Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

وزارة التعليم العالي والبحث العلمي

BADJI MOKHTAR – ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR – ANNABA

جامعــة باجي مختار – عنابة

Faculté des Sciences de l'Ingéniorat

Année : 2019/2020

Département d'Informatique

THÈSE

Présentée en vue de l'obtention du diplôme de

Doctorat en Sciences

Sécurité et optimisation des applications NFC

Filière : Informatique

Option : Informatique Embarquée (INEM)

Par **CHABBI Samir**

Devant le jury :

Qualité	Nom & Prénom		Grade	Affiliation
Président	GHANEMI	Salim	Professeur	Université Badji Mokhtar – Annaba
Directeur	BOUDOUR	Rachid	Professeur	Université Badji Mokhtar – Annaba
Co-directeur	SEMCHEDDINE	Fouzi	Professeur	Université de Setif
Examinateur	KIMOUR	Med Tahar	Professeur	Université Badji Mokhtar – Annaba
Examinateur	REDJIMI	Mohamed	Professeur	Université du 20 Août 1955 – Skikda
Examinateur	BOURAS	Zineddine	MCA	ESTI – Annaba

Dédicaces

À ma chère mère ;

À ma femme ;

À mes enfants ;

Au père de ma femme à sa mère ;

À toute la famille de ses frères et sœurs ;

À mes frères et leur famille et à ma sœur et sa famille ;

À toute ma famille ;

À tous mes amis ;

À tous ceux qui me sont chers ;

Remerciements

Mes remerciements les plus sincères et les plus chaleureuses s'adressent en premier lieu à mes directeurs de thèse monsieur BOUDOUR Rachid, Professeur à l'Université Badji Mokhtar – Annaba et monsieur SEMCHEDINE Fouzi, Professeur à l'Université de Setif, pour m'avoir confié ce travail de recherche, pour leur gentillesse, leur disponibilité ainsi que leurs précieux conseils tout au long de ces années de doctorat.

Je tiens à exprimer toute ma reconnaissance et mon profond respect à monsieur GHANEMI Salim, Professeur à l'Université Badji Mokhtar – Annaba, qui m'a fait l'honneur de présider le jury de thèse. J'adresse aussi mes sincères remerciements aux membres de jury, monsieur KIMOUR Med Tahar, Professeur à l'Université Badji Mokhtar – Annaba, monsieur REDJIMI Mohamed, Professeur à l'Université du 20 Août 1955 – Skikda et monsieur BOURAS Zineddine MCA à l'ESTI – Annaba d'avoir bien voulu examiner et juger ce travail.

Je témoigne ici ma profonde gratitude et mes vifs remerciements à monsieur CHAFROUR Djalel pour son aide précieux.

الملخص

لقد خضعت تقنيات الاتصال بدون تلامس وبشكل أساسي RFID (تحديد ترددات الراديو) و NFC (اتصالات المجال القريب) لتطورات سريعة في السنوات الأخيرة. لقد تم استخدامها في العديد من التطبيقات ، مثل الحساب و الشراء الإلكتروني, إدارة المفاتيح, حجز التذاكر (النقل والترفيه), قراءة المعلومات (في مجال النقل, تسيير المخزن والطب) ,التحكم في المرور, بطاقة العمل الإلكترونية وما إلى ذلك.

ومع ذلك ، فإن استخدام هذه التقنيات يطرح مشاكل أمنية, و على وجه الخصوص بالنسبة للدفع الإلكتروني باستخدام آلة الصراف الآلي (ATM) أو نقطة بيع و تسمى أيضًاPOS . يجب حماية أمن الاتصالات الذي يتطلب التحقق من ثلاثة خصائص أساسية ، وهي مصادقة الأطراف المتصلة, سلامة البيانات وسريتها ، ضد التهديدات والهجمات الكبيرة (مثل: هجوم الترحيل ، رفض و منع الخدمة ، الرجل في الوسط ، وما إلى ذلك) من أجل ضمان حماية البيانات الشخصية الحساسة للغاية وبالتالي حماية خصوصيتها.

وتتميز أجهزة RFID و NFC المستخدمة مثل العلامات والبطاقات الذكية المشغلة من غير تلامس بقيود من حيث الموارد (الذاكرة والطاقة وسعة الحوسبة وما إلى ذلك). تسجيل البيانات البيومترية على سبيل المثال على هذه الأجهزة يطرح مشكلة الحجم الكبير لهذه البيانات مقارنة بقدرات هذه الأجهزة.

وبالتالي ، تمت التوصية بالعديد من الأساليب والتقنيات والبروتوكولات وأيضًا حلول تستخدم الأجهزة لضمان أمن البيانات السرية ، من ناحية ، أثناء المعالجة المختلفة: التسجيل في أجهزة RFID أو NFC ، وذاكرة التسجيل ، أو أثناء التواصل مع قارئ RFID أو NFC من ناحية أخرى ، لرفع الأداء من حيث تكلفة المعالجة , تكلفة الإتصال ومساحة التخزين.

من بين الطرق الفعالة المستخدمة لضمان اتصالات RFID أو NFC آمنة وفعالة ، استخدام تقنيات كلمة المرور الذكية وبروتوكولات المصادقة البسيطة والآمنة والفعالة التي تستخدم دوال التجزئة البسيطة لتشفير البيانات المتبادلة.

تركز أطروحتنا على اقتراح طريقتين نحاول أن نثبت أنهما آمنان وفعالان ، هذان الطريقتان يستخدمان لضمان اتصال البيانات في الدفع الإلكتروني باستخدام الهاتف الذكي وجهازالصراف الآلي و المجهز كلاهما بتقنية NFC.

تقدم الطريقة الأولى تقنية كلمة المرورالتي يتم إرسالها إلى السحابة بطريقة مشفرة إلى الخادم أو الحاسوب الرئيسي الذي يتحقق من ذلك في قاعدة بيانات مخزنة في ذاكرة التخزين المؤقت. كما أنها تقترح دالة التجزئة ، بروتوكول المصادقة وتقنية بسيطة تمثل اختبار الاختراق.

تتوخى الطريقة الثانية تطوير تطبيق Java الذي يمثل تقنية جديدة لإدخال كلمة المرور ، محميًا من عدد من الهجمات كما تم تزويدها أيضا باختبار الاختراق.

يتم التحقق من أمان الطرق المقترحة عن طريق منطق التحليل وأدوات AVISPA & SPAN (Security Protocol ANimator) و قد تم حساب أوقات المصادقة من خلال تقييم دالة تجربة.

الكلمات الرئيسية: RFID، NFC ، القياسات الحيوية ، المصادقة ، سلامة البيانات ، السرية ، دالة التجزئة ، اختبار الاختراق.

Abstract

Contactless communication technologies and essentially RFID (Radio Frequency Identification), and NFC (Near Field Communication) have undergone rapid developments in recent years. They are used in several applications, such as electronic payment, key management, ticketing (transport, entertainment), information reading (transport, store, medicine), access control, electronic business card, etc.

However, the use of these technologies poses security problems in particular for electronic payment using an Automatic Teller Machine (ATM) or a Point of Sale also called PoS. The Communication security requiring verification of three essential properties, namely party authentication, data integrity and confidentiality, must be defended against major threats and attacks (e.g. relay attack, denial of service, Man- In-The-Middle, etc.) in order to ensure the protection of very sensitive personal data and therefore to protect privacy.

RFID and NFC devices used as Tags and contactless smart cards are characterized by limitations in terms of resources (memory, energy, computing capacity, etc.). The recording of biometric data for example on these devices poses the problem of the voluminous size of this data compared to the capacities of these devices.
Thus, several methods, techniques, protocols and also hardware solutions have been recommended in order to ensure the security of confidential data during recording in RFID or NFC devices and during communication with an RFID or NFC reader or to raise the performance in terms of costs: processing, communication and storage space.

Among the effective methods used to ensure secure and efficient RFID or NFC communication, the use of intelligent password techniques, simple, secure and efficient authentication protocols using simple hash functions to encrypt exchanged data.

Our thesis focuses on the proposal of two methods that we will try to prove their safety and performance. The methods are used to ensure data communication in an electronic payment via a smartphone and an ATM, both equipped with NFC technology.

The first method offers a password technique, the encrypted password is sent to the cloud server which verifies it in a database stored in a cache memory. It also offers a hash function, an authentication protocol and a simple technique of intrusion test.

The second method envisages the development of a Java application representing a new technique of entering the password, protected against a number of attacks and also provided with an intrusion test.

The security of the proposed methods is verified by analysis logic and AVISPA & SPAN (Security Protocol ANimator) tools. Authentication times are calculated by an evaluating experiment.

Keywords: RFID, NFC, biometrics, authentication, data integrity, privacy, hash function, intrusion test.

Résumé

Les technologies de communication sans contact et essentiellement la RFID (Radio Frequency Identification), et la NFC (Near Field Communication) ont connu des évolutions rapides au cours des dernières années. Elles sont utilisées dans plusieurs applications, telles que le paiement électronique, la gestion des clés, la billetterie (transport, spectacle), lecture d'informations (transport, magasin, médecine), contrôle d'accès, carte de visite électronique, etc.

Néanmoins l'utilisation de ces technologies pose des problèmes de sécurité en particulier pour le paiement électronique utilisant un guichet automatique bancaire (GAB) appelé aussi ATM (Automated Teller Machine) ou un point de vente aussi appelé PoS (Point of Sale). La sécurité des communications nécessitant la vérification de trois propriétés essentielles à savoir l'authentification des parties, l'intégrité des données et leur confidentialité, doit se défendre contre des menaces et attaques importantes (ex. : attaque relais, déni de service, Man-In-The-Middle, etc.) afin d'assurer la protection des données personnelles très sensibles et par conséquent protéger la vie privée. Les dispositifs RFID et NFC utilisés comme des Tags et des cartes à puce sans contact sont caractérisés par des limitations en termes de ressources (mémoire, énergie, capacité de calcul, …). L'enregistrement des données biométriques par exemple sur ces dispositifs pose le problème de la taille volumineuse de ces données par rapport aux capacités de ces dispositifs. Ainsi, plusieurs méthodes, techniques, protocoles et aussi solutions matérielles ont été préconisées afin d'assurer d'une part, la sécurité des données confidentielles lors de différents traitements : enregistrement dans les dispositifs RFID ou NFC, une mémoire d'enregistrement, pendant la communication avec un lecteur RFID ou NFC, d'autre part, élever la performance en termes de coûts : traitement, communication et espace de stockage.

Parmi les méthodes efficaces utilisées pour assurer une communication RFID ou NFC sécurisée et performante, l'utilisation des techniques intelligentes de mots de passe, des protocoles d'authentification simples, sécuritaires et performants utilisant de simples fonctions de hachage pour crypter des données échangées.

Notre thèse se focalise sur la proposition de deux méthodes qu'on va essayer de prouver leurs sécurité et performance. Ces méthodes sont utilisées pour assurer une communication de données dans un paiement électronique via un smartphone et un guichet automatique bancaire, tous les deux équipés de la technologie NFC.

La première méthode propose une technique de mot de passe, ce dernier est envoyé en cloud d'une manière cryptée au serveur qui le vérifie dans une base de données stockée dans une mémoire cache. Elle propose aussi une fonction de hachage, un protocole d'authentification et une technique simple de test d'intrusion.

La deuxième méthode envisage un développement d'une application Java représentant une nouvelle technique de saisie du mot de passe, protégée contre un certain nombre d'attaques et pourvue aussi d'un test d'intrusion. La sécurité des méthodes proposées est vérifiée par une logique d'analyse et des outils AVISPA & SPAN (Security Protocol ANimator). Les temps d'authentification sont calculés par évaluation d'une expérience.

Mots-clés : RFID, NFC, biométrie, authentification, intégrité des données, confidentialité, fonction de hachage, test d'intrusion.

Table des matières

Chapitre 3 : Un mot de passe en cloud et un protocole d'authentification pour un paiement NFC sécurisé entre ATM et Smartphone

Chapitre 4 : Dynamic Array PIN : une nouvelle approche pour sécuriser le paiement électronique NFC entre l'ATM et le smartphone

Liste des figures

Liste des tableaux

Liste des acronymes

3D	3 Dimensions
3G, 4G, 5G	$3^{éme}$, $4^{éme}$, $5^{éme}$ Génération
ABI	Allied Business Intelligence
AES	Advanced Encryption System
ATM	Automated Teller Machine
ATSE	Attack Searcher
AVISPA	Automated Validation of Internet Security Protocols and Applications
BLE	Bluetooth Low Energy
BRFID	Biométrique et RFID
CEI	Commission électrotechnique internationale
Cm	Centimètre
CPASS	Cloud Pass Word
CWPIN	Color Weel PIN
DAP	Dynamic Array PIN
DES	Data Encryption System
DOS	Denial Of Service
ECMA	European Computer Manufacturers Association
EMPS	Expanded Modular Power System
EMV	Europay Master and Visa
EMVco	EMV and American Express, Discover, JCB
ETSI	European Telecommunications Standards Institute
GAB	Guichet Automatique Bancaire
GPS	Global Positioning System
HLPSL	High-Level Protocol Specification Language
I5	Intel processor 5
IEC	International Electro-technical Commission
IEEE	International Electrical and Electronics Engineers
IF	Intermediate Format
IP	Internet Protocol
IPS	Intrusion prevention System
ISACA	Information System Audit and Control Association
ISO	International Standard Organization
ITSO	Integrated Transport Smart card Organization
Kbits/s	Kilo bits par seconde
LAN	Local Area Network
MAC	Media Access Control
Mbits/s	Méga bits par seconde
MD5	Message Digest 5
Ms	Milliseconde
NFC	Near Field Communication
OCR	Optical Character Recognition
OFMC	On-the-Fly-Model-Checking
OS	Operating System
PACS	Physical Access Control System

PC	Personal Computer
PDA	Personal Digital Assistant
PDF	Portable Document Format
PIN	Personal Identification Number
POS	Point Of Sale
QR	Quick Response
RF	Radio Frequency
RFID	Radio Frequency Identification
SCCP	Secure Credit Card Protocol
SD	Secure Digital
SE	Secure Element
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMC	Secure Memory Card
SMS	Small Message Service
SPAN	Security Protocol Animator
TIC	Technologie de l'Information et de la communication
TLS	Transport Layer Security
TRF	Transaction Reversal Fraud
TSM	Trusted Service Manager
UICC	Universal Integrated Circuit Card
UIT	Union internationale des télécommunications
UK	United Kingdom
URL	Uniform Resource Locator
USSD	Unstructured Supplementary Service Data
UUID	Universally Unique Identifier
WAP	Wireless Application Protocol
Wi-Fi	Wireless Fidelity
XOR	Ou Exclusif

Introduction générale

Sommaire

1. Contexte général et problématique

Au jour d'aujourd'hui, les technologies de télécommunication ont connu un développement rapide et très remarquable essentiellement dans la branche des communications sans fils. Au sein d'un Partenariat, l'Union internationale des télécommunications (UIT) est responsable de la collecte, de l'harmonisation et de la diffusion des principaux indicateurs d'accès aux TIC (Technologies de l'information et de la communication) et des ménages TIC et examine régulièrement les définitions des indicateurs pour s'assurer qu'ils restent pertinents pour l'évolution rapide des TIC. Le Groupe d'experts sur les indicateurs des télécommunications / TIC, qui comprend plus de 1 100 membres, et le Groupe d'experts sur les indicateurs des ménages TIC, qui comprend plus de 800 membres, mènent leurs travaux par le biais de forums de discussion en ligne et rendent compte des résultats de leurs travaux au World Télécommunication / Symposium sur les indicateurs TIC. Les résultats les plus récents des travaux des deux groupes d'experts ont été présentés lors du Symposium qui s'est tenu à Genève en décembre 2019 [Economic and Social Council 2020]. Ainsi, les utilisateurs ont bénéficié d'un grand nombre de services sans fils qui assurent la transmission des données, des voix, des images et des vidéos. Ces services ont été réalisés par un ensemble de technologies sans fil, inventées au cours des dernières années comme la technologie Bluetooth, Wi-Fi (Wireless Fidelity), code-barres, QR (Quick Response) code etc. Bien que les différentes technologies de communication ont influencé favorablement (dans la majorité des cas) la vie des utilisateurs, certaines technologies classées dans le domaine de la communication sans contact, ont prouvé leur importance dans les activités usuelles et vitales des personnes comme le marketing, le paiement, le transport, le contrôle d'accès, le tourisme, la médecine etc. Parmi ces technologies, on peut citer celles du code-barres, QR code, RFID (Radio Frequency Identification) et NFC (Near Field Communication). Suivant le domaine d'utilisation de la technologie sans contact, des applications spécifiques ont été créées. Chaque application inventée est caractérisée par un certain niveau de qualité, de mobilité, de fiabilité, de souplesse, d'efficacité et surtout de sa sécurité.

La technologie NFC est l'une des nouvelles technologies sans contact qui sont basées sur l'émission d'un champ électromagnétique contenant des données accessibles par un ou plusieurs systèmes de réception appelés transpondeurs. Cette technologie peut être utilisée dans plusieurs domaines à savoir la gestion des clés, la billetterie (transport, spectacle), lecture d'informations (transport, magasin), contrôle d'accès, carte de visite électronique et surtout le

paiement électronique. Un paiement en 2020 consistera à transférer de la valeur et à fournir des solutions stratégiquement importantes à l'appui d'une activité plus large dans des domaines tels que le commerce, l'investissement, la vente en détail et aux secteurs publics [Dominic 2014].

Les systèmes de paiement sont passés ces dernières années de la simple transaction par carte de crédit vers différents types de systèmes de paiement mobile. Cette transition a eu lieu en raison de changements dans l'économie, de développements sur Internet, de la prolifération des réseaux sociaux et de l'utilisation accrue des appareils mobiles. Étant donné que les smartphones sont de nos jours un produit omniprésent, les consommateurs bénéficient de la facilité et de la commodité de payer des biens et des services à l'approche de ce nouveau moyen de paiement. Les systèmes de paiement mobiles ont adapté non seulement une réalité libre principalement numérique et mobile, mais un nouveau climat des affaires, facilitant les transactions commerciales partout, à tout moment et pour tout le monde [De Luna et al. 2019].

Comme les smartphones offrent dans nos jours, de nombreuses options de connexion, telles que 3G (3^{éme} Génération), 4G, Wi-Fi, GPS (Global Positioning System), NFC et Bluetooth, ils sont maintenant des cibles idéales pour des auteurs malveillants. Basiquement, les systèmes d'exploitation mobiles (OS : Operating System) peuvent être vulnérables à des attaques malveillantes en raison de l'exécution de nombreuses applications pendant la navigation sur le Web ou durant le téléchargement d'applications depuis Internet. Actuellement, les gens connaissent mieux les différents smartphones et leurs entreprises, mais très peu d'entre eux ont suffisamment d'informations sur les systèmes d'exploitation mobiles et ses vulnérabilités [Taleby et al. 2020].

Bien que le système Android devienne très populaire aujourd'hui, il est exposé à des attaques et il est de plus en plus vulnérable en raison de la présence de logiciels open source où tout le monde peut librement développer des applications. Un auteur (ou développeur) de logiciels malveillants peut profiter de ces fonctionnalités pour développer des applications malveillantes. A cet effet, les smartphones peuvent être facilement vulnérables aux activités malveillantes telles que le phishing, le piratage, etc. qui pourraient voler les informations sensibles à l'insu de l'utilisateur. En général, les utilisateurs s'articulent de plus en plus les smartphones pour les transactions de paiement, telles que les services bancaires mobiles et les achats en ligne, et en outre, il existe probablement plus de fausses applications (c'est-à-dire des

applications malveillantes en couverture de vraies applications) conçues pour faire des profits pour les auteurs malveillants [Taleby et al. 2020].

En outre, selon le dernier rapport publié par Kaspersky en 2019, les résultats suivants ont été révélés :

- 19,8% des ordinateurs des utilisateurs ont été soumis à au moins une classe d'attaques malware sur le Web au cours de l'année.
- Les solutions Kaspersky ont repoussé 975 491 360 attaques lancées par des ressources en ligne situées partout dans le monde.
- 273 782 113 URL (Uniform Resource Locator) ont été reconnues comme malveillantes par des composants antivirus Web.
- L'antivirus Web de Kaspersky a détecté 24 610 126 objets malveillants.
- 755 485 ordinateurs d'utilisateurs uniques ont été ciblés par des attaquants de chiffrement.
- 259 038 ordinateurs d'utilisateurs ont été ciblés par des mineurs.
- Les solutions Kaspersky ont bloqué les tentatives de lancement de logiciels malveillants capables de voler l'argent via les services bancaires en ligne sur 766 728 appareils.

Ces statistiques incluent non seulement les logiciels malveillants bancaires mais aussi les programmes malveillants pour les distributeurs automatiques de billets et les terminaux de point de vente [Kaspersky 2019]. De 2017 à 2019, il y a eu une augmentation marquée des attaques ATM, en raison de quelques familles particulièrement actives. Ces systèmes cibles dans le monde entier, quel que soit le fournisseur, ont l'un des deux objectifs suivants : voler les informations des clients ou acheminer les fonds directement de la banque [Kaspersky 2020]. Les logiciels malveillants ATM / PoS continueront à évoluer et nous continuerons donc de surveiller de près l'écosystème. WinPot est un logiciel malveillant, découvert pour la première fois en 2018, actif cette année dans différentes parties du monde [Kaspersky 2020].

Vues les risques des attaques sur les smartphones, les ATM et les POS, nous avons fourni des efforts pour proposer des solutions qui essayent de donner une pousse à la sécurité afin de protéger les informations sensibles des utilisateurs et donc protéger l'argent contre les pirates.

2. Contributions de la thèse

Cette thèse peut être perçue comme une contribution au développement de nouvelles méthodes pouvant être exploitées dans le domaine de la sécurisation du paiement NFC utilisant un smartphone et un guichet automatique bancaire aussi appelé ATM, vues les menaces et les attaques qui peuvent affecter un smartphone afin de voler les données confidentielles pour

effectuer un paiement frauduleux au sein du compte de la victime ou affecter un GAB pour voler les informations d'une carte bancaire, ou des billets d'argents de la banque.

La première contribution propose :

- Une technique de mot de passe, envoyé en cloud d'une façon cryptée, réceptionné par un serveur et vérifié dans une mémoire cache.
- Une fonction de hachage simple et efficace, développée en Java et utilisée pour la signature des messages.
- Un protocole d'authentification écrit en langage HLPSL, simple et sécuritaire utilisant la fonction de hachage proposée.
- Un simple test d'intrusion utilisé pour avertir l'utilisateur dans le cas d'une nouvelle attaque créée (cas échéant).

La deuxième contribution propose :

- Une nouvelle méthode de saisie de mot de passe, développée en Java, testée sur un échantillon de 30 personnes et prouvée qu'elle est sécuritaire et efficace.
- Un test d'intrusion utilisé également pour alerter l'utilisateur dans le pire des cas qu'une attaque nouvellement créée a menacé son compte bancaire.

3. Organisation du manuscrit

Ce manuscrit est organisé en quatre chapitres organisés en deux parties et suivies d'une conclusion générale et des perspectives. La partie I composée des chapitres 1 et 2, constitue un état de l'art sur la sécurisation des dispositifs et applications NFC du point de vue des attaques contre le smartphone, la carte de crédit ou la carte bancaire et le GAB et les contre-mesures proposées pour lutter contre ces attaques.

Le chapitre 1 donne un aperçu de l'état de l'art sur les technologies de communication sans contact en présentant les technologies de communication sans fil et les techniques d'identification et d'authentification. Il est mis en avant dans ce chapitre les services sans contact avec une concentration sur le service de paiement. La dernière section abordée est consacrée à la présentation des dispositifs et applications NFC. Nous commençons cette section par une brève explication du panorama NFC, puis nous présentons les dispositifs NFC nécessaires et qui ont un lien avec notre travail et nous terminons avec un recensement des applications NFC.

Le chapitre 2, dresse une revue de la littérature des attaques qui peuvent influencer les dispositifs et les applications NFC et les contre-mesures envisagées afin de lutter contre ces attaques. Deux classes majeures d'attaques ont été considérées, à savoir les attaques physiques

et les attaques logiques. Pour chaque classe, nous avons détaillé les attaques contre la carte NFC (de crédit ou bancaire), le smartphone et le GAB. Enfin, le chapitre décrit brièvement les solutions proposées sous forme matérielle, techniques d'authentification (Mot de passe, protocole) ou techniques de cryptage (fonction de hachage) en spécifiant les avantages et les inconvénients de chaque solution.

La partie II comporte les chapitres 3 et 4. Bien que le chapitre 3 présente la première contribution se résumant en un mot de passe crypté, envoyé en cloud et vérifié dans une mémoire cache d'un serveur, une fonction de hachage, un protocole d'authentification et un test d'intrusion. Le chapitre 4 expose la seconde contribution matérialisant le développement d'une application en java et qui représente une nouvelle approche de saisie d'un mot de passe en utilisant un GAB.

Le chapitre 3 est centré donc sur la présentation de la première contribution. Il commence par présenter la technique du mot de passe envoyé en cloud après sa concaténation avec l'identificateur de l'élément sécurisé et son chiffrement avec la fonction de hachage proposée, puis il passe à la présentation de l'implémentation de notre fonction de hachage et à la présentation de notre protocole d'authentification écrit en langage HLPSL et du test d'intrusion. A la fin, ce chapitre présente les résultats de calcul du temps d'authentification et des temps de transmission des messages utilisés dans notre protocole, et aussi les résultats de simulation de notre protocole par l'outil AVISPA (Automated Validation of Internet Security Protocols and Applications). Nous poursuivons ce chapitre par une analyse logique et automatique de la sécurité de notre solution, une étude de sa performance et une comparaison avec plusieurs méthodes récentes.

Le chapitre 4 est focalisé sur le détail de la deuxième contribution. Il commence par présenter et expliquer la technique DAP (Dynamic Array PIN), qui est une nouvelle méthode de saisie du mot de passe en utilisant un GAB. Puis il expose l'expérimentation établie afin d'évaluer le temps d'authentification de notre méthode développée en Java et testée sur un échantillon de 30 participants. Le chapitre présente aussi un test simple d'intrusion proposé pour alerter la victime en cas d'anomalie. A son achèvement, ce chapitre présente les résultats de calcul du temps d'authentification, puis il termine par une analyse logique basée sur la démonstration de la sécurité de notre solution, par une étude de sa performance et enfin par une comparaison avec plusieurs méthodes récentes.

Première partie

I. **Positionnement** : Etat de l’art sur la sécurité dans la communication en champ proche

Chapitre 1

Chapitre 1 : Technologies de communication sans contact

Sommaire

1.1 Introduction

Au cours des dernières années, les technologies de communication sans contact sont en évolution progressive et sont devenues de plus en de plus importantes en raison de leurs larges applications dans tous les aspects de notre société. Elles représentent une nécessité pour effectuer des services et des usages qui sont de grande utilité dans la vie moderne, tels que le contrôle d'accès à des zones très sensibles et dangereuses comme les sites nucléaires, le transport public, la gestion des clés comme le cas des voitures et des hôtels, la billetterie, et le paiement.

De telles technologies ont un but d'identification des personnes, des objets, des animaux et des produits en transit et cela d'une façon simple. Ces technologies qui sont devenues très populaires, sont connues à un certain moment par les code-barres qui ont révolutionné le domaine des systèmes d'identification. Cependant, le coût très bas d'un code-barres est compensé par de gros défauts comme la très faible capacité de stockage d'informations et l'impossibilité de sa reprogrammation. Une solution alternative consiste à stocker les données dans une puce programmable. Aujourd'hui, cette solution est largement déployée dans les cartes de crédit ou dans les puces téléphoniques. Cependant, cette solution repose sur le contact mécanique, contact qui est trop souvent gênant lors de son utilisation. Ainsi, pour éviter tout contact mécanique, une nouvelle technologie de transfert de données sans contact entre un outil contenant des informations et un lecteur est en constante évolution depuis quelques années. Ces systèmes d'identification sans contact sont appelés systèmes RFID. La technologie RFID comprend plusieurs technologies dont celle de NFC. La NFC est donc une technologie permettant l'échange de données entre plusieurs outils mais qui a la particularité de se concentrer sur des communications de petites distances (de l'ordre de quelques centimètres). Cette courte distance de communication a permis au NFC de sécuriser les données échangées.

Dans ce chapitre, nous commençons par définir les technologies de communication sans fil en expliquant brièvement quelques-unes, puis nous abordons les techniques d'identification et d'authentification. Ensuite, nous présentons les services sans contact et nous nous concentrons sur le paiement. Nous nous focalisons ensuite sur les dispositifs et les applications NFC. Nous présentons dans cette dernière section un panorama du NFC en spécifiant ses normes, ses modes de communication, l'architecture de son système et ses marchés. Nous exposons ensuite les dispositifs NFC utilisés dans le paiement électronique NFC en mettant en avant l'architecture physique et logique d'un ATM et d'un smartphone. Enfin, et avant la

conclusion, nous recensons quelques applications NFC effectuées par un smartphone doté de la NFC avec une brève explication.

1.2 Technologies de communication sans fil

Tous les jours, la communication sans fil joue un rôle important dans notre vie. Outre la communication, la technologie sans fil fait désormais partie intégrante de nos activités quotidiennes. La transmission de données ou d'informations d'un endroit à un autre sans fil est appelée communication sans fil. Cela permet un échange de données sans aucun conducteur via des signaux radio. Les informations sont transmises à travers les appareils sur quelques mètres à des centaines de kilomètres via des canaux bien définis. La technologie de communication sans fil est classée en différents types en fonction de la distance de communication, de la gamme de données et du type d'appareils utilisés. Parmi ces types, on peut citer la communication radar, la communication par satellite, le système de positionnement global, Wifi, Bluetooth, Identification radiofréquence etc. [TypesnUses.com 2019]. Récemment, la demande de services de données multimédia a augmenté rapidement avec l'évolution des technologies de communication sans fil [Mehallel 2019]

1.2.1 Bluetooth

La technologie sans fil Bluetooth est une norme de transmission RF (Radio Frequency) à courte portée. Elle est basée sur des liaisons radio à faible coût et à courte portée entre les appareils portables et de bureau (Figure 1.1). Cette technologie ne remplace pas les réseaux locaux sans fil mais les complète. La technologie sans fil Bluetooth présente de nombreux avantages par rapport aux autres technologies LAN (Local Area Network) sans fil, ce qui la rend attrayante pour de nombreuses applications. L'une de ces applications concerne les capteurs et les jauges à bord des navires et des sous-marins. Comme les objets dans cette technologie sont connectés sans fil, une énorme quantité de câbles est éliminée et la mobilité des utilisateurs est accrue [Aljuaied 2001].

Bluetooth est une technologie de communication conçue pour l'interconnexion de dispositifs qui ne partagent préalablement aucune information. Les nœuds peuvent effectuer une découverte de voisinage qui leur permet ensuite de communiquer. Les versions de Bluetooth 2.0 et 2.1 permettent des débits de l'ordre de 3 Mbit/s (Mégabits par seconde). La version 3.0 dont la norme a été adoptée le 21 avril 2009, permet des débits de l'ordre de 24 Mbit/s. Les premiers

équipements utilisant cette norme étaient par exemple le téléphone Samsung Galaxy S [Albert 2010].

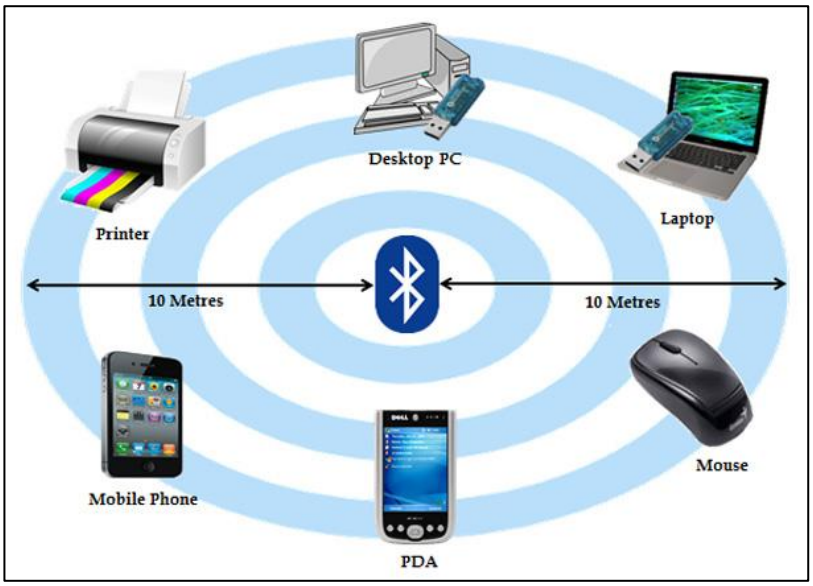

Figure 1.1 : La technologie Bluetooth [ICT Lounge 2020]

1.2.2 Wi-Fi

Wi-Fi est la technologie de réseau sans fil la plus populaire. Elle est fortement utilisée et dans plusieurs endroits (Figure 1.2). Elle est une famille de normes pour les réseaux sans fil définies dans l'IEEE (Institute of Electrical and Electronics Engineers) 802.11. L'interopérabilité de ces normes a été testée et approuvée par le Wi-Fi Alliance. Le Wi-Fi fournit un réseau à un dispositif via une connexion sans fil en utilisant la radiofréquence. Cette technologie n'est pas confondue avec d'autres technologies sans fil comme 3G, Bluetooth, etc., malgré qu'elle utilise un ensemble différent de spécifications IEEE. Cette technologie est caractérisée par un ensemble d'avantages à savoir :

- Elle permet le déploiement de réseaux locaux (LAN) sans fil pour des périphériques clients, ce qui réduit généralement les coûts de déploiement et d'extension du réseau,
- Un réseau wifi peut être hébergé dans des espaces où les réseaux filaires ne peuvent pas être installés.
- Les produits Wi-Fi sont largement disponibles sur le marché et le prix reste décroissant,
- La technologie Wi-Fi a un ensemble de normes mondiales [Li 2011].

