES round related measurement area.

Final versions of the scripts are thus limited to 4000 analysed cycles. As a result, the complete analysis computing time was also reduced to 15 min.

To improve key detection, two major improvements were developed. The first one was to sort and display the automatically guessed key bytes in computation order to provide an easy error detection mechanism to the forensic analyst. The second one was to allow the analyst to automatically check the AES key and to brute-force one byte of the key.

Computing order, retrieved from AES encryption assembly analysis (see Section 3.2), is 1, 5, 9, 13, 6, 10, 14, 2, 1, 6, 11, 3, 15, 7, 12, 8, and 4. For example, Fig. 20 shows a misaligned peak on byte 7 plot. Further investigations would have to be conducted on that byte.

The other major improvement in AES key detection was the integration of an AES toolbox within the tool. The toolbox scripts allow to check if inputs encrypted with the guessed key match the outputs. The AES toolbox can also be called by the forensic analyst to brute force a key byte, checking all 256 possible combinations.

Only one case remained problematic. This case is related to a skimmer with a different hardware. Deeper assembly code inspection also revealed strong differences between internal codes, so that no compatibility with the current study could be found.

4. Discussion

4.1. DPA as a forensic tool

According to the results, the proposed method to handle AES skimmer cases is an efficient tool. DPA is thus a credible non invasive alternative to current invasive solutions to extract an encryption key from protected media.

Advantages of DPA as a forensic tool are obvious and numerous. First PAA requires low material investments, only few thousand euros are necessary to set up a full adaptive solution. Next, the method does not require any external modification of the device and thus matches forensically sound tool requirements. Finally, the overall method allows fast case processing: only 2 h and 15 min are necessary to run a full process (measurements – 2 h and attacks – 15 min).

However DPA has also several disadvantages. One of the most important is that PAA requires control of the device in order to conduct the process. It is thus necessary to understand its behaviours and structure.

Black and/or white box analyses are often necessary and are part of the proposed method. These analyses are device dependent and need to be conducted for each new implementations. This part of the method may be strenuous and time consuming, requiring for example an invasive attack of a reference device (if it exists).

PAA and, more generally, Side Channel Attacks (SCAs) have to be considered as legitimate solutions to forensically process secured (encrypted) media. They offer affordable and efficient means to retrieve the encryption key which would otherwise prevent the investigator from accessing potentially valuable data.

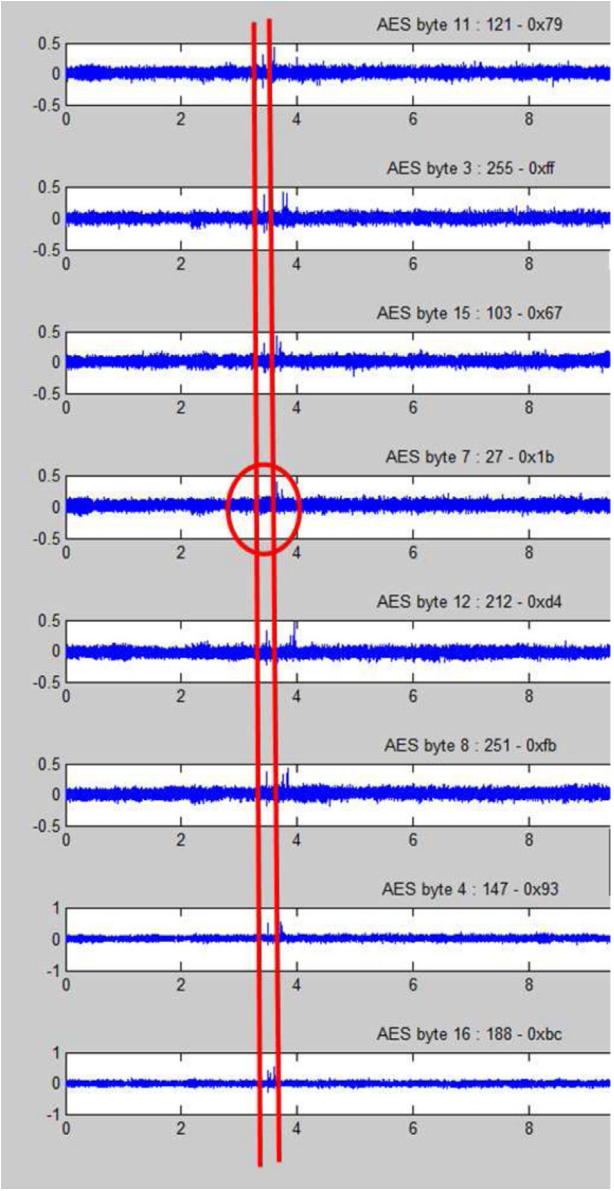


Fig. 20. An example of computation ordered guessed key display.

4.2. Method improvements

Some improvements could be developed to limit difficulties and improve its efficiency against modern DPA proof implementations.

New approaches have appeared since the initial DPA work of Kocher et al. [13]. Second-Order Power Analysis [14] [15] and Correlation Power Analysis (CPA) [16] represent interesting alternatives to investigate.

Another alternative to power consumption analysis attacks is to run an analysis of the electro-magnetic (EM) emission during the encryption process.

Various research works [17,18] promote this attack as more efficient and easier to process than Power Analysis Attacks. In fact, EM's main advantage is that it can be done on the initial board as non circuitry modification is necessary (to add a measurement resistor for example). An EM probe can be directly positionned above the microcontroller's surface to measure EM fields.

Minor tests were conducted within this work (data not shown) to measure EM fields during encryption. The EM measurement process consisted of recording the EM field on the surface of the skimmer's microcontroller using BKA's EM probes (Electro-Metrics EM-6992).

No relevant measurements were recorded. No further tests were conducted to check if the used EM probe was suitable for this process or if the generated EM field was sufficient enough, making it necessary to decapsulate the package.

5. Conclusion

The aim of this study was to obtain an alternative to the current Bundeskriminalamt (BKA) solution [9] to extract cryptographic keys from microcontroller's using Side Channel Attacks (SCA) as a forensic tool.

The work was designed to conduct a Power Analysis Attack (PAA) on a skimmer microcontroller running an Advanced Encryption Standard (AES) implementation.

For this purpose, a full measurement solution, based on Matlab scripts and Arduino boards, emulated the sending of card data, monitoring power consumption of the microcontroller and finally controlling the storage of the examined skimmer board.

Once the measurements were done and the cleaning/preprocessing Matlab scripts were run, Differential Power Analysis (DPA) could be launched. Based on correlation between measured power traces and intermediate hypothetical values, DPA produced 256 correlation traces per key byte that needed to be reviewed by the forensic analyst.

Finally, high-correlation peaks located on the correlation traces by automation script or by the forensic analyst revealed AES key portions (here: one byte). After 16 PAA – one per key byte – the whole secret key was retrieved.

Up to now, more than 30 cases of skimming fraud have been solved using PAA.

DPA also appears to be an operational alternative to "traditional" chip extraction.

The PAA-based solution is cheaper (a few thousand euros of equipment rather than many hundreds of thousands of euros), faster (hours rather than days), efficient and adaptive.

Results described open up new possibilities to deal with protected devices. Though this study was designed for payment card skimmers, the concept and developments can be applied (with some human interaction issues to be considered/emulated) to many different digital devices, including protected and/or encrypted memory sticks and other memory storage devices.

Concerning the process itself, several further configurations can be tested or expanded upon. First a common/general framework could be set up to deal with other kinds of AES skimmers/media devices. Then, to handle more complicated systems, an on-system attack using electro-magnetic (EM) probes could be developed using state-of-the art techniques [17].

As Side Channel Attacks (SCAs) appear to be efficient solutions to retrieve protected data in a non-invasive way, further research could be conducted to find other types of leakage of information that can be used by the forensic laboratories. If time and power consumption are now well known, other types of information leakage still remain to be studied.

Acknowledgements

The authors would like to thank the proofreaders, especially Francis Hermitte and Matthieu Regnery from the French Gendarmerie Forensic's Lab (IRCGN), Natacha Laniado from the Sorbonne University and Dan Embury from the Royal Canadian Mounted Police (RCMP), for their appreciated support to publish this article.

References

[1] Europol, EU organised crime threat assessment: Octa 2011, Tech. rep. (2011).
[2] 2011 annual report of the observatory for payment card security, Tech. rep., Observatoire de la Securité des Cartes de Paiement (2012).
[3] 2010 annual report of the observatory for payment card security, Tech. rep., Observatoire de la Securité des Cartes de Paiement (2011).
[4] 7th SEPA progress report: beyond theory into practice, Tech. rep., Eurosystem, 2010, p. 36.
[5] E.P. Council, Resolution: preventing card fraud in a mature EMV environment, Tech. rep., resolution 1 (January 2011).
[6] L. Padilla, Track Format of Magnetic Stripe Cards, 2002.
[7] G. Masters, P. Turner, Forensic data recovery and examination of magnetic swipe card cloning devices, Digital Investigation 4 (Supplement) (2007) 16–22.
[8] N. FIPS, 197: announcing the advanced encryption standard (AES), Information Technology Laboratory, National Institute of Standards and Technology, November.
[9] J. Frinken, Projektbericht: "fuses", Unpublished results.
[10] P. Kocher, J. Jaffe, B. Jun, Introduction to Differential Power Analysis and Related Attacks, 1998.
[11] S. Mangard, E. Oswald, T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer Science + Business Media, New York, 2007.
[12] S. Skorobogatov, M. Kuhn, Power analysis of the Motorola mc68hc908az60a microcontroller, Master's thesis, University of Cambridge (2005).
[13] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Advances in Cryptology – Proceedings of Crypto '99, Springer, 1999, p. 789.
[14] T. Messerges, Using second-order power analysis to attack dpa resistant software, in: C. Koç, C. Paar (Eds.), Cryptographic Hardware and Embedded Systems – CHES 2000, vol. 1965 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2000 pp. 238–251.
[15] E. Oswald, S. Mangard, C. Herbst, S. Tillich, Practical second-order dpa attacks for masked smart card implementations of block ciphers, in: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006, vol. 3860 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2006, pp. 192–207.
[16] E. Brier, C. Clavier, F. Olivier, Correlation power analysis with a leakage model, in: Cryptographic Hardware and Embedded Systems – CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11–13, 2004. Proceedings, Lecture Notes in Computer Science, vol. 3156, Springer, 2004, pp. 16–29.
[17] L. Sauvage, Cartographie électromagnétique pour la cryptanalyse physique, Ph.D. thesis, Télécom Paris Tech (2010).
[18] N. Selmane, Attaques en fautes globales et locales sur les cryptoprocesseurs aes: mise en oeuvre et contremesures, Ph.D. thesis, Télécom Paris Tech (2010).

B Payment card forensic analysis: From concepts to desktop and mobile analysis tools

Digital Investigation 11 (2014) 143–153

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Payment card forensic analysis: From concepts to desktop and mobile analysis tools

T. Souvignet [a, b, *], J. Hatin [c], F. Maqua [a], D. Tesniere [c], P. Léger [c], R. Hormière [d]

[a] Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), Digital Forensics Department (INL), 1 boulevard Théophile Sueur, 93110, Rosny-Sous-Bois, France
[b] PRES Sorbonne Universités – Université Panthéon-Assas Paris II, 12 place de Panthéon, 75005, Paris Cedex 05, France
[c] ENSICAEN, 6 boulevard maréchal Juin, 14050, Caen Cedex 4, France
[d] INSA Lyon, 20 avenue Albert Einstein, 69100, Villeurbanne, France

ARTICLE INFO

Article history:
Received 21 February 2014
Received in revised form 26 June 2014
Accepted 27 June 2014
Available online 16 July 2014

Keywords:
Payment card fraud
Skimming
Carding
Forensic tool
Payment card analysis

ABSTRACT

While one would not even consider them alike, payment cards are one of the most valuable and widely used embedded systems. Payment card systems are probably the most attacked and counterfeited. In fact, even though the use of smart cards have introduced high security capabilities, criminal activity has not been deterred and payment card fraud remains a lucrative activity.