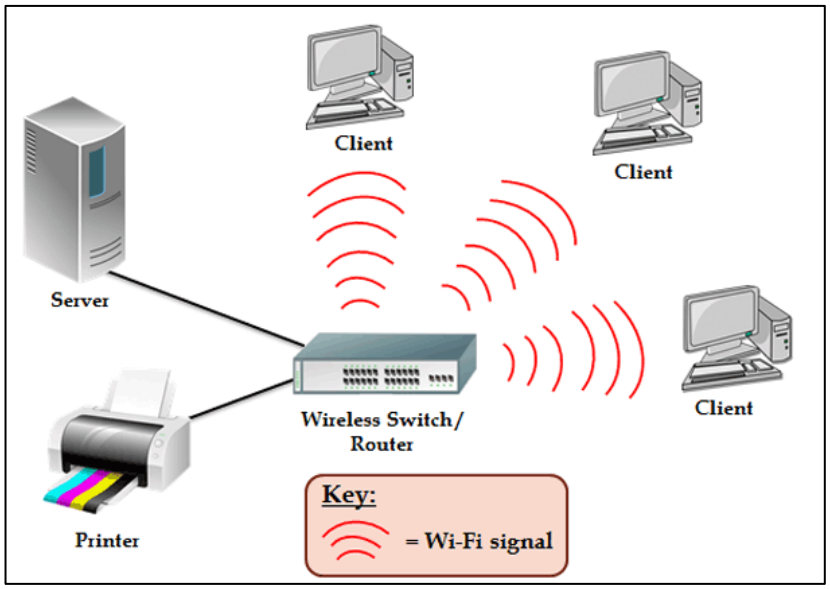

Figure 1.2 : La technologie Wi-Fi [ICT Lounge 2020]

1.3 Techniques d'authentification

1.3.1 Identification et authentification

L'identification correspond à la recherche de l'identité fournie par une personne qui se présente, dans une base de données. Elle est très importante pour assurer la sécurité des systèmes et des organisations. Elle peut servir à autoriser ou non l'utilisation des services. Elle est utilisée par exemple dans le but du contrôle d'accès à une zone très sensible pour laquelle seul un effectif limité de personnes (sauvegardés dans une base de données) y a l'autorisation d'accès. Elle peut être aussi utilisée par la police judiciaire [Benchennane 2015].

L'authentification est une opération de vérification de l'identité (Figure 1.3). Elle représente une comparaison "un à un", où le système essaye de valider l'identité d'une personne en utilisant un système de comparaison entre les informations saisies (données biométriques par exemple) et les informations caractérisant réellement la personne (par exemple le modèle biométrique de la personne). Les informations réelles qui caractérisent la personne sont stockées dans une base de données du système. En utilisant le principe d'authentification, le système peut répondre à la question : « Suis-je réellement la personne que je suis en train de proclamer ?» [Guerfi 2008]. Actuellement l'authentification est réalisée par un numéro d'identification personnel (mot de passe, code PIN), un nom d'utilisateur, une carte à puce, une modalité biométrique ou un protocole d'authentification.

Figure 1. 3 : Identification et Authentification [Digitalminution 2013]

1.3.2 Le mot de passe

L'authentification basée sur les mots de passe a été mise en place comme méthode d'authentification la plus couramment utilisée (Figure 1.4). On peut s'attendre à ce que les mots de passe représentent la plus grande partie de l'authentification, même dans un avenir proche. Pour cette raison, il vaut la peine d'explorer les forces et les faiblesses de l'authentification par mot de passe et de rechercher de nouvelles améliorations. Il existe différentes formes de mots de passe mémorisés qui sont décrits avec leurs points forts et leurs points faibles. Les mots de passe sont des cibles à différentes attaques contre leurs hachages, ce qui oblige à créer des mots de passe sûrs et solides.

Une perte de mot de passe doit être évitée au regard des deux points suivants. Le premier est d'empêcher l'utilisateur d'écrire le mot de passe sur une petite feuille de papier intitulée « mon mot de passe » et de le laisser quelque part à l'adversaire. Ceci n'est pas une mesure technique raisonnable. Il faut forcer l'utilisateur à ne pas agir comme ça. Le deuxième a cependant de meilleures perspectives. Il consiste à utiliser des bases de données pour stocker les mots de passe des utilisateurs. Les mots de passe de cette façon peuvent être protégés par des couches de mesures de sécurité contre les attaquants. Ces mesures vont des éléments de défense actifs comme les pares-feux et les IPS (Intrusion Prevention System) aux mesures passives qui servent de dernier recours au cas où l'attaquant aurait pénétré par effraction [Martin 2009].

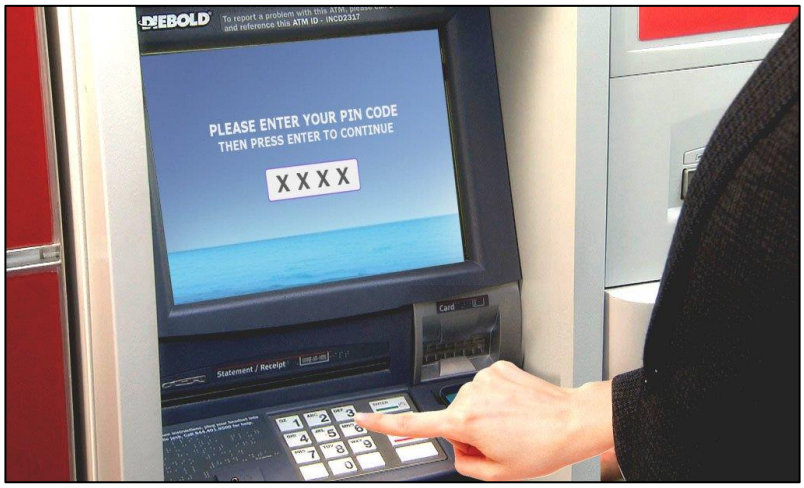

Figure 1.4 : Authentification par mot de passe devant un ATM [science ABC 2019]

1.3.3 La reconnaissance optique

La reconnaissance optique consiste à utiliser une source d'optique à l'exposé d'une image contenant des objets ou des caractères ou à l'exposé d'une source de geste afin d'extraire l'ensemble des objets (reconnaissance des objets), l'ensemble des caractères (reconnaissance des caractères) ou l'ensemble des gestes (reconnaissance de gestes).

La reconnaissance du geste a pour but l'identification et l'interprétation automatique des gestes d'une personne acquis par un dispositif comme un capteur, une caméra ou autres [Hiyadi 2016].

La reconnaissance de caractères ou OCR (en anglais : Optical Character Recognition) est une technologie qui convertit un document de type papier scanné, PDF (Portable Document Format) ou photo numérique vers un format modifiable qui peut être exploité. La technologie d'OCR a été largement appliquée dans le domaine d'industries ces dernières années [El Gajoui and Fadoua 2014].

La reconnaissance d'objets sert à détecter les objets contenus dans une image (Figure 1.5). Une fois la détection est établie, le processus fait correspondre des objets à ceux détectés dans l'image [Elbahri 2015].

Figure 1.5 : Authentification par reconnaissance optique devant ATM [Emerj 2019]

1.3.4 La reconnaissance de la parole

La reconnaissance automatique de la parole est un moyen d'intervention avec le logement, et permet de fournir des instructions vocales et de détecter des situations douteuses. La reconnaissance automatique de la parole peut être utilisée comme un système de surveillance à domicile afin de détecter des situations anormales d'un certain type de gens comme les plus âgés. Dans un smart home, on peut utiliser un dispositif de reconnaissance automatique de la parole dans le but de commander des appareils domotiques et des appareils qui permettent de faciliter et maintenir le lien social. Elle peut aussi être utilisé pour détecter les appels de détresse et les appels vers les aidants (ex. : « Aidez-moi », « Docteur »). [Aman 2014].

La reconnaissance automatique de la parole est une technique qui analyse des sons interceptés par des moyens comme le microphone pour les transformer sous forme d'une suite de mots qui sera exploitée par des dispositifs dédiés (Figure 1.6). Cette technologie est apparue dans les années 1950, puis, elle a été améliorée avec la définition des connaissances linguistiques et acoustiques qui sont obligatoires pour bien comprendre la parole d'une personne [Orasanu 2015].

Figure 1.6 : Authentification par reconnaissance de la parole [IdTechEx 2018]

1.3.5 La reconnaissance de modalité biométrique

La reconnaissance biométrique est la tâche d'identifier un individu sur la base de ses traits physiologiques ou comportementaux. La nécessité de développer des systèmes de sécurité à toute épreuve a donné une impulsion indispensable à la recherche biométrique. Au cours des dernières décennies, de nombreux travaux ont été réalisés pour développer des systèmes basés sur les empreintes digitales (Figure 1.7), le visage, l'iris, la voix, etc. Certaines de ces mesures biométriques ont montré un potentiel énorme dans les applications médico-légales [Goudelis et al. 2008].

Figure 1.7 : Authentification par empreinte digitale devant ATM [Siddiqui 2013]

1.4 Technologies d'identification

La technologie d'identification par capture de données peut être utilisée dans différentes activités quotidiennes comme par exemple dans une bibliothèque, elle peut assurer l'auto-enregistrèrent, le retrait, l'auto-rectification, la création de cartes de bibliothèque, l'autogestion, la détection antivol, la vérification des stocks, etc. Elle offre un système d'identification automatique rapide, précis et facile pour les approches de collecte de données. Une fois les données capturées, elles peuvent être stockées ou analysées par un ordinateur ou un autre appareil. Les techniques d'identification ne nécessitent généralement pas l'intervention humaine pour capturer des données, ces méthodes comprennent des technologies à savoir la biométrie, le code QR, les codes à barres, la RFID, etc. Ces informations peuvent être utilisées pour les fonctions de contrôle pertinentes pour les éléments spécifiques [Singha and Manoj 2019].

1.4.1 Le code-barres

Les omniprésents codes-barres ont véritablement révolutionné le domaine des systèmes d'identification (Figure 1.8). Cependant, le très faible coût d'un code-barres est contrebalancé par de gros défauts. En effet, ce dernier possède une très faible capacité de stockage d'informations et il ne peut pas être reprogrammé. Une solution alternative est de stocker les données dans une puce programmable. De nos jours, cette solution est très largement déployée dans les cartes de crédit ou dans les puces de téléphones. Mais cette solution repose sur un contact mécanique, contact trop souvent gênant lors de son utilisation [Tornambé 2016].

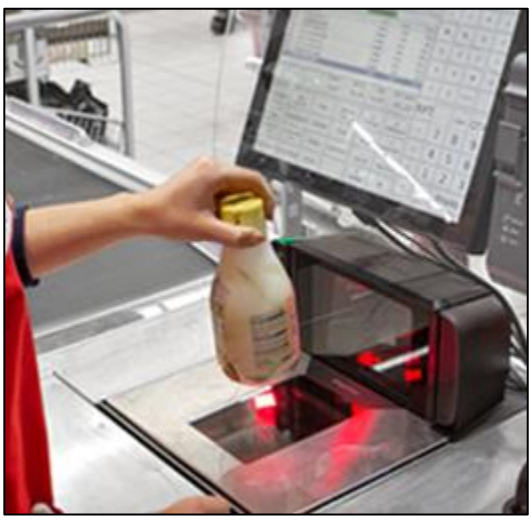

Figure 1.8 : Identification avec code-barres devant un point de vente [Datalogic 2020]

1.4.2 Le QR code

Le QR Code est une gamme de barres de codage de dimension standard. QR code (Quick Response : "code de réponse rapide") est une marque déposée de la société Denso Wave Inc. Ils sont régulièrement utilisés par les smartphones mobiles, car les codes QR peuvent représenter (la codification) des adresses de sites Internet (type URL) ; pour un accès rapide à un site souhaité, l'utilisateur a seulement besoin de scanner le code QR à l'aide de la caméra d'un téléphone portable. Un lecteur logiciel interprète l'image et décode le code, et achemine le navigateur du téléphone de l'utilisateur vers l'URL en question. La simplicité de ces connexions à partir du monde physique au monde électronique, connu sous le nom de "hyperliens physiques" (en anglais hardlink), explique leur popularité.

Un code QR peut stocker un maximum de 7089 caractères numériques et 4296 caractères alphanumériques. Il existe deux principaux types de code QR : "Micro QR" et "Design QR" [Cornelia et al. 2017]. Au niveau des magasins, un lecteur est dédié à lire le code-barres d'un article pour le comptabiliser (Figure 1.9).

Figure 1.9 : Identification par QR code devant un point de vente [CNA 2018]

1.4.3 La RFID

La RFID aussi appelée Identification par ondes Radiofréquences, est une technologie souple et performante qui permet d'effectuer des actions de lecture d'une manière automatique. Elle est utilisée pour des raisons d'identification en manipulant les ondes radio fréquences afin de lire les données embarquées dans des dispositifs portant le nom d'étiquette ou Tag RFID. La technologie RFID utilise un lecteur pour lire les données enregistrées dans les Tags. Cette technologie permet aussi l'écriture et le stockage d'un ensemble d'informations de manière cryptée. Elle peut être utilisée en mode lecture seule ou en mode lecture et écriture en même

temps. Elle se rencontre avec d'autres technologies comme le code-barres en un ensemble d'avantages et se caractérise par d'autres qui lui sont spécifiques. La technologie RFID a comme objectifs l'identification, le suivi de trace et la surveillance des personnes, des animaux et des objets à une certaine distance (Figure 1.10). Les Tags RFID sont plus coûteux que les codes-barres mais dans l'ensemble plus bénéfiques [Dhaouadi 2014].

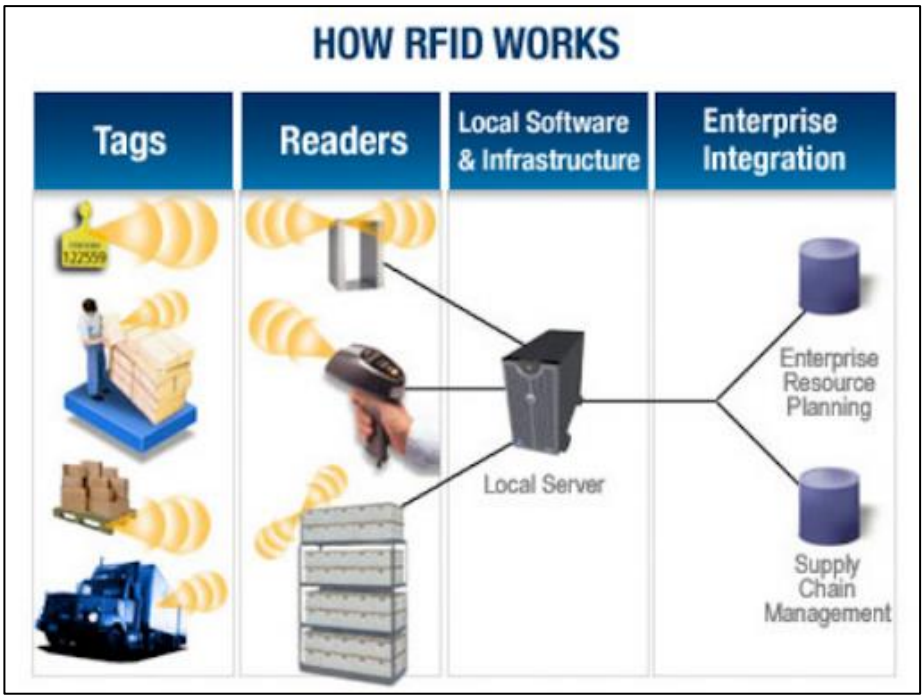

Figure 1.10 : Différentes utilisations du système RFID [Download.zone 2020]

1.4.4 La NFC

La NFC aussi appelée communication par champ proche, est une technologie inclue dans la technologie RFID. Elle est utilisée pour la communication de données entre plusieurs dispositifs qui se placent à de petites distances (quelques centimètres). Cette courte distance de transmission a été choisie pour permettre à cette technologie d'être utilisée pour effectuer des applications sécurisées où l'utilisateur doit être protégé pour réaliser avec un simple geste et à sa guise un échange de données pour en bénéficier d'un service comme, par exemple, le paiement sans contact (Figure 1.11) ou l'identification à un point de contrôle d'accès. Ces applications appelées applications NFC sont devenues de nos jours populaires et très demandées surtout avec l'apparition des dispositifs technologiques comme les smartphones et les tablettes [Tornambé 2016].

La NFC qui est donc dérivée du RFID, est parue dans les années 70 suite à des travaux de Roland Moreno et Michel Hugon sur leurs « cartes à puce » entre 1974 et 1979 et sur les premiers circuits intégrés pour cartes à puce à contact en 1979 qui sont créées par les entreprises CII-Honeywell Bull et Motorola [Moreno 2001].

En 2004, la NFC est lancée officiellement par Sony et Philips avec l'ouverture du forum NFC, un consortium international visant à promouvoir la technologie NFC. Peu après le lancement du forum, le consortium a été rejoint par d'autres grands acteurs de la téléphonie mobile tels que Nokia, Samsung et Panasonic.

Aujourd'hui, la norme NFC « permet d'échanger des données entre un lecteur et n'importe quel terminal mobile ou entre les terminaux eux-mêmes, à un débit maximum de 424 Kbits/s (Kilo bits par seconde) jusqu'à une distance maximale de 10 cm (centimètre) [Hervé 2012].

Figure 1.11 : Paiement utilisant carte et point de vente dotés de NFC [RBC Royal bank 2020].

1.5 Services sans contact

La communication en champ proche est une nouvelle technologie sans fil à courte portée, une technologie de communication qui offre de grandes et diverses promesses dans des services tels que le paiement, billetterie, jeux, crowdsourcing, vote, navigation et bien d'autres. La technologie NFC permet l'intégration de services à partir d'une large gamme d'applications en un seul téléphone intelligent [Coskun et al. 2015].

1.5.1 Domination des services sans contact

Les technologies sans contact facilitent l'acceptation des instruments de paiement au point de vente. La caractéristique clé des technologies sans contact est la transmission d'informations de paiement à partir d'un appareil physique sans qu'il soit nécessaire d'établir un contact physique entre l'appareil d'acceptation du bénéficiaire et l'instrument de paiement du payeur. Les informations utilisées pour les paiements sans contact peuvent être stockées et / ou accessibles via une variété d'appareils physiques (par exemple, les cartes de paiement, les téléphones portables, les appareils portables) et comprend également d'autres technologies, par exemple les codes Bluetooth basse énergie (BLE : Bluetooth Low Energy) et QR. Le nombre de dispositifs de paiement émises avec des technologies sans contact a considérablement augmenté en Europe (Figure 1.12). Aux Pays-Bas, en Suède, en Suisse et au Royaume-Uni, la majorité des cartes émises disposent déjà de technologies sans contact. Au Danemark, 72% de tous les paiements par carte au point d'interaction ont été effectués sans contact au troisième trimestre 2019 [Committee on Payments and Market Infrastructures 2020].

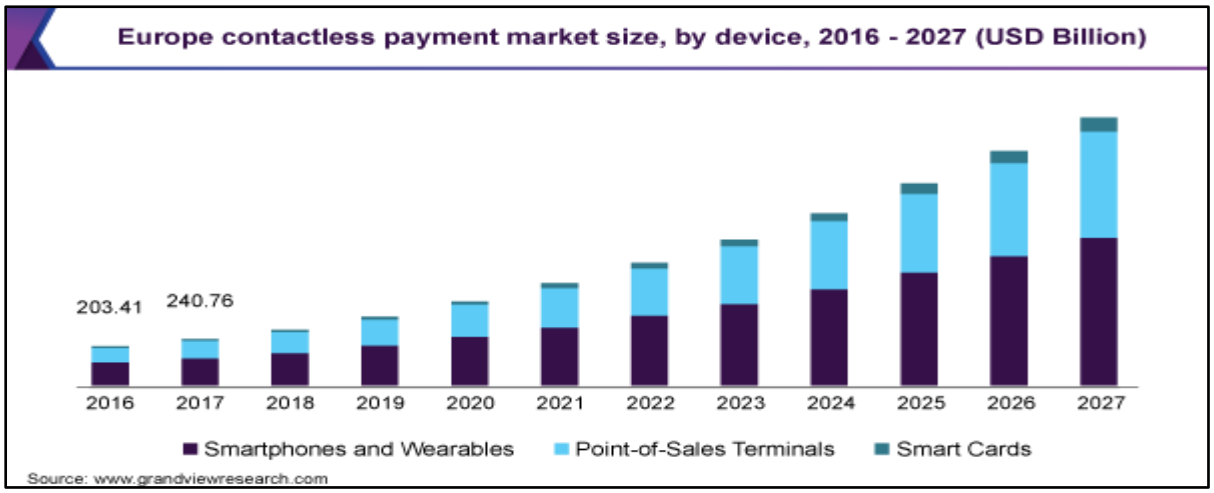

Figure 1.12 : Dispositifs de paiement avec technologies sans contact en Europe [www.grandviewresearch.com 2020]

1.5.2 Service de paiement mobile

Généralement, le M-paiement (Paiement mobile) est classé en deux types : de proximité ou distant.

Nous nous intéressons au paiement de proximité qui permet aux clients de stocker leurs informations relatives au paiement dans leurs appareils mobiles, par exemple, le paiement NFC au point de vente. Les terminaux de point de vente embarquant la NFC sont à grande échelle, cependant certains chercheurs se posent la question sur la possibilité d'effectuer des paiements NFC de personne à personne (P2P) en utilisant des téléphones portables. Récemment un

fournisseur - Paypal - a découvert une nouvelle solution de paiement P2P permettant à un utilisateur Android d'effectuer un paiement par jeton (tag) à un autre en rapprochant leurs appareils compatibles NFC à proximité. Cependant, ces méthodes de paiement sont confrontées à des défis importants en raison de la complexité de l'écosystème et du manque d'infrastructures de support [Okereke and Mary 2017].

1.5.2.1 Transaction dans un paiement mobile

Le m-paiement représente une avancée intuitive et une évolution des modes de paiement qui étaient basés sur des espèces, des chèques et des cartes de crédit et maintenant ont évolué dans un format purement électronique utilisant peu de moyens physiques via des applications smartphones dédiées, basés sur des systèmes de paiement adaptés à cet effet. Les transactions de paiement sont effectuées par l'utilisation exclusive des smartphones ou des appareils PDA (Personal Digital Assistant) [Kolaki 2017]. Une transaction dans un paiement mobile représente une opération de paiement réalisée, à partir d'un support connecté (ex : smartphone, tablette), mais dont la terminaison fait appel obligatoirement à un des moyens de paiement existants.

1.5.2.2 Paiement par carte à puce (Smart card)

Les cartes à puce sont des dispositifs qui comprennent des circuits intégrés, une unité de mémoire ou une puce de microprocesseur. La motivation des cartes à puce est la nécessité d'un traitement et d'un transfert de données efficaces et sécurisés et l'enregistrement des applications portables pouvant être mis à jour ainsi que le stockage et le traitement d'informations personnelles et privées. Les cartes à puce sont utilisées dans différents domaines : l'authentification, l'autorisation, le stockage de données, l'identification, la banque, la vente au détail et le transport (Figure 1.13). L'un des principaux avantages du système de carte à puce est de pouvoir traiter, stocker et transférer efficacement les données sous forme électronique [Akman 2015].

Figure 1.13 : Carte à puce utilisée dans le transport public [Dreamstim 2018].

1.5.2.3 Paiement par smartphone

Les paiements mobiles, généralement définis comme l'utilisation d'un appareil mobile pour initier, autoriser et confirmer un échange de valeur financière en échange de biens et de services [Ok et al. 2010], sont devenus un axe majeur des activités commerciales et de recherche dans les dernières années. De nombreux pays ont été recensés, couvrant un large éventail de situations de paiement (Figure 1.14), d'approches techniques et de modèles commerciaux. S'il est déjà possible de trouver de multiples solutions de paiement dans de nombreux pays, les paiements mobiles restent essentiellement une technologie émergente, cherchant à combler l'écart entre le potentiel envisagé et l'utilisation généralisée [Coskun et al. 2015].

Figure 1.14 : Paiement près d'un point de vente en utilisant un smartphone NFC [PNGEgg 2020].

1.6 Dispositifs et applications NFC

Un nombre croissant d'appareils utilisent les normes NFC pour améliorer notre vie quotidienne. European Panasonic Industry offre une variété de composants qui offrent de nouvelles opportunités aux développeurs et aux entreprises. Des améliorations en termes de durabilité et de sécurité garantiront que les appareils connectés NFC nous accompagneront à l'avenir [Panasonic Industry 2019].

1.6.1 Panorama du NFC

La technologie NFC est conçue pour une distance de fonctionnement de quelques centimètres, ce qui rend plus difficile pour les attaquants d'enregistrer la communication entre un appareil NFC Forum et une étiquette NFC Forum par rapport à d'autres technologies sans fil qui ont une distance de fonctionnement de plusieurs mètres [NFC Forum 2020].

1.6.1.1 Historique

NFC est un sous-ensemble de la technologie d'identification par radiofréquence (RFID) avec une portée de communication plus courte à des fins de sécurité. Le premier brevet associé à la RFID a été accordé à Charles Walton en 1983.

En 2003, Sony et Philips ont créé la communication en champ proche (NFC), et plus tard, ISO/IEC (International Standard Organisation / International Electro-technical Commission) a adopté 18092, une spécification d'interface et de protocole qui sert de base à la fonctionnalité NFC.

En 2004, Nokia, Philips et Sony ont créé le Forum de communication en champ proche (NFC) pour promouvoir et développer la nouvelle technologie.

En 2006, le premier ensemble de spécifications pour les étiquettes NFC a été produit par le groupe ‘Near Field Communication’. Le cahier des charges des affiches « intelligentes » a également été créé. Les affiches intelligentes contiennent des informations qu'un appareil compatible NFC peut lire lorsqu'il est passé dessus. Le premier téléphone portable compatible NFC, le Nokia 6131, a également été fabriqué.

En 2010, Android a produit son premier téléphone NFC, le Samsung Nexus S.

Cependant, en 2011 et 2012, un certain nombre de projets pilotes de haut niveau des parties prenantes ont attiré une attention plus large sur la technologie NFC.

En 2014, Asia NFC Alliance a établi quatre grands opérateurs de télécommunications (HKT de Hong Kong, Chunghwa Telecom de Taïwan, SK Planet de Corée du Sud et KDDI du Japon) pour fournir des services compatibles NFC simples et rapides aux clients voyageant entre ces pays [Ali 2015].

1.6.1.2 Normes du NFC

La technologie NFC est intégrée dans divers dispositifs tels que les cartes à puce, les lecteurs de cartes, les téléphones portables etc. Pour assurer l'ajustement des consommateurs de cette technologie, les acteurs concernés (fabricants, opérateurs, développeurs, etc.) doivent travailler en étroite collaboration et les applications doivent être interopérables. Cela nécessite un accord entre les organismes de normalisation qui ont la responsabilité principale d'assurer l'interopérabilité des différents dispositifs NFC. Les principales normes NFC sont fixées par les organismes suivants :

- ISO/IEC;
- ECMA (European Computer Manufacturers Association);
- ETSI (European Telecommunications Standards Institute).

Un consortium international connu sous le nom de « NFC Forum » a été créé en 2004 à l'initiative de Sony et Phillips qui a pour objectif principal de promouvoir l'utilisation de la technologie NFC [Chabbi 2015].

1.6.1.3 Architecture et fonctionnement d'un système NFC

La communication NFC se produit entre deux appareils compatibles NFC placés à quelques centimètres l'un de l'autre en utilisant la fréquence de fonctionnement de 13,56 MHz. Elle permet une communication facile entre divers appareils NFC sur des interfaces radio ISO / IEC 18000-3, avec des taux de transfert de 106, 212 et 424 kbits par seconde. L'appareil qui démarre la communication est appelé l'initiateur, tandis que le dispositif répondant est la cible. Les smartphones et les lecteurs NFC utilisent leurs propres alimentations, donc ils sont des appareils actifs, tandis qu'une balise NFC utilise la puissance de l'autre partie, et donc, elle est appelée un appareil passif. Tous les périphériques initiateurs sont généralement des périphériques actifs, mais un périphérique cible peut être actif ou passif, selon son mode de fonctionnement [Coskun et al. 2015]. Pour assurer une communication radiofréquence entre les dispositifs émetteurs et récepteurs, ces appareils utilisent des antennes et des circuits qui utilisent des couplages inductifs et magnétiques et des techniques de modulation et de codage.

– ***Couplage inductif NFC***

La NFC repose sur le principe de couplage inductif entre les dispositifs d'émission et de réception (Figure 1.15), et diffère de la communication RF en champ lointain, qui est utilisée pour les applications sans fil à longue portée [Coskun et al. 2015]

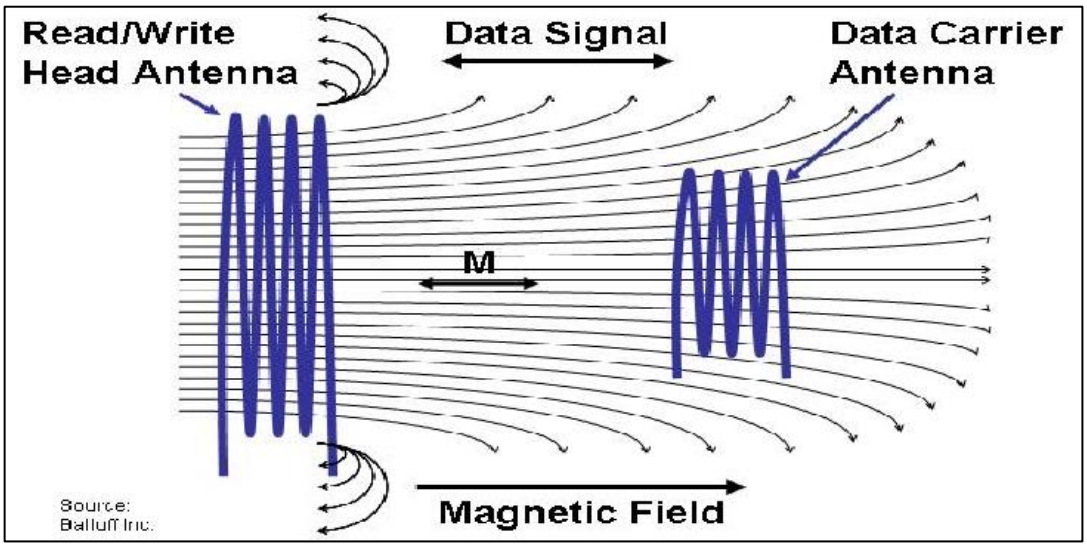

Figure 1.15 : Couplage inductif [Research gate 2013].

– ***Antennes et couplage magnétique***

Un premier circuit de communication en champ proche (NFC) comprend une antenne, un circuit de charge, un circuit émetteur-récepteur et un circuit de retard de transmission. L'antenne est configurée pour se coupler par induction aux signaux émis par un deuxième circuit NFC. Le circuit de charge est configuré pour émettre la puissance fournie par le couplage inductif à travers l'antenne aux signaux émis par le deuxième circuit NFC (Figure 1.16). Le circuit émetteur-récepteur est configuré pour être alimenté par le circuit de charge afin de transmettre des données pour la réception par le deuxième circuit NFC. Le circuit de retard de transmission est configuré pour être alimenté par le circuit de charge et commander le circuit émetteur-récepteur pour retarder la transmission des données jusqu'à l'expiration d'un temps de retard défini après que le circuit émetteur-récepteur est devenu suffisamment allumé pour fonctionner et transmettre les données [Nambord and Emil 2017].

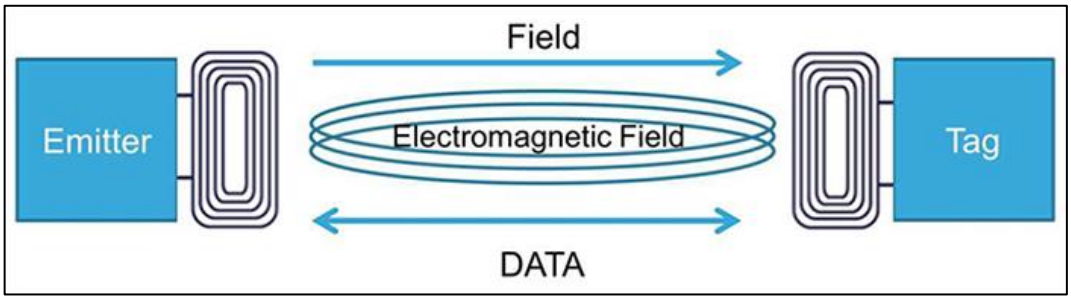

Figure 1.16 : Antennes et couplage magnétique [Mouser Electronics 2020].

– ***Techniques de modulation / codage***

Dans la technologie NFC, les transactions sont effectuées avec des appareils à proximité à l'aide de protocoles de communication normalisés. Un exemple d'un tel protocole est l'ISO / CEI (Commission électrotechnique internationale) 14443. Ce protocole se compose de quatre parties et décrit deux types de cartes : Type A et Type B, qui communiquent toutes les deux par radio à 13,56 MHz. Les principales différences entre ces types concernent les méthodes de modulation (Figure 1.17), les schémas de codage et les procédures d'initialisation de protocole. Par exemple, dans un protocole, la NFC utilise deux codages différents pour transférer des données. Si un appareil actif transfère des données à 106 kbits / s, un codage Miller modifié avec une modulation à 100% est utilisé. Dans tous les autres cas, le codage Manchester est utilisé avec un taux de modulation de 10%. Les cartes de type A et de type B utilisent le même protocole de transmission. Le protocole de transmission spécifie l'échange de blocs de données et les mécanismes associés : enchaînement de blocs de données ; prolongation du temps d'attente ; multi-activation, etc. Il existe d'autres types de protocoles définis, tels que le type F, etc. [Levy et al. 2016].

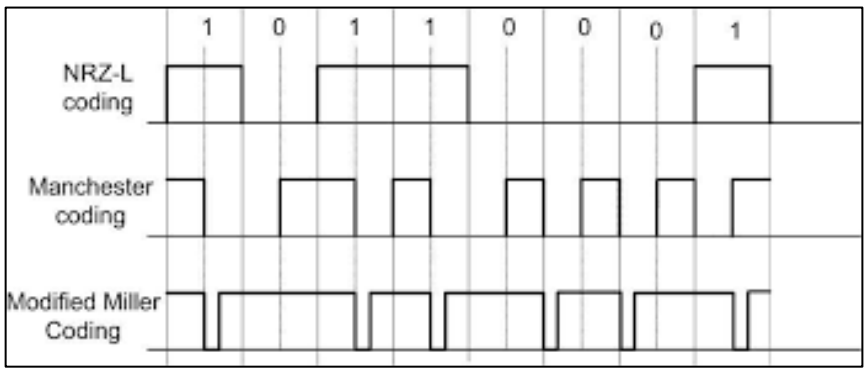

Figure 1.17 : Techniques de modulation et codage [Rohde & schwarz 2013].

1.6.1.4 Modes de communication

Trois types d'appareils NFC sont impliqués dans la communication NFC : les smartphones, les tags NFC et les lecteurs NFC. Les styles d'interaction possibles entre les appareils NFC offrent trois modes de fonctionnement différents (Figure 1.18) : modes de fonctionnement lecteur / enregistreur (Lecture du contenu d'un tag ou d'une balise NFC par un smartphone), peer-to-peer (Echange de données entre deux smartphones) et émulation de carte (Le contenu du smartphone est lu par un lecteur NFC) [Coskun et al. 2012], [Coskun et al. 2013] [Coskun et al. 2015].

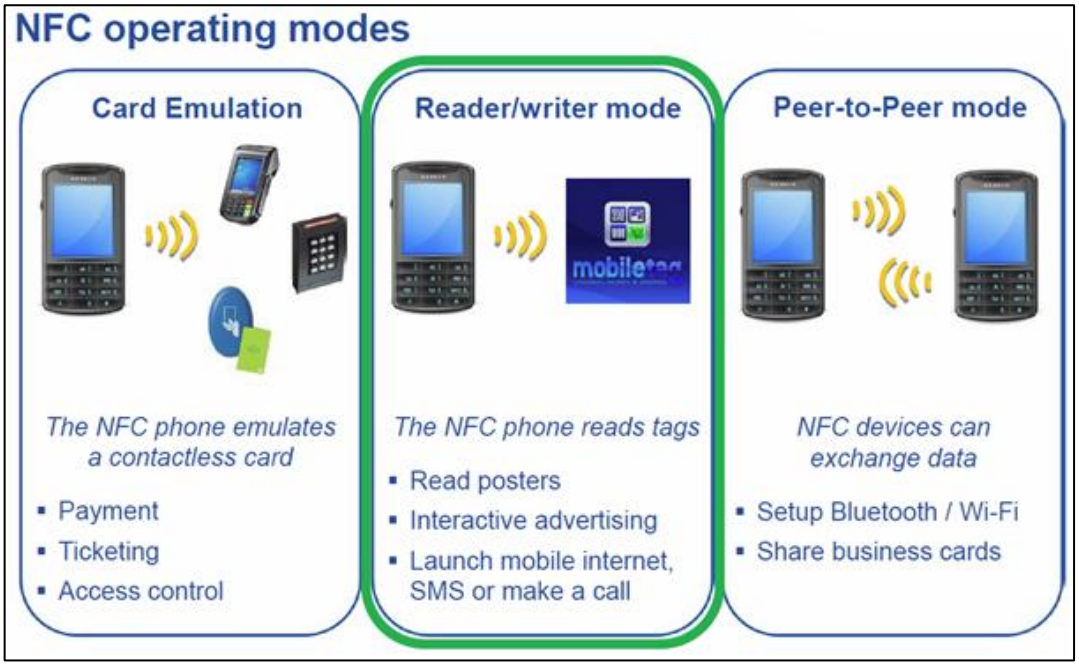

Figure 1.18 : Modes de communication NFC [The RFIP Blog-Wordpress.com 2016].

1.6.1.5 Marchés du NFC

La technologie NFC est en développement rapide à cause de la demande croissante d'applications de paiement sans contact et de la nécessité du contrôle d'accès destinés aux dispositifs mobiles (tablette, smartphone etc.). En effet, selon la recherche ABI (Allied Business Intelligence), le marché NFC a démarré vers 2009/2010 avec des volumes de ventes de puces NFC limités et a très vite dépassé 350 millions de pièces vendues en moins de 3 ans. Ce marché est estimé à 1 milliard d'unités vendues en 2016 et environ 2,3 milliards d'unités en 2019 [Tornambé 2016]. La figure 1.19 donne une idée sur l'évolution du marché NFC en spécifiant, le volume des smartphones et PC (Personal Computer) dotés de la technologie NFC vendus selon les années spécifiées.

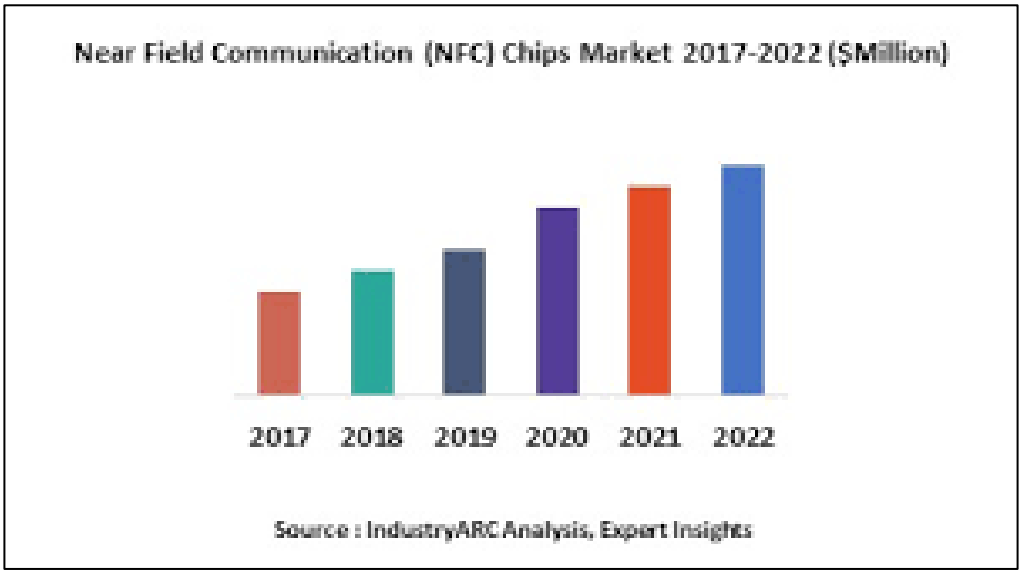

Figure 1.19 : Marché des chips NFC [Industry ARC 2020].

1.6.2 Dispositifs NFC

La communication en champ proche (NFC) est un ensemble de normes définies par le NFC Forum qui permet des communications de faible puissance basées sur la proximité entre les appareils électroniques grand public tels que les téléphones mobiles, les tablettes, les ordinateurs personnels ou les appareils portables. Un dispositif, l'initiateur, utilise l'induction magnétique pour créer un champ d'ondes radio que la cible peut détecter et accéder, permettant à de petites quantités de données d'être transférées sans fil sur une courte distance (à moins de 4 cm en pratique) [U.S. Payments Forum 2019]. Parmi les dispositifs NFC, on peut citer aussi les ATM NFC et le point de vente (POS) NFC qui peuvent communiquer avec une carte ou un téléphone NFC pour effectuer des paiements.

1.6.2.1 Point de vente (*Point of sale*)

Un point de vente est l'endroit où une transaction de vente au détail est effectuée et où un client effectue un paiement au commerçant en échange de biens ou de services [U.S. Payments Forum 2019].

Les systèmes de paiement sans contact pour un point de vente devraient apporter les avantages suivants : rapidité et commodité au point de vente, plus grand niveau de protection des consommateurs par rapport à l'argent comptant, réduction de l'utilisation de l'argent comptant et des coûts associés, plus de choix pour les clients lors des paiements. Les paiements sans contact représentent les paiements sans espèces qui ne nécessitent pas de contact physique entre le téléphone mobile du consommateur et les terminaux de point de vente du commerçant.

Les plus grands établissements de paiement prennent en charge ces types de paiements. La mise en œuvre des systèmes de paiement sans contact est basée sur la même infrastructure qui existe pour les cartes de paiement à bande magnétique et ne nécessite pas d'investissements supplémentaires de la part de l'entreprise et des institutions financières, à part la mise à niveau des terminaux POS existants (Figure 1.20) [Lacmanovié and Izabela 2011].

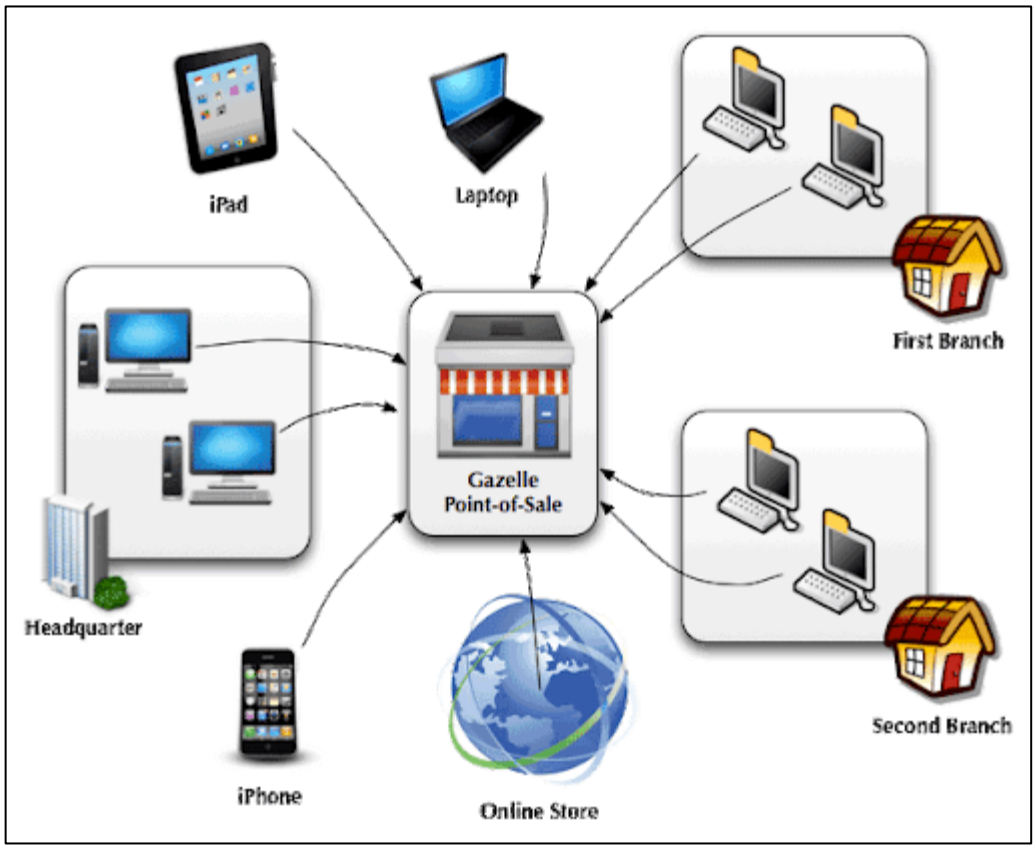

Figure 1.20 : Un point de vente en architecture Gazelle [PNG wing 2016].

1.6.2.2 Guichet automatique bancaire

Cette section décrit le matériel, les logiciels et la configuration ATM requis pour prendre en charge les transactions EMV (Europay Master card et Visa) sans contact.

Chaque fournisseur ATM peut avoir des exigences propriétaires spécifiques ou prendre en charge des fonctionnalités propriétaires uniques. Chaque propriétaire / opérateur ATM devrait communiquer avec son ou ses fournisseurs ATM pour comprendre tous les aspects uniques ou exclusifs d'une marque ou d'un modèle ATM particulier, car cela peut avoir un impact sur la configuration EMV et / ou sans contact pour cet équipement. De plus, le propriétaire / opérateur de l'ATM doit s'assurer que les fournisseurs de matériel / logiciel ATM comprennent les exigences commerciales associées [U.S. Payments Forum 2019].

– ***Architecture hardware***

Les GAB qui ne prennent actuellement pas en charge les lecteurs NFC auront besoin d'un lecteur NFC pour prendre en charge les transactions EMV sans contact. Le fournisseur de matériel est responsable de l'obtention de l'approbation des réseaux de paiement mondiaux auprès d'EMVCo (EMV and American Express, Discover, JCB). [U.S. Payments Forum 2019].

– ***Architecture software***

Les déployant ATM doivent établir une vérification auprès de leurs fournisseurs de logiciels pour déterminer si leur logiciel d'application qui est compatible EMV est compatible avec la configuration sans contact qu'ils prévoient de déployer. Individuellement, chaque réseau de paiement nécessite une lettre d'approbation et une autre de certification. Le logiciel ATM lui-même ne nécessite ni test ni approbation EMVCo [U.S. Payments Forum 2019].

– ***Fonctionnement***

Pour les guichets automatiques qui peuvent accepter des transactions sur plusieurs interfaces, toutes les interfaces autorisées doivent être mises à la disposition du commerçant / titulaire de la carte pour effectuer une transaction. Cependant, pour éviter les interférences entre la puce de contact et l'interface sans contact, le lecteur doit toujours éteindre l'interface sans contact avant que le dispositif ATM ne réinitialise la carte pour lancer une transaction de puce de contact. L'interface sans contact doit rester hors tension pendant la durée de la transaction effectuée à l'aide de l'interface de puce de contact. De même, lorsque l'interface sans contact est utilisée, la fente de l'ATM pour la carte doit être désactivée [U.S. Payments Forum 2019].

1.6.2.3 Smartphone

Un Smartphone est un téléphone portable géré par un système d'exploitation et qui peut soutenir des applications tierces natives. Un smartphone contient de multiples interfaces de communication qui ont la capacité de maintenir la connectivité [Guerar 2017].

– ***Architecture physique***

Un smartphone est composé de circuits intégrés combinant des différentes fonctionnalités. Le processeur gère les instructions qui sont liées aux applications et aussi qui sont relatives à la fréquence radioélectrique, pour établir des connexions aux différents réseaux. Les composants attachés s'occupent de la gestion des interfaces de connexions, de la caméra,

de l'audio, des capteurs de la mémoire externe, de la batterie, et de l'interface utilisateur [Grossi 2019].

– ***Architecture logique***

Cette architecture est composée du système d'exploitation (généralement Android) et des applications développées.

1.6.3 Applications NFC

Les smartphones dotés de la technologie NFC permettent plusieurs services mobiles innovants, tels que le paiement, la billetterie, le couponnage et la contrôle d'accès [Rodrigues 2014].

1.6.3.1 Contrôle d'accès

Un scénario physique typique de contrôle d'accès est un bureau d'entreprise avec plusieurs départements protégés par des portes à commande électronique. Un employé peut ouvrir une porte en présentant son téléphone à un lecteur NFC situé près de la porte (Figure 1.21). Le lecteur et le téléphone se communiquent afin de vérifier que l'utilisateur a accès. Par la suite, la porte électronique est ouverte et l'employé peut entrer dans le bâtiment.

Un système de contrôle d'accès physique (PACS : Physical Access Control System) peut être défini comme un système qui restreint l'accès à une ressource physique, par ex. bâtiment, chambre, parking ou un casier à un nombre sélectionné d'utilisateurs. Un PACS prend en charge deux activités principales : l'authentification et l'autorisation. Lorsqu'un utilisateur demande l'accès à une ressource physique, elle revendique une identité (par exemple, son nom) et le processus d'authentification vérifiera la validité de cette réclamation. L'autorisation consiste à déterminer ce qu'un utilisateur est autorisé à faire une certaine tâche [Bolhuis 2014].

Figure 1.21 : Contrôle d'accès par un smartphone NFC [Security Magazine 2011].

1.6.3.2 Transport

L'utilisation d'une carte à puce électronique pour les services de transport comme alternative des moyens d'accès et de paiement émerge maintenant comme une option viable pour de nombreux opérateurs. Avec l'introduction récente des cartes à puce Oyster dans le domaine de transport (Figure 1.22) à Londres et leur intégration dans le domaine de billetterie, le Royaume-Uni est familiarisé avec le transport utilisant des cartes à puce dirigées par les autorités locales. L'interopérabilité entre les systèmes est en cours, elle est abordée par l'ITSO (Integrated Transport Smart Card Organisation) qui a fourni une version finale d'une spécification pour le transport des cartes à puce au début 2004 [Blythe 2004].

Figure 1.22 : Utilisation d'un smartphone NFC dans le transport public [The straits times 2016].

1.6.3.3 Billetterie

Un cas d'utilisation important d'une billetterie NFC est la carte de voyage dans les transports publics des grandes villes. L'utilisateur achète sa carte auprès du vendeur des cartes de voyage. La carte de voyage peut être débitée en fonction de différentes périodes prédéfinies à partir de la période minimale jusqu'à un mois ou même pour une période plus longue. Pendant la validité du billet, chaque fois que l'utilisateur utilise les transports en commun, il rapproche sa carte de voyage NFC près d'un lecteur compatible NFC mobile se trouvant dans le véhicule ou bien il la remet au contrôleur pour effectuer cette opération. Le lecteur NFC confirme la validation du ticket par un feu vert et un son spécifique. L'invalidation de ticket est indiquée par une lumière rouge et un son spécifique associé. Le lecteur NFC indique l'heure d'expiration imminente de la carte de voyage par une combinaison de lumière verte et jaune et un son associé. L'option alternative d'acheter un temps d'utilisation pour la carte de voyage est de charger la carte de voyage avec une valeur monétaire. Dans ce cas, l'utilisateur peut payer ses transports publics séparément pour chaque utilisation en tenant la carte de voyage compatible NFC à proximité du lecteur NFC et en appuyant sur le bouton de la zone de voyage de son choix dans le lecteur. Le lecteur compatible NFC communique avec la carte de voyage NFC et vérifie si la valeur monétaire disponible dans la carte de voyage est suffisante pour la zone de voyage choisie. S'il y a une valeur monétaire suffisante dans la carte de voyage, le lecteur facture la somme du solde de la carte indiquant le succès de l'opération par un feu vert, un son associé et affichant également les informations attachées sur le moniteur de l'appareil. Si le solde de la carte de voyage est insuffisant pour la zone de voyage choisie, le lecteur NFC le signale par une lumière rouge et un son spécifique. Dans certaines villes, l'utilisateur peut même utiliser la valeur monétaire de la carte de voyage compatible NFC pour payer les frais d'entrée pour les piscines publiques équipées de lecteurs compatibles NFC.

Un autre cas d'utilisation intéressant pour la billetterie NFC est l'utilisation des tickets de cinéma. Outre la méthode traditionnelle de vente des billets de cinéma. [Akman 2015].

La billetterie NFC est utilisée aussi dans les systèmes d'identification utilisés pour automatiser des stations de Gaz et pétrole d'une entreprise (Figure 1.23). Ces systèmes basés sur la technologie NFC facilitent le contrôle et optimisent la consommation de carburant des véhicules de la société. Ils sont conçus pour faciliter l'enregistrement et le contrôle du processus et pour permettre le remplissage sans la présence de l'opérateur [Lekic 2013].

Figure 1.23 : Payer au parking avec NFC smartphone [Istock 2019].

1.6.3.4 Couponing

Le couponing est une technique de promotion des ventes basée sur l'utilisation de coupons de réduction ou de remboursement partiel liés à l'achat d'un produit. Les coupons peuvent être distribués avant l'achat, apparaître sur le produit ou sur un autre produit de la marque (coupon croisé). Dans le cas d'un smartphone NFC, il faut le mettre à proximité du terminal **NFC** et la caisse, qui y est connectée, analysera les informations des coupons et le montant total à payer sera automatiquement déduit de la remise accordée (Figure 1.24).

Figure 1.24 : Scanner QR code présenté par un commerçant pour ajouter un coupon [BCV 2017].

1.6.3.5 Paiement

Les paiements mobiles sans contact sont des paiements en magasin que les consommateurs effectuent en utilisant des applications installées sur leur appareils mobiles. Parmi les applications mobiles qui sont actuellement disponibles : Amex Pay, Apple Pay, Barclays Contactless Mobile, Google Pay et Samsung Pay. Ces applications permettent aux consommateurs de télécharger les détails de leur carte sur l'application pour effectuer des paiements à partir de leurs appareils.

D'un point de vue technique, lorsqu'un consommateur souhaite utiliser une application de paiement mobile sans contact, l'application doit communiquer avec le système du point de vente (POS) d'un détaillant. En UK (United Kingdom), la grande majorité des systèmes de paiement mobile sans contact lancés via des appareils mobiles utilisent la NFC. Au terminal POS du détaillant, une transaction avec une application de paiement mobile sans contact est identique à une transaction par carte sans contact. L'application de paiement mobile communique avec l'antenne de l'appareil NFC de l'utilisateur pour envoyer le paiement au terminal de point de vente du détaillant [PSR 2018]. La figure 1.25 représente un paiement mobile à base de NFC entre un smartphone et un guichet automatique bancaire (ATM).

Figure 1.25 : Paiement mobile NFC avec smartphone et ATM [Insight Vault-co-op Financial services 2017].

1.7 Conclusion

Dans ce chapitre, nous avons présenté un panorama de l'état de l'art sur les technologies de communication sans contact, qui sont considérées parmi les technologies les plus importantes de nos jours. Concrètement, nous avons évoqué les technologies de communication sans fil et sans contact, les techniques d'identification et celles d'authentification ; les services sans contact et précisément le service de paiement et la technologie NFC en détail avec présentation des dispositifs et applications liées à cette technologie.

A travers ce chapitre, différentes technologies sans contact et sans fil qui se sont imposées dans la vie courante des utilisateurs ainsi que des techniques d'identification et d'authentification utilisées lors de communication sans contact ont été recensées.
Quelques services sans contact et spécifiquement le paiement ont été également présentées.

Nous avons présenté la technologie NFC à travers une exploration qui a commencé par une vue d'ensemble de cette technologie incluant ses normes, l'architecture de son système et ses modes de communication, puis s'en est suivie une présentation des dispositifs NFC utilisés généralement lors du paiement sans contact à savoir un POS, un ATM et un smartphone, ensuite, elle est terminée par une considération des principales applications NFC.

Dans le prochain chapitre, nous allons donner une vue d'ensemble des différentes attaques physiques et logiques contre une carte de crédit ou une carte bancaire, un smartphone ou un ATM proposé dans la littérature. Nous discuterons brièvement des méthodes, des techniques et des contre-mesures proposées dans la littérature pour faire face à ces attaques en indiquant sous forme synthétique les limites et les inconvénients.

Chapitre 2

Chapitre 2 : Sécurisation des dispositifs et applications NFC

Sommaire

2.1 Introduction

La sécurité NFC est d'une importance capitale pour un très grand nombre de consommateurs, particulièrement pour leurs comptes bancaires. La NFC commence tout juste à atteindre une visibilité du grand public, aidée par son introduction en tant que « Android Beam » dans Android. Google Wallet, un système de paiement sans contact, a considérablement accru la popularité du paiement sans contact grâce à la NFC et a mis en cause les implications de sécurité NFC. La technologie NFC est une technologie en pleine croissance qui est sur le point d'être acceptée par le grand public, les vulnérabilités d'une technologie avec une telle utilisation projetée, notamment pour les transactions financières, sont extrêmement importantes pour ceux qui souhaitent la mettre en œuvre par eux-mêmes. La NFC est plus sûre que son prédécesseur, la RFID, mais son utilisation généralisée comme système de paiement sans contact nécessite un examen attentif de la sécurité d'une cible aussi lucrative pour les attaquants.

Ce chapitre donne un aperçu des vulnérabilités NFC, ainsi que des méthodes et techniques de lutte contre ces vulnérabilités. Nous remarquons dans ce chapitre, les efforts de plusieurs auteurs pour lutter contre les attaques qui peuvent cibler une carte de crédit, un smartphone ou un GAB.

2.2 Défis de sécurisation des dispositifs et applications NFC

L'utilisation des applications et des dispositifs NFC nécessitent souvent la manipulation et le traitement des informations confidentielles de l'utilisateur qui peuvent être restituées par des tiers malveillants. Par conséquent, il est nécessaire, voire inévitable d'alimenter ces systèmes par des techniques, des méthodes, des solutions et des protocoles qui augmentent le niveau de sécurité des applications et des appareils NFC afin de protéger les informations contre toute révélation ou utilisation non autorisée. Les stratégies de sécurité doivent protéger les informations confidentielles et sensibles qui sont stockées sur un dispositif NFC et aussi les données transmises.

2.3 Méthodologie d'une attaque

L'ingéniosité des attaquants peut être parfois illimitée. Généralement, ils peuvent s'adapter et exploiter efficacement les ressources disponibles et les vulnérabilités. La réalisation d'attaques se décompose souvent en plusieurs étapes (voir Figure 2.1) :

- Collecte d'informations : Elle consiste essentiellement à connaitre les mécanismes et les niveaux de sécurité en vigueur concernant l'identification, l'authentification, le contrôle d'accès, la cryptographie et la surveillance et à identifier les failles techniques, organisationnelles et humaines de l'environnement. De plus, l'attaquant pourra éventuellement profiter de la naïveté ou de la crédulité des utilisateurs pour leur soutirer des informations facilitant la création d'une attaque (notion d'ingénierie sociale). Ainsi, il pourra obtenir les clés d'entrée dans les systèmes informatiques (identification de l'utilisateur et mot de passe), pénétrer les systèmes et exécuter toute sorte d'opération de lecture ou d'écriture.
- Le fraudeur s'emploie également à détecter et à exploiter les failles de sécurité qui sont parfois connues mais non encore réparées (c'est-à-dire non patchées). Il pourra alors utiliser les techniques d'attaques préexistantes et éventuellement disponibles en ligne
- Paramétrer les attaques en fonction de ses besoins pour accéder au système ciblé et exécuter son action malveillante
- A la phase d'exfiltration, l'attaquant fait en sorte que l'attaque ne puisse être détectée ou du moins ni facilement ni rapidement et qu'il ne laisse pas de trace pouvant servir à son identification. Pour contribuer à cela, il essaye de rester anonyme, il utilise de fausses identités, il utilise l'identité numérique d'utilisateurs, il brouille les pistes en passant par plusieurs systèmes intermédiaires par exemple. Le principe d'un malveillant est de ne pas laisser la trace de sa présence dans les systèmes visités. En effet, pour sa sécurité personnelle, s'il a effectué un acte illégal aux suites judiciaires, il a tout intérêt à savoir effacer toute information qui permet de lier la preuve de sa présence et de ses actions illicites à des données, qui permettent sa localisation et son identification [Akrout 2012].

Figure 2.1 : Une étape d'attaque [ENSICAEN 2020].

2.4 Concepts de base de la sécurité

La sécurité informatique est l'ensemble des moyens consacrés pour réduire le maximum possible de vulnérabilité d'un système vis-à-vis des menaces et des attaques accidentelles ou bien intentionnelles. Son objectif est de protéger les ressources matérielles ou logicielles d'un parc informatique contre des utilisations qui sont hors du cadre fixé ou par des personnes qui ne sont pas autorisées [Yende 2018].

2.4.1 Menaces et attaques

Les menaces sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité. Pour remédier aux failles et pour contrer les attaques, la sécurité informatique se base sur un certain nombre de services qui permettent de mettre en place une réponse appropriée à chaque menace. Une menace est un danger (interne ou externe) tel qu'un hacker, un virus, etc. [Yende 2018]. Une menace fait référence à un incident nouveau ou nouvellement découvert qui peut nuire à un système ou à une entreprise dans son ensemble. Il existe trois principaux types de menaces :

- Menaces naturelles, telles que les inondations, les ouragans ou les tornades
- Menaces involontaires, comme un employé accédant par erreur à des informations erronées
- Menaces intentionnelles, tels que les logiciels espions, les logiciels malveillants, les sociétés de publicité ou les actions d'un employé mécontent.

Les vers et les virus sont classés comme des menaces, car ils pourraient nuire à une organisation en s'exposant à une attaque automatisée, par opposition à une attaque perpétrée par des humains. Plus récemment, le 12 mai 2017, l'attaque WannaCry Ransomware a commencé à bombarder des ordinateurs et des réseaux à travers le monde et a depuis été décrite comme la plus grande attaque de son genre. Les cybercriminels proposent constamment de nouvelles façons créatives de compromettre les données, comme le montre le rapport 2017 sur les menaces de sécurité Internet [David 2020].

Une attaque informatique est définie comme une exploitation délibérée de systèmes informatiques, entreprises et réseaux dépendants de la technologie. Les attaques informatiques utilisent du code malveillant pour modifier le code informatique, la logique ou les données, entraînant des conséquences perturbatrices qui peuvent compromettre les données et conduire à des crimes informatiques, tels que le vol d'informations et d'identité [Junaidu 2011].

2.4.2 Propriétés de sécurité

Au regard de la sécurité, les utilisateurs s'attendent d'un système informatique vérifiant des exigences fondamentales en sécurité informatique qui peuvent être résumées en :

- Confidentialité : Seules les personnes habilitées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.
- Intégrité : Il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.
- Disponibilité : Il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement se mesure en

divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.

- Non-répudiation : Une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'émission et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée.
- Authentification : Elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données [Yende 2018].

2.4.3 Cryptographie

La cryptographie est la science de rendre inintelligible, de coder et de chiffrer un message pour ceux qui ne sont pas autorisés à le connaitre, c'est l'écriture de manière cachée. La cryptographie est aussi l'étude des techniques permettant d'envoyer des informations de manière confidentielle (chiffrée) sur un support donné [Raphael 2018]. Elle est utilisée surtout pour assurer la propriété de confidentialité.

2.4.3.1 Définitions

– ***La cryptanalyse***

Une tache effectuée par une personne non habilitée permettant de décrypter un message. Elle représente l'ensemble des stratégies d'attaques d'un système cryptographique. Son objectif est de reconstituer le texte en clair à partir de textes chiffrés en découvrant les clés ou en détectant les failles des algorithmes utilisés.

– ***Le cryptosystème***

C'est l'ensemble des clés possibles, des textes en clairs et des textes chiffrés correspondants à un algorithme donné.

– ***Principe de Kerckhoffs***

La sécurité d'un système cryptographique ne doit pas être basée sur la non divulgation des fonctions et des algorithmes de chiffrement et de déchiffrement qui sont utilisées mais sur la non divulgation des clés utilisées [Raphael 2018].

2.4.3.2 Algorithmes de chiffrement symétrique

Pour assurer la confidentialité d'un document électronique en utilisant un algorithme de chiffrement symétrique, on le chiffre en lui appliquant une fonction mathématique ayant comme paramètre une seule clé (K) qui est une suite de bits de différentes tailles (56 bits, 128, 256, etc.) générée aléatoirement et qui sera utilisée pour le chiffrement et le déchiffrement et qui doit rester

secrète et transmise de façon sûre (figure 2.2). Dans ce type d'algorithmes, la clé est utilisée dans des opérations de substitution et de transposition de bits du texte clair. Les algorithmes les plus répandus sont : AES, DES, 3DES, RC4, RC5, Vernam etc. L'avantage de ce type d'algorithmes est la rapidité. Son inconvénient est la distribution de la clé entre les deux entités et aussi, dans les grands systèmes où le nombre des utilisateurs est élevé, le nombre de clé sera élevé aussi [Raphael 2018].

Dans le domaine de paiement électronique utilisant la RFID ou la NFC, les algorithmes (fonctions) cryptographiques symétriques représentent une faiblesse si les clés cryptographiques correspondantes ne peuvent pas être suffisamment sécurisées sur les cartes et sur les lecteurs. L'algorithme à utiliser doit être fort examiné et reconnu par la communauté scientifique formée des experts en cryptographie et basé sur le principe de kutckhoffs [Jedaida 2016].

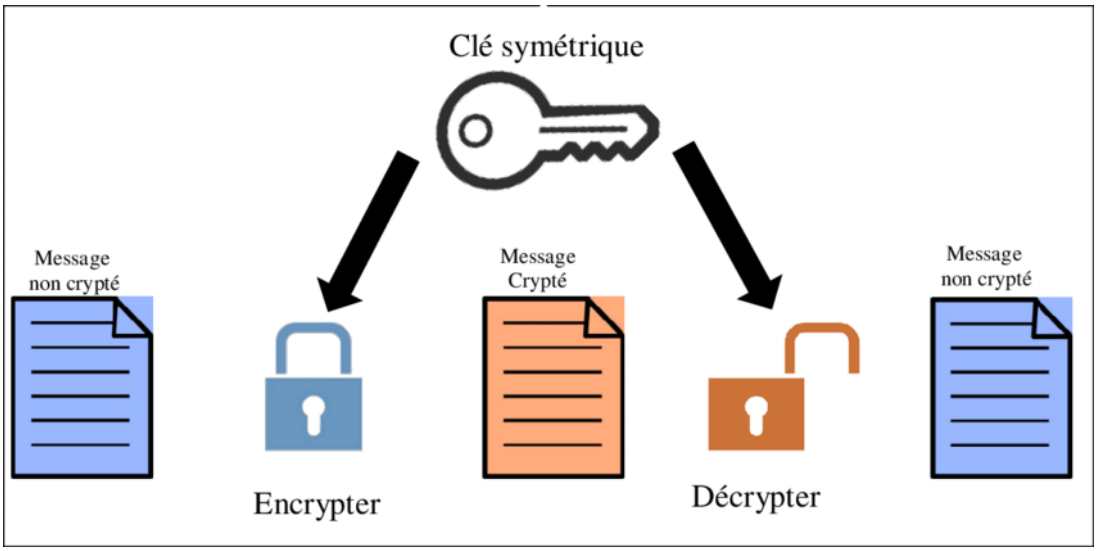

Figure 2.2 : Cryptographie symétrique [Litayem 2014]

2.4.3.3 Algorithmes de chiffrement asymétrique

Un algorithme de chiffrement asymétrique utilise une paire de clé (privée, publique). Il est appelé aussi chiffrement à clé publique. Tandis que la clé privée est connue seulement par son propriétaire, la clé publique est publiquement connue. La clé publique est dérivée de la clé privée, alors que l'inverse est mathématiquement impossible. La clé privée est utilisée pour le déchiffrement d'un message, alors que la clé publique est utilisée pour chiffrer un message. Le chiffrement asymétrique a comme but d'assurer la confidentialité et l'authenticité (figure 2.3).