From low-tech (carding) to high-tech (man in the middle attack) fraud, all payment card based frauds require stealing or modifying card data and reusing it with a direct profit. Physical forms of fraud, such as Automated Teller Machine (ATM) withdrawals or in store payments, are mostly based on and associated with manipulated cards. Through their nefarious actions, that may include overwriting the magnetic strip data or injecting attacks on the embedded microcontroller, criminals are able to realise significant monetary gains. To effectively deal with these fraud cases, investigators have to quickly determine whether a card is authentic or a counterfeit. Currently no known easy forensic tool exists that provides a quick effective and accurate response.

In this article, after having conceptualised payment cards as multi-interface embedded systems, we propose simple and fast forensic analysis methods to finally provide investigators with associated desktop and mobile forensic tools.

© 2014 Elsevier Ltd. All rights reserved.

Introduction

Payment cards represent the most used non-cash means of payment, surpassing wire transfers and bank cheques, due to the extra protections they afford (The UK Cards Association, 2014; Comité Consultatif du Secteur Financier, 2011). The total number of payment cards issued in the EU in 2011 reached 726906710 and the value of legitimate non-cash associated transactions within the region exceeded 3000 billion euros (Europol, 2012).

To support such a large volume and value, payment cards are no longer just a simple plastic card with an account number, nor a simple magnetic stripe card. Since the end of the 20th century, payment cards are smart cards, with an Integrated Circuit (IC) moulded in the card plastic. According to Eurosmart (Eurosmart, 2013), more than 1.5 billion payment smart cards will be shipped in 2014, which will make payment cards one of the most widely distributed embedded systems.

* Corresponding author. Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), Digital Forensics Department (INL), 1 boulevard Théophile Sueur, 93110, Rosny-Sous-Bois, France.

E-mail addresses: thomas.souvignet@gendarmerie.interieur.gouv.fr, thomas@souvignet.net (T. Souvignet), julien.hatin@ecole.ensicaen.fr (J. Hatin), fabrice.maqua@gendarmerie.interieur.gouv.fr (F. Maqua), damien.tesniere@ecole.ensicaen.fr (D. Tesniere), pierre.leger@ecole.ensicaen.fr (P. Léger), romain.hormiere@insa-lyon.fr (R. Hormière).

http://dx.doi.org/10.1016/j.diin.2014.06.006
1742-2876/© 2014 Elsevier Ltd. All rights reserved.

Due to the associated ease of use and fast money they represent, payment cards are attractive items for organised criminal groups. In response, Law Enforcement Agencies (LEA) have had to develop investigative and forensic analysis methods to fight payment card fraud. It is paramount that LEA continue these efforts to address the escalating threat to the global banking industry.

Payment card related fraud

According to Europol (Europol, 2012), payment card fraud reaches around 1.5 billion euros per year in Europe. It is also a profitable activity for organised criminal groups which develop and exploit every possible form of this crime. Essentially, all of the alleged and associated activities are based on a two step crime: first obtain the payment card data, and then use it.

Even if no serious studies have been conducted to provide a formal link between each form of data theft and each form of data usage, likely due to the complexity of this task, it is commonly admitted that payment card fraud can be classified into 2 main categories:

- Card Not Present (CNP) or online frauds, where data comes from payment card breaches, phishing, or malware;
- physical fraud, where data originates from lost and stolen cards, skimming, shimming,[1] man in the middle attacks, Automated Teller Machine (ATM) reverse engineering, etc.

Most of the complaints are due to skimming, that consists of stealing payment card details and Personal Identification Numbers (PIN) against cardholder vigilance. Stolen data is then reused to make counterfeit cards, known as carding. These cards are then used at ATMs to withdraw money or at shops to buy goods.

Investigating such complaints requires the investigators to fully understand payment card mechanisms and to be able to detect if a card is genuine or counterfeit.

Payment cards

In order to simplify payment card understanding and integrity analysis, we propose to consider payment cards as multi-interface embedded systems that contain both static and dynamic data.

Nowadays payment card characteristics, mostly based on ISO 7813 (International Organization for Standardization, 2006b) and EMV standards (EMV book 1, 2011; EMV book 2, 2011; EMV book 3, 2011; EMV book 4, 2011; EMV book D, 2013), can be defined by 4 interfaces:

- visual interface;
- magnetic stripe interface;
- IC contact interface;
- IC contactless interface.

Visual interface

The first and most obvious interface of every card is its visual one. The visual interface is much more standardised than might be expected. The following ISO standards define this interface:

- ISO 7810 defines the plastic card physical characteristics with ID1 dimensions;
- ISO 7811 defines location of "identification number line" and "name and address area", and characteristics of readable characters (International Organization for Standardization, 2002a);
- ISO 7811 also defines location of magnetic stripes (International Organization for Standardization, 2002b, 2008a, 2008b);
- ISO 7812-1 defines the PAN format (International Organization for Standardization, 2006a);
- ISO 7816 defines location of the contacts (International Organization for Standardization, 2004).

Payment card visual interface is thus easily characterised and the following elements can be found on Fig. 1:

1. Primary Account Number (PAN)
2. Cardholder name
3. Expiration date
4. Payment authority logo
5. Card not present payment verification code (CVV/CVC)
6. Manufacturer serial number
7. Cardholder signature
8. Holograms and UV securities

Fig. 1. Payment card visual interface.

[1] Skimming applied to chip-terminal transactions.

Magnetic interface

The second interface which is well established is the magnetic one. The magnetic interface consists of three magnetic tracks (Fig. 2). The first two tracks, called track 1 and track 2, are the most commonly associated with payment. Their location and the encoding principle are defined in the ISO 7811 standard (International Organization for Standardization, 2002b).

The ISO 7813 (International Organization for Standardization, 2006b) standard describes the data written on payment card tracks 1 and 2.

The main difference between the two tracks is the encoding density. The bits are slightly shorter on track 1, allowing for more information to be written (Fig. 3).

On track 1 we find an alpha numeric encoding of the PAN, the cardholder name, the expiration date and the service code. The service code indicates if the card has a chip or not.

Track 2 contains the same information except that the cardholder name that is not present. A one character Longitudinal Redundancy Checksum (LRC) is calculated to ensure data integrity for each track separately.

Chip contact interface

The third interface, chip contact (Fig. 4), is already in widespread use throughout Europe and Canada, but other regions have been slow to adopt this more secure method due to prohibitive costs.

Due to recent security breaches in their magnetic stripe only payment system, the United States of America will commence the global roll-out to “Chip and PIN” payment cards (Levick, 2014).

The application protocol used by payment chips is defined by EMV, acronym for Europay, Mastercard and Visa. It defines a global standard for the interoperability of the chip card with the Point Of Sale (POS) and ATM. The EMV standard describes the physical, electrical and data link layer. It is based on the ISO 7816 standard for the contact interface.

The ISO 7816 standard is a command response protocol. The chip card is passive and only answers to the POS and ATM commands.

In order to communicate with a chip card, the EMV protocol defines Application Protocol Data Units (APDU). These APDU can be sent directly after the initialisation sequence.

The commands are called C-APDU and the responses are called R-APDU. After a command has been sent, a R-APDU is replied. This response is comprised of status words and optional data, with the status word dependent upon the

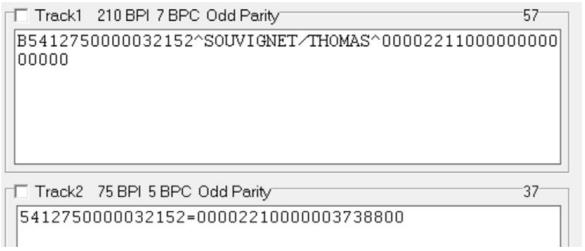


Fig. 3. Data encoded on tracks 1 and 2.

card state. The EMV protocol requires that the status word is equal to NORMAL (0x9000) when a transaction is completed successfully. The data is encoded using the Basic Encoding Rules (BER) Tag Length Value (TLV) Abstract Syntax Notation One (ASN.1) format.

According to the EMV flowchart (EMV book 3, 2011), the first two steps of a chip card transaction are the Initiate Application followed by the Read Application Data. The Initiate Application step is done through the SELECT APDU. A chip card could have multiple payment applications installed. For example, most French cards host a domestic payment application in addition to the international Mastercard or Visa payment applications.

The EMV standards define 4 mandatory data objects:

Tag (hexadecimal)	Value	Description
5F24	Application Expiration Date	Expiration date of the payment application
5A	Application Primary Account number	Number that identifies the account lean against the payment application
8C	Card Risk Management Data Object List 1	Data required by the card to seal the transaction with a MAC calculation
8D	Card Risk Management Data Object List 2	Data required by the card to seal the transaction with a MAC calculation

Other optional or conditional data could also be present for cryptographic processing and personalisation. A common data object is the Cardholder Name (tag “5F20”). Another common piece of data is the Track 2 Equivalent Data (tag “57”) which is an emulation of the magnetic stripe track 2.

This data is stored in records on the card that are personalised during the creation of the card before being issued. The records store the data of a payment application and can be read using the READ RECORD APDU.

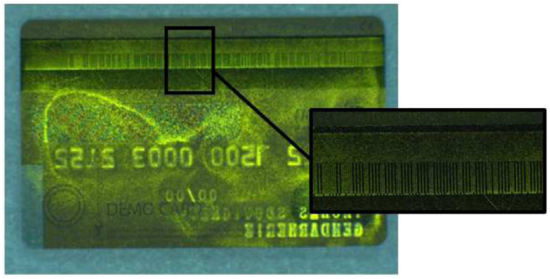


Fig. 2. Payment card magnetic stripes revealed.

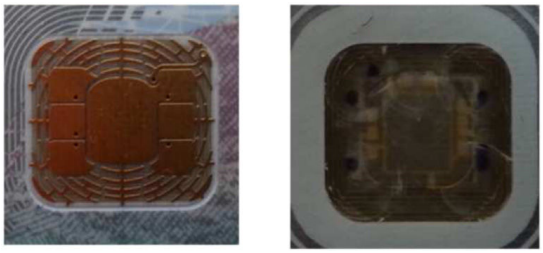


Fig. 4. Payment card IC contact interface.

Chip contactless interface

The final interface associated with payment cards is the recently introduced contactless interface (Fig. 5).

In its 2014 contactless smartcart forecast, Eurosmart estimated that more than half of the card shipments will be generated by the banking industry (Eurosmart, 2013).

The contactless interface is defined by the EMV contactless (EMV book D, 2013) specification. Some differences exist between the contact and the contactless interfaces. The first one is the communication protocol on which the EMV standard relies, since the contactless interface is based upon the ISO 14443 (EMV book D, 2013). The EMV book D defines an operating distance up to 4 cm high. This implies a transaction with the contactless card could be executed up to 4 cm from the POS payment terminal.

The data present on the contactless interface can also be altered in order to ensure privacy. As an example the Cardholder Name (tag "5F20") is often not present in the contactless interface (Mastercard, 2011), with it replaced by space (ASCII code 0x20) instead.

Payment card analysis methods

We have already presented the concept of multi-interface embedded systems when we introduced payment card internals. This simple concept is important when considering the development of methods to analyse payment cards.

Published research in several papers discuss skimmer forensic analysis (Masters and Turner, 2007; Guo and Jin, 2010; Souvignet and Frinken, 2013) but does not focus on payment card analysis. In this paper, we propose 3 analysis steps that provide coverage for most types of fraud and meet investigative requirements. The first analysis consists of detecting if a card is genuine or counterfeit. The second deals with detection and identification of particular types of fraud. The last process consists of extracting valuable data for the investigators.

Genuine detection analysis

Thanks to our multi-interface concept, detecting counterfeit cards is as simple as comparing numbers. In fact, this method simply relies on reading data from all available interfaces and matching them together.

Fig. 5. Payment card IC contactless interface.

Thus, analysing a classic EMV payment card consists of:

- transcribing PAN, cardholder name and expiry date from the visual interface;
- extracting data from tracks 1 and/or 2 using a magnetic stripe reader;
- extracting EMV data from contact chip;
- extracting EMV data from contactless chip;
- comparing relevant data to one another.

Data common to all interfaces is comprised of cardholder name, PAN and expiration date.

Cardholder name can be found on the front face of the card (embossed or screen printed), on magnetic stripe track 1, in EMV data object CARDHOLDER NAME (tag "5F20") but should not be provided by the contactless interface (Mastercard, 2011).