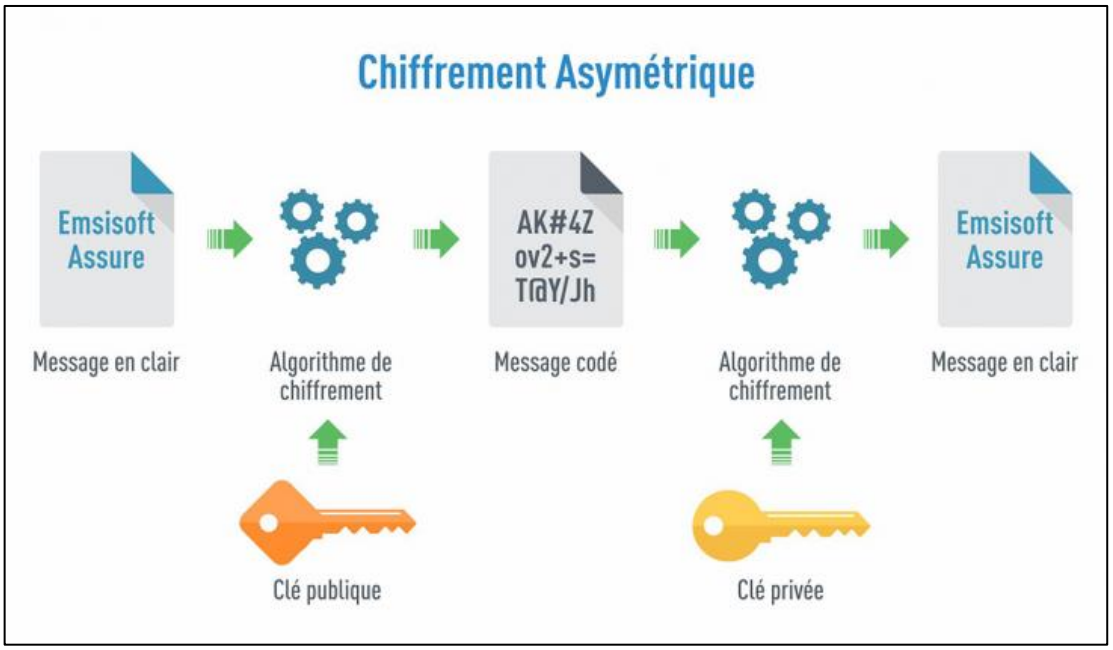

Figure 2.3 : Cryptographie asymétrique [Rajewski 2017]

2.4.3.4 Signature électronique (numérique)

Pour assurer la propriété d'intégrité et de non-répudiation, un algorithme de chiffrement asymétrique peut être renforcé par un mécanisme (système) de signature électronique. Dans ce système, avant d'envoyer un message chiffré avec la clé publique, l'émetteur calcule l'empreinte du message clair (en appliquant une fonction de hachage), le résultat est appelé empreinte ou condensé, puis chiffre cette empreinte avec sa clé privée. Le résultat obtenu est appelé signature numérique. Avant l'envoi, cette signature est ajoutée au message chiffré (concaténation), qui devient un message signé. A la réception, le récepteur sépare la signature numérique du message chiffré, déchiffre le message avec sa clé privée pour retrouver le message original, déchiffre la signature avec la clé publique de l'émetteur pour trouver l'empreinte reçue, applique la même fonction de hachage sur le texte clair retrouvé pour obtenir l'empreinte calculée, si l'empreinte reçue et calculée sont égales, alors le destinataire déduit que le message est intègre (n'est pas modifié), sinon le message reçu est altéré. Du même coup, l'émetteur ne peut nier l'envoi du message vu qu'il est le seul détenteur de la clé privée ayant servi à signer le message.

2.4.3.5 Fonction de hachage

Une fonction de hachage est une fonction mathématique qui, à partir d'un message (texte) de n'importe quelle longueur, génère un nombre de taille fixe inférieur à la taille du message. Ce nombre est appelé condensé, empreinte ou message digest (figure 2.4). MD5 (Message

Digest 5) est une fonction de hachage très répandue, qui calcule une empreinte sur 128 bits. Une fonction de hachage (H) est caractérisée par les propriétés suivantes :

- Irréversible : Étant donnée 'h', il est difficile de trouver 'x' tel que : h = H(x)
- La complexité est de l'ordre de 2n tels que n : est le nombre de bits du message digest.
- Étant donné x, il est impossible de trouver y différent de x avec H(x) = H(y)
- Le calcul est facile et rapide (plus rapide que le cryptage symétrique)

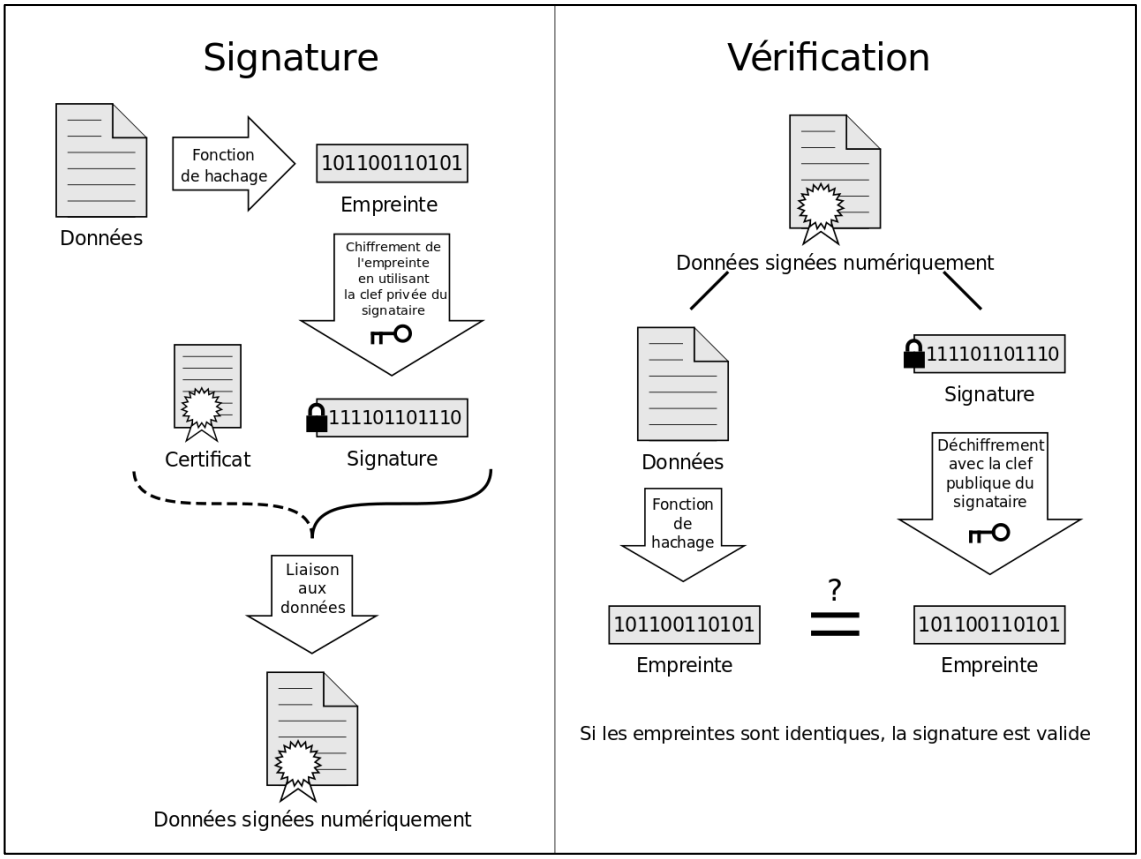

Figure 2.4 : Principe de fonction de hachage [Ryx 2017].

2.4.3.6 Certificat électronique

Dans le chiffrement asymétrique, il est considéré qu'une entité connaissait la clé publique d'une autre entité simplement en consultant un serveur web. Le problème est qu'il n'y a pas de garantie qu'une clé publique récupérée est correcte. Pour résoudre ce problème, un mécanisme supplémentaire appelé 'certificat électronique' ou 'certificat à clé publique' a été créé afin d'assurer la validité de la clé publique.

Un certificat est un document électronique contenant une clé publique, l'identité de son propriétaire (une personne, une machine, une application) et l'application pour laquelle il est émis. Pour une personne, le certificat prouve son identité, pour une application, il assure qu'elle

est dans le périmètre de ses fonctions (n'a pas été détournée), pour un site, il assure que c'est bien le vrai site. Un exemple de certificat à clé publique est le certificat X.509.

2.4.3.7 Cryptographie à courbes elliptiques

La cryptographie utilisant les courbes elliptiques est une branche de la cryptographie asymétrique. Le crypto système dans ce type de cryptographie est défini à partir d'un groupe déterminé sur des courbes elliptiques. Les notions et les avantages suivants sont tirés du principe de fonctionnement des courbes elliptiques [Jedaida 2016] :

– ***Courbe elliptique***

Une courbe elliptique sur un corp K est toute courbe d'équation :
$Y^2 = X^3 + aX + b$, avec 'a' et 'b' deux éléments de K tels que delta = $4a^3 + 27b^3$ différent de 0

– ***Loi d'addition dans les courbes elliptiques***

Soient 'E' une courbe elliptique, 'O' un point caractéristique à l'infini de 'E', 'P' et 'Q' deux points distincts de la courbe E, 'S': est un point d'intersection entre la courbe 'E' et la droite qui passe par les deux points 'P' et 'Q'. On définit '-S': le point symétrique de 'S' par rapport à l'axe des abscisses. La loi d'addition est définie comme suit : P + Q = -S. Cette loi vérifie les propriétés de fermeture, identité, commutativité et associativité.

– ***Paramètres du domaine***

Les paramètres du domaine sont les éléments qui définissent la courbe elliptique que les dispositifs communicants doivent se mettre d'accord. Ces paramètres sont les suivants :

- Les deux valeurs 'a' et 'b'
- Un point générateur de la courbe 'E' désigné par 'G'
- L'ordre de la courbe 'E' désigné par 'h'

– ***Génération des clés***

Soit 'p' un très grand nombre premier et 'G' le point générateur de la courbe 'E'. Chaque entité communicante doit générer une paire (Q, n) de clé publique et privée de la manière suivante :

- Choisir aléatoirement un entier 'n' de l'intervalle [1,p -1].
- Calculer 'Q' sur le groupe de la courbe elliptique de la façon : Q = n*G

– ***Avantages***

La cryptographie en utilisant les courbes elliptiques est caractérisée par les avantages suivants :

- Réduction de la taille des clés et des données échangées
- Equivalence du niveau de sécurité à d'autres algorithmes cryptographiques tels que : RSA (Rivest, Shamir & Adleman) et DSA (Digital Signature Algorithm).

2.5 Attaques dans NFC

Un dispositif NFC (carte, smartphone, ATM) peut être victime d'une attaque logique ou physique. Une attaque logique est une attaque qui entrave le logiciel de l'appareil. Les attaques logiques permettent aux cybercriminels de modifier le logiciel de l'appareil.

Dans les attaques physiques, les attaquants utilisent des objets, des produits (du matériel) pour avoir l'autorité de commandement sur l'appareil [Arun 2020].

2.5.1 Attaques physiques

Une carte de crédit, carte bancaire ou un smartphone peuvent subir des attaques physiques comme le vol et la perte ou des attaques sur l'infrastructure telles que la falsification physique des stations de base, qui peuvent être installées dans des locaux publics.

2.5.1.1 Attaques contre la carte ou le smartphone

– ***Attaques de vol ou perte***

Si un attaquant réussit à voler ou à trouver une carte ou un smartphone (Figure 2.5), il peut l'utiliser pour effectuer des paiements s'il a déjà volé le mot de passe. De plus, pour une carte volée, l'attaquant peut appliquer une attaque de clonage en utilisant une carte vierge afin de créer une nouvelle carte identique à celle volée afin de l'utiliser dans des futurs paiements.

– ***Attaques de l'infrastructure***

Une carte ou un smartphone peuvent être détruits d'une manière mécanique (Figure 2.6) ou chimique. Mécaniquement, le dispositif peut être exposé à un champ magnétique ou frappé par un outil par exemple un marteau. Chimiquement, le dispositif peut être détruit en utilisant des produits chimiques. Pour une carte, l'attaquant peut viser l'antenne en le découpant ou la puce en la détruisant [Thevenon 2011].

Figure 2.5 : Attaque vol du smartphone carte [Cnet France 2019].

Figure 2.6 : Attaque physique contre [WikiHow 2019].

2.5.1.2 Attaques contre ATM

– ***Attaques utilisant des explosives à gaz ou à solide***

Les attaques contre ATM utilisant des explosives à gaz ou des explosives à solide, exploitent les trous existants pour permettre l'insertion et la détonation de la charge explosive dans l'enceinte. Lors de la détonation, la pression explosive exerce une pression énorme sur tous les côtés de l'enceinte, y compris la porte. Si l'attaque réussit, le côté le plus faible se détachera, permettant l'accès à l'argent liquide se trouvant dans le GAB [ATMIA 2014].

– ***Attaques Ram Raid***

Cette attaque représente le cas où l'ATM est physiquement supprimé de son environnement d'installation (Figure 2.7) [Global Cyber Security Center 2016].

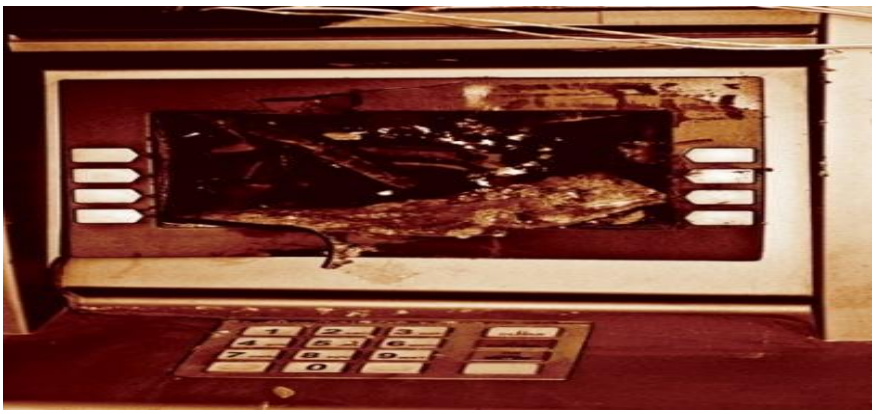

Figure 2.7: Attaque Ram Raid contre ATM [Security solutions Media 2012].

– ***Attaques de braquage***

Cette attaque signifie le retrait illégal d'espèces d'un GAB par la force ou l'intimidation (Figure 2.8). Cette attaque appliquée aux guichets automatiques n'est qu'un des nombreux problèmes où la police est appelée à en faire face. Elle peut comprendre :

- Vol de courriers qui remplissent les distributeurs automatiques de billets en espèces ;
- Vol de numéros d'identification personnels (PIN) (y compris vol par "surf à l'épaule") ;
- Vol par interception électronique de données ;
- Vol par transactions électroniques frauduleuses ;
- Vol d'argent dans les distributeurs automatiques de billets par un service bancaire ;
- Cambriolage des distributeurs automatiques de billets (y compris le vol de l'ATM entier) ;
- Présence de sans-abris dormant dans des vestibules des ATM ;
- Vandalisme des distributeurs automatiques de billets ;
- Utilisation frauduleuse de cartes ATM obtenues auprès de clients grâce à des guichets automatiques factices qui conservent leurs cartes [Michael 2001].

Figure 2.8 : Attaque de braquage contre ATM [Hyderabad studio N 2018].

– ***Attaques par piégeage de cartes ou de billets***

Le piégeage de carte ATM vole la carte physique elle-même via un périphérique connecté à l'ATM. Les cybercriminels placent un appareil directement sur ou dans le lecteur de carte ATM. Ces appareils sont conçus pour capturer les cartes une fois que les clients les ont insérées. Dans un environnement de bande magnétique ou un environnement de puce et de signature, les attaquants n'ont pas besoin du code PIN (Personal Identification Number) car le piégeage de cartes ou de billets à partir d'un GAB est suffisant pour compromettre le compte d'un client. La communication sans contact peut aider à lutter contre cette fraude.

Le piégeage d'espèces est un but pour les cybercriminels qui utilisent des appareils pour piéger physiquement l'argent qui est distribué et viennent ensuite le récupérer une fois que le client a quitté le guichet automatique [Owen 2016]. Cette attaque nécessite le placement d'un appareil de piégeage d'argent ou de faux présentateurs devant le distributeur de billets (Figure 2.9). Lors du traitement d'une transaction, un GAB distribue des billets dans le piège tendu par les cybercriminels plutôt que de présenter l'argent au client qui suppose que l'ATM a mal fonctionné

et qui va partir. Le cybercriminel revient alors, enlève le piège d'argent ou le faux présentateur, et repart avec de l'argent qui était destiné au client. Les propriétaires de GAB doivent mettre en place des mesures qui aident à atténuer les menaces internes [Kasanda and Jackson 2018].

Figure 2.9 : Attaque de piégeage de billets contre ATM [Malwarebytes labs 2019].

– ***Attaque par faux équipements***

Une autre préoccupation pour les opérateurs de distributeurs automatiques de billets est l'attaque utilisant des faux équipements ATM qui se présentent comme des dispositifs complémentaires tels que les faux lecteurs de cartes ou même les faux guichets automatiques. La première attaque de ce type était en 1993, quand un gang criminel connu sous le nom de Buckland Boys a installé un faux ATM dans un centre commercial de Manchester. Comme la plupart des faux équipements, il n'a pas été conçu pour voler de l'argent. Il est apparu aux clients comme un ATM qui ne fonctionnait pas tout en volant les données de la carte de tout client qui a tenté de l'utiliser [Saket et al. 2012].

– ***Attaque par superposition de faux clavier***

L'attaquant peut placer une superposition de faux clavier sur un vrai clavier (Figure 2.10). Ensuite, ce dispositif stocke les touches du clavier enfoncées avec l'heure. Ces informations peuvent être utilisées pour compromettre le code PIN. Désormais, un attaquant peut facilement utiliser une carte ATM de n'importe quel utilisateur [Anand et al. 2013].

Figure 2.10 : Attaque de faux clavier [State bank of Lincoln 2018].

2.5.2 Attaques logiques

Ces jours-ci, les attaquants utilisent de plus en plus les attaques logiques pour manipuler un logiciel ATM afin de retirer de l'argent ou capturer les données des clients. Connu sous le nom d'attaques logiques, elles peuvent devenir de plus en plus sophistiquées et basées sur une exécution bien organisée. Pour des représentants de logiciels malveillants, tels que Skimer, Ploutus, ou Stuxnet, ces attaques apportent de nouveaux défis pour sécuriser les guichets automatiques et pour fournir des services bancaires sécurisés [Braeuer et al. 2016].

2.5.2.1 Attaques contre la carte ou le smartphone

La plupart des applications NFC sont vulnérables aux mêmes types d'attaques des applications embarquées dans une carte RFID. Elles utilisent les mêmes faibles fonctions cryptographiques [Jdaida 2016].

– ***Attaques par rejeu***

L'attaque par rejeu est une technique par laquelle un utilisateur malveillant pourrait implémenter un appareil pour intercepter une transaction NFC et l'exécuter plus tard, en utilisant un autre appareil ou même dans différents emplacements (Figure 2.11).
Google Pay est la nouvelle version d'Android Pay. Cette application utilise des cryptogrammes validés dans le cloud pour effectuer des transactions NFC. En mars 2018, un problème est trouvé dans l'application, qui pourrait être exploitable par des utilisateurs malveillants pour intercepter et effectuer des transactions frauduleuses [Salvador 2018].

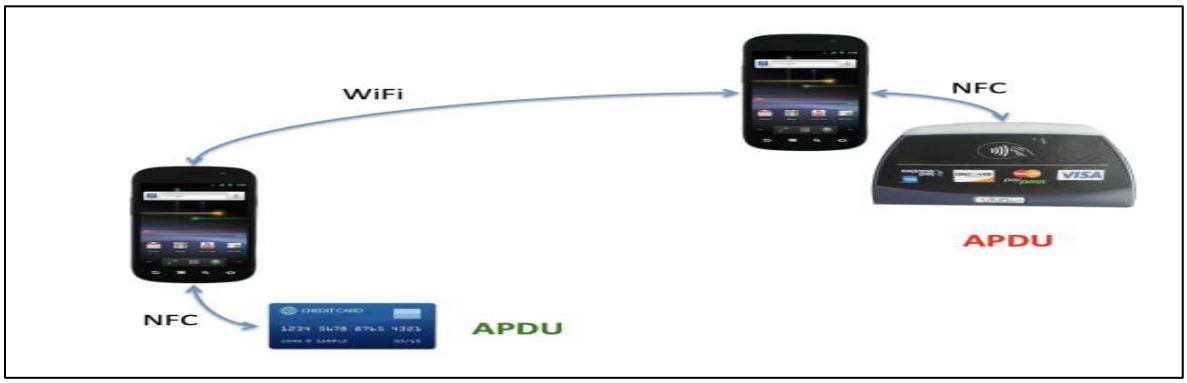

Figure 2.11 : Attaque par rejeu [Salvador Mendoza 2018].

– ***Attaques par force brute***

Un attaquant peut découvrir un mot de passe en essayant toutes les combinaisons possibles de chiffres et de lettres (Figure 2.12). Certaines personnes montrent une négligence

dans le choix du nom d'utilisateur et du mot de passe. Le fait de les choisir simples représente une étape risquée. Un attaquant recueille d'abord les informations fondamentales sur l'utilisateur. Par exemple, le nom complet de l'utilisateur, le numéro de chambre, le numéro du véhicule, les noms des enfants, etc. L'attaquant essaie en permanence des mots de passe aléatoires sur la base des informations personnelles de l'utilisateur jusqu'à ce qu'il réussisse. Cela peut également prendre des heures, des jours, des mois ou des années [Dave 2013].

Figure 2.12 : Le principe de l'attaque Force brute [TechJury 2020].

– ***Attaque Eavesdropping***

Un utilisateur malveillant peut collecter toutes les communications échangées entre le lecteur et la carte sur la liaison sans fil (Figure 2.13) [Di Pietro et al. 2018]. Pour ce faire, l'attaquant peut utiliser un récepteur standard, une antenne d'écoute et un oscilloscope dans le but d'observer le signal récupéré [Diakos et al. 2013].

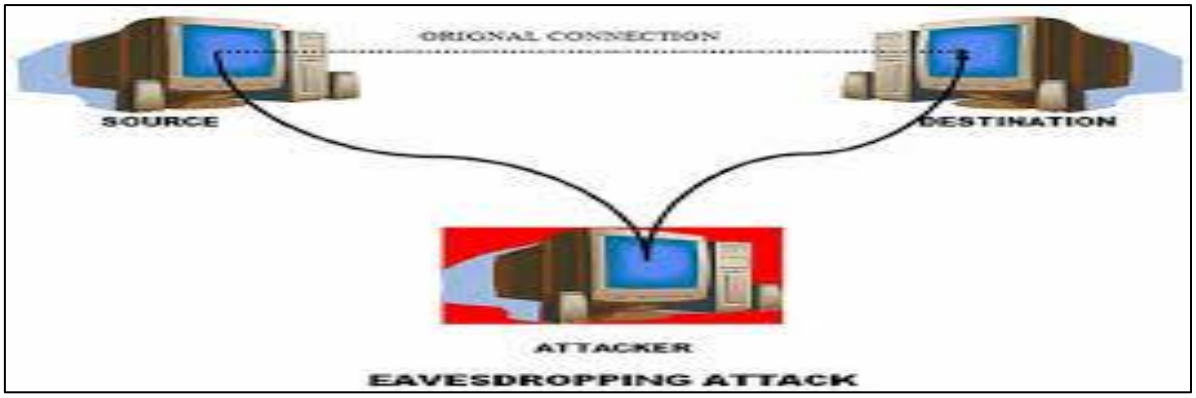

Figure 2.13 : Attaque Eavesdropping [Researchgate 2015].

– ***Attaques par relais***

Une attaque relais est définie comme un transfert de l'ensemble de la communication sans fil sur une grande distance. Elle peut être passive ou active. Une attaque par relais passif

transmet les données sans modification, contrairement à une attaque relais active [Hancke et al. 2009] [Vila and Ricardo 2015]. Un utilisateur malveillant peut transmettre la communication entre une carte de crédit fictive (c'est-à-dire un proxy) qui est utilisée pour effectuer certaines transactions à un moment donné avec le lecteur (par exemple de vente). Le proxy reçoit les signaux à partir d'un dispositif appelé môle qui a un accès physique à la véritable carte de crédit [Di Pietro et al. 2018].

– ***Attaques par skimming***

Un utilisateur malveillant peut capturer des données à partir d'une carte de crédit (plus généralement : données de tag) pour les réutiliser plus tard (Figure 2.14) [Di Pietro et al. 2018]. Le skimming dans le domaine de paiement est donc la capture et le transfert non autorisés des données de paiement à une autre source afin d'effectuer par la suite une attaque. Avec le skimming, l'attaquant peut voler les données de paiement en utilisant un escroc appareil physique planté sur place. Les normes de sécurité des paiements sans contact contiennent actuellement un certain nombre d'exigences et de recommandations pour se prémunir contre cette attaque. En outre, il y a des Conseils qui ont établi des documents qui présentent aux commerçants des exemples et des meilleures pratiques et des outils pour contrecarrer cette attaque dans le but d'assurer un niveau approprié de sécurité des données des titulaires de carte [PCI 2009].

Figure 2.14: Attaque Skimming [Daily Mirror 2019].

– ***Attaques par clonage***

La technologie NFC est utile dans les services de billetterie tels que les billets électroniques ou les billets numériques. Le clonage de tickets à partir de NFC peut se produire si les tickets ont été copiés et partagés avec d'autres avant d'être vérifiés [Chen et al. 2014], [Ceipidor et al. 2013]. Tout le monde peut utiliser le ticket de clonage comme un nouveau ticket, par exemple pour obtenir une remise sur l'achat de produits (Figure 2.15). Si le ticket a été vérifié, il peut être utilisé jusqu'à son expiration. Le cas de clonage peut se produire de deux

manières différentes, selon la conception du système de billetterie. Le but du clonage de ticket est de partager le ticket jusqu'à son expiration [Singh et al. 2018].

L'attaque de clonage est essentiellement appliquée sur les cartes de paiement sans contact EMV permettant à un attaquant de créer des clones fonctionnels d'une carte contenant les données de carte de crédit nécessaires ainsi que des codes d'autorisation. La carte clonée peut être ensuite utilisée pour effectuer un nombre limité des transactions EMV sur n'importe quel terminal EMV de paiement sans contact [Roland and Langer 2013].

Figure 2.15 : Attaque de clonage [Maxfield Chen 2020].

2.5.2.2 Attaques contre le smartphone

– ***Attaques par logiciels malveillants***

La prolifération explosive de virus et de logiciels malveillants affectant les appareils mobiles face au danger très réel des appareils perdus ou volés a instillé un sentiment de malaise dans l'esprit des consommateurs quant aux implications de perdre une grande partie de leur vie numérique. Si nous ajoutons à cela une seconde dimension d'argent et le risque de paiements non autorisés en cas de perte ou de vol d'un appareil mobile, la liberté financière sera mise en cause [Enisa 2016].

– ***Attaques par spyware***

Si un pirate parvient à trouver un moyen de récupérer le PIN de la victime, il pourrait être en mesure de réaliser des gains financiers aux frais de la victime. Cette attaque suggère un moyen possible de pirater le code PIN en utilisant une espèce de logiciel espion notoire connue sous le nom de Key Loggers qui est un type de spyware [Agarwal et al. 2007].

– ***Attaques par hameçonnage***

La pratique de phishing la plus courante consiste à envoyer « des e-mails qui semblent provenir de sources fiables dans le but d'influencer ou d'obtenir des informations personnelles

». Afin d'inciter la victime à fournir des informations sensibles, le message peut inclure un appel à l'action tel que " vérifier votre compte " ou " mettre à jour vos informations personnelles ". Une fois que les mots de passe ou autres informations d'identification personnelles ont été révélés, les hameçonneurs peuvent utiliser le compte de la victime à des fins frauduleuses ou pour spammer d'autres utilisateurs en ligne. Plusieurs juridictions font référence à l'hameçonnage des services bancaires à domicile [FinCoNet 2016].

– ***Attaques par effraction***

Les attaques par effraction sont des attaques qui peuvent pénétrer dans un nœud et révéler ses voisins dans la chaîne de communication. Son principe est que l'attaquant essaye de prendre le contrôle partiel ou total d'une entité victime. Pour la réaliser, l'attaquant injecte un code afin d'exploiter les erreurs de programmation logiques d'une entité (application ou appareil) qui représente la cible. L'exploitation des erreurs logiques (comme le débordement d'une zone buffer) peut influencer sur les propriétés de sécurité d'une entité (confidentialité, disponibilité et intégrité) en permettant à l'attaquant de restituer des données de l'entité, En combinant des attaques par effraction avec des attaques de congestion, les attaquants peuvent aggraver considérablement les dommages, par opposition à une congestion aléatoire pure. En fait, les attaquants peuvent employer les résultats des attaques par effraction (nœuds divulgués) pour guider les attaques de congestion ultérieures sur les nœuds divulgués.

Lors d'attaques intenses par effraction, l'attaquant peut traverser la chaîne de communication entre le transitaire nœuds, et peut même divulguer le serveur pour éventuellement le congestionner et annuler complètement les services [Wang et al. 2006].

– ***Attaques par déni de service***

Les attaques DoS (Denial of Service) constituent l'une des principales menaces parmi les problèmes de sécurité du réseau d'aujourd'hui. Leur objectif est de rendre une entité (appareil, service, réseau) inexploitable par son utilisateur. Ces attaques peuvent facilement consommer les ressources informatiques et la communication de la victime ou perturber et obstruer la disponibilité des ressources pour les utilisateurs prévus dans un court laps de temps. Le problème du Déni de service est une grave préoccupation dans le domaine de la sécurité des réseaux [Kumar 2016]. Un attaquant peut envoyer un trafic énorme à un appareil mobile afin de le saturer pour le rendre inutilisable et ceci peut être facile à cause de la limite de la capacité de traitement d'un appareil mobile comparable à un ordinateur ou à un serveur. Parmi les autres formes de l'attaque déni de service, l'épuisement de la batterie de l'appareil mobile. Pour

atteindre ce but, cette attaque exploite plusieurs tâches CPU qui nécessitent une grande quantité d'énergie (cryptographie complexe par exemple) et de cette façon, l'appareil sera éteint après un court laps de temps. Il existe des attaques DoS qui peuvent forcer l'appareil à rallumer quelques-unes de ses parties [Guerar 2017].

2.5.2.3 Attaques contre ATM

Ces jours-ci, les attaquants utilisent de plus en plus les attaques logiques pour manipuler un logiciel ATM afin de retirer de l'argent ou de capturer les données des clients. Les logiciels malveillants ATM sont conçus pour voler les données des titulaires de carte comme le PIN ou pour retirer de l'argent [Lowe 2010] [ATMSWG 2009]. En règle générale, les logiciels malveillants se cachent dans le système pour ne pas être détectés le plus longtemps possible. Ils portent atteinte à la confidentialité, à l'intégrité et à l'authenticité de la transaction des données pour une intention particulière [Diebold 2012] [GMV 2011]. Les réseaux ATM sont basés sur le protocole Internet et font face aux mêmes attaques comme d'autres réseaux IP (Internet Protocol), par exemple : déni de service (DoS), l'homme au milieu ou écoute clandestine [Kaltschmid 2016] [GMV 2011]. La communication entre l'ATM et l'hôte peut être utilisée comme point d'entrée pour lancer des attaques à distance [Diebold 2012]. Les périphériques tels que les routeurs et les commutateurs dans un réseau peuvent être ciblés [Benecke and Ellermann 1998]. La logique de la sécurité se concentre sur le maintien d'un réseau sécurisé avec un OS protégé et la conception d'un système afin que les intrus ne puissent pas menacer les données et les composants logiciels du titulaire de la carte [Diebold 2012] [GMV 2011] [Braeuer et al. 2016].

– ***Attaques par enregistrement d'écran***

Dans ce type d'attaque, l'attaquant installe une caméra près du GAB et invisible aux utilisateurs afin de filmer les saisies de mot de passe. La caméra utilisée est une caméra mobile ou une caméra de surveillance. Cette attaque appelée aussi attaque d'enregistrement vidéo a comme but l'observation pour voler le mot de passe saisi par l'utilisateur. L'authentification par code PIN dans les ATM traditionnels contribue à une croissance des fraudes ATM, parce que les PIN ou les mots de passe des utilisateurs qui sont saisis dans des espaces ouverts peuvent être volés par des attaquants qui utilisent des téléphones mobiles équipés de caméras ou des caméras miniatures ou qui installent des caméras invisibles dans des endroits cachés du GAB [Nti 2017]. L'attaquant peut donc être capable d'enregistrer et de jeter un coup d'œil sur les étapes d'authentification de l'utilisateur, y compris les modèles d'entrée et gestes

comportementaux (Figure 2.16). De plus, l'attaquant peut acquérir l'accès physique au smartphone en l'absence de l'utilisateur, puis déverrouiller le smartphone [Ku et al. 2019].

Figure 2.16 : Attaque par enregistrement caméra [Vietnam Investment Review 2018].

– ***Attaque par enregistrements multiples***

Elle représente une attaque qui utilise un appareil d'enregistrement tel qu'une caméra mobile ou un malware qui pourrait enregistrer plusieurs sessions d'activités à l'écran de saisie d'un mot de passe qui est basé sur une technique indirecte ou intelligente. Cette attaque qui utilise ensuite une série de vidéos pour découvrir le mot de passe est très difficile à défendre [Wu et al. 2014]. En effet, l'attaquant peut visionner la vidéo enregistrée autant de fois que nécessaire et reproduire progressivement le code PIN [Srinivasan 2018].

– ***Attaques ''Jackpot''***

De nouveaux crimes ATM comme les attaques Jackpotting (Figure 2.17) et Skimming ont vu le jour. Ces attaques logiques ont continué de croître ces dernières années. En janvier 2018, un total de 1 million de dollars américains a été volé dans de divers distributeurs automatiques de billets aux États-Unis d'Amérique par le biais d'attaques Jackpotting [Bloomberg 2018]. Le terme ATM Jackpotting vient du terme Jackpot. Ces attaques provoquent l'éjection de billets de banque de distributeurs automatiques par une technique qui permet d'extraire de l'argent d'un distributeur sans manipuler le compte bancaire d'un client. À l'heure actuelle, il existe une enquête entre l'organisme de droit public allemand Bayerischer Rundfunk et Motherboard qui a donné de nouvelles connaissances concernant un ensemble d'attaques de jackpotting [Schmidt 2020]. Dans ce type d'attaque, les cybercriminels obtiennent d'énormes sommes d'argent du GAB à la fois. Les cybercriminels utilisent deux méthodes pour effectuer cette attaque [Kasanda and Jackson 2018] :

- Black Box Attack
- Malware Attack

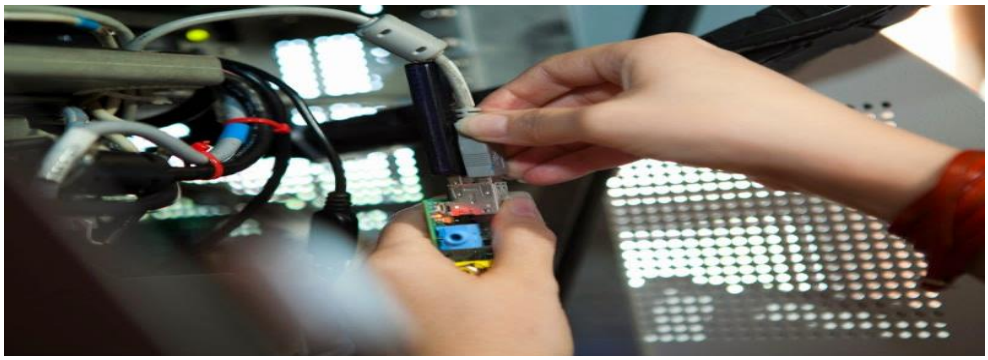

Figure 2.17 : Attaque de Jackpot [Security Affairs 2017].

– ***Attaques ‘’TRF’’ : Nouvelle méthode de fraude par guichet automatique préférée***

La fraude par inversion de transaction (TRF : Transaction Reversal Fraud) implique la création d'une erreur qui donne l'impression que l'argent n'a pas été distribué (Figure 2.18) [Owen 2018]. Le compte est recrédité du montant « retiré » mais le criminel empoche l'argent. Il peut s'agir d'une capture physique (similaire au piégeage d'espèces) ou d'une corruption du message de transaction. Ce type d'attaque s'est produit dans un certain nombre de pays comme en UK, Ukraine et Canada [Owen 2018]. L'attaquant y parvient en créant une erreur sur le GAB lors d'une opération de distribution d'espèces, à provoquer un changement d'hôte par son commutateur. Le compte ne sera pas débité bien que le criminel enlève l'argent du GAB. Pour éviter d'être pris, les attaquants utilisent des cartes volées ou clonées [Kasanda and Jackson 2018].

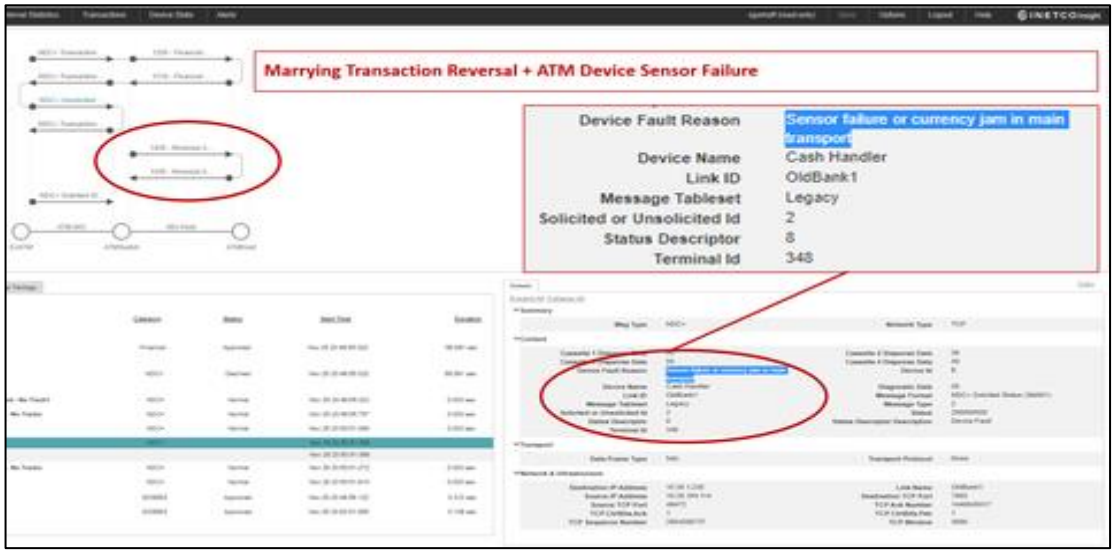

Figure 2.18 : Attaque TRF [INETCO 2019].

2.6 Solutions proposées

2.6.1 Brouillage actif (*Active jamming*)

Le principe de cette méthode est d'utiliser un dispositif émettant un champ radiofréquence assez fort et qui possède la même bande de fréquence que le système sans contact dans le but d'empêcher un lecteur appartenant à un attaquant d'accéder à la carte du système ou de comprendre sa réponse (Figure 2.19). Cette solution peut résoudre le problème de l'attaque de skimming mais son inconvénient est qu'elle crée un déni de service et qu'elle peut détruire les systèmes sans contact de proximité si le signal de brouillage émis est très puissant [Thevenon 2011].

Figure 2.19: Active Jamming [davidzou.com 2016].

2.6.2 Délimitation de la distance (*Distance bounding*)

Un certain nombre de protocoles de délimitation de distance (algorithmes de cryptographie) ont été proposés ces dernières années et ont été mis en œuvre. Ces protocoles se diffèrent en termes de performances et de degré de sécurité garantie. Certains protocoles utilisent le traitement des symboles courts [Drimer and Murdoch 2007], [Kuhn et al. 2010], tandis que d'autres utilisent le traitement analogique des flux de signaux (fonctionnant de manière similaire aux systèmes radar) [Rasmussen and apkun 2010] [Cremers et al. 2012]. En utilisant un de ces protocoles, un appareil peut juger que sa communication avec un autre appareil est en toute sécurité si la réponse de ce dernier n'a pas dépassé une limite supérieure correspondante à sa distance car le protocole définit une limite d'éloignement entre l'émetteur et le récepteur. Cette contre-mesure est utilisée pour détecter les attaques relais dans les réseaux filaires, mais dans les réseaux de communication sans contact tels que la RFID, cette méthode est consolidée par la technologie UWB (Ultra Large Bande) afin de mesurer la distance d'éloignement entre les deux parties communicantes. L'implémentation de cette technologie est coûteuse et complexe dans un système RFID ou NFC et d'autre part, cette solution est difficile à mettre en œuvre pour les raisons suivantes :

- Le calcul du temps de propagation est difficile parce qu'il est faible devant le temps de traitement dans le dispositif.
- Le moment de réponse du dispositif (carte ou appareil mobile) est variable (n'est pas fixe)
- Le temps de traitement du signal peut être supérieur au temps de relais et l'attaquant peut agir sur ce dernier temps en le minimisant de telle sorte qu'il sera invisible devant le temps de traitement et le temps de propagation [Thevenon 2011].

2.6.3 Application "Google Wallet"

L'application mobile Google Wallet (Figure 2.20) prétend non seulement stocker les cartes de crédit sur le téléphone, mais faire des remises et des offres pour les clients sur une carte de fidélité. Quand une personne vérifie qu'un magasin accepte l'application Google Wallet, elle peut payer et échanger des offres juste en tapant avec le téléphone sur un point de vente [Caldwell 2012]. L'application google Wallet est vulnérable contre l'attaque de relais [Roland et al. 2013]. Une vulnérabilité plus grave a été démontrée par des chercheurs en février 2012. Cette faille affecte uniquement les utilisateurs qui empruntent leur smartphone. Google Wallet stocke un hach du code PIN sur l'appareil mobile lui-même, plutôt que sur l'élément sécurisé (SE). Cet hach est une chaîne codée en hexadécimal créée par le protocole SHA 256. L'attaquant peut réussir à trouver le code PIN en utilisant l'attaque force brute après un nombre maximum de tests de 10 000 hach créés par SHA256 de tous les nombres à quatre chiffres possibles [Ghag and Saket 2012]. L'application Google Wallet est aussi menacée par les attaques de phishing, d'ingénierie sociale, d'installation involontaire d'applications malveillantes et d'autorisations d'accès au système d'exploitation mobile [Bosamia et Dharmendra 2019].

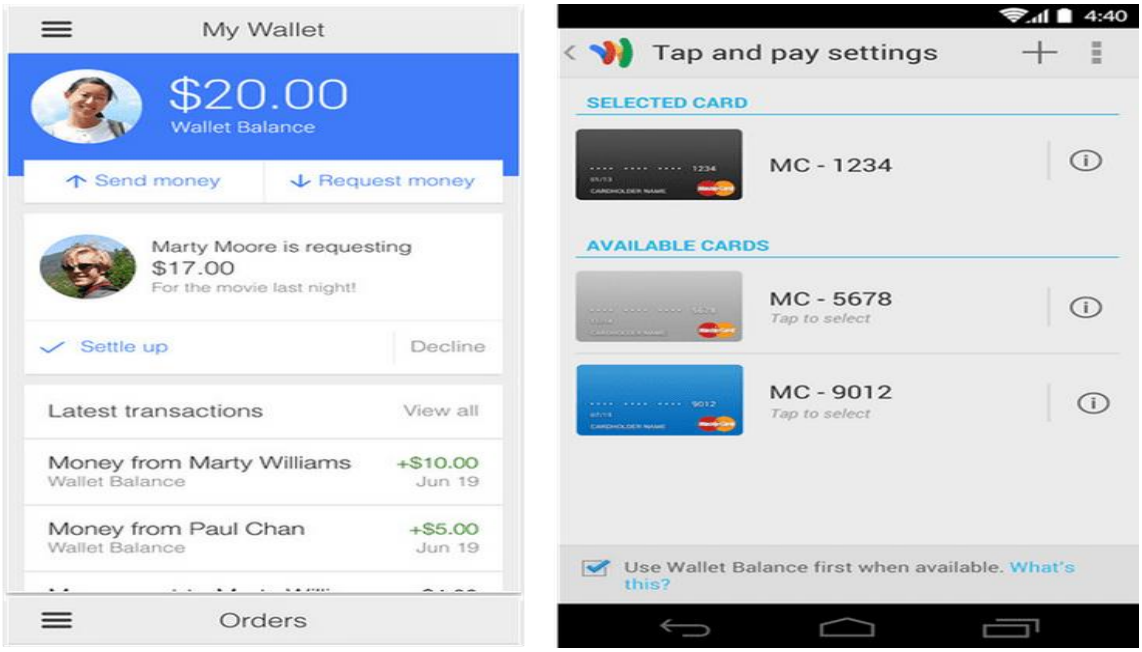

Figure 2.20: Application Google Wallet [The Balance 2019].

2.6.4 Cartes de paiement françaises

Contrairement à quelques pays comme le Japon et la Corée du Sud, où les utilisateurs utilisent fréquemment la technologie sans contact, les français doivent se familiariser avec cette technologie progressivement. La France vient de rattraper son retard grâce à l'utilisation de quelques services liés à la NFC comme les cartes sans contact (Pass-NAVIGO). Les fournisseurs doivent contrôler ces premières utilisations et être très soucieux aux réactions des utilisateurs [Pasquet et al. 2008]. Bien que le taux de fraudes sur les paiements par carte en France ait baissé pendant plusieurs années et soit encore relativement bas, il a augmenté en 2011 pour les transactions « carte présente », à la fois pour les achats et retraits de comptes bancaires. (Les transactions sur carte présente sont celles où la carte est effectivement présente à l'endroit du paiement [Sullivan 2013]. En 2018, il y a eu une augmentation des fraudes sur les transactions de paiement et de retrait effectuées en utilisant des cartes françaises par rapport à 2017. Cette augmentation est évaluée à 13,4 % de fraude et à 5,9 % d'euros [Villeroy 2018].

2.6.5 Cartes à puces EMV

Nommé d'après les organisations d'origine qui ont créé la spécification - Europay, MasterCard et Visa (EMV). Les spécifications de la puce EMV ont été publiées pour la première fois en 1996. Près de vingt ans plus tard, il y a maintenant plus de deux milliards de cartes à puces EMV actives utilisées pour le paiement par carte de crédit et débit, avec plus de 35 millions terminaux d'acceptation EMV déployés dans le monde [EMVCO 2014]. Malheureusement, cette technique qui a utilisé la technologie NFC et qui a facilité le paiement à travers le monde entier, est fragile contre quelques attaques qui sont dues à ses vulnérabilités comme par exemple l'utilisation d'une carte NFC clonée, la conviction d'un point de vente d'utiliser le PIN en clair hors ligne plutôt que le PIN chiffré hors ligne, récupération des données bancaires non cryptées envoyées par un point de vente non professionnel utilisé par les petits commerçants [El Madhoun et al. 2019].

.2.6.6 Elément sécurisé (*Secure element*)

Un SE (Secure Element) est une plate-forme inviolable (généralement un microcontrôleur sécurisé à une puce) capable d'héberger en toute sécurité des applications et leurs données confidentielles et cryptographiques (par exemple des clés cryptographiques) conformément aux règles et aux exigences de sécurité fixées par des autorités de confiance bien identifiées. Il existe différentes formes de SE :

- SE intégré SIM / UICC (Subscriber Identity Module / Universal Integrated Circuit Card) ;

- Micro SD (Secure Digital) intelligent (embedded secure element) ;
- Les cartes à puce (Carte SMC amovible : combinaison d'une carte mémoire ainsi que d'une carte à puce).

Les SE existent sous différentes formes pour répondre aux exigences des différentes implémentations commerciales et aux besoins du marché. Le SE peut souffrir de l'attaque d'écoute si les messages transmis entre le SE et le terminal ne sont pas cryptés [Jayasinghe et al. 2016]. Un SE est un exemple de trusted computing.

2.6.7 Le trusted computing

Le *trusted computing* (informatique digne de confiance) représente l'ensemble des technologies qui permettent d'assurer une confiance dans un système. L'objectif d'une telle technologie est de garantir l'exécution des applications sensibles et des processus critiques dans un environnement sécurisé et isolé et cela à chaque fois que le système est utilisé. Ce type de technologies utilise généralement des mécanismes matériels et logiciels pour réaliser la tâche de vérification. Les composants d'un *trusted computing* sont appelés composants de confiance de base : Trusted Computing Base (TCB). L'ensemble de ces composants comporte le processeur (ou le processeur en mode sécurisé), la sécurisation du stockage et une partie des logiciels [Jadla 2018].

2.6.7.1 Domaines d'application du trusted computing

Les domaines d'application du Trusted Computing incluent [Jadla 2018] :

– ***Le démarrage sécurisé (trusted boot)***

Pour chaque démarrage du dispositif, l'intégrité du logiciel doit être vérifiée en calculant le hash cryptographique du code.

– ***L'exécution isolée (isolated execution)***

L'exécution des processus sensibles et le traitement de leurs données doivent être isolés des autres processus et du système d'exploitation. Pour atteindre cet objectif, des moyens matériels et logiciels peuvent être utilisés.

– ***Les mises à jour sécurisées (secure updates)***

Etablir des mises à jour du dispositif, et s'assurer que la version de mise à jour est bien supérieure à celle installée.

– ***Le stockage sécurisé (secure storage)***

Le stockage sécurisé des données des utilisateurs, du système d'exploitation et des codes de démarrage contre les attaques physiques et les attaques cryptographiques est indispensable.

– ***La gestion des droits numériques (digital rights management)***

Assurer la protection des contenus médias des fournisseurs de services.

2.6.7.2 Implémentation du trusted computing

Le trusted computing est implémenté de différentes méthodes :

– ***Modules de sécurité externes***

Cette méthode offre un grand niveau de sécurité matérielle et logicielle. Elle est basée sur des smart cartes externes à brancher à l'ordinateur pour assurer des services de sécurité comme l'authentification et le cryptage de données. Parmi ces cartes, on peut citer les cartes FORTEZZA.

– ***Modules de sécurité intégrés***

Ils sont des modules intégrés directement sur la carte mère. Cette architecture diminue légèrement les garanties de sécurité mais augmente les performances par exemple pour les opérations cryptographiques qui sont optimisées au niveau matériel du processeur.

– ***Virtualisation***

La virtualisation est une technique d'isolation logicielle (par exemple Xen, Vmware). Cette technologie utilise au maximum les ressources matérielles. Les machines virtuelles sont populaires et très utilisées dans le domaine de sécurité informatique. Elles sont isolées et faciles à installer et à configurer. La majorité des logiciels de virtualisation sont gratuits et open source.

– ***Processeurs sécurisés***

Ils permettent l'exécution des processus sensibles de manière isolée des autres programmes et du système d'exploitation pour assurer leurs protections. Ce mécanisme est sous forme d'implémentations logiciels qui permettent à un processeur d'offrir un niveau élevé de sécurité et d'isolation [Jadla 2018].

2.6.7.3 Environnement d'exécution sécurisée

L'environnement d'exécution sécurisée : Trusted Execution Environment (TEE) est l'exécution isolée, combinée avec le stockage sécurisé. Un TEE assure une exécution sécurisée isolée du REE (Rich Execution Environment) qui est l'environnement non sécurisé du système d'exploitation. Le passage du REE vers le TEE se fait à travers une API (Application Programming Interface) [Jadla 2018].

2.6.8 Solutions d'authentification

Plusieurs techniques sont proposées pour assurer l'authentification. Le choix de telle ou telle technique dépend en grande partie de l'usage que l'on souhaite en faire : authentification de l'expéditeur d'un email, authentification d'un utilisateur qui se connecte à distance, authentification d'un administrateur au système, authentification des parties lors d'une transaction de B2B (Business to Business), etc. L'authentification est donc assurée de plusieurs manières. Par exemple, Android Pay propose un certain nombre d'options pour authentifier l'utilisateur avant le paiement. Elle accepte l'authentification par empreinte digitale (non activée par défaut), le code PIN, le mot de passe ou le modèle pour authentifier une transaction.

Alors que dans les paiements par carte traditionnelles, l'utilisateur a tendance de protéger le code PIN (qui l'authentifie), les modèles de sécurité mobiles sont généralement affichés en public et peuvent présenter une menace importante pour l'utilisateur d'Android Pay [enisa 2016].

L'authentification du client est une méthode pour vérifier l'identité du client. Elle peut être effectuée de différentes manières : en utilisant ce que le client sait comme un mot de passe, ce que le client possède comme une carte à puce, ou ce que le client est concerné par comme la biométrie. Les méthodes traditionnelles d'authentification des clients telles que les mots de passe ou les cartes à puce, authentifient l'utilisateur à l'aide de ses connaissances ou de ses biens. Un mot de passe ou une carte à puce peuvent être facilement être volés ou donnés à d'autres [Ahamad et al. 2016] ce qui permet à un attaquant d'effectuer des paiements à la place de la victime. Un mot de passe (simple, graphique ou mouvement) peut être reconnu par des spyware sophistiqués qui ont la capacité d'accéder aux ressources critiques et partager même des ressources avec le système d'exploitation.

2.6.8.1 Authentification par mot de passe

Il existe deux stratégies qui ont aidé les consommateurs à gérer leurs mots de passe, toutes les deux présentent des inconvénients en termes de sécurité :

- Utiliser le même mot de passe pour tout, ce qui n'est pas une bonne idée pour des raisons évidentes.
- Utiliser un gestionnaire de mots de passe. La sécurité dépend alors du gestionnaire de mots de passe, ce qui représente en théorie un autre point de vulnérabilité.

Les mots de passe peuvent être statiques ou dynamiques. Les mots de passe simples sont devinés facilement, ce qui entraîne l'application de paramètres de longueur, de complexité et de délai d'expiration. Mais de telles exigences peuvent rendre difficile la saisie du mot de passe à l'aide d'un appareil mobile. Une meilleure approche consiste à combiner les mots de passe avec des politiques qui répondent aux besoins mobiles, comme par exemple permettre aux utilisateurs de recevoir des notifications sans entrer de mot de passe et fournir un processus de récupération de mot de passe mobile [Secure technology Alliance 2017]. Dans ce qui suit, nous allons présenter quelques méthodes d'authentification qui sont basées sur l'utilisation des mots de passe.

– ***Méthode FakePIN***

La méthode FakePIN propose un mot de passe composé d'un texte alphanumérique et d'une direction. Pour la direction, l'utilisateur peut sélectionner Haut, Bas, Gauche ou Droite. Cette information secrète est appelée « direction du mot de passe ». Elle représente le secret de permettre à une clé (le mot de passe d'origine) d'être saisie dans le sens de la direction du mot qui a été défini précédemment avec le mot de passe d'origine. Le mot de passe d'origine est acquis donc en combinant en interne la valeur entrée et la direction du mot de passe [Kim et al. 2014]. A chaque session d'authentification, la méthode affiche un clavier aléatoire, pour saisir un caractère du PIN, l'utilisateur frappe la touche qui, en la combinant avec la direction donne le caractère du mot de passe réel (Figure 2.21). Cette technique est utilisée pour tromper un observateur qui applique une attaque de shoulder-surfing lors de l'authentification car la valeur saisie est une valeur clé fictive (fausse). En analysant cette méthode, on trouve qu'elle souffre de l'attaque d'enregistrements multiples parce qu'un attaquant peut découvrir le PIN original en combinant deux ou plusieurs PIN saisis par l'utilisateur et qui sont enregistrés par une caméra.

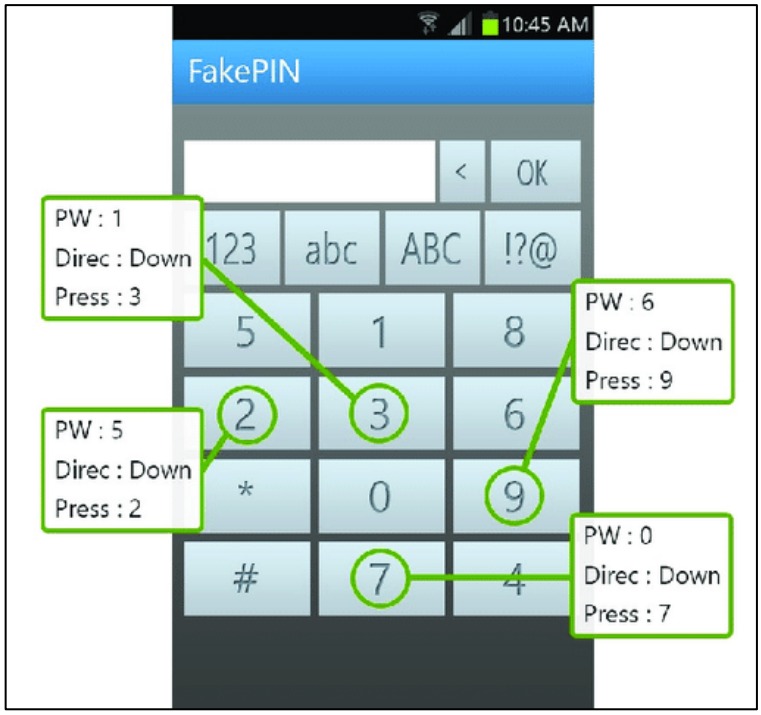

Figure 2.21 : Méthode FakePIN [Kim 2014]

– ***Méthode PassWindow***

Cette méthode représente un nouveau schéma d'authentification basé sur la saisie d'un PIN par les appareils mobiles. Ce schéma appelé *PassWindow*, évite la saisie directe du mot de passe en permettant de le saisir via une fenêtre aléatoire configurée en grille, empêchant ainsi les attaques shoulder-surfing. Ce système d'authentification mobile est aussi résistant à l'attaque d'enregistrement tactile utilisant des capteurs multimodaux et à l'attaque key logger. Cette méthode fournit une entrée supplémentaire qui utilise les capteurs dans les appareils mobiles. *PassWindow* utilise un code PIN et une valeur secrète supplémentaire sous forme d'image comme mot de passe sélectionné pendant l'étape de configuration du mot de passe. L'image est appelée *Pass-Icône* et est utilisée par l'utilisateur pour identifier l'emplacement où le code PIN sera entré. A chaque session d'authentification, le système sélectionne au hasard des icônes, qui sont ensuite stockées avec l'icône de passe. Le type de la valeur secrète peut être image, texte, couleur etc. et l'utilisateur peut déterminer celui qui lui est plus facile à mémoriser.

A chaque session d'authentification, l'utilisateur identifie l'emplacement qui correspond au code PIN à l'aide de l'image affichée sur la grille. Cette grille, appelée *Passwindow*, se compose de l'icône de passe et d'autres icônes aléatoires. L'utilisateur doit mémoriser l'emplacement aléatoire du *Pass-Icon* dans la grille. Ensuite un clavier virtuel composé de chiffres et *PassWindow* sans les images sont affichés au centre de l'écran. L'utilisateur déplace

le *PassWindow*, qui flotte sur le clavier virtuel en inclinant l'appareil, de sorte que chaque chiffre du PIN coïncide avec l'emplacement du *Pass-Icon*. [Yi et al. 2014] (Figure 2.22). L'inconvénient de cette méthode est qu'elle est vulnérable à l'attaque d'enregistrements multiples et que son temps d'authentification est élevé.

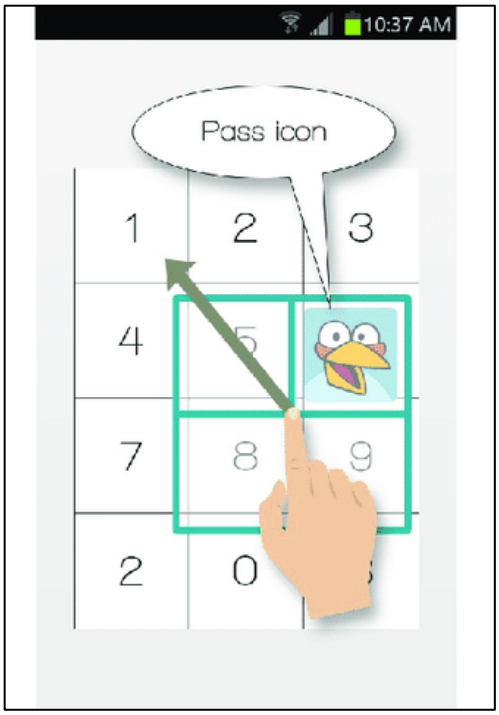

Figure 2.22 : Méthode PassWindow [Yi 2014]

– ***Méthode Cappcha***

La méthode de *Cappcha* (Completely Automatic Public Physical test to tell Computers and Humans Apart) a été proposé afin d'empêcher les logiciels malveillants de réaliser des essais d'authentification automatique. Elle permet l'authentification en entrant un code PIN avec l'opération d'inclinaison de l'appareil d'un degré affiché à l'écran pendant une seconde. Ce degré d'inclinaison peut être généré de manière aléatoire dans les smartphones qui utilisent la technologie ARM Trust Zone pour empêcher les malwares de reconnaitre le degré de mouvement mesuré par l'accéléromètre du téléphone à chaque transaction ou sous forme des valeurs stockées dans le SE (cas du smartphone contenant un SE qui embarque un capteur d'accéléromètre) et envoyées par un matériel de confiance (accéléromètre) à l'utilisateur pour choisir une, et dans ce cas, le SE ne peut pas être trompé par un malware présent sut l'appareil. [Guerar et al. 2018] (Figure 2.23). Malgré que cette technique soit bien protégée contre les malwares, elle est vulnérable à l'attaque shoulder-surfing et enregistrement par caméra car le mot de passe est saisi en direct. Si par la suite, le smartphone est volé ou emprunté, l'attaquant peut effectuer des paiements à la place de la victime.

Figure 2.23 : Méthode Cappcha [Guerar 2018]

– ***Méthode BrightPass***

Cette technique est une méthode d'authentification basée sur la luminosité de l'écran car il est prouvé que les méthodes de capture et d'enregistrement d'écran sont inaptes à différencier le niveau de luminosité de l'écran et par conséquent un spyware ne peut pas baser sur ce type d'attaque pour capturer les frappes de l'utilisateur durant la saisie d'un code PIN. Dans cette technique, le SE génère une séquence de 0 et 1 appelé *Lie Overhead*. Dans cette séquence, une série de cercles de différentes luminosités est affichée sur l'écran du smartphone dans la zone réservée à la saisie du code PIN. Le cercle d'une faible luminosité (correspondant à la valeur 0) indique à l'utilisateur de taper un chiffre aléatoire (faux chiffre) qui ne fait pas partie du code PIN, tandis que le cercle de haute luminosité (correspondant à la valeur 1) indique à l'utilisateur de saisir un vrai chiffre qui fait partie du code PIN (Figure 2.24). Cette technique est utilisée pour lutter contre l'attaque de spyware qui essaie de trouver le code PIN tapé par les techniques de capture d'écran ou d'enregistrement qui n'aboutissent à aucun résultat car elles ne sont pas capables de différencier les niveaux de luminosité [Guerar et al. 2016]. La technique BrightPass est réellement bien protégée contre les attaques de spyware qui utilisent les techniques de capture et d'enregistrement d'écran, mais en l'analysant on trouve qu'elle souffre également de l'attaque shoulder-surfing et l'attaque d'enregistrement par caméra car on trouve que le mécanisme de saisie est lisible pour un attaquant qui peut mémoriser les chiffres saisis dans les cercles qui sont visibles pour lui avec les différents niveaux de luminosité.

Figure 2.24 : Méthode BrightPass [Guerar 2016]

– ***Méthode Color Wheel PIN***

Dans cette méthode, le serveur partage avec l'utilisateur un secret composé du code PIN et d'un tableau de dix couleurs qui est stocké dans l'élément sécurisé du smartphone, qui lorsqu'il est rapproché à l'ATM, ce dernier affiche une roue colorée divisée en 10 portions numérotées de 0 à 9, un code QR et un *seekba*r pour faire tourner la roue. L'utilisateur scanne le QR code par son smartphone pour recevoir le tableau de couleurs avec une disposition aléatoire des indices de couleurs. Pour s'authentifier, l'utilisateur doit faire glisser le seekbar pour faire tourner la roue de sorte que la couleur qui correspond au premier chiffre du code PIN dans le tableau de couleurs affiché sur le smartphone, coïncide avec le deuxième chiffre du Code PIN sur la roue de couleurs. Après que l'utilisateur relâche le seekbar, la roue tourne de manière aléatoire. Ensuite, l'utilisateur glisse le seekbar pour la deuxième fois afin que la couleur qui correspond au troisième chiffre du code PIN dans le tableau de couleurs sur le smartphone coïncide avec le quatrième chiffre du code PIN sur la roue, et ainsi de suite jusqu'à la fin du processus [Guerar M. et al. 2016]. En analysant cette méthode, on trouve que le code PIN peut être reconnu par l'attaque force brute après un nombre maximum d'essais égal à 100 pour un code PIN formé de quatre chiffres et ceci si l'attaquant arrive à enregistrer l'opération d'authentification (écran du

smartphone et écran de l'ATM) en utilisant une caméra installée près de l'ATM. D'un autre côté, cette méthode est coûteuse par rapport à la nôtre parce qu'elle utilise un QR code qui doit être généré par le serveur et scanné par l'utilisateur en utilisant le smartphone. En ce qui concerne la mémorisation de la correspondance entre le chiffre et la couleur sur le tableau de couleurs affiché sur le smartphone et sur la roue de couleurs affichée sur l'écran de l'ATM ceci semble difficile surtout pour les utilisateurs âgés et surtout, lorsque le nombre de chiffres du code PIN dépasse les quatre chiffres. Enfin, on peut signaler deux autres inconvénients pour cette méthode, le premier concerne le fonctionnement de cette méthode si le nombre de chiffres du PIN est impair, le deuxième est que la fin de saisie du PIN n'est pas indiquée dans cette méthode.

2.6.8.2 Authentification par systèmes biométriques

Le système d'authentification par le biais d'une donnée biométrique est composé des étapes suivantes :

- Présentation de la donnée biométrique par la personne voulant s'authentifier ;
- Acquisition de cette donnée par un lecteur biométrique ;
- Traitement de cette donnée par un dispositif électronique qui la transforme en une information numérique, sous forme d'un fichier, ce codage peut utiliser des techniques cryptographiques ;
- Comparaison de ce fichier caractérisant la personne avec une donnée de référence enregistrée ;
- Décision, à partir de la comparaison effectuée d'authentifier ou non la personne.

Le risque de ce système est le vol de la donnée biométrique (par exemple l'empreinte digitale) qui représente une information très sensible et qui fait partie de la personne et qui inchangeable par comparaison avec le mot de passe qui peut être volé. D'autre part le cout engendré par le lecteur biométrique (capteur) et le dispositif électronique de transformation de la donnée biométrique en une information numérique.

2.6.8.3 Authentification par carte à puce

Aujourd'hui, Les cartes RFID et les cartes NFC qui sont des cartes à puce sont appelées des jetons (tag en anglais) et sont utilisées dans des services très populaires tels que le transport en commun, le contrôle d'accès physique, et le paiement électronique en communiquant avec un lecteur relié à une infrastructure fixe qui représente dans ces technologies l'émetteur. Dans ces technologies, le lecteur, après identification de la carte, envoie cette information à un système de contrôle d'accès appelé backbone pour donner à la carte ou à son porteur l'autorisation d'accéder ou non à une ressource. Dans les cartes RFID de la première génération,

l'authentification était basée sur un identifiant unique (UID) de 64 bits qui est transmis par la carte au lecteur qui le lit et le retransmet au contrôleur d'accès qui décide d'autoriser ou non le porteur de la carte d'accéder à la ressource (effectuer un paiement). La faiblesse de ces cartes est qu'elles sont vulnérables à l'attaque de clonage. Il est prouvé qu'en utilisant peu de ressources matérielles, on peut réaliser un cloneur de carte qui peut acquérir un identifiant (UID) afin de le réécrire sur une carte RFID ou NFC vierge ou de le retransmettre par le cloneur de carte pour émuler la carte originale et enfin accéder illégalement à la ressource sachant qu'il existe sur le marché des dispositifs comme Proxmark III qui permettent de réaliser ce type d'attaques.