PAN and expiration date can be gathered from the front face of the card (embossed or screen printed), on magnetic stripe tracks 1 and 2, and in EMV data objects "Application Primary Account Number" (tag "5A") and "Application Expiration Date" (tag "5F24") provided by the contact and contactless interfaces.

Usually, a simple comparison between retrieved PAN and expiration dates is enough to detect counterfeit card in most instances.

The following example demonstrates the data retrieved from a card whose magnetic stripe would have been overwritten with data from another card.

Particular fraud analysis

Unfortunately, some counterfeit cards cannot be detected with such a basic approach. For these rare occurrences, advanced analyses have to be conducted. As some of these particular activities are yet unknown, analyses have to be designed on a case by case scenario.

Visual interface	Cardholder name	THOMAS SOUVIGNET	Front face / "name and address area"
	PAN	5412750000032152	Front face / "identification number"
	Expiration data	00/00	Front face / "name and address area"
Magnetic interface	Cardholder name	JOHN/DO.MR	Track 1
	PAN	45XXXXXXXXXX45	Tracks 1/2
	Expiration data	14/06	Tracks 1/2
Contact interface	Cardholder name	THOMAS SOUVIGNET	Tag 5F20
	PAN	5412750000032152	Tag 5A
	Expiration data	00/00	Tag 5F24
Contactless interface	*Not present*		

A practical example of such a fraud involves Man In the Middle (MIM) cards. This fraud, based on Cambridge University research (Murdoch, 2009; Murdoch et al., 2010),

relies on adding a microcontroller between the card contact and the legitimate card IC (cf. sample on Fig. 6). This microcontroller can intercept EMV commands and responses in order to manipulate the EMV data flow.

As described in the Murdoch et al. paper, an interesting command to experiment with on a lost or stolen card is the VERIFY PIN command. In fact, if the "microcontroller in the middle" does not pass the C-APDU containing the VERIFY PIN command to the card IC but instead generates a R-APDU containing an answer status word NORMAL (0x9000), the card expects a non PIN verified transaction while the terminal is tricked into thinking that a PIN verified transaction is currently taking place.

Detecting such a fraud can be very challenging for investigators particularly if the microcontroller insertion is done fairly well. An interface comparison analysis would only detect the fraudulent modification if the IC comes from another card, since this would easier for criminals to prepare and implant.

If the IC is the original one, an advanced analysis is necessary. A simple and efficient custom analysis would then consist of sending a VERIFY PIN command outside any context of payment transaction, when the application is not even selected. If the card answers with a 0x9000 to this testing C-APDU, it can be declared that the card has been manipulated with a MIM based attack.

This simple test, and custom fraud analyses in general, when provided to local digital investigators or first responders could be a great way for them to quickly determine if someone is in possession of manipulated cards.

Stored data analysis

Local investigators are not all involved in investigating payment card crimes but payment cards can be a very interesting source of information. Such information is especially valuable if it can be accessed in-the-field and not after time consuming requests. Payment card stored data can provide investigators with transaction history and issuer details.

Transaction log

The advent of smart cards within the payment card context does not only provide security but also memory.

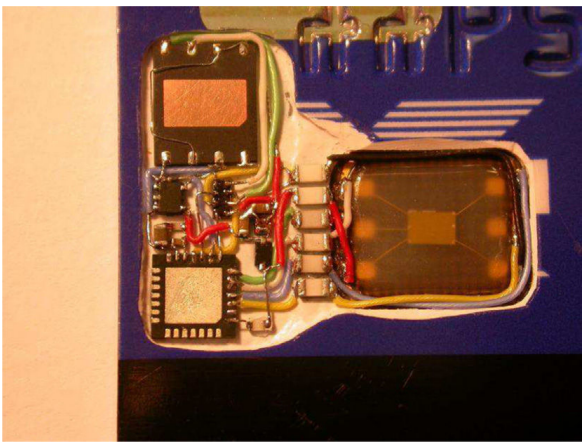


Fig. 6. MIM card example from Bond et al. article (Bond et al., 2014).

Thus EMV provides an interesting feature for investigators: log entries. By "provid[ing] support for accessing a transaction log file by special devices" (EMV book 3, 2011), some EMV payment cards offer a variable size payment and withdrawal history.

This feature is optional and may vary between payment schemes, issuers and even personalisation versions. For example, we have not found any American Express card with transaction log entries while most French cards disclose EMV card history (from 10 entries to dozens).

If a Log Entry data element is provided (tag "9F4D") when the application is selected, it indicates that the card supports transaction logging whose format is defined by the Log Format data element (tag "9F4F"). For example, a Log Format data element equal to "9f02069f27019f1a025-f2a029a039c01" indicates that the transaction log records have the following content: Amount, Authorised (6 bytes), Cryptogram Information Data (1 byte), Terminal Country Code (2 bytes), Transaction Currency Code (2 bytes), Transaction Date (3 bytes) and Transaction Type (1 bytes).

To get the log entries, stored based on a First In First Out rule, it is necessary to read the records mentioned in the Log Entry data element and then apply the Log Format to them. For example, a "0000000011904002500978130803 00" log entry means an accepted (40) payment (00) made in France (250) on the 3rd of August 2013 (130803), for an amount of 11,90 (000000001190) euros (0978).

As dozens of records may be available, transaction logs can be a valuable source of information for investigators in order to immediately prove an individuals presence in a mentioned country.

Resolve issuer from PAN

Another typical solution for retrieving payment card history is to contact the card issuer who will be retaining all the card history; however, getting the issuer fraud department details might be quite challenging and generally requires previously engaged inside contacts or the time consuming establishment of new contacts within the payment related fraud service.

Analysing the PAN can also be a method of identifying the issuing bank. The ISO 7812-1 standard breaks down the PAN into 3 different parts: the Issuer Identification Number (IIN – 1 digit), the individual account number (max 12 digits) and a check digit (1 digit) (International Organization for Standardization, 2006a). The first digit of the IIN is known as Major Industry Identifier (MII) where 3, 4 and 5 belong to the banking industry and 7 belongs to the petroleum industry. To check digit is based on a Luhn checking algorithm.

Difficulties in getting the issuing bank from the IIN would require querying the American Bankers Association as stated by the American National Standards Institute, which is in charge of IIN registration (American National Standards Institute, 2014), but would only provide payment scheme details. To solve this issue, several websites provide Bank Identification Number (BIN – IIN applied to bank industry) databases or lists; however, most of them are outdated or not very accurate.

In order to resolve the issuer from the PAN to obtain even more details, we contacted the main payment

schemes (AMEX, Mastercard and Visa) to gain access to their directories or, at least, relevant local focal points.

By having access to these directories, investigators can resolve the issuing bank, getting their name and also obtaining fraud service addresses and phone numbers. Providing such a service to field investigators can also save precious time by aiding investigators with the ability to contact the right person.

Tools

General introduction

We have previously seen that several analyses can be conducted on the widely distributed embedded systems contained within payment cards.

However, investigators efforts are inhibited by the lack of software to conduct such forensic analyses. To alleviate these shortcomings, we are also proposing two tools to meet their requirements.

The first one is a desktop tool to process payment cards in order to verify card integrity, check some known discrepancies and extract/provide valuable data to the investigators, including transaction logs and issuer details.

The second one is a mobile version of this tool to allow the extraction of payment card data in the field in order to conduct a first responder analysis.

Both of these tools have been designed as and with open source software utilising inexpensive readers.

Desktop tool

Targeted systems

As most police officers' terminals are workstation, we first designed a desktop tool to conduct computer assisted payment card analysis. Due to the variety of operating systems (Windows, Linux, Mac OS) used across the European police forces, the tool was developed in JAVA (1.6 and higher) which is known for its portability.

Java Runtime Environment (JRE) 1.6 includes the package javax.smartcardio which was defined in the Java Portlet Specification 2.0 (JSR 268). It defines a Java API for communication with Smart Cards using ISO 7816-4 APDUs. It thereby allows Java applications to interact with Smart Cards, to store and retrieve data on the card with a PC/SC reader.

Card processing

Visual interface. The data acquisition is performed manually. The pictures of the front and of the back of the card can

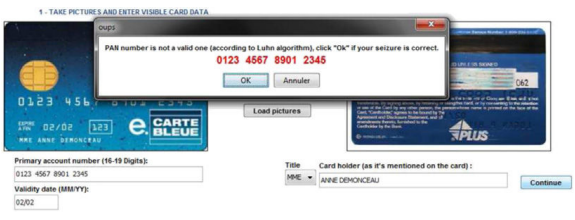


Fig. 7. Visual data acquisition.

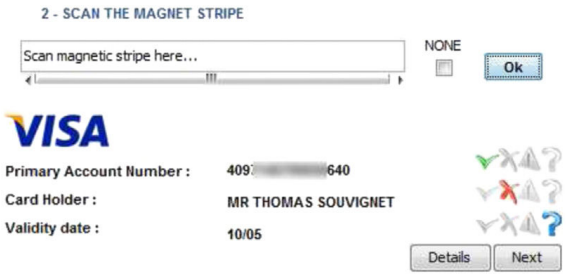


Fig. 8. Magnetic stripe data acquisition.

be imported from pictures files or captured directly with a webcam. These pictures are saved to confirm the data entries.

The handwritten data will be used as reference for comparison with the data extracted from the other interfaces.

When the user confirms his input, the PAN is checked according to the Luhn algorithm. If it is stated as invalid, the user is asked to verify it (Fig. 7). This is a first clue regarding the card's integrity.

Magnetic interface. We chose to use a "MSR90" 3 tracks magnetic stripe Universal Serial Bus (USB) reader. This reader has been chosen due to its low cost of around 20 euros.

First, this reader decodes the magnetic stripe data with Longitudinal Redundancy Checksum (LRC) and sends it to the application as keyboard strokes.

Then the string is checked using a regular expression to ensure that the data is compliant with ISO 7811 part 2 specifications and contains payment data. Data from track 1 and/or track 2 are extracted from the string using the split method with standardised separator characters.

Finally, the magnetic stripe's payment data are compared to the data from the visual interface entered previously.

Depending on comparison results, some visual hints (tick, cross, warning, question mark) regarding the card integrity is displayed (Fig. 8).

Users can also get some results which are not displayed by default by clicking the "Details" button (Fig. 9).

Chip contact and contactless interface. After visual data and magnetic stripe data acquisition, users can extract data from the chip. Before starting the extraction, users have to configure the application in order to use their card reader under the Settings menu. The configuration is very easy and multiple card readers can be used, including both contact readers and contactless readers.

Once done, the IC data extraction can be performed following the transaction flow detailed in Fig. 10.

Interesting data (PAN, cardholder name, etc.) is then extracted from these transactions to be compared with other interface values as shown on Fig. 11.

For example, reading and decoding the following record (using Application File Locator tag "94") would offer two main pieces of information:

```
----------
READ RECORD Command : 00B201143E
Answer :

70 3C --- READ RECORD Response Message Template

        5F25 03 --- Application Effective Date
        091201

        5F24 03 --- Application Expiration Date
        120131

        5A 08 --- Application Primary Account Number
            (PAN)
        0123456789012345

        5F34 01 --- Application Primary Account
            Number (PAN) Sequence Number
        07

        5F28 02 --- Issuer Country Code
        0250

        9F4A 01 --- Static Data Authentication Tag
            List
        58

        8D 17 --- Card Risk Management Data Object
            List 2 (CDOL2)
        8A032F02069F03069F1A
        0295055468A29A054C01
        9F3704

status word --- 9000 --- Command successfully
    executed ----------
```

If a contactless interface is available, users can also analyse it using a previously configured contactless card reader, in order to get the result as shown above. As some cards do not have a contactless interface, this step can be skipped in those instances.

Integrity analysis and reporting

After analyses, the investigator is asked to make a decision on card integrity. He or she can declare the card as being counterfeit or genuine but can also decide not to make any judgement, rather postponing for later decision.

For accountability purposes, it can be useful to know what exactly happened during the analysis; therefore, users can get an entire log of all commands and responses by switching to expert mode.

After the investigator has made his or her decision, the case can be saved and a time stamped report can be generated. The report is a summary of all data extracted from all cards included in the case, including transaction logs, ending with the decision taken by the investigator.

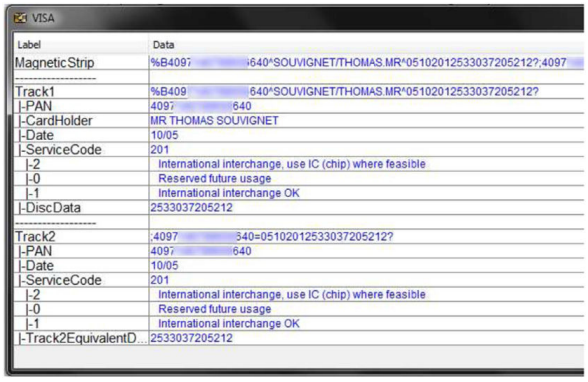


Fig. 9. Details.

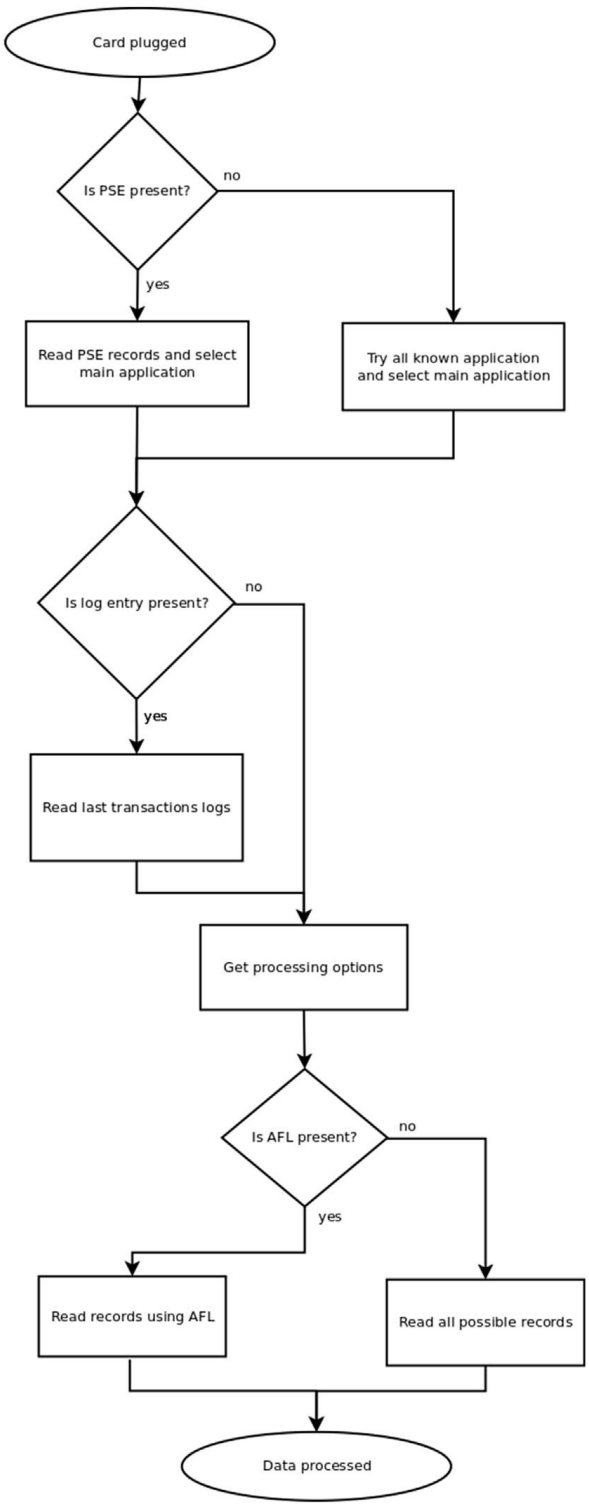


Fig. 10. Data extraction flow on the contact interface.

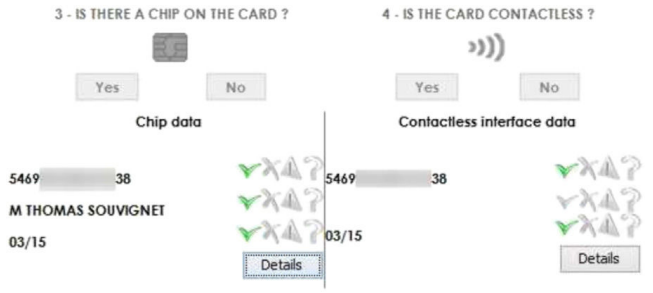


Fig. 11. IC data acquisition via contact interface.

Mobile tool

Targeted systems

According to Gartner (Gartner, 2013), 82% of the mobile phones sold during Q3 of 2013 run on the Android operating system. In order to address this dominant platform, the mobile tool for investigators was developed for devices running Android 4.0 or newer.

Android phones have been able to use the USB On-The-Go (OTG) since version 3.1 (Honeycomb). USB On-The-Go introduces the concept that a device can perform both the master and slave roles. In our application we could then use a USB card reader to perform the data acquisition.

More recent Android phones also propose a Near Field Communication (NFC) management that could be used to retrieve information on the contactless interface. The NFC technology has been available since version 2.3.3 (Gingerbread MR1).

The mobile tool process was designed to be is very similar to that of the desktop tool. Some concessions had to be made due to limitations of the mobile platform. However, as smartphones have become more and more powerful, the ability to offer an easy to use solution for the investigators in the field has been realised.

Card processing

Visual interface. The data acquisition is performed manually. Pictures of the front and back sides of the card are taken. To perform these captures, the Android smart phone camera is used.

Capturing these pictures provides good data integrity to ensure that no data has been mistyped. The data captured is set as a reference (Fig. 12). All applicable additional data captured on other interfaces will be compared to this.

Magnetic interface. In order to extract the magnetic stripe data, a 1 euro audio jack magnetic stripe was chosen (Fig. 13). These dongles are recognised as a microphone by Android phones, giving them the ability to read the signal and transmit it as waveforms to the audio processing unit of the phone.

The provided "square API" was used to decode the magnetic stripe. In order to be sure of the data acquisition, we verified both the longitudinal redundancy checksum and the format.

The audio jack reader is limited to track 2 and thus cannot read track 1 data. As cardholder name is not present

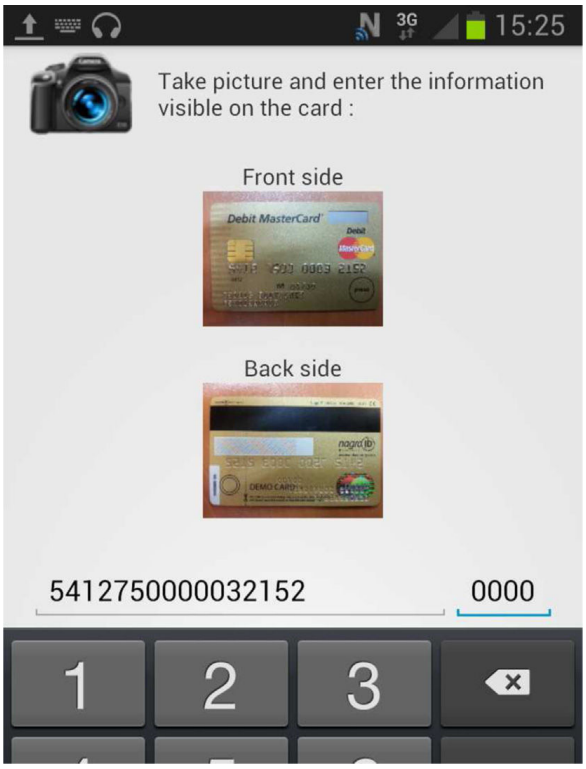


Fig. 12. Visual interface data acquisition.

on track 2, we can only extract the PAN and the expiration date.

Extracted data appears as a string which is checked using a regular expression to ensure that the data is compliant with the specifications of ISO 7811 part 2. We also verify that the resulting string contains payment data.

Due to the lack of track 1 analysis, the cardholder name is not verified; however, PAN and expiration date are sufficient to get relevant results (Fig. 14).

Smartcard contact interface. This acquisition is done through a contact smart card reader. The reader is connected using the USB On-The-Go technology as shown in Fig. 15. An API developed by the Spanish National Institute of

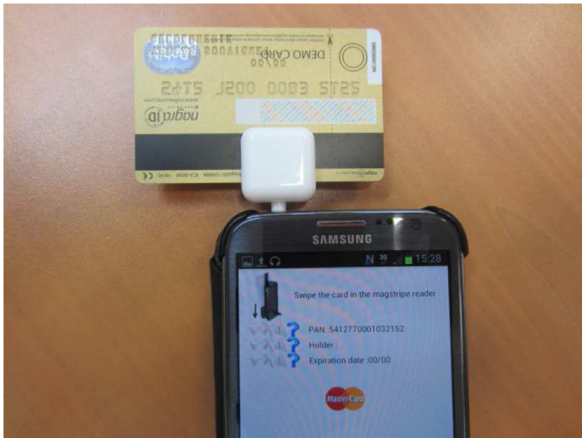


Fig. 13. Visual interface data acquisition.

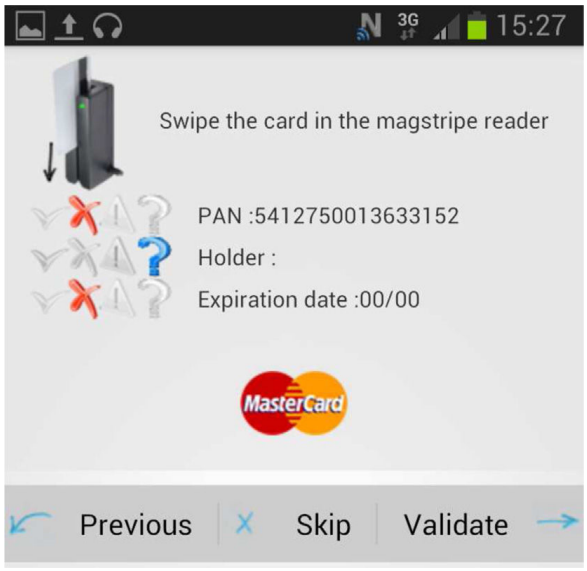


Fig. 14. Magnetic interface data acquisition.

Communication Technologies (INTECO), called DNIe Droid 1.0 API (INTECO, 2012), has been used to implement a software driver that handles the card reader. To the authors' knowledge, this library is compatible with all PC/SC/CCID readers.

APDU are sent to the smart card. The first step is the selection process. The selection has been implemented following the EMV standard. On the contact interface, the PSE (1PAY.SYS.DDF01) application is usually present. This application is a directory of all the payment applications available on the card. If this application is not present, the EMV standard asks the terminal to select all known applications. We implement the same behaviour based on Java EMV Reader list (sasc, 2012). Then, we select the main application.

If this application contains transaction logs (tag "9F4D"), the last transactions performed with this card can be retrieved by issuing the READ RECORDS command.

Two different methods to retrieve the payment data from the records were implemented.

Fig. 15. Contact interface data acquisition.

The first one is to use the basic EMV process. After issuing a Get Processing Option command, the card normally answers with an object, the Application File Locator (AFL – tag "94"), that indicates the list of its records. We use this list to read all of the records in the card.

In some case, if the data inserted in the GET PROCESSING OPTION was not suitable for the card, we were unable to recover the AFL from the card. A second method consists of retrieving data trying all possible records on the card.

Smartcard contactless interface. This acquisition can be done with a contactless PC/SC reader. In this case, we used the USB OTG technology as described in the contact data extraction. A second solution is to use the NFC capability of the Android device.

The data extraction process is very similar to the contact interface (Fig. 16). The only difference is in the application selection process. The application directory is not the PSE (1PAY.SYS.DDF01) but rather the PPSE (2PAY.SYS.DDF01). The information is displayed differently but is the same as what is present in the contact interface.

In each case, the data acquisition follows the same principles as those described in Fig. 10.

Integrity analysis and reporting

After each data acquisition, data integrity is verified. This is done using a simple comparison between the payment information from each interface. Depending on comparison results, some visual hints (tick, cross, warning, question mark) regarding the card integrity are displayed.

For example, the following diagram (Fig. 17) shows how we choose the visual hint for the PAN.

At the end of the data capture process, all the information from the card, as well as the result of this analysis, can be exported as an archive (ZIP file) that contains all the data in one XML file, including the card pictures that were taken at the first step.

This archive can be transformed into a full report in PDF format with the desktop application. This does not require any additional data capture.