Pour contrer à la faiblesse des cartes RFID de la première génération, des cartes de deuxième génération ont été créées. Ces cartes contiennent une puce capable de réaliser des calculs cryptographiques simples vue sa capacité limitée. Les protocoles d'authentification utilisés sont basés sur le principe de défi-réponse qui signifie que le défi (la question du lecteur) et la réponse (de la carte) changent à chaque session d'authentification ce qui rend difficile la reproduction du comportement de la carte par l'attaquant. Ce principe est utilisé pour s'assurer que le dispositif est réellement l'entité autorisée et ceci avant de transmettre les informations sensibles (comme l'UID). Malheureusement, les fonctions cryptographiques embarquées dans les cartes de deuxième génération utilisées par les commerçants n'étaient pas sécuritaires parce que d'un côté, elles étaient à clé symétrique, et de l'autre côté, leurs détails n'étaient pas publiés et examinés par la communauté internationale d'experts en cryptographie. Cette dernière tâche est très importante, par exemple lorsque les fonctions cryptographiques embarquées dans les cartes HID iClass produites par la société HID Global et utilisées dans les systèmes de contrôle physique ont été découvertes, des chercheurs ont créé des protocoles de cryptanalyse qui ont permis de reconstruire la clé cryptographique secrète et donc de cloner ce type de cartes. Le problème donc réside toujours même avec les cartes de deuxième génération, ceci est naturellement logique parce les cartes RFID ou NFC ont des capacités limitées et sont alimentées par leurs propres batteries, ce qui oblige que les calculs cryptographiques effectués doivent être simples et par conséquent vulnérables à l'attaque de clonage d'où la nécessité d'utiliser une technologie permettant d'effectuer des calculs cryptographiques plus importants tels que des algorithmes à clé symétrique reconnues et fortes comme AES, ou à clé asymétrique telles que RSA ou El-Gamal, ce qui a pousser à utiliser des plateformes mobiles comme les smartphones. Les manufacturiers des plateformes mobiles ont développé et déployé dans leurs nouveaux téléphones, la technologie NFC pour utiliser les téléphones comme jeton

d'authentification dans plusieurs applications (par exemple le paiement) tout en gardant la possibilité de communication de ces smartphones NFC avec des lecteurs de cartes RFID [Jedaida 2016].

2.6.8.4 Authentification par certificat à clé publique

L'infrastructure à clé publique (Public Key Infrastructure : PKI) est un mécanisme utilisant le certificat à clé publique dans le domaine d'authentification. Pour s'authentifier, le détenteur des clés utilise un certificat qui sera inséré dans un message lors d'un paiement sur Internet par exemple. Un autre exemple est que l'accès externe au réseau interne d'une entreprise (intranet) peut être authentifié par un certificat électronique validé auprès de la PKI de l'entreprise. Il existe des prestataires spécialisés en gestion des infrastructures PKI comme Certplus (en France) et Verisign (aux États-Unis), ou encore auprès d'une banque. Il faut noter par exemple qu'un client d'une banque française jouant le rôle de tiers certificateur, qui achète sur un site américain, aura du mal à imposer son certificat si son organisme bancaire n'est pas reconnu aux États-Unis comme un prestataire digne de confiance. Par remarque, la gestion d'une PKI (Public Key Infrastructure) est plus complexe qu'une simple base de données basée sur des couples (nom, mot de passe).

2.6.8.5 Authentification par protocole

– ***Protocole BioRFID (Brfid)***

Le système est proposé comme un système d'authentification basé sur la combinaison de deux sous-systèmes : un système RFID et un système biométrique. Il est utilisé pour authentifier l'utilisateur et les deux appareils communicants dans une communication RFID. Ce système peut être utilisé dans un paiement électronique NFC entre une carte NFC et un lecteur. Le protocole BIORFID (Biométrique et RFID) est résistant à l'attaque de trace, Man in the Middle, Replay et Monitoring [Chikouche et al. 2012]. Ce protocole utilise l'empreinte digitale pour assurer l'authenticité, et utilise le chiffrement par une fonction de hachage 'H' qui n'est pas spécifiée sur des messages qu'il compose après application des opérateurs de concaténation et du Xor (Ou Exclusif). Après l'analyse de ce système, on le trouve vulnérable aux attaques de vol de cartes et d'empreintes digitales des utilisateurs. Si un attaquant parvient à voler l'empreinte de l'utilisateur et entre temps la carte de paiement, il pourra effectivement faire des paiements à la place de la victime. De plus, ce système est coûteux par rapport à notre protocole parce qu'il utilise un capteur pour l'empreinte digitale de l'utilisateur.

– ***Protocole sécurisé de carte de crédit***

Il s'agit d'un protocole de carte de crédit proposé avec une fonction de hachage pour assurer un paiement NFC en utilisant un point de vente. Dans ce protocole, le lecteur NFC (point de vente) sollicite la carte pour son numéro de carte de crédit et sa date d'expiration. Le message de sollicitation contient *un défi aléatoire ch* qui sera utilisé par la carte de crédit dans sa réponse. La carte répond en envoyant les éléments suivants :

- A = UUID, un identifiant universel unique utilisé pour identifier la carte sans révéler les informations de la carte aux écoutes ou à toute autre partie.
- B = H (info, ch, iCVV) est utilisé pour authentifier l'identité de la carte. H est une fonction de hachage proposée. iCVV est une valeur de vérification de la carte, elle représente un jeton de sécurité dynamique destiné à authentifier le message et qui est fraichement générée à chaque réponse d'une sollicitation et est fréquemment utilisée par la banque pour valider la transaction.
- C = le nom de la banque est transmis en clair, afin que le point de vente puisse acheminer sa demande de facturation vers l'entité appropriée.

Une fois cette opération terminée, le point de vente envoie une demande de facturation à la banque émettrice de la carte de crédit. Le point de vente transmet simplement l'identification de la carte (A) et l'authentification (B) à la banque spécifiée par C. Le point de vente envoie également le défi ch afin que la banque puisse vérifier que B est valide ainsi que le montant à facturer. La banque utilise UUID comme index dans sa base de données des comptes. Lorsqu'elle reçoit une demande de facturation, elle identifie l'enregistrement correspondant à A, recherche $info_{banque}$ et $iCVV_{bank}$. Elle calcule ensuite $B_{bank} = H (info_{banque} ; ch ; iCVV_{bank})$ et vérifie que $B = B_{bank}$. Cette étape représente une vérification des informations de la carte de crédit et de iCVV afin d'autoriser ou non l'achat, et également elle effectue des vérifications supplémentaires, comme par exemple est ce que la carte n'a pas été déclarée perdue ou volée, ou l'emplacement de cet achat fait partie des emplacements connus du titulaire de la carte. Enfin, la banque répond au point de vente par une décision d'autorisation ou non de la demande de transaction de paiement. [Jensen et al. 2016]. Nous trouvons dans cette solution que le protocole est vulnérable à l'attaque du vol ou de la perte de la carte de crédit car le propriétaire de la carte de crédit n'est pas authentifié avec un numéro d'identification personnelle (PIN). Dans le cas où un mot de passe est utilisé avec ce protocole, la solution peut être vulnérable aux attaques : Enregistrement par caméra, logiciels espions, shoulder-surfing et force brute.

– ***Protocole de sécurité amélioré basé sur NFC pour protection de la confidentialité***

Ce protocole utilise une technique de chebyshev-map et de cryptographie à clé publique sans certificat. Pour le processus d'enregistrement et de vérification de la véritable identité de

l'utilisateur, le protocole utilise le TSM (Trusted Service Manager) en tant que tiers de confiance [Ling et al. 2017]. Lorsque nous analysons le protocole, nous constatons qu'il vérifie beaucoup plus la propriété de confidentialité sans s'occuper de l'authenticité. De plus, il est compliqué et utilise plus de messages et de calculs par rapport à notre protocole, ce qui implique qu'il est coûteux en temps de calcul et de transmission de messages.

2.6.9 Autres solutions

2.6.9.1 Amélioration des fonctions de sécurité des ATM

Proposition d'un dispositif de sécurité d'authentification basé sur plusieurs facteurs (PIN et empreinte digitale) pour améliorer la sécurité et la sûreté de l'ATM et de ses utilisateurs. Le système proposé présente une structure de conception à trois niveaux. Le premier niveau est le module de vérification, qui se concentre sur la phase d'inscription, d'amélioration, d'extraction des fonctionnalités et de correspondance des empreintes digitales. Le deuxième niveau est la base de données qui agit comme un entrepôt pour stocker les empreintes digitales de tous les utilisateurs des ATM préenregistrés en tant que des modèles et les codes PIN en tant que du texte. Le dernier niveau présente un système de plate-forme pour relier les transactions bancaires telles que les demandes de solde, les mini relevés et les retraits [Nti 2017]. L'analyse de ce mécanisme montre qu'il y a une absence de spécification de la technique de protection du PIN et de l'empreinte lors de leur introduction pendant l'étape d'authentification. De plus, les deux facteurs (PIN et empreinte) ne sont pas protégés contre le vol, et le code PIN peut être récupéré par les attaques de logiciels malveillants, par l'enregistrement d'écran ou par caméra. De plus, beaucoup de messages sont générés par ce système ce qui implique que le temps de leur transmission peut être coûteux.

2.6.9.2 Générateur symétrique de fonction aléatoire

Ce générateur crée une chaîne de sortie symétrique équilibrée dans le nombre de 1 et de 0 et indépendamment de la chaîne d'entrée. Il génère une fonction qui combine des variables et qui est composée de fonctions booléennes de base. Cette fonction peut être utilisée dans les algorithmes de hachage, les chiffrements de flux et les chiffrements par blocs pour être plus robuste. Le résultat de cette fonction est obtenu comme suit : Une sélection aléatoire de deux variables d'entrée est établie à partir des « N » variables. Ensuite, nous appliquons une porte logique aléatoire parmi quatre opérations : AND, OR, NOT et XOR sur les deux variables. Le résultat est le premier terme (terme1). Pour générer le deuxième terme, une variable est obtenue à partir de la liste des variables et combinée avec terme1 en utilisant une porte logique aléatoire

parmi les quatre déjà citées. Le résultat est le terme2. Cette opération se répète jusqu'à la génération du dernier terme qui représente le résultat du générateur de fonctions. Les auteurs prouvent que le générateur de fonctions peut être utilisé pour n'importe quel algorithme de cryptographie et ne peut pas être retracé en raison de son caractère aléatoire. Leurs travaux proposés peuvent être utilisés dans l'algorithme MD5 (Message Digest 5) ou SHA (Secure Hash Algorithm), les fonctions de chiffrement par blocs, les chiffrements de flux et les modules de fonctions de cryptographie. Ils prouvent par leur expérimentation que les fonctions générées par le générateur proposé offrent une bonne non-linéarité, une résilience et un effet équilibré [Saha and Geetha 2017]. Cette solution est destinée à assurer la propriété de confidentialité grâce à sa forte cryptographie, mais pour la propriété d'authenticité, on trouve qu'elle ne traite pas ce cas de figure. Par exemple, si parmi les variables traitées par le générateur est le mot de passe, cette variable qui peut être volée par un attaquant, peut être introduite à ce système qui va l'inclure avec la liste des « N » variables et l'algorithme va continuer à fonctionner d'une façon normale. A ce fait, on peut conclure que cette technique n'est pas capable de lutter contre les attaques qui brisent la propriété d'authenticité.

2.6.9.3 Tokenisation des paiements

Dans une transaction de paiement par carte de crédit, un jeton créé avec un numéro de compte associé au numéro de compte réel, est transféré par l'émetteur. Ce jeton ne constitue pas le compte réel pour fournir un haut niveau de sécurité à la transaction de paiement. Si un attaquant récupère frauduleusement le jeton, le vrai numéro de compte ne peut pas être généré [Gaddam et al. 2018]. La technique de tokenisation dans une communication NFC, peut être utilisée après l'étape d'authentification qui nous intéresse en plus, c'est-à-dire dans la phase de transmission des données relatives aux clients comme le numéro de compte, le montant et relatives à la banque comme le nom de la banque etc. Mais la technique de tokenisation seule ne suffit pas pour sécuriser une communication NFC à cause de l'absence de l'authentification de l'utilisateur ce qui implique qu'elle peut être vulnérable à toutes les attaques déjà listées.

2.7 Limites des solutions proposées

Les limites des méthodes citées sont présentées dans le tableau 2.1

Solution	Limites
Brouillage actif	Création d'un déni de service et possibilité de détruire les systèmes sans contact à proximité si le signal de brouillage émis est très puissant
Délimitation de la distance	Réalisation difficile puisque l'implémentation de l'UWB (Ultra-Wide Band : Ultra large bande) dans un système RFID engendre un coût et une complexité non négligeables. De plus, il est difficile d'isoler le temps de propagation car il est faible par rapport au temps de traitement et n'est pas constant. Problème de mesurer le temps dans le cas où la carte ne répond pas toujours au même moment, le temps de traitement du signal peut augmenter la durée du relais et l'attaquant peut agir sur le relais.
Application ''Google Wallet''	En fin 2011, elle souffre de deux attaques. La première consistait à récupérer par « Force brute » le code personnel de protection de l'utilisateur, afin d'accéder à toutes les cartes enregistrées dans Google Wallet. La seconde consistait à réinitialiser l'application Google Wallet pour prendre la main sur un moyen de paiement.
Cartes de paiement françaises	Des informations sensibles ont été divulguées par des attaques (nom, prénom, numéro de carte, historique des transactions, ...) et ne respectent pas les réglementations bancaires (PCI : Payement Card Industry et DSS : Data Security Standard) [Lifchitz 2012].
Cartes à puces EMV	Vulnérabilité de ces cartes à l'attaque du vol et à certaines attaques dans le cas d'absence de protocoles d'authentification sécuritaires.
Elément sécurisé	Vulnérabilité de ce circuit à l'attaque du vol du smartphone et à certaines attaques dans le cas d'absence de solutions d'authentification sécuritaires.
FakePIN	Vulnérable à l'attaque d'enregistrements multiples.

PassWindow	Vulnérable à l'attaque d'enregistrements multiples et que son temps d'authentification est élevé.
Cappcha	Vulnérable à l'attaque Shoulder-Surfing ou à l'attaque enregistrement par caméra si ces attaques sont suivies par l'attaque du vol de smartphone car un attaquant ou une caméra peut utiliser une observation directe en regardant ou filmant l'entrée directe du mot de passe.
BrightPass	Vulnérable à l'attaque Shoulder-Surfing ou à l'attaque enregistrement par caméra si ces attaques sont suivies par l'attaque du vol de smartphone car un attaquant ou une caméra peut utiliser une observation directe en regardant ou filmant l'entrée directe du mot de passe.
Color Wheel PIN	Problème si le nombre de chiffres du mot de passe est impair. La fin de saisie du mot de passe n'est pas spécifiée. Difficile à utiliser pour les personnes âgées.
Protocole BioRFID	Vulnérable à l'attaque vol ou clonage de la carte avec vol de l'empreinte digitale de l'utilisateur.
Protocole sécurisé de carte de crédit	Non utilisation du mot de passe, il est vulnérable contre l'attaque du vol ou clonage de la carte.
Protocole de sécurité amélioré basé sur NFC pour protection de la confidentialité	Vulnérable aux attaques qui visent l'authenticité. Il est compliqué et utilise beaucoup de calcul et de messages. Les temps de calcul et de transmission de messages peuvent être élevés.
Amélioration des fonctions de sécurité des ATM	Vulnérable aux attaques vol du PIN et de l'empreinte et récupération du PIN par malware, enregistrement d'écran et par enregistrement caméra. Beaucoup de messages utilisés dans le protocole, temps de transmission des messages doit être énorme
Générateur symétrique de fonction aléatoire	Cette solution renforce le système de cryptographie d'un ensemble de variables. Le problème est que si la variable (le mot de passe par exemple) est volée, le générateur fonctionne comme dans le cas normal. La méthode est vulnérable aux

	attaques destinées pour casser la propriété d'authenticité parce qu'elle est basée sur la cryptographie et donc elle protège beaucoup plus la confidentialité
Tokenisation des paiements	Elle ne protège que le numéro de compte, elle n'intervient pas à l'authentification de l'utilisateur, elle peut être vulnérable à toutes les attaques déjà listées si elle est utilisée seule dans une communication NFC.

Tableau 2.1 : Limites des méthodes

2.8 Conclusion

Dans ce chapitre, nous avons passé en revue les attaques qui peuvent cibler une carte de crédit ou bancaire, un smartphone ou un ATM. Deux grandes familles d'attaques sont discutées ; les attaques physiques qui ont un effet direct sur le dispositif NFC (carte, smartphone, ATM), et les attaques logiques qui ont généralement un effet sur les données stockées dans l'entité utilisée lors de la communication NFC. Nous avons présenté aussi les solutions proposées qui varient entre mots de passe, protocoles d'authentification, fonctions de hachage et solutions matérielles. Nous avons expliqué les idées de base derrière ces méthodes en spécifiant les avantages et les inconvénients de chaque méthode.

Pour les solutions d'authentification, nous avons basé sur les techniques utilisées pour authentifier l'utilisateur en utilisant un mot de passe ou un protocole d'authentification utilisant les modalités biométriques, les cartes de crédit ou les fonctions de hachage. Après avoir passé en revue la littérature existante, nous avons constaté que la simplicité et l'efficacité résident dans la découverte d'une technique de mot de passe intelligente, un protocole d'authentification sécuritaire et simple et une fonction de hachage efficace.

Deuxième partie

II. Contributions : Vers une communication NFC plus sécuritaire et économique en temps d'authentification dans un paiement électronique entre smartphone et ATM

Chapitre 3

Chapitre 3 : Un mot de passe en cloud et un protocole d'authentification pour un paiement NFC sécurisé entre smartphone et ATM

Sommaire

3.1 Introduction

Dans cette démarche, nous nous focalisons sur la proposition d'une solution qui assure un paiement sécurisé entre un smartphone et un ATM en garantissant les trois propriétés de sécurité fondamentales et qui sont : la confidentialité, l'authentification et l'intégrité de données. La confidentialité des données privées de l'utilisateur suppose de les chiffrer de façon à ne pas permettre à un attaquant qui a récupéré les messages contenant les informations confidentielles de comprendre les contenus. L'authentification implique de ne donner l'autorisation d'utiliser le paiement NFC qu'uniquement à une identité prédéfinie (utilisateur autorisé). Ceci nécessite l'utilisation de méthodes d'authentification comme le mot de passe ou la technologie biométrique [Promontory 2017]. L'authentification consiste donc à vérifier l'identité du dispositif NFC (smartphone et ATM) avant une transaction de paiement. L'intégrité des données privées et confidentielles de l'utilisateur (mot de passe, identifiant d'élément sécurisé) exige une protection contre toute modification pendant leur transfert entre le smartphone et l'ATM [Pourghomi 2014]. Le smartphone utilisé dans notre système embarque un élément sécurisé qui est un circuit implémenté dans le smartphone afin de stocker des applications NFC, des protocoles et des routines cryptographiques, des clés secrètes et les données privées de l'utilisateur [Vincent 2012]. Plusieurs solutions sont proposées pour sécuriser le paiement électronique via l'ATM à l'aide de la technologie RFID ou NFC. L'analyse montre que la majorité des solutions est basée sur l'utilisation d'un mot de passe, d'une donnée biométrique ou d'un protocole d'authentification. Cependant, chaque solution présente des faiblesses.

Dans notre solution, nous proposons un mot de passe sécurisé envoyé en cloud et un protocole d'authentification basé sur l'utilisation de nonce et de l'identifiant de l'élément sécurisé. Nous proposons aussi une fonction de hachage simple et un test d'intrusion aisé. Le protocole intégré dans l'élément sécurisé du smartphone, essaie d'authentifier l'utilisateur avec le mot de passe, en utilisant la fonction de hachage proposée. En revanche, le serveur lance un test d'intrusion à tout accès au compte utilisateur par son propriétaire ou par un attaquant. De plus, la solution permet à l'utilisateur de sélectionner une carte de crédit ou une carte bancaire à partir d'une liste de cartes intégrées dans le smartphone. Les propriétés de sécurité (confidentialité, authentification mutuelle et intégrité) sont vérifiées par la logique d'analyse et par l'outil AVISPA qui sera défini par la suite. La solution proposée garantit la protection de la vie privée de l'utilisateur en protégeant ses données confidentielles. Nous prouvons au cours

de ce chapitre que cette méthode est sécurisée contre onze attaques les plus répandues dans le domaine RFID et NFC et qu'elle présente un temps d'authentification très court. Nous allons montrer qu'elle est simple en manipulation parce qu'elle utilise quelques opérateurs comme le xor et l'opérateur de concaténation, qu'elle effectue peu d'opérations de fonction de hachage et qu'elle est utilisable sans difficulté même par les agents âgés. La solution proposée utilise aussi la technique de la mémoire cache au niveau du serveur pour lui permettre de gagner du temps d'accès. Une comparaison avec certaines solutions existantes est établie dans ce travail afin d'évaluer les performances et l'efficacité de notre solution.

Nous présentons dans le reste de ce chapitre, l'architecture de notre système sécurisé en décrivant ses principaux composants, puis nous expliquons la technique du mot de passe en cloud, le protocole d'authentification, la fonction de hachage et le test d'intrusion, ensuite nous étudions la sécurité de la solution proposée contre de multiples attaques en utilisant une vérification double par analyse et automatique. Enfin, nous effectuons une comparaison entre notre solution et certaines méthodes bien connues utilisées dans le but d'authentification, et nous présentons une évaluation des performances suivie d'une conclusion.

3.2 Système de paiement sécurisé

Notre solution est composée d'un mot de passe envoyé en cloud, d'un protocole d'authentification, d'une fonction de hachage et d'un test d'intrusion. Ces outils sont utilisés dans le système matériel suivant avec les notations indiquées dans le tableau 3.1 :

Notation	Définition
Natm	Nombre aléatoire généré par l'ATM
ATM	Guichet automatique bancaire
BcN	Numéro de carte bancaire
Icvv	Valeur imprévisible fraîchement générée pour chaque réponse à une sollicitation, utilisée ensuite par le serveur de la banque pour valider la transaction
Id	Identifiant de l'élément sécurisé
CCode	Mot de passe
Amount	Montant retiré de l'ATM
H	Fonction de hachage
‖	Concaténation
⊕	xor (ou exclusif)

Tableau 3.1 : Notations utilisées [Chabbi 2020a].

3.2.1 Système hardware

Le système matériel est composé d'un smartphone (SP), d'un guichet automatique bancaire (ATM) et d'un serveur (S) (voir figure 3.1.).

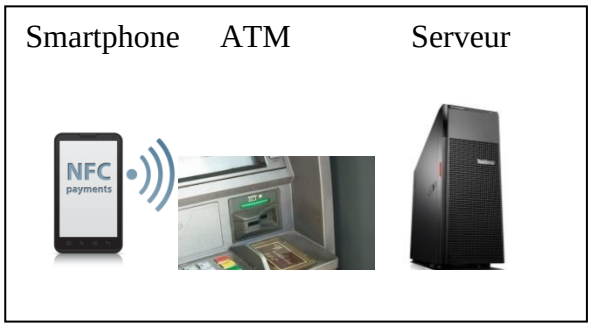

Figure 3.1 : Système de paiement NFC [Chabbi 2020a]

3.2.1.1 Smartphone

Le smartphone proposé a une architecture SIM non centrée où l'élément sécurisé est implémenté sous la forme d'un support sécurisé mobile doté d'un type de carte mémoire (Secure Memory Card: SMC) [Otterbein et al. 2017] (figure 3.2.). Le smartphone équipé de la technologie NFC embarque l'élément sécurisé mobile qui stocke son identifiant (Id), le mot de passe, le protocole d'authentification et les applications NFC (par exemple l'application de paiement), etc. L'architecture choisie pour l'élément sécurisé représente un avantage pour

l'utilisateur qui peut le changer en cas de changement de pays (voyage par exemple) ou le désactiver par l'opérateur en cas de vol du smartphone.

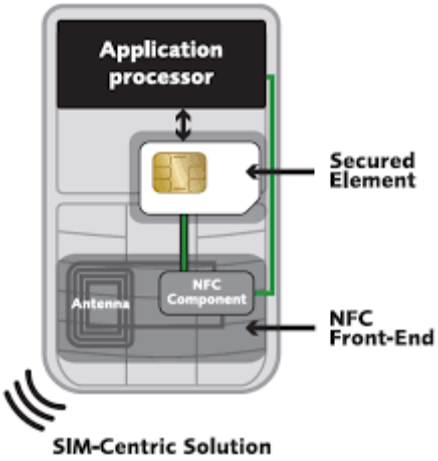

Figure 3.2 : Mobile NFC avec une architecture SMC [NovaCard 2013].

3.2.1.2 Guichet automatique bancaire (ATM)

L'ATM dans notre système a la possibilité de lire une carte bancaire intégrée dans un smartphone. Il est capable aussi de générer des nombres aléatoires (nonce) et de les communiquer au smartphone. Il établit une communication NFC avec le smartphone et une autre en ligne avec le serveur. Dans notre système, l'ATM a l'avantage de générer des nonces qui sont utilisés dans le cryptage pour se protéger contre l'attaque de rejeu.

3.2.1.3 Serveur

Le serveur est caractérisé par :

- Une base de données contenant un ensemble d'enregistrements dont chacun contient l'identifiant (Id) de l'élément sécurisé, le mot de passe, le résultat de l'application de la fonction de hachage au message représentant la concaténation entre l'Id et le mot de passe (ce résultat représente l'indice de recherche) dans la base de données. L'enregistrement contient un champ qui représente l'état du mode d'accès (activé ou désactivé) et une référence à la base de données contenant la liste des informations relatives aux cartes de crédit ou aux cartes bancaires de l'utilisateur. Chaque carte de crédit ou carte bancaire est spécifiée par son numéro, le nom de la banque, le numéro de compte utilisateur, son montant, etc. Les informations sont enregistrées lors de la phase d'enregistrement par l'opérateur dans la base de données et dans l'élément sécurisé dont le contenu est mis à jour dans le cas où le propriétaire change de smartphone.
- L'activation de l'état du mode d'accès dans l'enregistrement correspondant à l'utilisateur désirant effectuer un paiement lorsqu'il envoie au serveur, son mot de passe concaténé avec l'identifiant de l'élément sécurisé et signé par la fonction de hachage. Le serveur désactive l'état du mode d'accès juste après la fin de l'opération de paiement.
- Une mémoire cache contenant seulement les enregistrements dont le mode d'accès est activé, ce qui représente un avantage pour accélérer le temps d'accès à l'enregistrement de l'utilisateur qui souhaite effectuer une transaction avec l'ATM.

- Une application qui permet à l'utilisateur d'envoyer son mot de passe dans le cloud loin de l'ATM qui peut être ciblé par des attaques. La figure 3.3, ci-dessous présente l'architecture de notre système synthétisé en trois phases.

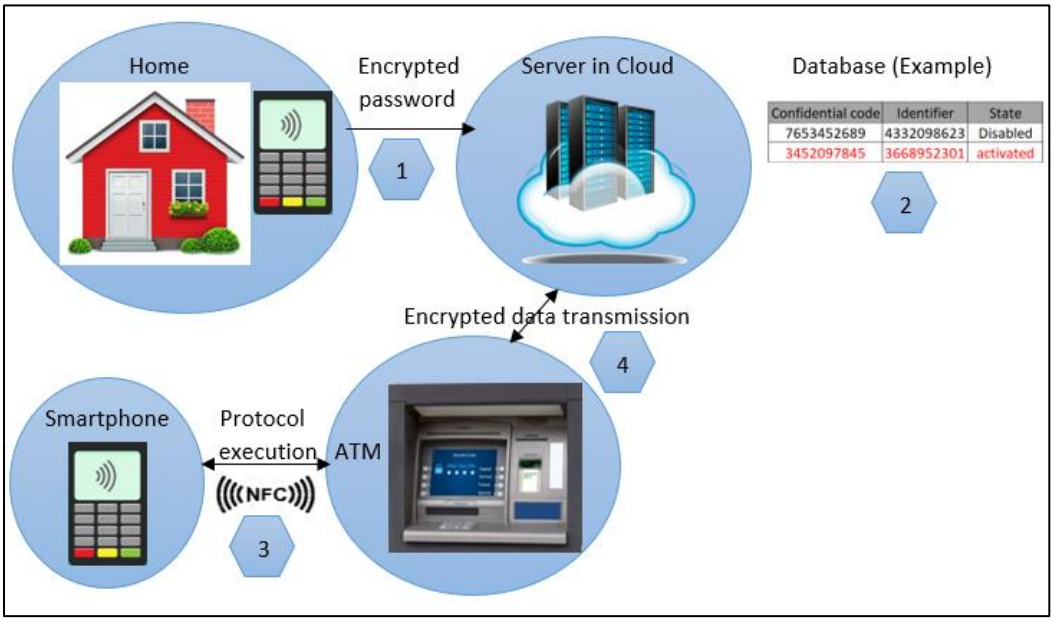

Figure 3.3 : Architecture du système [Chabbi 2020a]

(1) L'utilisateur loin de l'ATM, envoie au serveur le mot de passe crypté (message S) ;
(2) Activation de l'enregistrement correspondant dans la base de données du serveur ;
(3) Authentification entre le Smartphone et l'ATM à l'aide du protocole d'authentification ;
(4) Transmission de données cryptées entre l'ATM et le serveur en utilisant le protocole.

3.2.2 Objectifs

L'ATM effectue deux communications : l'une par radiofréquence avec le smartphone et l'autre en ligne avec le Serveur. La dernière communication est considérée sécurisée par le protocole TLS (Transport Layer Security).

Notre système propose la saisie d'un mot de passe à l'aide du smartphone en utilisant une application de l'opérateur afin d'authentifier le propriétaire du smartphone. Il concatène l'identifiant de l'élément sécurisé avec le mot de passe, chiffre le résultat avec une fonction de hachage proposée et envoie le message chiffré sur le cloud. Ce message est considéré sécurisé en utilisant le protocole TLS car notre objectif principal est de sécuriser le paiement NFC entre l'ATM et le smartphone. Le serveur de l'opérateur qui a une base de données indexée sur la valeur de fonction de hachage du mot de passe concaténé avec l'identifiant de l'élément sécurisé, recherche la valeur envoyée, s'il la trouve, il active l'état du mode d'accès dans l'enregistrement déjà trouvé (l'enregistrement correspond à l'identifiant d'élément sécurisé et à

son propriétaire) et le met dans la mémoire cache, et c'est seulement dans ce cas (mode d'accès activé) que l'utilisateur est autorisé à effectuer le paiement NFC via l'ATM. La solution proposée sécurise bien la communication entre le smartphone NFC et l'ATM par un simple protocole proposé en sécurisant les messages transmis lors du paiement NFC. Nous pensons que notre solution est économique en termes de coût de calcul, de coût de communication et de coût d'espace de stockage. Elle est aussi efficace et sûre au regard des propriétés de sécurité suivantes :

- Confidentialité : l'identifiant de l'élément sécurisé (son adresse MAC : Media Access Control) et le mot de passe de l'utilisateur ne sont pas envoyés en clair sur l'interface radiofréquence ou sur le cloud mais chiffrés à l'aide de la fonction de hachage.
- Authentification de l'utilisateur : l'utilisateur est authentifié par l'identifiant de l'élément sécurisé chiffré avec le mot de passe.
- Authentification du smartphone : dans notre solution, le serveur est capable d'authentifier le vrai smartphone. Cela sera abordé lors de la présentation du protocole.
- Authentification de l'ATM : le smartphone doit garantir qu'il communique avec le vrai ATM. Cela sera prouvé aussi lors de la présentation du protocole.
- Intégrité des données : dans notre solution, la sécurité de l'identifiant de l'élément sécurisé et le mot de passe ne sont pas infectés par la perte de messages, l'absence d'énergie ou la perte de connexion. D'un autre côté, toute modification du message par un attaquant peut être détectée par notre fonction de hachage.

Après avoir vérifié les propriétés non fonctionnelles ci-dessus, le protocole autorise les transactions de paiement : ile interdit l'exécution de l'opération du paiement si l'une des propriétés de sécurité fait défaut (cas d'attaque), dans le cas contraire, il autorise le traitement du paiement.

3.2.3 Protocole d'authentification

Le protocole proposé est appelé Cpass (Cloud Password). Il s'inspire du protocole nommé SCCP (Secure Credit Card Protocol) utilisé dans l'achat par une carte NFC et un point de vente [Jensen et al. 2016]. Notre protocole est adapté au paiement électronique avec un ATM via un smartphone. Il se distingue par l'authentification de l'utilisateur avec son mot de passe et l'identifiant de l'élément sécurisé par sa fonction de hachage et par la protection du paiement NFC contre onze attaques notamment l'attaque vol du smartphone. En revanche, le serveur effectue un test d'intrusion et affiche le montant retiré avec le solde du compte et une confirmation SMS sur l'écran du smartphone lors de chaque retrait (modification du montant de compte) par l'utilisateur ou par une nouvelle attaque (le pire des cas). Notre protocole, embarqué dans l'élément sécurisé, utilise l'identifiant de ce dernier, et pour le chiffrement, une

fonction de hachage, un numéro de challenge, et les opérateurs xor (ou exclusif) et de concaténation.

Un des avantages et pas des moindres de notre solution par rapport à SCCP est qu'elle permet à l'utilisateur de sélectionner une carte de crédit ou une carte bancaire à partir d'une liste de cartes intégrées dans le smartphone. Les phases de la solution sont décrites dans ce qui suit :

3.2.3.1 Phase d'enregistrement

L'opération d'enregistrement est une phase critique dans notre solution, vue que les informations à stocker dans la base de données du serveur ou sur la mémoire de l'élément sécurisé sont très sensibles. Pour le smartphone, nous proposons l'utilisation de l'architecture SIM non centrée où l'élément sécurisé est une carte mémoire sécurisée (SMC) et ce pour les avantages suivants :

- Il offre un haut niveau de sécurité ;
- Il est conforme à EMV, GlobalPlatform, ISO / IEC 7816, javacard ;
- Il a une capacité de mémoire importante ;
- Il est mobile de telle sorte qu'il peut être placé avec ses applications NFC et ses clés secrètes dans un nouveau Smartphone.

Chez l'opérateur local, les informations suivantes sont enregistrées dans la base de données du serveur :

- Le mot de passe ;
- L'ID : l'UUID (Universally Unique IDentifier) utilisé pour identifier l'élément sécurisé ;
- Le numéro de téléphone ;
- L'état du mode d'accès (désactivé) ;
- Le numéro de carte bancaire qui fait référence à une liste contenant des informations comme le nom de la banque, le numéro de compte utilisateur, son montant, les historiques des transactions, etc.

Les messages échangés au cours du processus de protocole sont illustrés en figure 3.4.