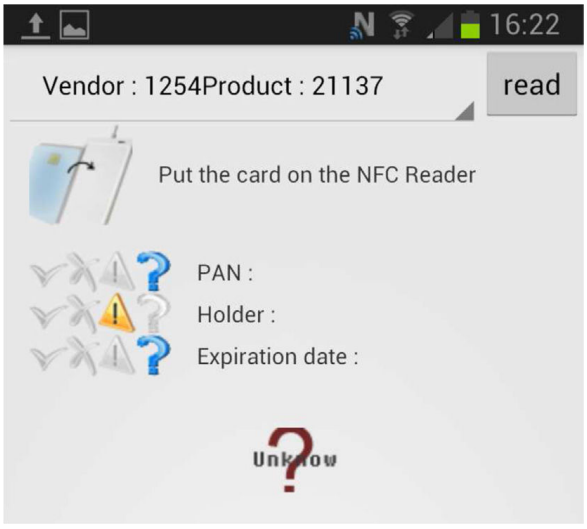


Fig. 16. Contactless data acquisition: choice between smart phone NFC embedded reader or OTG attached one.

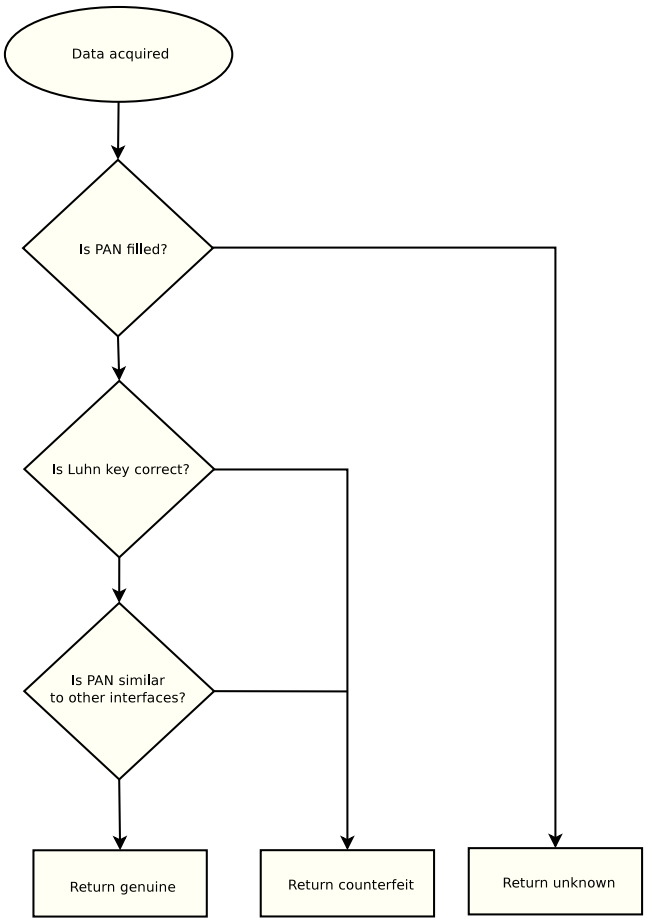


Fig. 17. Data extraction flow on the contact interface.

Discussion

This paper addressed card reuse fraud only by providing methods and tools for law enforcement agencies to determine payment card data status and/or retrieve valuable information from them.

Payment card reuse fraud can only be possible if at first acquisition fraud already occurred. Even if is not within the scope of this current research, it is important to examine and improve solutions to prevent payment card data theft in an effort to tackle the whole fraud.

Current solution to prevent payment card data theft

Many solutions already exist to prevent payment card information from being stolen at every level of the payment process: issuer, cardholder, acquirer, merchant, etc.

Over the last decade, the main preventative measures have come from the PCI Security Standards which issues physical and logical requirements for either proximity or online payments. These requirements include the usage of encryption and tamperproof mechanisms to prevent illegal access and usage of gathered data.

However, these security countermeasures cannot prevent criminals from stealing payment card data from the cardholder himself/herself, by way of stealing cards, phishing, or using portable skimmers. Advanced payment solutions have been developed to enforce cardholder presence at the time of card use. Even if they dramatically reduce online fraud, strong authentication solutions based on token, password or text message, such as 3DSecure, Verified by Visa, MasterCard SecureCode, still suffer from social engineering and mobile malware vulnerabilities.

Proposed solution to prevent payment card data theft

An upcoming European solution to prevent skimmer/carding issues is geoblocking which consists of blocking any payment made out of an authorised geographic area (e.g. country). Another technique, that can be seen as the first step to removing the magnetic stripe, seems to have had great results in countries such as the Netherlands and Slovenia and initial figures would be very interesting to analyse.

Finally, a better solution to monitor card related crimes would be to require all stakeholders, including banks, citizens, payment schemes, terminal manufacturers, and police, work together within an alert and fraud prevention network. This would be an efficient solution to share resources usually dedicated to preventing, identifying and fighting crimes.

Conclusion

At approximately 1.5 billion euro per year, payment card fraud is an attractive field for organised criminal groups. Fighting this crime is a challenging issue for law enforcement agencies that have to investigate online and in the field. They also have to develop new methods to analyse and keep up with the ever-changing techniques of innovative fraudsters.

Detecting counterfeit cards is one of the challenges that sometimes have to be performed by first responders. In this article we proposed some methods to extract and analyse data from payment cards. We also proposed two tools, a desktop one and a mobile alternative, to assist non specialised investigators in their duties.

First results and current development

Initial beta test feedback reveals that such an application is a global need for investigators who, up to now, were using some old fashioned, non-forensic, techniques, like doing a micro payment at a local store in order to get the magnetic stripe details from the merchant receipt.

While beta testers were first interested by the counterfeit card detection feature, most of them also showed high interest in accessing cards' transaction logs, when available.

Current developments of interest consist of integrating payment scheme directories into a law enforcement restricted version of our application. The report generated by this version would instantly communicate the fraud service details to the issuer if available.

Future developments

The next challenges will be to get these tools distributed and maintained. In terms of the maintenance issue, the

tools will be released as open source (except law enforcement restricted features) on the future Europol development platform. Such a distribution will enable large scale review and possible adoption by the majority of European police forces.

As smart cards have become more and more widespread embedded systems, their analysis is increasingly valuable for the investigation. Future developments could consist of expanding these methods and tools to other card applications such as transportation, loyalty and petroleum.

Ultimately, these applications have been developed with a modular and "next fraud ready" intent. With the possibility for easy EU global adoption, due to free software distribution and low cost readers, they could represent an innovative major incident response vector in the event of an emerging global fraud threat.

Acknowledgements

The authors would like to thank the proofreaders, especially Dan Embury from the Royal Canadian Mounted Police (RCMP) and Johan van Heerden from the South African Police Service, for their appreciated support to publish this article.

References

American National Standards Institute. Issuer identification number (iin) [online; last seen on 2014/02/20]; 2014.

M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, R. Anderson, Chip and skim: cloning emv cards with the pre-play attack, 35th IEEE Symposium on Security and Privacy, 2014.

Comité Consultatif du Secteur Financier. L'utilisation du chèque en France. Tech. rep; 2011.

EMV book D. emv contactless specifications for payment systems, book d: contactless communication protocol; 2013.

EMV book 1. emv integrated circuit card specification for payment systems, book 1: application independent icc to terminal interface requirements; 2011.

EMV book 2. emv integrated circuit card specification for payment systems, book 2: security and key management; 2011.

EMV book 3. emv integrated circuit card specification for payment systems, book 3: application specification; 2011.

EMV book 4. emv integrated circuit card specification for payment systems, book 4: cardholder, attendant and acquirer interface requirements; 2011.

Europol. Payment card fraud in the European Union. Tech. rep; 2012.

Eurosmart, figures; november 2013.

Gartner. Gartner says smartphone sales accounted for 55 percent of overall mobile phone sales in third quarter of 2013 [online; last seen on 2014/02/08]; november 2013. URL, http://www.gartner.com/newsroom/id/2623415.

Guo H, Jin B. Forensic analysis of skimming devices for credit fraud detection. In: Information and Financial Engineering (ICIFE), 2010 2nd IEEE International Conference on, IEEE; 2010. pp. 542–6.

INTECO. Dnie droid 1.0 api [online; last seen on 2014/02/08]; 2012. URL, http://zonatic.usatudni.es/dniedroid/api/.

International Organization for Standardization. Identification cards, recording technique, part 1: embossing. ref. no. iso 7811:2002; 2002.

International Organization for Standardization. Identification cards, recording technique, part 2: identification cards recording technique. ref. no. iso 7811:2002; 2002.

International Organization for Standardization. Identification cards, identification of issuers, part 2: application and registration procedures. ref. no. iso 7816:2004; 2004.

International Organization for Standardization. Identification cards, identification of issuers, part 1: Numbering system. ref. no. iso 7812:2006; 2006.

International Organization for Standardization. Indentification cards, financial transaction cards. ref. no. iso 7813:2006; 2006.

International Organization for Standardization. Identification cards, recording technique, part 6: magnetic stripe – high coercity. ref. no. iso 7811:2008; 2008.

International Organization for Standardization. Identification cards, recording technique, part 7: magnetic stripe – high coercity, high density. ref. no. iso 7811:2008; 2008.

Levick R. Mastercard vs. target: is there a data security war ahead?; february 2014.

Mastercard. Paypass – m/chip requirements; 2011.

Masters G, Turner P. Forensic data recovery and examination of magnetic swipe card cloning devices. Digit Investig 2007;4:16–22.

Murdoch SJ. Reliability of chip & pin evidence in banking disputes. Digital Evidence & Elec Signature L Rev 2009;6:98.

Murdoch SJ, Drimer S, Anderson R, Bond M. Chip and pin is broken. In: Security and Privacy (SP), 2010 IEEE Symposium on. IEEE; 2010. pp. 433–46.

sasc. Java emv reader/terminal [online; last seen on 2014/02/20]; 2012. URL, https://code.google.com/p/javaemvreader/.

Souvignet T, Frinken J. Differential power analysis as a digital forensic tool. Forensic Science International 2013;230(13):127–36 {EAFS} 2012 6th European Academy of Forensic Science Conference The Hague, 20-24 August 2012, http://dx.doi.org/10.1016/j.forsciint.2013.03.040. URL, http://www.sciencedirect.com/science/article/pii/S0379073813001965.

The UK Cards Association. Annual report 2014. Tech. rep.; 2014

C Case study: From embedded system analysis to embedded system based investigator tools

Digital Investigation 11 (2014) 154–159

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Case study: From embedded system analysis to embedded system based investigator tools

T. Souvignet [a, b, *], T. Prüfer [c], J. Frinken [c], R. Kricsanowits [c]

[a] Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), Digital Forensics department (INL), 1 boulevard Théophile Sueur, 93110 Rosny-Sous-Bois, France
[b] PRES Sorbonne Universités – Université Panthéon-Assas Paris II, 12 place de Panthéon, 75005 Paris Cedex 05, France
[c] Kriminaltechnisches Institut (KTI) des Bundeskriminalamtes (BKA), Äppelallee 45, 65173 Wiesbaden, Germany

ARTICLE INFO

Article history:
Received 21 February 2014
Received in revised form 7 June 2014
Accepted 13 June 2014
Available online 5 July 2014

Keywords:
Skimming
Embedded systems
Payment card fraud
Forensic tools
Bluetooth forensics
Arduino
Android

ABSTRACT

Since mid-2012, France and Germany have had to deal with a new form of payment card skimming. This fraud consists of adding a wireless embedded system into a point-of-sale payment terminal with the fraudulent goal of collecting payment card data and personal identification numbers (PIN).
This case study details the strategy adopted to conduct the digital forensic examination of these skimmers. Advanced technologies and analyses were necessary to reveal the skimmed data and provide useful information to investigators for their cross-case analysis.
To go further than a typical digital forensic examination, developments based on embedded systems were made to help investigators find compromised payment terminals and identify criminals.
Finally, this case study provides possible reactive and proactive new roles for forensic experts in combating payment card fraud.

© 2014 Elsevier Ltd. All rights reserved.

Introduction

Europol estimates payment card fraud proceeds of approximately 1.5 billion euros per year (Europol, 2012). This fraud is thus a profitable means for organised crime groups that invest in technical skills to enhance their modus operandi and increase their rewards.