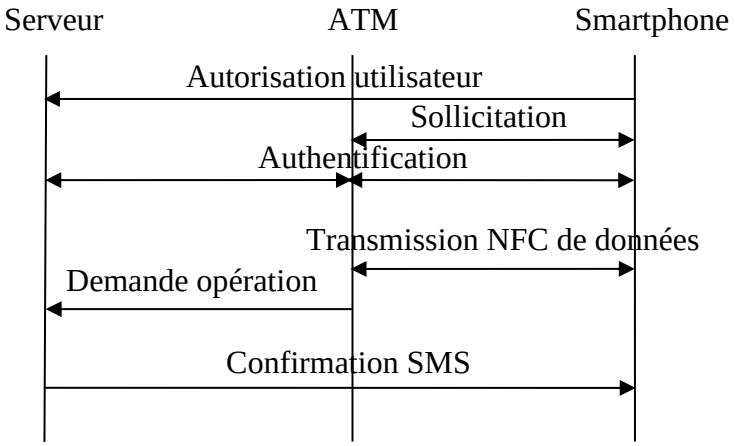

Figure 3.4 : Protocole sécurisé pour paiement NFC entre smartphone et ATM [Chabbi 2020a]

3.2.3.2 Phase d'authentification et de confidentialité

Cette phase comporte les étapes suivantes consignées dans le tableau 3.2 :

Numéro Etape	Nom Etape	Taches
0	Autorisation utilisateur	Elle est importante avant chaque opération avec l'ATM. Elle informe le serveur que le propriétaire d'un compte bancaire veut effectuer une transaction auprès de l'ATM dans la journée courante. ▪ Avant chaque opération, l'utilisateur situé dans un endroit sécurisé loin de l'ATM (par exemple dans sa voiture, quelques minutes avant d'accéder à l'ATM), utilise une application smartphone fournie par l'opérateur pour saisir son mot de passe qui est secret et confidentiel. ▪ Cette application crée une valeur S = H (Id‖CCode), qui représente l'index de l'utilisateur dans la base de données du serveur de l'opérateur. ▪ La valeur S est envoyée au serveur qui la recherche dans sa base de données. Si elle est trouvée, le serveur active l'état du champ mode d'accès dans l'enregistrement correspondant qui le met dans le cache pour autoriser l'opération. Sinon, aucune opération n'est autorisée avec l'ATM. Initialement, l'état du mode d'accès est désactivé, et il sera également désactivé automatiquement par le serveur après la fin de l'opération immédiatement. Afin de se protéger contre les logiciels espions qui peuvent exister dans le smartphone et qui peuvent voler le mot de passe, la technique BrightPass peut être utilisée par l'élément sécurisé du smartphone.
1	Sollicitation	▪ L'ATM sollicite le smartphone pour ses informations. Il envoie un message au smartphone identifiant le type de la carte bancaire.

		▪ Le smartphone envoie un message au GAB en identifiant le type de carte bancaire embarquée dans le smartphone et qui est sélectionnée par l'utilisateur.
2	Authentification	▪ L'ATM génère un nombre aléatoire Natm puis, l'envoie avec une demande au smartphone. ▪ Le smartphone calcule le message A = H (Id⊕Icvv‖Natm) et l'envoie à l'ATM avec Icvv et le nom de la banque. L'Icvv et le nom de la banque sont enregistrés sur la carte bancaire intégrée au smartphone et sélectionnée par l'utilisateur. ▪ L'ATM renvoie le message reçu A, Icvv et le Natm au serveur. ▪ Le serveur recherche dans la mémoire cache qui contient l'ensemble des enregistrements ayant l'état activé du mode d'accès, pour un enregistrement avec un élément identifiant sécurisé Idi tel que : Ai = H (Idi⊕ Icvv‖ Natm) est égal au message A. Il utilise la mémoire cache pour minimiser le temps de recherche. La mémoire cache ne contient que les enregistrements des utilisateurs qui souhaitent effectuer le paiement NFC dans la journée en cours. Si Idi existe, le smartphone est considéré comme légitime et il est authentifié. Sinon, il est considéré illégitime et le protocole est interrompu. ▪ Dans le premier cas (smartphone légitime), le serveur calcule le message Bi et l'envoie à l'ATM. Bi = H (Idi‖Icvv‖Natm) ▪ L'ATM renvoie le message Bi au Smartphone. ▪ Le smartphone calcule B = H (Id‖Icvv‖Natm) et le compare au message Bi. S'ils sont égaux, l'ATM est considéré comme authentifié. Sinon, le protocole est interrompu.
3	Transmission de données NFC	▪ Le Smartphone répond à la sollicitation en renvoyant les informations suivantes au GAB : - Le numéro de la carte bancaire (La carte sélectionnée par l'utilisateur sur le smartphone). - La date d'expiration de la carte bancaire.
4	Demande opération	▪ L'ATM envoie une demande d'une opération au serveur. Cette demande contient : - Le numéro de carte bancaire. - La date d'expiration de la carte bancaire. - Le montant.
5	Confirmation SMS	▪ La transaction est exécutée. Le serveur envoie au smartphone une confirmation SMS (considérée comme sécurisée par TLS) indiquant les détails de la transaction (le numéro de compte utilisateur, le montant retiré, le solde, la date et l'heure de la transaction, etc.). L'état du mode d'accès est désactivé.

Tableau 3.2 : Liste des tâches de la phase d'authentification et de confidentialité [Chabbi 2020a].

La figure 3.5 montre le protocole proposé en détail.

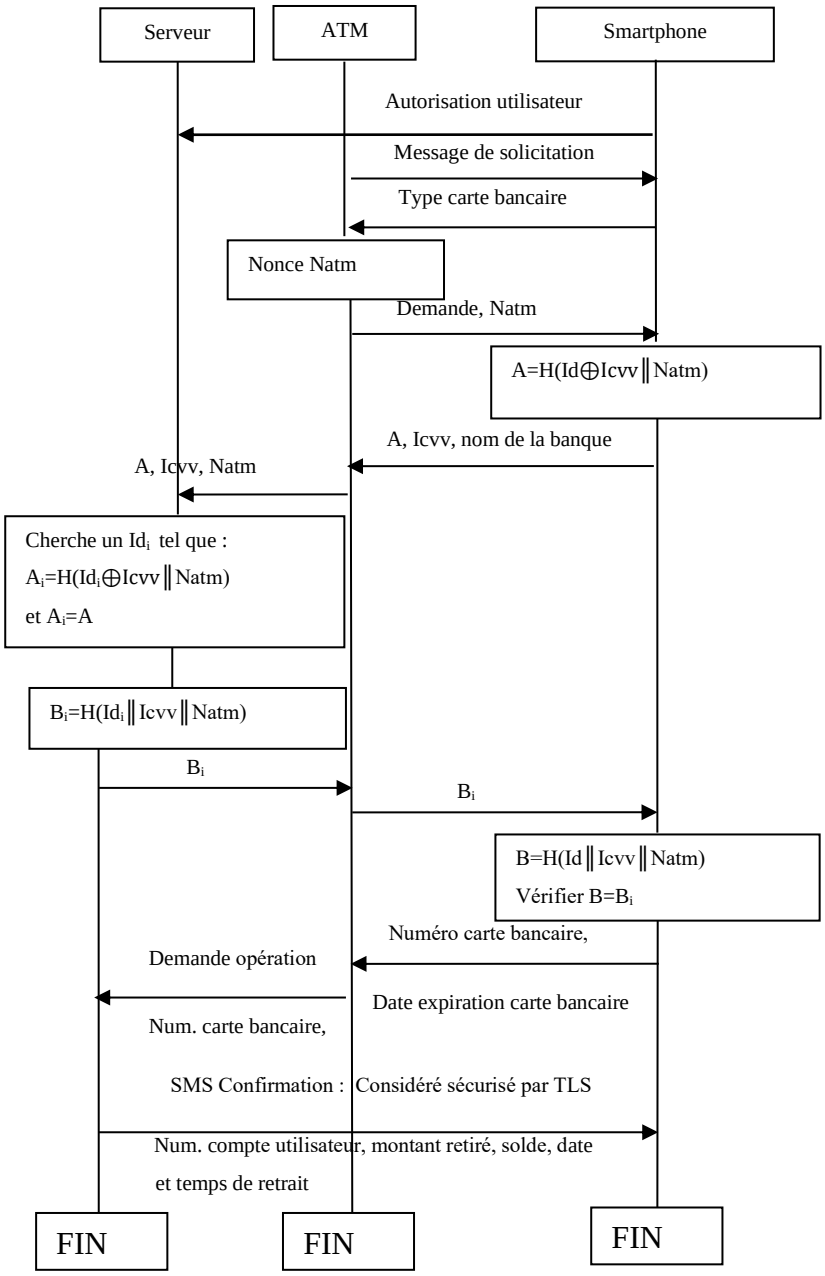

Figure 3.5 : Protocole proposé en détail [Chabbi 2020a]

3.2.3.3 Mesures

- Le taux de transfert entre un smartphone et un ATM dans une communication de paiement NFC est : Débit1 = 424 Kbit / s [Bouazzouni 2017].
- Étant donné que le GAB utilisé dans le paiement NFC et connecté à un modem avec une puce 4G dédiée, le taux de transfert entre un serveur et un ATM est de l'ordre de : Débit2 = 100 Mbps en downlink et Débit3 = 50 Mbps en uplink [Patel et al. 2018].
- La taille du nombre aléatoire Natm peut être de 128 bits [Saha et Geetha 2017]: les 128 bits concaténés avec les 32 bits de Icvv donnent 160 bits qui peuvent être liés à l'Id qui est de 160 bits en utilisant l'opérateur XOR pour former les messages A ou Ai.
- La taille de la variable Icvv est : 32 bits [Jensen et al. 2016].

- La taille de l'identifiant d'élément sécurisé (Id) est : 20 caractères = 20 octets = 160 bits [Jdaida 2016].
- La taille de la clé de banque est : 20 caractères = 160 bits.
- La taille du nom de la banque est : 30 caractères = 240 bits.
- Le plus gros message à crypter avec notre fonction de hachage est : Id || Icvv || Natm avec une taille égale à : 160 + 32 + 128 = 320 bits. Les tailles des différents messages et variables sont présentées dans le tableau 3.3. Les notations et les mesures utilisées dans ce tableau seront utilisées dans le calcul du temps de réponse, y compris le temps d'exécution de la fonction de hachage.

Message ou variable	Spécification	Taille (bits)
Natm	Nombre aléatoire	128
Message1	Natm	128
Id	Identifiant de l'élément sécurisé	160
Bankey	Clé de la banque	160
Bankname	Nom de la banque	240
Icvv	Valeur imprévisible fraîchement générée pour chaque réponse à une sollicitation	32
A ou Ai	Id⊕Icvv||Natm	160
Message2	A+Icvv+Bankname	432
B ou Bi	Id||Icvv||Natm	320
Message3	Bi	320

Tableau 3.3 : Tailles des variables et messages [Chabbi 2020a].

3.2.3.4 Fonction de hachage proposée

La fonction de hachage proposée est utilisée par notre protocole pour générer les messages cryptés A et B dans le smartphone et les messages Ai et Bi dans le serveur. Pour décrire cette fonction de hachage, nous adoptons les trois étapes suivantes :

- Nous définissons la fonction de hachage H.
- Nous identifions quatre propriétés P1, P2, P3 et P4 que la fonction de hachage doit satisfaire.
- Nous prouvons que la fonction de hachage satisfasse les propriétés identifiées.

– ***Définition de la fonction de hachage***

Notre fonction de hachage permet de crypter un message contenant une information secrète (identifiant de l'élément sécurisé ou mot de passe) liée à d'autres informations (Icvv, Natm) à l'aide du xor ou de l'opérateur de concaténation. Ce message, dont la taille est généralement supérieure à 160 bits, est chiffré par cette fonction de hachage à l'aide de la clé de la banque (160 bits), comme suit :

- La fonction divise le message en parties ou champs de taille égale à la taille de la clé bancaire.
- La fonction chiffre chaque partie. Le résultat du chiffrement de chaque partie est un message de 160 bits généré comme suit : Si le bit de la partie à chiffrer est égal à 1, le bit généré est le résultat du xor entre ce bit et le bit correspondant (du même index) dans la clé de banque. Dans le cas contraire (le bit à chiffrer est égal à 0), le bit généré est le résultat du xor entre ce bit et la négation du bit correspondant dans la clé de banque. Le résultat du chiffrement de chaque partie sera un message de 160 bits.
- Enfin, la fonction effectue la somme binaire des parties résultantes pour générer un message crypté final sur un maximum de 161 bits (le pire des cas) sachant que le nombre maximum de parties dans notre protocole est de deux car le plus gros message à crypter est : ID || Icvv || Natm qui est de 320 bits = 160 * 2 bits.

L'implémentation de la fonction de hachage proposée est décrite algorithmiquement comme suit :

```
H (Message, Bankey, Result)
    ▷ Message, Bankey, Result and ht are bit
      sequences
    ▷ ht is an intermediate variable
    Init (result) ▷ empty initialization
    j ← 1
    while j <= Message.size() do
       i ← 1
       Init (ht)
       while i <= bankey.size() and j <= message.size()
          if (message[j] = 1)
             ht[i] ← message[j] xor bankey[i]
          else
             ht[i] ← messag[j] xor not (bankey[i])
          i ← i + 1
          j ← j + 1
     Result.insert (ht)
```

– ***Propriétés de la fonction de hachage H***

Pour garantir un chiffrement sécurisé, la fonction H doit satisfaire les propriétés suivantes :

- P1 : H est irréversible. Étant donné 'mh' un message crypté par la fonction « H ». Il est difficile de trouver le message 'm'tels que : mh = H (m) [Aste et al. 2017].

- P2 : étant donné 'x'. Il est impossible de trouver 'y' différent de 'x' tels que H (x) = H (y) [Zheng et al. 2018]
- P3 : si Icvv est aléatoire, alors H (m) est aléatoire (m : le message à chiffrer par H) [Jensen et al. 2016].
- P4 : Si on connait H (m) pour m = Id || Icvv || Natm, et on connait Natm et Natm0 avec Natm <> Natm0, il est impossible de déduire H (m') pour m'= Id || Icvv || Natm0 sans connaître Id et Icvv [Jensen et al. 2016].

– ***Vérification des propriétés***

La valeur de Icvv est choisie pseudo-aléatoire car la méthode de génération n'est pas connue du public et dépend de la banque qui peut utiliser sa propre fonction de génération arbitraire [Jensen et al. 2016].

- P1 : Étant donné 'mh' un message chiffré par la fonction 'H'. La question est : pouvons-nous déduire le message original 'm'? La réponse est non pour les raisons suivantes :
  Lorsqu'un attaquant traite un bit du message 'mh' = H(m) généré après l'ajout de deux nombres binaires, et que chaque bit d'un nombre est le résultat du xor entre un bit du message et soit le bit correspondant de la clé de banque, soit la négation de ce dernier, il ne peut y avoir aucune information sur le bit du message m. Il est donc impossible pour cet attaquant de reconstruire le message m.
- P2 : Pour cette propriété, nous démontrons qu'il est impossible de trouver une paire x, y telle que H (x) = H (y). Soit le tableau 3.4 représentant la table de vérité du xor.

Bit (message)	0	1	0	1
Bit (Bankkey)	0	0	1	1
Xor	0	1	1	0

Bit (message)	0	1	0	1
Bit Negation (Bankkey)	1	1	0	0
Xor	1	0	0	1

Tableau 3.4: Résultats xor [Chabbi 2020a].

A partir de ce tableau, nous constatons que chaque modification du bit de message, modifie le résultat xor. Cela implique l'obtention d'une nouvelle séquence binaire et donc un nouveau nombre, ce qui signifie une nouvelle empreinte et donc, un nouveau message crypté.

- P3 : Si Icvv est aléatoire, et nous avons déjà Natm un nombre aléatoire, alors le message m = Id || Icvv || Natm ou le message m = Id⊕Icvv || Natm est aléatoire et donc H(m) sera également aléatoire.
- P4 : Si nous connaissons H (m) pour m = Id || Icvv || Natm, et nous connaissons Natm, nous ne pouvons pas déduire le message m selon la preuve présentée en P1. De cette façon, le message m reste inconnu. Par conséquent, il est impossible de connaître les informations Id et Icvv. Cela implique que nous ne pouvons pas calculer m' = Id || Icvv || Natm0 même avec la connaissance de Natm0 et donc impossible de connaître H (m').

Comme les propriétés p1, p2, p3 et p4 sont vérifiées, on peut considérer que notre fonction avec son code simple est une fonction de hachage sécurisée.

3.3 Analyse de la sécurité

Deux types de vérification de la sécurité de notre méthode sont établis :

3.3.1 Contrôle de la sécurité par analyse

L'analyse de la solution proposée montre qu'elle est infranchissable par les attaques suivantes : Force brute, Clonage de carte, enregistrement par caméra, Spyware, Shoulder-Surfinf, Eavesdropping, Skimming, déni de service, relais, replay, Man-In-The-Middle et le vol du smartphone.

3.3.1.1 Attaque par Force brute

Cette attaque nécessite l'installation de logiciel malveillant sur l'ATM ou sur le smartphone qui essaie toutes les combinaisons possibles de caractères ou de chiffres pour trouver le mot de passe saisi par l'ATM ou par le smartphone. Concernant l'ATM, notre solution lutte contre cette attaque car il n'y a pas de transfert de mot de passe vers l'ATM via l'interface radiofréquence. Dans le cas du smartphone, notre méthode est protégée contre cette attaque par la technique BrightPass et en plus, après un certain nombre de tentatives infructueuses (deux ou trois fois), le serveur bloque l'application de l'opérateur utilisée pour saisir le mot de passe. Bien que la communication entre le smartphone et le serveur est considérée comme sûre, notre objectif est de sécuriser la communication entre l'ATM et le smartphone et nous avons prouvé qu'elle est sécurisée contre ce type d'attaques.

3.3.1.2 Attaque par clonage de carte

Cette attaque exige l'utilisation de dispositifs de clonage installés sur l'ATM et qui ne sont pas détectables par l'utilisateur, afin d'enregistrer secrètement les données embarquées dans la carte bancaire intégrée dans le smartphone et cela dans le but de créer une copie clonée pour une utilisation ultérieure. Dans notre système, l'utilisation d'une copie de la carte bancaire ou même d'une copie de l'élément sécurisé n'est pas suffisante pour valider une transaction avec l'ATM car cela nécessite l'activation de l'état du mode d'accès dans la base de données du serveur en saisissant correctement le mot de passe, et comme l'attaquant n'a pas le mot de passe qui n'est jamais saisi près de l'ATM, et qu'il n'a qu'une copie clonée de la carte bancaire ou de la carte de crédit ou de l'élément sécurisé, il ne peut pas réaliser de transaction avec l'ATM. En revanche, pour l'attaquant qui a réussi à restaurer les informations relatives à la carte bancaire, il ne peut pas décrypter les messages chiffrés transmis pour trouver l'identifiant de l'élément sécurisé ou le mot de passe et il ne peut les restituer car ils sont stockés d'une manière protégée dans l'élément sécurisé sachant que ces deux informations sont nécessaires à l'exécution du protocole.

3.3.1.3 Attaque d'enregistrement par caméra

Dans une telle attaque, l'attaquant utilise une caméra à proximité de l'ATM pour enregistrer le mot de passe entré par l'utilisateur à l'aide du smartphone ou de l'ATM. Étant donné que la solution est basée sur la saisie d'un mot de passe aussi loin de l'ATM et que ce mot de passe est envoyé au serveur cloud et non à l'ATM, cette attaque n'aura aucun effet.

3.3.1.4 Attaque par Spyware

Dans ce cas, l'attaquant utilise un logiciel malveillant qui sera installé sur l'ATM ou sur le smartphone. Le Spyware va enregistrer les frappes de touches de saisie de l'utilisateur afin de voler ces informations d'identification et en particulier le mot de passe. Pour la solution proposée, cette attaque est inefficace sur l'ATM parce que d'un côté, l'attaquant ne peut pas récupérer le mot de passe qui n'est pas saisi par l'ATM. D'un autre côté, s'il récupère l'identifiant de l'élément sécurisé, il ne peut rien faire avec car il va le trouver chiffré avec un nombre aléatoire (c'est-à-dire Natm).

Cette attaque est aussi inefficace sur smartphone car le mot de passe saisi par ce dernier est protégé contre le Spyware en utilisant la technique BrightPass.

3.3.1.5 Attaque par Shoulder-surfing

Par cette attaque, l'attaquant se déplace prêt du GAB et attend l'arrivée d'un utilisateur pour se situer derrière lui afin de lire et mémoriser le mot de passe saisi. Étant donné que la solution utilise un mot de passe saisi dans un emplacement sécurisé loin du GAB, cette attaque n'aura aucun effet.

3.3.1.6 Attaque par canal auxiliaire

L'attaque par canal auxiliaire utilise un logiciel espion qui exploite les ressources partagées entre le système d'exploitation mobile et l'élément sécurisé pour faire réussir ce type d'attaque [Guerar 2017], et ceci dans le but de capturer les frappes de l'utilisateur. Étant donné que l'élément sécurisé utilise des moyens de protection pour sécuriser les données sensibles saisies par l'utilisateur et que la technique BrightPass est utilisée sur le smartphone afin de protéger la saisie du mot de passe contre ce type d'attaque, notre solution est bien protégée contre l'attaque par canal auxiliaire. Sur le GAB, si le logiciel espion est installé, il n'aura aucun effet car il n'y a pas de mot de passe à saisir par le GAB.

3.3.1.7 Attaque Eavesdropping

On suppose que malgré la distance courte entre le GAB et le smartphone pendant la transmission des données sensibles lors du paiement NFC, ou pendant qu'un utilisateur envoie son mot de passe en cloud dans un certain endroit, un attaquant et grâce à des nouveaux moyens très sophistiqués a réussi de capturer les informations envoyées. Il n'a qu'à recevoir un identifiant d'élément sécurisé 'Id' et un mot de passe qui sont bien cryptés par les opérateurs xor et de concaténation et par notre fonction de hachage et par aussi une valeur aléatoire (Natm) ce qui garantit qu'aucune information sensible en clair ne soit divulguée ou déchiffrée. L'espion ne peut pas alors recevoir en clair ni l'identifiant, ni le mot de passe pour les faire cloner sur une autre carte ou un autre smartphone ou pour les faire rejouer lors d'une prochaine opération de paiement avec l'ATM, surtout lorsque des nombres aléatoires sont utilisés dans le chiffrement.

3.3.1.8 Attaque Skimming

Le skimmer qui a réussi à recevoir les messages chiffrés envoyés ou reçus par le smartphone, va être bloqué pour effectuer un paiement avec le GAB pour la raison que les messages utilisent un défi aléatoire Natm qui sera différent du défi aléatoire généré par le GAB lors d'une nouvelle opération de paiement. A cet effet, cette attaque n'aura aucun effet sur un paiement NFC avec l'ATM.

3.3.1.9 Attaque Déni de Service (*DOS*)

La solution ne nécessite pas de synchronisation. La perte de messages, le manque d'énergie et la panne de connexion n'affectent pas la sécurité de l'identifiant de l'élément sécurisé ou du mot de passe. Cela signifie que la solution peut résister à l'attaque par déni de service. En revanche, avec une courte distance entre le smartphone et le GAB, il est difficile de réaliser l'inondation du réseau (*network flooding*) ou l'interruption de la connexion.

3.3.1.10 Attaque de relais

Dans cette menace, il y a deux attaquants qui coopèrent, l'un est appelé *môle* et l'autre est appelé *proxy*. Comme un smartphone est utilisé à la place d'une carte de crédit ou une carte bancaire pour faire du paiement, il est impossible pour un *môle* d'activer le mobile de la victime sans son consentement car le smartphone doit être allumé et l'option NFC doit être activée par l'utilisateur. Malgré ça, nous supposons que le *môle* a reçu par une application similaire à celle du GAB par exemple des informations sensibles de la carte bancaire sachant qu'elles sont chiffrées et il les a transmises au proxy. Le proxy qui est proche d'un ATM ne peut pas effectuer une transaction de paiement avec ce dernier car le paiement nécessite l'activation de l'état du mode d'accès qui sera réalisé par l'envoi du mot de passe en cloud, et comme ni le *môle*, ni le *proxy* ne peut réaliser cette tâche à cause de l'inconnaissance du mot de passe, une transaction avec l'ATM ne peut être réalisée. En revanche, lors d'une attaque par relais, le *môle* envoie un défi aléatoire Natm1 au smartphone de la victime, il reçoit un message A1 = H (Id⊕Icvv‖ Natm1) du smartphone, ensuite il va envoyer le message A1 au proxy. Le proxy essaie d'effectuer une transaction avec l'ATM qui lui génère et envoie un challenge aléatoire Natm2. Le proxy ne peut pas construire le message A2 = H (Id⊕Icvv‖Natm2) et n'a que le message A1 qui ne peut pas être utilisé à la place du message A2 pour effectuer une transaction avec l'ATM. Par cette démonstration, nous pouvons conclure que notre méthode est bien protégée contre l'attaque par relais.

3.3.1.11 Attaque vol du smartphone

Après avoir volé le smartphone de la victime, l'attaquant ne peut pas effectuer une transaction avec le GAB car il n'a pas envoyé en cloud le mot de passe de l'utilisateur et qui est inconnu pour lui. Ce blocage est justifié comme suit :

- Si le voleur rapproche le smartphone de la victime près de l'ATM, le protocole sera interrompu à l'étape 2 (authentification) lorsque le serveur ne trouvera pas l'enregistrement

approprié dans l'ensemble des enregistrements se trouvant en mémoire cache et qui sont caractérisés par un état activé du mode d'accès. Ainsi, l'état du mode d'accès de l'enregistrement utilisateur dans la base de données reste désactivé et la transaction NFC ne peut pas être établie.

- Si le voleur utilise l'application de l'opérateur sur le cloud et tente de saisir un mot de passe CCode0) différent du CCode, le message M0 = H (Id‖CCode0) sera transmis au serveur. Le serveur après avoir vérifié dans la base de données, n'active pas l'état du mode d'accès car il n'y a pas de valeur index de recherche égale à M0. Dans ce cas, le protocole sera interrompu par le serveur à l'étape 2 (authentification). D'un autre côté, lorsque l'assaillant saisit un mot de passe CCode0 différent du CCode, le SE détecte la différence et n'envoie pas au serveur le message chiffré constitué par l'ID avec le mot de passe de l'utilisateur. Ainsi, l'état du mode d'accès reste désactivé et il est impossible d'effectuer une transaction NFC avec le GAB.

Après cette analyse basée sur la logique, nous pouvons avancer que nous avons prouvé la sécurité de notre méthode contre les 11 attaques susmentionnées.

3.3.2 Contrôle automatique de la sécurité

Cette section présente les résultats de validation de notre solution à l'aide de l'outil AVISPA qui permet la vérification automatique de la sécurité de notre protocole. Avant de présenter ces résultats, faisant un aperçu sur l'outil de simulation.

3.3.2.1 Outils de simulation

L'outil de simulation utilisé appelé AVISPA, est une plateforme équipée d'une interface utilisateur graphique qui prend en charge l'édition des spécifications de protocole et permet à l'utilisateur de sélectionner et de configurer les différentes fonctionnalités de l'outil. Si une attaque sur un protocole est trouvée, l'outil l'affiche sous forme de diagramme de séquence de messages. L'interface propose des menus spécialisés pour les utilisateurs apprentis et experts. Un mode XEmacs pour l'édition des spécifications de protocole est également disponible. L'outil AVISPA se compose de modules développés indépendamment, comme indiqué en bas à gauche (Figure 3.6). Un concepteur de protocole interagit avec l'outil en spécifiant un problème de sécurité d'un protocole lorsqu'une propriété de sécurité n'est atteinte. Le protocole est écrit dans un langage de spécification de protocole de haut niveau appelé HLPSL (High-Level Protocol Specification Language) qui est un langage formel, expressif, modulaire, basé sur les rôles et qui permet de spécifier des modèles de flux

de contrôle, des infrastructures de données, des modèles d'intrus alternatifs, des propriétés de sécurité complexes, ainsi que différentes primitives cryptographiques et leurs propriétés algébriques. Ces caractéristiques rendent HLPSL bien adapté pour spécifier des protocoles modernes à l'échelle industrielle. Ce langage utilise l'analyse et la vérification formelle [Luca 2006].

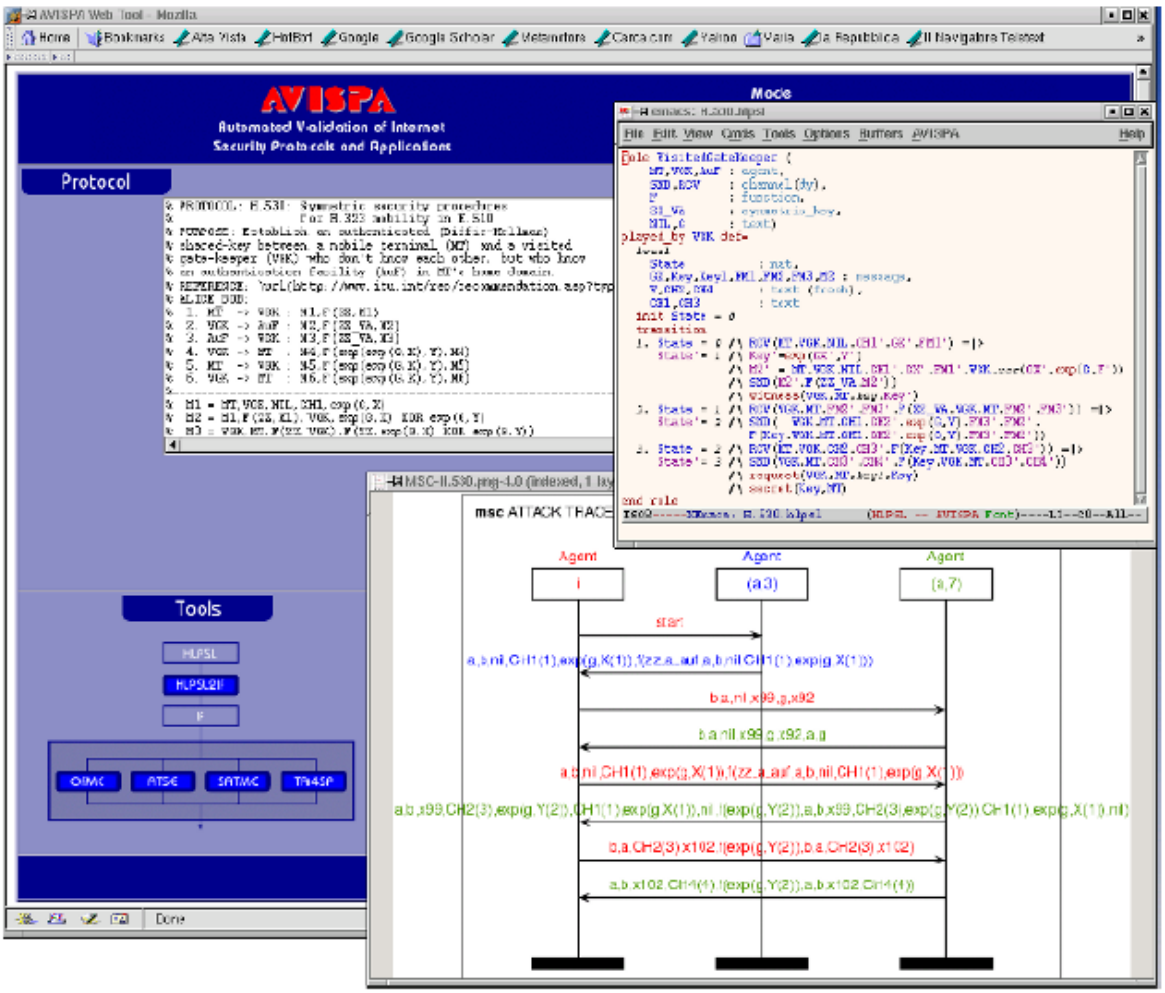

Figure 3.6 : Interface graphique de AVISPA [Luca 2006].

3.3.2.2 Résultats de simulation

La figure 3.7 montre une partie de la spécification de notre protocole qui pourrait détecter les attaques par rejeu et Man-In-The-Middle si elles existent.

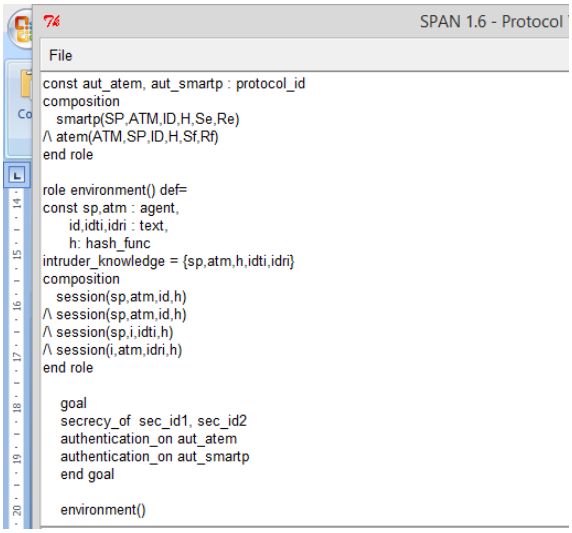

Figure 3.7 : Spécification HLPSL du protocole [Chabbi 2020a]

Après la vérification du protocole par l'outil OFMC (On-the-Fly-Model-Checking) d'AVISPA, le résultat est illustré à la figure 3.8.

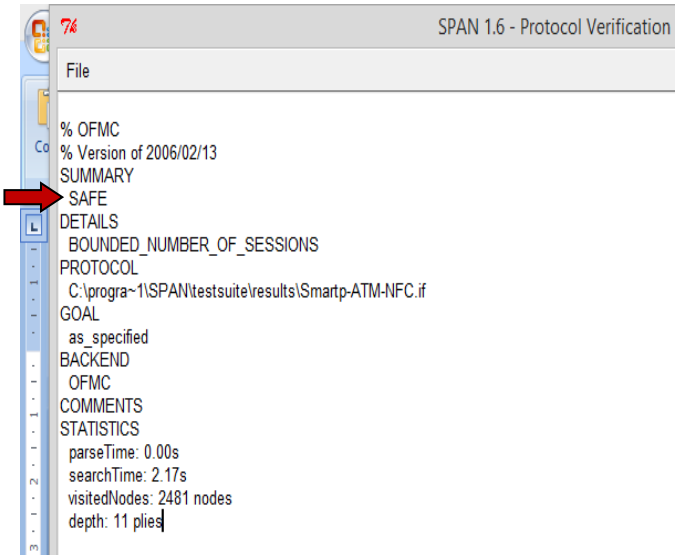

Figure 3.8 : Résultat du Protocole généré par l'outil OFMC [Chabbi 2020a]

Après la vérification du protocole par l'outil ATSE (Attack Searcher) d'AVISPA, le résultat est illustré à la figure 3.9.