One of the types of payment card fraud is skimming, with the aim of collecting payment card data contained in the magnetic stripe and PIN codes despite cardholder vigilance. Technically speaking, skimming is based on purpose built embedded systems, called skimmers, which are designed to collect several analog signals from the standard magnetic read head, as well as video record PIN entry surreptitiously.

Over the last few years, experts in France and Germany have seen the evolution of skimmer internals from raw signal storage to state-of-the art encryption usage (Souvignet and Frinken, 2013). Forensic analysis techniques have had to follow that evolution, resulting in advanced analysis methods that are currently in place.

In order to fully demonstrate the complexity of a basic embedded system analysis, this case study first describes the strategy adopted to analyse a new type of skimming fraud based on manipulated point-of-sale (POS) payment terminals. Further efforts by police researchers to develop embedded systems to counter the criminal efforts are explained, with the goal of assisting investigators in detecting fraudulent activities to help tackle this lucrative fraud.

* Corresponding author. Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), Digital Forensics department (INL), 1 boulevard Théophile Sueur, 93110 Rosny-Sous-Bois, France.
E-mail addresses: thomas@souvignet.net, thomas.souvignet@gendarmerie.interieur.gouv.fr (T. Souvignet), thomas.pruefer@bka.bund.de (T. Prüfer), juergen.frinken@bka.bund.de (J. Frinken), ralf.kricsanowits@bka.bund.de (R. Kricsanowits).

http://dx.doi.org/10.1016/j.diin.2014.06.004
1742-2876/© 2014 Elsevier Ltd. All rights reserved.

As some investigations and court trials may still be ongoing, only the minimal information necessary to illustrate the case study will be disclosed, with some data anonymised for confidentiality.

Context

In mid-2012, French investigators had to face a new form of skimming as POS payment terminals were manipulated by inserting an electronic system (Le Parisien, 2013). It was believed that Germany was also targeted by this fraud; however, German investigators had already faced a similar type of fraud in the past (NDR 1, 2013).

Differences in POS terminal fraud between countries can easily be explained by comparing national payment scheme regulations. In France, all payment acquirers must comply with Anti Fishing-Anti Skimming (AFAS) standards imposed by Cartes Bancaires, the French national system. Cartes Bancaires requires POS terminals to use separate insertion slots for magnetic stripe and smartcard chip payments. Combined with the requirement to prevent full insertion of the card while managing chip payments, the French standard tends to prevent skimming involving an illegitimate magnetic reading head on POS terminals. Such requirements seem to not be in place in Germany where all-in-one slot POS terminals are widespread.

The fraud involved modifying POS terminals of various models to add an internal integrated circuit (IC) and installing them in stores by eluding the vigilance of the cashier vigilance. This skimmer circuitry consisted of an additional magnetic read head, the IC connectors, the genuine magnetic read head and some data lines of the terminal, all powered by the terminal power supply itself. Finally, as shown in Fig. 1, the French version of the skimming device required an extension of the legitimate insertion slot to bypass the aforementioned AFAS security mechanisms.

Both French Gendarmerie Nationale Forensic Laboratory (IRCGN) and German Forensic Science Institute (BKA/KT) were asked to conduct the forensic analysis of these fraud related exhibits.

Strategy

The strategy adopted by both agencies was quite traditional. Fully developed in Souvignet and Frinken (2013), it consisted of three stages: black box analysis, white box analysis, and stored data analysis based on the two previous results.

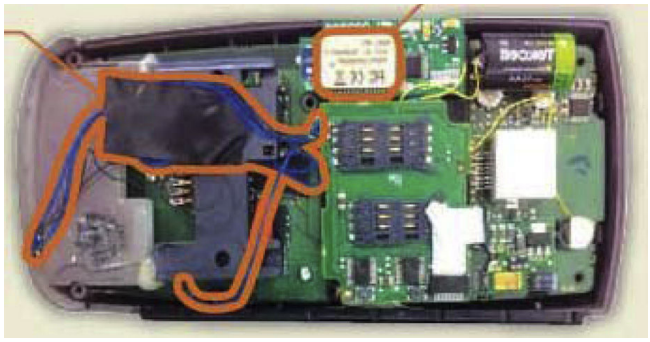


Fig. 1. Skimmer within the manipulated payment terminal (source: Le Parisien, 2013).

Black box analysis

First, the skimmer board was analysed to understand its design and the data stored in the flash memory was checked to determine if it was stored in plaintext or encoded/encrypted.

Visual analysis of the printed circuit board indicated that the skimmer was designed using the following components:

- magnetic read heads,
- double frequency phase coherence (F/2F)[1] application specific intergrated circuit (ASIC) decoder,
- microcontroller (Atmel ATMega640),
- flash memory,
- Bluetooth module (Roving Networks RN41).

This design implied that data storage would be in 7-bit (track 1) or 5-bit (track 2) ISO format and data collection would be completed wirelessly. The researchers were able to collect data wirelessly by providing the default PIN of 1234, as well as read the flash memory directly. Both datasets were found to be identical, indicating that no data manipulation was performed prior to transmitting over the Bluetooth serial interface.

Stored data analysis, however, did not reveal 7-bit or 5-bit ISO formatted data. Further statistical analysis indicated that the data was equally distributed, indicating that encryption was used. Deeper analysis of the encrypted data, particularly redundant areas, indicated that 128-bit electronic codebook encryption (EBC) was used.

White box analysis

Using the process described in (Souvignet and Frinken, 2013), the ATMega640 microcontroller was deprotected using focused ion beam (FIB) (Fig. 2) in order to gain access to the protected assembly program code in the exhibit.

The Atmel AVR assembly code was examined using IDA Pro, ultimately allowing for the identification of the encryption routine. It was found that the encryption used some AES-like substitution and mix columns subroutines, but no known AES constants were found and only three rounds were processed.

The encryption algorithm was then reproduced with a custom Python script and checked with plaintext/ciphertext samples that were produced by simulating the assembly code running within the AVR Studio Simulator. Once the encryption algorithm was verified, it was then possible to successfully design the decryption algorithm and the necessary Python script.

In order to retrieve the last paired Bluetooth devices, the Roving Networks RN41 Bluetooth Module was also

[1] Encoding used for storing data within magnetic tracks.

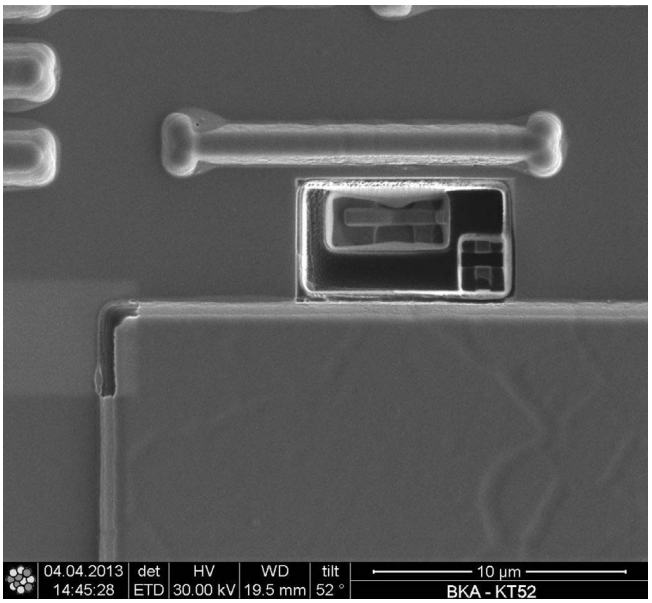


Fig. 2. POS skimmer microcontroller FIB modification showing one new conductor created and one conductor cut.

reversed engineered since the datasheet (Roving Networks, 2013) indicated that an external flash memory device was incorporated. Once the Bluetooth module shield was decapsulated, a ball grid array (BGA) flash memory package was effectively found and successfully read. A raw search for known paired media access control (MAC) addresses on a populated reference test device allowed for the identification of a data zone where the module life was recorded. After a quick tag-length-value (TLV) storage format reversal, it was then possible to extract most actions that occurred with the analysed module, including MAC address setting, PIN/name changes, and Bluetooth pairing activities.

Data analysis

Following the black and white box analyses, it was possible to extract most of the information from the encrypted Bluetooth-based skimmer.

Applying the Python decryption script to the flash memory data extracted from the exhibit revealed numerous structured records that followed a simple format consisting of the following repeating pattern: timestamp, record type, length, value, timestamp. The nature of the record was then easily recognisable using the record type value. Several record types were found, including the PIN entry that was collected from data line tapping, digital magstripe data decoded from the F/2F data, analog magstripe data, and IC log data.

Bluetooth module analysis of several different exhibits revealed some common name changing, some individual PIN changing, and similar MAC pairings.

Following the three stages of analysis, the forensic data examination was considered complete and the most relevant information was provided to the investigators. Specifically, the skimmed data, including card details and PINs, and MAC information of the suspected perpetrators were provided for further analysis and corroboration with other evidence.

Challenges

In parallel with the lab examination conducted jointly with the BKA, the IRCGN was also tasked by the investigators in charge to assist with the actual case investigation.

After having been educated about the underlying technical principles, the investigators had to face several challenges while investigating this unusual fraud. These challenges were mostly centred around three types of questions: Where? When? How?

Where were the manipulated POS terminals installed? Unlike automated teller machine (ATM) skimmers, these skimmers were self-powered and the skimmed data was remotely collectable, so they could stay in place longer, virtually undetectable.

If some were found, when could it be expected for the criminals to come and collect the data? A 24/7 surveillance operation would have been quite expensive and unreliable since it may have been difficult to distinguish between a legitimate smartphone/computer user and a possible suspect within a shop.

Finally, if someone was arrested, how can he or she be linked to the actual skimmers in order to lay charges? Material evidence would be needed in such a case since the suspects would likely not provide self-incriminating evidence.

To assist the investigators in overcoming these challenges, the IRCGN researcher provided a custom developed tool based on embedded systems, namely an Android smartphone application and an Arduino development board.

Where?

To solve the skimmer location problem, an immediate mechanical solution was first advised to check if the payment card was inserted deeper into the POS than usual; however, this solution would have required a manual check of every POS terminal that would have been a long and tedious task if an entire shopping mall needed to be checked. Moreover, this suggestion would have only been effective on the French type of POS terminal that required the insertion slot modification.

To provide an easy, efficient and durable solution, the IRCGN researcher developed and distributed an Android application (Fig. 3) with the goal of detecting Bluetooth-based skimmers.

The detection application monitors Bluetooth broadcasting messages that provide the MAC address and name of a discoverable device, without any interaction with the device. Based on the black box analysis, the researchers determined the crucial characteristics of the skimmers that need to be identified to detect potentially manipulated payment terminals. To this end, the application user would be provided with detailed location information showing the signal strength, as well as alerts in the form of: visual (displayed first, in red), auditory (optional alarm) and tactile (vibration) feedback. Another useful feature of this simple application would provide an optional permanent search that could allow for scanning a full shopping centre

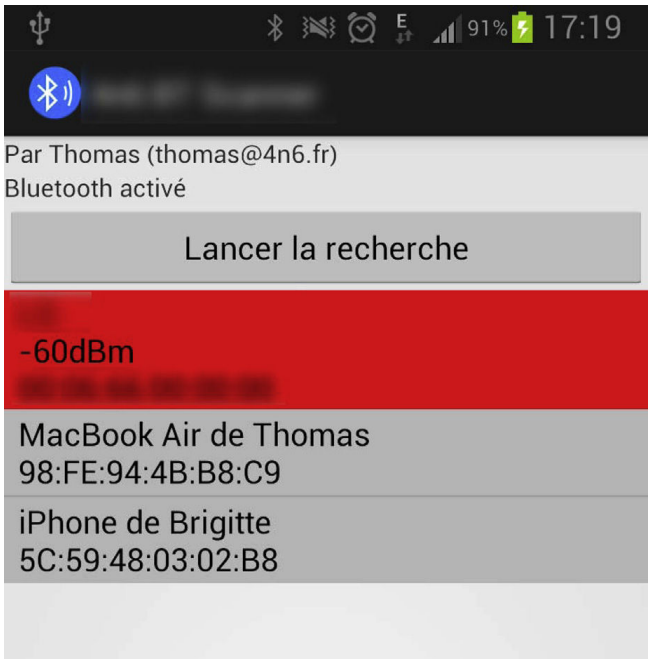


Fig. 3. Android Bluetooth detection application.

at once, while most Bluetooth discovery apps stop after a few seconds.

Download and usage details of this app were shared with French and German investigators in charge of combating this type of digital crime. At the time of writing, approximately 1000 effective installations have been performed, with roughly 2/3 of the users being in France and 1/3 in Germany.

The effectiveness of the tool has been verified by the first author of this paper who successfully found seven manipulated POS terminals in his local area while conducting testing.

When?

While previous applications permitted finding skimmers within France and Germany, it remained difficult for investigators to predict when a criminal would come to collect the skimmed data.

A proposal was made to investigators to provide them with a system to detect the presence of the skimmer operator. Out of several solutions that could be used to attain such a goal, the first plan was to monitor Bluetooth traffic to detect connection attempts with the skimmer; however, due to the possible requirement to comply with French lawful interception regulations, it was decided to not intercept any traffic. Instead, another solution was designed based on an Arduino embedded system development board.

Rather than designing a solution based on monitoring traffic, the detection system was designed to receive this traffic. In fact, a simulator was created that replicated the behaviour of the original skimmer. By substituting the manipulated payment terminal for the simulated system, the criminal would unknowingly connect to it, triggering a Short Message Service (SMS) alert to the appropriate authorities.

The hardware was composed of an Arduino Android Development Kit (ADK), a Global System for Mobile communications (GSM) shield, and a Cambridge Silicon Radio (CSR) Bluetooth dongle (Fig, 4). To fully emulate the skimmer, the system needed to clone the skimmer Bluetooth parameters. Thus, an initial Arduino sketch program was designed to update the CSR Bluetooth MAC address using the proprietary CSR write command (Holtmann, 2004). Next, a second sketch, based on the Universal Serial Bus (USB) Host library for Arduino (Mazurov, 2013), provided the USB layers and Streaming Parallel Port (SPP) emulation which permitted the setting of the USB class and service name and, most importantly, the detection of connection requests.

As a result, the Bluetooth broadcasts of the simulated system looked like those of the original skimmer. When a criminal would have attempted to connect to the detection system, the connection would either fail to connect, since the PIN is not cloned and set to 1234, or would indeed connect but would fail to download the data, since this feature was not created. Regardless of the connection result, both would trigger an SMS alert providing the remote device name and its MAC address, as well as a timestamp from the SMS itself (cf. Fig. 5).

This type of detection system enhanced the opportunities for investigators since they could remotely identify criminal presence on site and possibly identify them on closed circuit television (CCTV) recordings. Moreover, if they were to respond rapidly enough, they could react to the alert and arrest the person trying to connect. Following the development of this solution, both scenarios were successfully realised by authorities using this tool.

How?

Finally, providing evidence against a suspected perpetrator would be no more complicated than the forensic analyses described previously. Bluetooth MAC addresses reported on SMS alerts and found on a smartphone or computer would allow investigators to conduct advanced cross analysis.

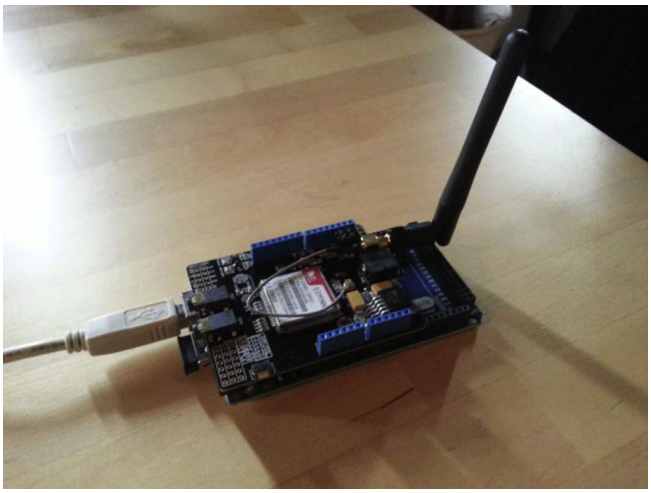


Fig. 4. Criminal detection system.

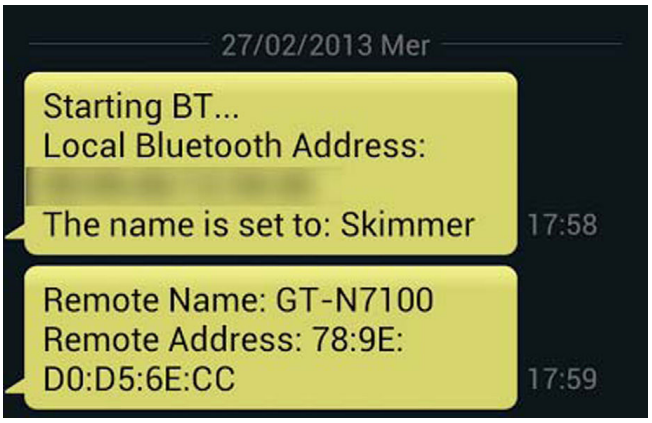


Fig. 5. SMS alert sample.

Even if the person was not immediately arrested, the SMS alert could help to identify him or her on CCTV recordings, as well as provide information about the potentially used Bluetooth equipment (e.g. GT-N7100 is the default name for a Samsung Galaxy Note II). Additional skimmers that might be analysed and found to have the same pairing information would essentially link the perpetrator to these as well.

Outcomes

Several outcomes could be drawn from this case. The first were related to embedded systems analysis while the others concerned the role of forensic experts within the judiciary process.

Embedded systems forensic analysis

The forensic analysis strategy that was applied to handle these payment terminal fraud exhibits, namely black box analysis, white box analysis and data analysis reinforced the fact that most embedded systems are not supported by commercial tools and require case-by-case analytic strategies to develop solutions.

In fact, generally only basic feature phones, smartphones, and standalone GPS devices are effectively supported by commercial forensics tools. As a result, all other embedded devices, such as automotive navigation systems, set top boxes, skimmers, industrial supervisory control and data acquisition (SCADA) systems, digital video recorders (DVRs), digital cameras, and personal video recorders require custom analysis and tools.

In most cases, when following the data extraction/data analysis model, these types of forensic analysis processes often require significant development and sample testing, as well as considerable investments in specialised equipment, such as the FIB that costs approximately 1 million, and state-of-the-art techniques, such as side channel attacks.

Embedded systems as forensic tools

As a result of this case study, custom developed embedded systems have been proven to be effective as forensics tools. In Souvignet et al. (2013), Arduino boards were previously used to develop an AES key retrieval tool using differential power analysis. Its simple usage required a minimal amount of technical skill.

In this case study, it was shown that working on embedded systems was not an exclusive privilege for experts, since the tools that were described were designed for field investigator use. With the results that have been demonstrated thus far, dozens of manipulated payment terminals have been discovered with the Android Bluetooth detection app, allowing for many perpetrators to be arrested. It is because of these successes that strong interest has been expressed by investigators for additional technical solutions to assist them in their daily work.

The role of forensic experts

The role of digital forensic experts within the investigation process is generally reduced to an after the fact laboratory analysis with an exhibit as the input and a formal report as the output.

This case study has demonstrated that even though this traditional role is important and valuable for the investigation process, digital forensic experts can also have an essential role while trying to understand the crime and develop novel investigation methods.

As shown in Fig. 6, digital forensic experts could be involved earlier in the process for unique cases, rather than remaining in the traditional role at the end of the investigation performing digital examination. A more valuable reactive role for the digital forensic expert earlier on in the investigation, where the expert learns from his or her examinations to improve results for the investigators, as well as develop novel crime detection techniques, is surely attainable.

In this case study, the new reactive role that was undertaken permitted the police officer in charge to not only fully understand the fraud, but also to be equipped with some novel and useful tools.

As a further extension, a more proactive role for digital forensic experts involving the proposal of security improvements and anti-fraud measures during standards definition and product design cycles could also be established in order to prevent the crime from being committed in the first place.

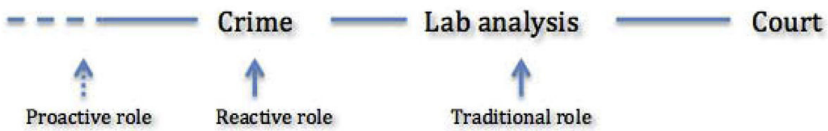


Fig. 6. Traditional vs. evolving roles of digital forensic experts.

Conclusion

Smart cards and payment terminals are now widely available across the full range of retail and commercial environments, demonstrating that embedded systems form the crucial basis of payment card systems. At the same time, embedded systems are also used in payment card fraud where skimmers are used to collect payment card details despite cardholder vigilance.

This case study has fully described a practical strategy to analyse modern skimmers with advanced encryption and Bluetooth communication abilities. Considerable efforts in hardware hacking, assembly code reverse engineering, and encryption reversal were necessary to process what was initially believed to be a rudimentary skimmer implementation.

Well beyond simple analysis, a novel yet complex solution using embedded systems, in the form of an Android application and an Arduino board, was constructed to help investigators in finding manipulated POS terminals and detecting criminal presence.

Finally, this case study should be taken as a solid proof of concept regarding other roles that digital forensic laboratory experts can assume. A reactive role is possible by technically assisting the investigator when the crime occurs, that is, detecting the crime based on their experience. A proactive role is also possible by integrating technical crime experts into the working groups responsible for the design of standards and security measures for embedded systems.

Following the excellent operational success of this case, members of the BKA and the IRCGN are continuing to strengthen their collaboration. Additionally, researchers from the IRCGN are currently developing some interesting new tools based on knowledge gained by assisting field investigators in a reactive manner.

Acknowledgements

The authors would like to thank the proofreaders, especially Dan Embury from the Royal Canadian Mounted Police (RCMP), for their appreciated support to publish this article.

References

Europol. Payment card fraud in the European union. Tech. rep.; 2012

Holtmann M. Bluez – bdaddr.c sources; 2004 [online; last seen on 2014/02/08].

Le Parisien. L'imparable escroquerie à la carte bancaire; January 2013.

Mazurov O. Usb host shield 2.0; 2013 [online; last seen on 2014/02/08].

NDR 1. Skimming: Hunderte kunden abgezockt; April 2013.

Roving Networks. Rn41/rn41n class 1 bluetooth module; 2013.

Souvignet T, Frinken J. Differential power analysis as a digital forensic tool. Forensic Science International 2013;230(13):127–36. EAFS 2012 6th European Academy of Forensic Science Conference The Hague, 20–24 August 2012, http://dx.doi.org/10.1016/j.forsciint.2013.03.040. URL, http://www.sciencedirect.com/science/article/pii/S0379073813001965.

Bibliographie

[1] Ross Anderson : Why cryptosystems fail. *In Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 215–227. ACM, 1993.

[2] Association francophone des spécialistes de l'investigation numérique : Satuts de l'afsin. https://www.afsin.org/statuts/. Dernière consultation : octobre 2013.

[3] Autorité de la Concurrence : Décision n°13-d-17 du 20 septembre 2013 relative à des pratiques de mastercard relevé es dans le secteur des cartes de paiement, septembre 2013.

[4] Autorité de la Concurrence : Décision n°13-d-18 du 20 septembre 2013 relative à des pratiques de visa relevé es dans le secteur des cartes de paiement, septembre 2013.

[5] Banque Populaire Lorraine Champagne : Conditions générales de fonctionnement des cartes cb, décembre 2010.

[6] Mike Bond, Omar Choudary, Steven J Murdoch, Sergei Skorobogatov et Ross Anderson : Chip and skim: cloning emv cards with the pre-play attack. *arXiv preprint arXiv:1209.2531*, 2012.

[7] botnets.fr : Banking - botnets. en ligne ; https://www.botnets.fr/index.php/Banking, mai 2012.

[8] Boursorama Banque : Conditions générales, février 2013.

[9] British Broadcasting Corporation (BBC) : Trojan virus steals banking info. en ligne ; http://news.bbc.co.uk/2/hi/technology/7701227.stm, octobre 2008.

[10] Charles Brookson, Graham Farrell, Jen Mailley, Shaun Whitehead et Dionisio Zumerle : Ict product proofing against crime. Rapport technique, European Telecommunications Standards Institute, février 2007.

[11] Cartes Bancaires : Adhésion au système de paiement par cartes bancaires cb "contrat commerçant" version automate de paiement en libre service, février 2007.

[12] Cartes Bancaires : Contrat d'acceptation en paiement de proximité des cartes "cb" ou agréées "cb", novembre 2009.

[13] Cartes Bancaires : Commissions interbancaires : l'autorité de la concurrence accepte les engagements proposés par le groupement des cartes bancaires cb. Communiqué de presse, juillet 2011.

[14] Mathiot Cédric : Stats de la délinquance : l ?intox illustr'ee par la carte bancaire. en ligne ; http://desintox.blogs.liberation.fr/blog/2011/10/lexemple-des-fraudes-aux-cartes-bancaires.html, octobre 2011.

[15] Isabelle Chaperon : La guerre des porte-monnaie virtuels. en ligne ; http://abonnes.lemonde.fr/economie/article/2014/04/20/la-guerre-des-porte-monnaie-virtuels_4404469_3234.html, avril 2014.

[16] Julia S. Cheney : Heartland payment systems: Lessons learned from a data breach. en ligne ; http://www.phil.frb.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2010/d-2010-january-heartland-payment-systems.pdf, janvier 2010.

[17] Caroline Desoubrie : Le skimming : Vers une stratégie européenne de lutte contre la criminalité organisée. Mémoire de D.E.A., Université de Strasbourg, 2013.

[18] EMVCo : Emv integrated circuit card specification for payment systems, book 2: Security and key management, novembre 2011. version 4.3.

[19] EMVCo : Emv integrated circuit card specification for payment systems, book 3: Application specification, novembre 2011. version 4.3.

[20] Mélanie Eudes : Le renseignement criminel : une approche pour lutter contre la cybercriminalité - le cas de la fraude aux cartes bancaires. conférence ; sixième journée d'échanges et de formation en informatique légale, septembre 2014. Assistante-Doctorante, Institut de Police Scientifique, Ecole des Sciences Criminelles, Université de Lausanne.

[21] European Central Bank : Payment statistics for 2012. en ligne ; http://www.ecb.europa.eu/press/pr/date/2013/html/pr130910.en.html, septembre 2013.

[22] European Central Bank : Third report on card fraud, février 2014.

[23] European Payments Council : Book 3 - data elements - sepa cards standardisation volume version 7.0, janvier 2014.

[24] European Telecommunications Standards Institute : Lawful interception. http://www.etsi.org/index.php/technologies-clusters/technologies/security/lawful-interception. Dernière consultation : octobre 2013.

[25] Europol : The internet organised crime threat assessment (iocta). en ligne ; https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-ioctas, septembre 2014.

[26] Eurosmart : Figures, novembre 2013.

[27] Fédération bancaire française : Banque de détail en france, juillet 2014.

[28] Financial Fraud Action UK : Fraud the facts 2014, février 2014.

[29] Eric Freyssinet et Jean-Yves Marion : Les botnets : découverte, investigation. conférence ; Journées Francophones de l'Investigation Numérique, octobre 2014.

[30] Jürgen Frinken : Projektbericht: "fuses". Rapport technique, BKA, 2007.

[31] John L. Gropper : Credit verifying unit, novembre 1969. Brevet US 3800283.

[32] Groupe de travail interministériel sur la lutte contre la cybercriminalité : Protéger les internautes - rapport sur la cybercriminalité. en ligne ; http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf, février 2014.

[33] Groupement des Cartes Bancaires : Rapport d'activité du groupement des cartes bancaires 2011. Rapport technique, Groupement des Cartes Bancaires, 2012.

[34] Hong Guo et Bo Jin : Forensic analysis of skimming devices for credit fraud detection. *In Information and Financial Engineering (ICIFE), 2010 2nd IEEE International Conference on*, pages 542–546. IEEE, 2010.

[35] Heartland Payment Systems : Letter to heartland merchants and prospects. archive en ligne ; http://web.archive.org/web/20090327154323/http://www.2008breach.com/, mars 2009.

[36] Tadao Inoyama, Kiichi Aomori et Hidekazu Terai : Automatic transaction equipment, mars 1978. Brevet GB2025106A.

[37] Kaspersky Lab : The evolution of phising attacks: 2011-2013. en ligne ; http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011-2013.pdf, juin 2013.

[38] Tracy Kitten : Global breach date now jan. 2011. en ligne ; http://www.bankinfosecurity.com/global-breach-date-now-jan-2011-a-4772, mai 2012.

[39] P. Kocher, J. Jaffe et B. Jun : Introduction to differential power analysis and related attacks, 1998.

[40] P. Kocher, J. Jaffe et B. Jun : Differential power analysis. *In Advances in Cryptology - Processings of Crypto '99*, pages 789–789. Springer, 1999.

[41] Brian Krebs : Banks: Credit card breach at home depot. en ligne ; http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot, septembre 2014.

[42] Brian Krebs : Spike in malware attacks on aging atms. en ligne ; http://krebsonsecurity.com/2014/10/spike-in-malware-attacks-on-aging-atms, ocotobre 2014.

[43] Le Parisien : L´imparable escroquerie à la carte bancaire, janvier 2012.

[44] Le Parisien : L´habile arnaque aux boîtiers de cartes bancaires. en ligne ; http://www.leparisien.fr/espace-premium/actu/l-habile-arnaque-aux-01-07-2013-2942939.php, juillet 2013.

[45] S. Mangard, E. Oswald et T. Popp : *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science, 2007.

[46] MasterCard Worlwide : History of the card payments system. en ligne ; http://www.mastercard.com/us/company/en/docs/History_%20of_payments.pdf, 2014.

[47] Gerry Masters et Philip Turner : Forensic data recovery and examination of magnetic swipe card cloning devices. *digital investigation*, 4:16–22, 2007.

[48] Steven J Murdoch, Saar Drimer, Ross Anderson et Mike Bond : Chip and pin is broken. *In Security and Privacy (SP), 2010 IEEE Symposium on*, pages 433–446. IEEE, 2010.

[49] MWR Labs : Pinpadpwn. Black Hat 2012, juillet 2012.

[50] Observatoire de la Sécurité des Cartes de Paiement : Rapport annuel de l'observatoire de la securité des cartes de paiement 2012. Rapport technique, Banque de France, 2013.

[51] Observatoire de la Sécurité des Cartes de Paiement : Rapport annuel de 2013 de l'observatoire de la sécurité des cartes de paiement. Rapport technique, Banque de France, juillet 2014.

[52] Ouest France : Trois personnes écrouées pour piratage de terminaux bancaire. en ligne ; http://www.ouest-france.fr/ofdernmin_-Trois-personnes-ecrouees-pour-piratage-de-terminaux-bancaire_6346-2176770-fils-tous_filDMA.Htm, mars 2013.

[53] Payment Card Industry (PCI) : Exigences de sécurité des pin, septembre 2011.

[54] Planet Monetic : Mise à jour cbemv bulletin 13. http://www.terminal-de-paiement.eu/9-non-categorise/113-mise-a-jour-bulletin-13.html, février 2013.

[55] SANS Institute : Pci dss and incident handling: What is required before, during and after an incident. en ligne ; http://www.sans.org/reading-room/whitepapers/compliance/pci-dss-incident-handling-required-before-incident-33119, février 2009.

[56] Seculert : Dexter - draining blood out of point of sales | seculert blog on advanced threats and cyber security. en ligne ; http://www.seculert.com/blog/2012/12/dexter-draining-blood-out-of-point-of-sales.html, décembre 2012.

[57] S. Sellami et C. Sterlé : L´ingénieux système des escrocs à la carte bancaire. Le Parisien, avril 2013.

[58] Stan Sienkiewicz : Credit cards and payment efficiency. en ligne ; http://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2001/paymentefficiency_092001.pdf, aout 2001.

[59] signal spam : Baromètre du spam avril/mai/juin 2014. en ligne ; https://www.signal-spam.fr/sites/default/files/Barom%C3%A8tre%20Signal%20Spam%20T2%202014.pdf, juilet 2014.

[60] Sony Computer Entertainment America : Kazuo hirai's letter to the u.s. house of representatives. en ligne ; https://www.flickr.com/photos/playstationblog/sets/72157626521862165/, mai 2011.

[61] Faure Sonya et Fansten Emmanuel : Le parquet doit s'adapter à la cybercriminalité. en ligne ; http://www.liberation.fr/societe/2014/08/31/le-parquet-doit-s-adapter-a-la-cybercriminalite_1090892, septembre 2014.

[62] Thomas Souvignet et Jürgen Frinken : Bka-gendarmerie cooperation in digital forensics: non-invasive solution to retrieve aes encryption keys. EAFS 2012 - 6th European Academy of Forensic Science Conference, août 2012.

[63] The ATM Security Team : European atm crime report 2014, octobre 2014.

[64] The Oriental Daily : Infection virale par un groupe criminel hi-tech (traduction du mandarin). en ligne ; http://orientaldaily.on.cc/cnt/news/20140529/00176_012.html, mai 2014.

[65] Trend Micro : New blackpos malware emerges in the wild, targets retail accounts. en ligne ; http://blog.trendmicro.com/trendlabs-security-intelligence/new-blackpos-malware-emerges-in-the-wild-targets-retail-accounts/, aout 2014.

[66] United States District Court of New Jersey : Indictment. archive en ligne ; http://www.wired.com/images_blogs/threatlevel/2009/08/gonzalez.pdf, 2009.

[67] Visa Corporate : History of visa. en ligne ; http://usa.visa.com/about-visa/our-business/history-of-visa.jsp, 2014.

L'expertise et la lutte contre la fraude monétique

Le montant annuel de la fraude européenne à la carte de paiement se monte à plus d'1,5 milliard d'euros. Cette manne aiguise l'appétit des groupes criminels qui exploitent la moindre faille de la monétique (écosystème de la carte de paiement).
Les cinq principaux acteurs de la monétique (porteurs, émetteurs, accepteurs, acquéreurs et systèmes de paiement) s'appuient pourtant sur des systèmes et réseaux normalisés dont la sécurité est encadrée par des standards internationaux contraignants. Néanmoins, la fraude monétique ne cesse de progresser alors que les moyens de lutte (étatiques, collaboratifs ou individuels) restent limités.
Après étude de la fraude monétique, cette thèse propose différentes actions (passives, réactives et proactives) visant à améliorer la lutte contre la fraude monétique. D'abord, il convient de mieux connaître la fraude en étudiant la provenance des données volées et plus seulement leur usage. Ensuite l'expertise de ces fraudes doit être améliorée, en développant par exemple une captation du progrès scientifique. Une expertise qui doit être en partie transmise aux enquêteurs afin qu'ils puissent conduire leurs enquêtes. Enquêtes qui peuvent être dynamisées par des opérations réactives associant investigateurs et sachants techniques. Enfin, de manière proactive, les enquêtes et analyses de demain doivent être facilitées par les technologies monétiques conçues aujourd'hui.

Descripteurs :
Fraude monétique, Terminaux, Carte de paiement, Expertise , Enquête, Cybercriminalité, Outils criminalitisques

---

Solid forensic assessment and the fight against payment card fraud

Every year, payment card fraud exceeds 1.5 billion euros in Europe. Organised crime groups are exploiting any vulnerability possible to take a piece of this lucrative activity.
Even though the five principal entities in the payment card industry (cardholders, issuers, acceptors, acquirers and payment system providers) are implementing binding security measures throughout standardized systems and networks, fraud continues to increase. Efforts by the state, industry collaboration, and individuals have been unsuccessful in decreasing criminal advances.
Having analysed the elements of payment card fraud, this thesis proposes several actions (passive, reactive and proactive) to help improve the fight against this fraud. First, it is relevant to gain knowledge of the source of the card details and not to focus only on its reuse. Next, forensic assessment has to be improved, for example by developing an increased scientific understanding of the technology. Such an expertise should then be passed on to investigators through effective training and knowledge transfer. Investigations should also be made more dynamic with reactive operations conducted in concert by investigators and technicians. Finally, in an ideal proactive spirit, future investigations and assessments should be oriented and facilitated by studying and influencing current payment card technology developments.

Keywords:
Payment card industry, Terminals, Payment card, Forensic assessment, Investigation, Cybercrime, Forensic tools