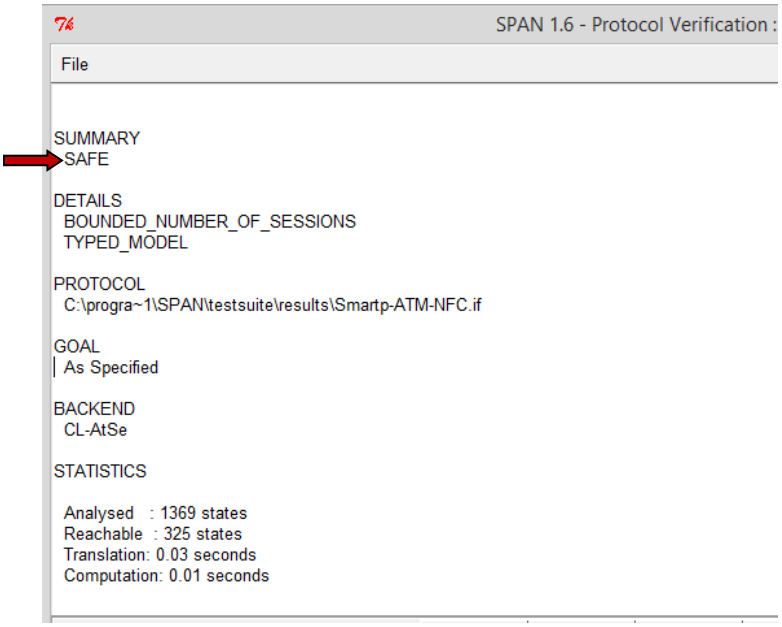

Figure 3.9 : Résultat du Protocole généré par l'outil ATSE [Chabbi 2020a]

Le résultat spécifié dans la figure 3.8 et la figure 3.9 signifie que le protocole est protégé contre l'attaque par rejeu et l'attaque Man-In-The-Middle.

3.4 Comparaison de performances

Dans cette section, nous comparons notre solution avec certaines méthodes existantes bien connues.

3.4.1 Evaluation de la sécurité

Le but de cette analyse est de vérifier la faiblesse de quelques méthodes et protocoles devant un ensemble d'attaques. Certains résultats sont obtenus par l'outil AVISPA et d'autres sont obtenus par l'analyse et la preuve de la faiblesse du protocole ou de la méthode contre une certaine attaque.

- Les méthodes FakePIN et PassWindow, malgré leur résistance contre l'attaque de shoulder-surfing et l'attaque de l'enregistrement par caméra, elles sont vulnérables contre l'attaque d'intersection des enregistrements multiples.
- Les méthodes BrightPass et Cappcha sont réellement protégées contre les logiciels malveillants mais, elles sont vulnérables à l'attaque Shoulder-surfing ou l'attaque d'enregistrement par caméra car un attaquant ou une caméra peut utiliser une observation directe en regardant ou filmant l'entrée directe du mot de passe. Dans la technique BrightPass, un attaquant qui connaît le principe de fonctionnement, enregistre dans sa

mémoire les nombres entrés dans les cercles ayant une luminosité élevée. Si par la suite l'attaquant peut voler ou emprunter le smartphone, il peut effectuer une transaction de paiement avec l'ATM en suivant les indications de l'élément sécurisé.

- Dans la solution proposée, l'attaque de Shoulder-Surfing ou l'attaque par enregistrement caméra est impossible car l'utilisateur peut saisir son mot de passe sur le cloud et dans un endroit sécurisé, par exemple à son domicile ou dans sa voiture, ce qui signifie que le vol de smartphone n'aura aucun effet concernant une transaction de paiement avec l'ATM.
  Les messages utilisés dans notre protocole sont difficiles à décrypter car ils sont chiffrés avec des nonces, opérateur xor, opérateur de concaténation et ils sont signés avec une fonction de hachage. Il est donc difficile de les déchiffrer et de retrouver le mot de passe ou l'identifiant de l'élément sécurisé en cas de restitution des messages cryptés.

Le contrôle de sécurité présenté dans cette section prouve que notre méthode présente un haut niveau de sécurité. Nous présentons dans le tableau 3.5, une comparaison entre notre solution et les autres méthodes utilisées pour sécuriser un paiement NFC ou RFID.

Attaque/ Méthode	GoogW	EmvCC	Brfid	FakeP	PassW	Capp	Bpass	Cpass
Vol de la carte ou du smartphone	V	/	/	R	R	R	R	R
Man-In-The-Middle	/	V	R	/	/	/	/	R
Rejeu	/	/	R	/	/	/	/	R
Suivi de trace	/	/	R	/	/	/	/	R
Vol de l'empreinte utilisateur et de la carte	/	/	V	/	/	/	/	R
Shoulder-surfing	V	V	/	R	R	/	/	R
Enregistrements multiples	V	V	/	V	V	R	R	R
Canal auxiliaire	V	V	/	R	R	R	R	R
Enregistrement simple	V	V	/	R	R	R	R	R
Force brut	/	/	/	V	V	R	R	R
Spyware	V	V	/	R	R	R	R	R
Enregistrement écran	V	V	/	R	R	R	R	R
Clonage de carte	/	/	/	R	R	R	R	R
Enregistrement par caméra	V	V	/	R	R	/	/	R
Eavesdropping	/	/	/	/	/	/	/	R
Skimming	/	/	/	/	/	/	/	R
Relai	/	/	/	/	/	/	/	R
ATM compromis	/	/	/	/	/	/	/	R
Déni de service	/	/	/	/	/	/	/	R
Enregistrement par camera et vol du smartphone	V	V	/	/	/	V	V	R
Shoulder-surfing et vol du Smartphone	V	V	/	/	/	V	V	R

Tableau 3.5 : Limites de sécurité de quelques méthodes et protocoles [Chabbi 2020a].

Le tableau 3.5 présente les limites de sécurité de quelques méthodes et protocoles bien connus. Nous notons par « V » et respectivement par « R » que la méthode ou le protocole est vulnérable respectivement résistant à l'attaque. Le tableau 3.5 montre donc la vulnérabilité et

la résistance aux attaques mentionnées concernant les méthodes suivantes : GoogW et EmvCC [Vincent 2012], FakeP, PassW, Capp et Bpass [Guerar, 2017]. Le reste des informations de ce tableau est obtenu par notre analyse. Selon ce tableau, nous montrons que chaque méthode mentionnée est vulnérable à quelques attaques à l'exception de la solution proposée (Cpass) qui lutte contre toutes les attaques mentionnées ce qui signifie qu'elle est la plus sécuritaire.

Nous pouvons maintenant passer en revue les points forts de la sécurité de la solution proposée.

- L'utilisation d'un mot de passe tapé dans un endroit sécurisé par l'utilisateur, chiffré avec l'identifiant de l'élément sécurisé et envoyé sur le cloud. Cela signifie que l'utilisateur tape son mot de passe dans un endroit loin des attaquants.
- L'identifiant d'élément sécurisé et le mot de passe sont protégés par un chiffrement en utilisant les opérateurs xor et concaténation et notre fonction de hachage proposée. Cela signifie que la confidentialité est vérifiée.
- L'utilisateur, le smartphone et l'ATM sont authentifiés.
- L'intégrité des données est vérifiée.
- Le type d'élément sécurisé utilisé offre un haut niveau de sécurité.
- Dans le pire des cas, si une nouvelle attaque supplémentaire est découverte et a franchi notre protocole, un SMS de confirmation est envoyé au smartphone du propriétaire représentant un message d'alarme, lui indiquant que le solde de son compte bancaire par exemple a changé. Cela signifie que le protocole utilise une technique de test d'intrusion.
- Le protocole n'utilise aucune modalité biométrique. Donc, l'utilisateur n'est pas exposé aux attaques associées.

3.4.2 Temps d'authentification

3.4.2.1 Test d'utilisabilité de la fonction de hachage

Nous présentons dans ce qui suit un test d'utilisabilité d'un code java qui représente notre fonction de hachage. Nous avons implémenté la fonction de hachage en Java. Le tableau 3.6 montre le temps d'exécution de la fonction de hachage sur les messages A (160 bits) et B (320 bits) :

Message	Temps execution (ms: milliseconde)										
	Essai 1	Essai 2	Essai 3	Essai 4	Essai 5	Essai 6	Essai 7	Essai 8	Essai 9	Essai 10	Moyenne
A	1	2	1	1	1	2	2	1	1	2	1.4
Ai	Idem au message A (même taille)										1.4
Bi	Idem au message B (même taille)										1.9
B	2	1	3	3	2	1	2	2	2	1	1.9

Table 3.6 : Temps d'exécution de la fonction de hachage [Chabbi 2020a].

Le temps d'exécution de la fonction de hachage pendant l'authentification est : 1,9 * 2 + 1,4 * 2 = 6,6 ms

– ***Calcul du temps de transfert des messages***

En analysant le diagramme de protocole, il est possible d'estimer le temps d'authentification 'At' en sommant les temps indiqués dans le tableau 3.7 :

Symbole	Définition
Tm1	Temps de transmission du Message1 de l'ATM au smartphone. Tm1 = taille du message 1 / débit1 = 128/424 ms = 0,30 ms.
Th1	Temps d'exécution de la fonction de hachage pour construire le message 'A' sur le smartphone. Th1 = 1,4 ms (tableau 3.6).
Tm2	Temps de transmission du Message2 du smartphone à l'ATM. Tm2 = taille du message 2 / débit2 = 432/424 ms = 1,02 ms.
Tm3	Temps de transmission du Message2 de l'ATM au serveur. Tm3 = taille du message2 / débit3 = 432/50 * 1024 * 8 ms = 0,001 ms.
Th2	Temps d'exécution de la fonction de hachage pour construire le message 'Ai' sur le serveur. Th2 = 1,4 ms (tableau 3.6).
Th3	Temps d'exécution de la fonction de hachage pour construire le message 'Bi' sur le serveur. Th3 = 1,9 ms (tableau 3.6).
Tm4	Temps de transmission du Message3 du serveur à l'ATM. Tm4 = taille du message3 / débit2 = 320/100 * 1024 * 8 ms = 0,0004 ms.
Tm5	Temps de transmission du Message3 de l'ATM au smartphone. Tm5 = taille du message 3 / débit1 = 320 / 424ms = 0,75 ms.
Th4	Temps d'exécution de la fonction de hachage pour construire le message 'B' sur le smartphone. Th4 = 1,9 ms (tableau 3.6).

Tableau 3.7 : Temps d'exécution de la fonction de hachage et de transmission des messages [Chabbi 2020a].

At = Tm1 + Th1 + Tm2 + Tm3 + Th2 + Th3 + Tm4 + Tm5 + Th4 = 0,30 + 1,4 + 1,02 + 0,001 + 1,4 + 1,9 + 0,0004 + 0,75 + 1,9 = 8,67 ms.

Le temps de transfert des messages lors de l'authentification est de : 2,07 ms (tableau 3.8). On conclut que le temps d'authentification est : 6,6 + 2,07 = 8,67 ms.

Message	Taille (Bits)	Parties communicantes		Temps de transmission (ms)
		Smartphone – ATM débit1 = 424kbit/s	Serveur – ATM débit2 = 100Mbps (downlink) débit3 = 50Mbps (uplink)	
Message1	128	*		Tm1=0.30
Message2	432	*		Tm2=1.02
Message2	432		*	Tm3=0.001
Message3	320		*	Tm4=0.0004
Message3	320	*		Tm5=0.75
Total				2.07

Tableau 3.8 : Temps de transfert des messages [Chabbi 2020a].

– ***Calcul de la complexité***

Dans la fonction de hachage, nous avons une boucle externe qui commence à partir du premier bit du message et se termine par le dernier. Dans cette boucle, on trouve une autre boucle interne ce qui implique que la complexité est égale à O (n).

3.4.3 Analyse de performances

Le but de cette analyse est de montrer que la solution proposée est économique et de prouver qu'elle représente le meilleur temps d'authentification et qu'elle est efficace.

Nous présentons dans le tableau 3.9 et la figure 3.10 les temps d'authentification en secondes de quelques méthodes bien connues avec celui de notre proposition pour effectuer une comparaison. Le tableau 3.9 montre les temps d'authentification des méthodes FakeP, PassW, Capp et Bpass [Guerar 2017]. Les tableaux et la figure cités montrent que le temps d'authentification estimé pour notre protocole est le meilleur et le plus réduit. En fait, le protocole ne nécessite aucune entrée de mot de passe devant l'ATM, ce qui fait gagner du temps.

Méthode	Temps d'authentification (s)
FakeP	10.90
PassW	18.12
App	4.12
Bpass	8.20
Cpass	0.00867

Tableau 3.9 : Comparaison de temps d'authentification [Chabbi 2020a]

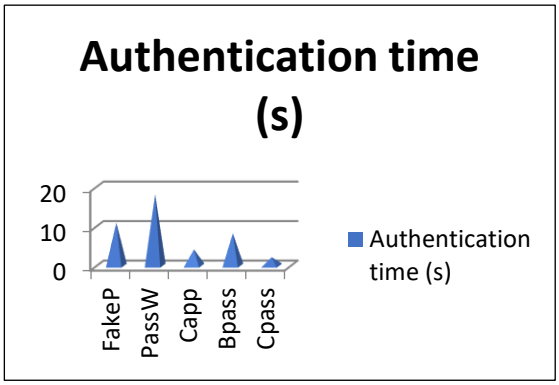

Figure 3.10 : Comparaison de temps d'authentification [Chabbi 2020a]

Nous calculons maintenant, pour notre protocole, le nombre d'opérations de fonction de hachage effectuées sur le smartphone pour évaluer le coût de calcul ; le nombre de variables stockées dans la mémoire de l'élément sécurisé pour évaluer l'espace de stockage et le nombre de variables transmises pour évaluer le coût de communication.

3.4.3.1 Coût de calcul

Le protocole proposé nécessite 03 opérations d'exécution de la fonction de hachage sur le smartphone. Cela signifie qu'il n'est pas coûteux en temps de calcul par rapport à la capacité de traitement du smartphone et la capacité de mémoire de l'élément sécurisé.

3.4.3.2 Espace de stockage

Le protocole nécessite une taille mémoire sur l'élément sécurisé égale à 04∗L (L : taille en bits pour chaque variable) pour stocker l'identifiant d'élément sécurisé (Id), l'Icvv, le numéro de carte bancaire et la date d'expiration de la carte bancaire. En outre, il n'y a pas de stockage de modalités biométriques, ce qui signifie un faible espace de stockage sur la mémoire sécurisée.

3.4.3.3 Coût de communication

Le protocole proposé est efficace en termes de coût de communication car il y a peu de messages échangés entre le smartphone et l'ATM lors du paiement électronique NFC sachant que l'authentification de l'utilisateur est séparée de la communication NFC. Le protocole est rentable en considérant les points suivants :

- Le protocole est sécurisé selon la vérification présentée.

- Au niveau du smartphone, il y a peu de calculs de la fonction de hachage (seulement deux) pour calculer le message 'A' et le message 'B' avec un temps égal à : Th1 + Th4 = 1,4 + 1,9 = 3,3 ms. Il est donc économique en coût de calcul.
- Le nombre de messages transmis entre le smartphone et l'ATM est de trois : message1, message2 et message3, avec un temps de transfert égal à : Tm1 + Tm2 + Tm5 = 0,30 + 1,02 + 0,75 = 2,07 ms. Il est donc économique en coût de communication.

Le protocole est comparé au protocole Brfid en considérant le nombre de xor, de concaténations et de la fonction de hachage utilisée. Le tableau 3.10 et la figure 3.11 présentent les résultats obtenus. Nous montrons que Cpass est le meilleur par rapport à Brfid car il présente le plus petit nombre d'opérateurs xor et ‖ et de fonctions de hachage.

Paramètre	Brfid	Cpass
Nombre de ⊕	5	2
Nombre de ‖	5	4
Nombre de fonction de hachage	5	4

Tableau 3.10: Cpass VS Brfid [Chabbi 2020a]

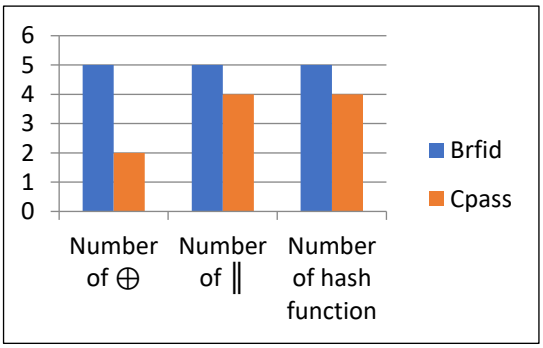

Figure 3.11: Cpass VS Brfid [Chabbi 2020a]

En revanche, en comparant Cpass avec le protocole sécurisé de carte de crédit (SCCP), nous pouvons tirer certaines caractéristiques de notre solution (voir tableau 3.11).

SCCP	Cpass
Utilise seulement une carte de crédit	Smartphone utilisé. L'utilisateur peut sélectionner une carte parmi une liste
Vulnérable contre l'attaque vol de la carte de crédit	Résistant contre l'attaque vol du smartphone
Pas d'utilisation de mot de passe	Utilisation de mot de passe
Pas de message de confirmation après le paiement	Utilisation d'un message de confirmation comme un test d'intrusion indiquant les détails de la transaction
Pas d'utilisation d'élément sécurisé	Utilisation de l'élément sécurisé

Tableau 3.11 : Cpass VS SCCP [Chabbi 2020a].

Lorsque nous comparons notre protocole avec le protocole de Jie et al., Nous constatons que le dernier utilise plus de messages et plus d'opérations de calcul. La comparaison est présentée dans le tableau 3.12

En analysant le protocole de Jie et al., on trouve que chaque appareil communiquant envoie 04 messages [Ling et al. 2017] : Par exemple, l'appareil 'A' envoie les messages suivants :

- Le message contenant le mot de passe et l'identité de l'appareil : {qA, IDA}
- Le message m1 contenant la concaténation du résultat 'h', de l'identité 'A' et de l'identité 'B' : m1 = h (IDA‖ IDB‖ SA) ‖ IDA ‖ IDB
- Le message {Q'A‖NA‖Q "A}
- Le message m3 = {MacTagA}

Les messages reçus par le dispositif 'A' sont les suivants :

- RB
- Le message m2 = Enc (QA, RB) ‖IDTSM‖STSM
- Le message m4 = {MacTagB}

Le dispositif 'A' effectue les calculs suivants :

- m1 = h (IDA‖ IDB‖ SA) ‖ IDA ‖ IDB
- Enc (QA, RB)
- Q'A = rAQA, Q "A = rAdAQS + QA
- PA = rAdAQ''BTSA (RB)
- Valeur 'Z' de 'P'
- SSK = KDF (NA, NB, IDA, IDB, Z)
- MagTagA = f (SSK, IDA, IDB, QA, QB)

Les vérifications établies par le dispositif 'A' sont les suivantes :

- Vérifier la signature TSM (STSM)
- Vérifier la validation du message m4

À la fin, les valeurs aléatoires générées par le dispositif 'A' sont :

- Le mot de passe qA
- L'IDA d'identité
- Le nonce NA
- Le nombre aléatoire rA

Cependant, pour le protocole proposé, les messages envoyés pour le smartphone sont les suivants :

- A, Icvv, nom de la banque

Les messages reçus sont les suivants :

- Demande, Natm
- Bi = H (Idi‖Icvv‖Natm)

Les opérations de calcul réalisées par le smartphone sont les suivantes :

- A = H (Id⊕Icvv‖Natm)
- B = H (Id‖Icvv‖Natm)

Les opérations de vérification sont les suivantes :

- Vérifier B = Bi

Paramètre / Protocole	**Protocole Jie et al.'s**	**Cpass**
Nombre de messages envoyés	04	01
Nombre de messages reçus	03	02
Nombre d'opérations de calcul	07	02
Nombre d'opérations de vérification	02	01
Nombre de valeurs aléatoires générées	04	00

Table 3.12 : Cpass vs le protocole Jie et al. [Chabbi 2020a].

Nous comparons maintenant notre solution avec la solution de Nana et al. La comparaison présentée dans le tableau 3.13 indique que notre solution est plus sécuritaire et plus économique.

Attaque/ Solution	**Solution Nana et al.**	**Cpass**
Faux lecteur de l'empreinte	V	R
Enregistrement par caméra (si mot de passe utilisé)	V	R
Shoulder-Surfing (si mot de passe utilisé)	V	R

Tableau 3.13 : Cpass vs la solution Nana et al. [Chabbi 2020a].

Maintenant, nous étudions la difficulté que les utilisateurs les plus âgés peuvent rencontrer lors de l'opération d'authentification avec un ATM en utilisant les quatre dernières méthodes (Fake PIN, Passwindow, Cappcha et BrightPass) et nous les comparons avec la solution proposée. Les résultats sont présentés dans les tableaux 3.14 et 3.15. Par hypothèse, nous pouvons évaluer chaque difficulté sur un point. Pour la méthode proposée, nous pouvons évaluer la difficulté de 0,5 point, car l'agent plus âgé n'a qu'à rapprocher son smartphone devant le GAB et à ne pas saisir de mot de passe.

Méthode	Difficultés
FakeP	- Mémoriser deux mots de passe : l'un est alphanumérique et l'autre est une direction. - Clavier virtuel qui peut être modifié à chaque tentative de paiement. - Le caractère à saisir est la combination entre le caractère du mot de passe et la direction.
PassW	- Mémoriser deux mots de passe : le code PIN et une icône présélectionnée. - Mémoriser l'emplacement de l'icône présélectionnée dans une grille modifiable contenant d'autres icônes aléatoires pour chaque opération d'authentification. - Affichage d'un clavier virtuel et d'une grille sans icônes. - Incliner le téléphone pour déplacer la grille sur le clavier virtuel afin d'entrer le chiffre PIN à l'emplacement de l'icône présélectionnée. - Masquer la loupe de la caméra.
Capp	- Mémoriser le code PIN. - Incliner le téléphone mobile à un degré spécifique affiché sur l'écran et maintenez-le dans une telle position pendant une seconde pour avoir accès au code PIN.
Bpass	- Mémoriser le code PIN. - Afficher un ensemble de petits cercles qui prennent la position des numéros de mot de passe. Dans un cercle de faible luminosité, l'utilisateur saisit un faux chiffre. En haute luminosité, un vrai chiffre est saisi.
Cpass	- L'utilisateur rapproche seulement son smartphone sans aucune saisie près du GAB car il a pris son temps pour introduire son mot de passe en toute sécurité en cloud et ceci loin du GAB.

Tableau 3.14 : Comparaison des difficultés rencontrées par les utilisateurs âgés [Chabbi 2020a].

Méthode	Degré de difficultés
Fakep	4
PassW	6
Capp	2
Bpass	2
Cpass	0.5

Tableau 3.15 : Comparaison du degré de difficulté pour utilisateurs âgés [Chabbi 2020a].

Les résultats présentés dans les tableaux 3.14 et 3.15 indiquent que la méthode Cpass proposée présente moins de difficultés pour les utilisateurs les plus âgés lors de leurs paiements en utilisant l'ATM.

3.5 Conclusion

Dans ce chapitre, il a été présenté en détail notre technique appelée cloud pass qui utilise un mot de passe concaténé avec l'identifiant d'élément sécurisé et signé avec une fonction de hachage proposée. Le message résultat est envoyé sur le cloud au serveur pour activer l'état du mode d'accès de l'enregistrement correspondant au propriétaire de l'élément sécurisé. Aussi, nous avons proposé un protocole d'authentification pour un système composé de : un serveur, un ATM et un smartphone NFC. Le protocole commande l'autorisation du paiement NFC. Nous avons vérifié le protocole proposé par analyse et par les outils AVISPA et nous avons prouvé son efficacité. Nous avons proposé une fonction de hachage afin de signer les messages et un test d'intrusion pour indiquer à l'utilisateur si son solde de compte a été modifié. De plus, nous avons comparé notre solution avec certains protocoles et méthodes bien connus. Les comparaisons ont montré que notre solution est la meilleure. De plus, nous avons prouvé qu'il est économique car il ne nécessitait pas de périphériques matériels supplémentaires. Nous avons montré qu'il assure bien les trois propriétés de sécurité : authentification, intégrité des données et confidentialité pour sécuriser le paiement NFC entre un GAB et un smartphone et, il résiste à plusieurs violations et attaques.

De plus, la solution proposée présente des fonctionnalités intéressantes :

- L'utilisation d'un smartphone qui remplace la carte bancaire ou le carte de crédit qui peut être sélectionnée par l'utilisateur.
- Le serveur accède rapidement à l'enregistrement dans la base de données de l'utilisateur souhaitant s'authentifier auprès du GAB pour le paiement NFC. En effet, lors de la tentative d'authentification, le serveur localise uniquement les enregistrements ayant l'état activé du mode d'accès (utilisation de la mémoire cache).
- Le type de l'élément sécurisé utilisé est conforme à EMV, Globalplatfrom et Javacard. et a une capacité de mémoire importante et il est mobile. Ainsi, il pourrait être placé avec ses applications NFC et ses clés secrètes sur un nouveau smartphone.
- La solution proposée n'utilise aucun capteur, ce qui signifie qu'elle est économique en termes de ressources matérielles.

Chapitre 4

Chapitre 4 : Dynamic Array PIN : Une nouvelle approche pour sécuriser le paiement NFC entre ATM et smartphone

Sommaire

4.1 Introduction

Dans ce chapitre, nous exposons notre deuxième contribution qui se manifeste en une nouvelle approche de saisie du mot de passe afin de sécuriser le paiement électronique NFC effectué en utilisant un smartphone et un GAB. La méthode d'authentification proposée utilisant la technique du mot de passe est appelée Dynamic Array PIN (DAP), elle vérifie les propriétés de sécurité mentionnée ci-dessus et sécurise le mot de passe de l'utilisateur. Notre processus d'authentification protège le paiement NFC effectué à l'aide du GAB et du smartphone contre les treize attaques suivantes : Clonage de la carte, shoulder-surfing, force brute, canal auxiliaire, enregistrement d'écran, rejeu, Spyware, enregistrement par caméra, attaque de smudge, vol du smartphone, enregistrements multiples, enregistrement par caméra suivi du vol du smartphone et l'attaque de shoulder-surfing suivi du vol du smartphone. Notre solution est caractérisée par son intuitivité, sa résilience, sa convivialité et sa réduction de temps d'authentification. Elle présente un temps d'authentification moyen de 5,20 secondes, elle n'utilise aucun périphérique matériel complexe, elle ne nécessite ni de code Quick Response (QR), ni de pavé numérique, ni de clavier visuel, elle n'utilise que deux tableaux affichés sur l'écran de l'ATM, ce qui signifie qu'elle présente moins de difficultés surtout pour les utilisateurs âgés. Une comparaison avec certaines solutions récentes bien connues est effectuée pour évaluer les performances et l'efficacité de notre solution.

Nous présentons dans le reste de ce chapitre, la description de notre système et le protocole proposé, puis nous expliquons la technique du mot de passe DAP, ensuite nous effectuons une analyse de sécurité de notre système pour prouver sa capacité à faire face à certaines attaques bien connues en utilisant la démonstration par la logique. Pour prouver sa rapidité en temps d'authentification, nous allons présenter les résultats de notre expérience obtenus à partir d'une évaluation basée sur un test d'utilisabilité sur un échantillon de 30 participants volontaires. Enfin, nous présentons une comparaison de sécurité et de performance entre la méthode proposée et certaines techniques récentes bien connues qui sont utilisées dans le domaine de l'authentification, et nous concluons ce chapitre par une conclusion.

4.2 Code PIN à tableau dynamique

Pour faire face à toutes les attaques mentionnées ci-dessus, nous avons proposé Dynamic Array PIN : une nouvelle méthode utilisée pour améliorer le mécanisme d'authentification sur les distributeurs automatiques de billets, pour renforcer le système de sécurité des paiements NFC avec l'ATM et pour faciliter la manipulation du code PIN, en particulier pour les

utilisateurs âgés. Notre solution représente une nouvelle approche utilisée pour introduire le code PIN afin d'authentifier l'utilisateur avant d'effectuer un paiement NFC avec un GAB à l'aide d'un smartphone. Cette technique est utilisée dans le système matériel suivant.

4.2.1 Système hardware

Notre système nécessite la présence des entités suivantes : L'utilisateur, son smartphone, le serveur bancaire et un guichet automatique (ATM) équipé d'un petit pavé tactile doté d'une cachette (voir figure 4.1). Ce dernier appareil est de coût inférieur par rapport au coût de l'ensemble du GAB et à celui d'un écran tactile.

Figure 4.1 : Système hardware du paiement NFC [Chabbi 2020b]

4.2.1.1 Utilisateur

Il représente le propriétaire d'un smartphone équipé de la technologie NFC intégrant une carte de crédit ou une carte bancaire. Pour s'authentifier auprès du GAB, il doit saisir un code PIN. Dans notre expérience, nous proposons un code PIN à quatre chiffres qui est une longueur de code PIN très courante, puis nous présentons des tests avec d'autres de 6 et 8 chiffres, bien sûr, des codes PIN plus longs peuvent être utilisés dans notre solution, mais ils constituent une charge pour l'utilisateur parce que la phase de saisie sera plus longue.

4.2.1.2 Smartphone

Le smartphone proposé possède une architecture de SIM non centrée où l'élément sécurisé est implémenté sous la forme d'un support sécurisé mobile doté d'un type de carte mémoire (Secure Memory Card: SMC) [Alcime et al. 2013] (illustration en figure 4.2). Le smartphone est équipé de la technologie NFC et se caractérise par un élément sécurisé mobile qui stocke le protocole, le code PIN et les applications NFC (par exemple l'application de paiement), etc.

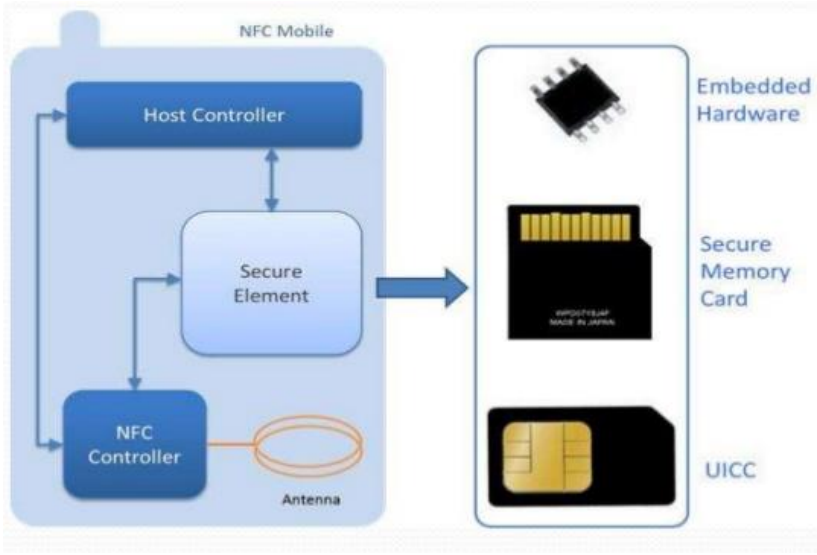

Figure 4.2: Architecture SMC d'un smartphone NFC [SlideShare 2015].

L'utilisation d'une architecture SIM non centrée où l'élément sécurisé est une carte mémoire sécurisée (SMC) présente les avantages suivants :

- Il offre un haut niveau de sécurité ;
- Il est conforme à EMV, GlobalPlatform, ISO / IEC 7816 et javacard;
- Il a une capacité de mémoire importante ;
- Il est mobile car il peut être placé avec son contenu (applications NFC, protocole, clés secrètes, code PIN, etc.) dans un nouveau smartphone.

4.2.1.3 Guichet automatique bancaire (*ATM*)

Il dispose d'un lecteur NFC capable de lire une carte de crédit intégrée dans un smartphone. Il communique avec le smartphone NFC et le serveur bancaire. Il est équipé d'un petit pavé tactile doté d'une cachette de protection.

4.2.1.4 Serveur

Le serveur stocke dans sa base de données les informations d'identification telles que le code PIN, l'identifiant de l'élément sécurisé intégré au smartphone, le numéro de téléphone et l'identifiant de la carte bancaire contenant l'affiliation de l'utilisateur comme le nom de la banque, le numéro de compte utilisateur, son montant, etc. Les informations sont enregistrées lors de la phase d'enregistrement par le TSM (Trusted Service Manager). Elles sont mises à jour en cas de changement de smartphone ou de changement de PIN. Le stockage des informations dans la base de données et la communication du serveur avec l'ATM sont considérés comme sécurisés et ne rentrent pas dans le cadre de cette étude.

Après avoir rapproché le smartphone du GAB, un échange de données sécurisées stockées dans l'élément sécurisé et la carte de crédit sera effectué (figure 4.3). Le serveur passe après pour authentifier l'utilisateur (le propriétaire du smartphone) en l'invitant à saisir le code PIN. Dans notre approche, l'ATM affiche deux tableaux de 10 chiffres chacun, affichés dans un ordre aléatoire (figure 4.4).

Figure 4.3 : Transmission de données NFC [Business Insider 2018].

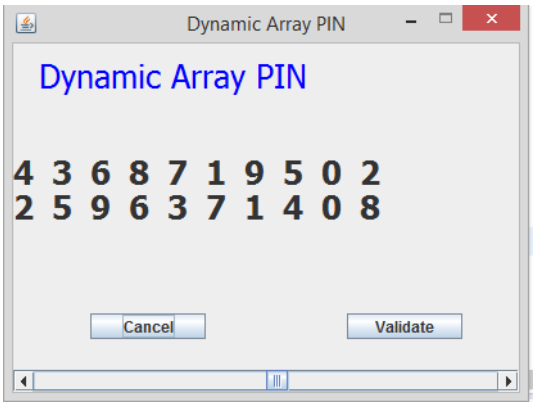

Figure 4.4 : Authentification de l'utilisateur en utilisant DAP [Chabbi 2020b]

4.2.2 Objectifs

L'ATM communique avec le smartphone par une communication radiofréquence (NFC) et par une communication en ligne avec le serveur. La dernière communication est considérée comme sécurisée (par l'utilisation du protocole TLS). Notre objectif est de sécuriser l'intervention de l'utilisateur avec l'ATM. La sécurité des informations stockées dans le serveur et des informations échangées entre le GAB et le serveur n'est pas abordée dans ce travail et est considérée comme sécurisée. Notre objectif principal est d'assurer l'authentification des utilisateurs avec une nouvelle approche du code PIN. Après l'authentification de l'utilisateur, le système autorise les transactions de paiement. Pour protéger le système contre les paiements illicites, notre méthode interdit l'exécution d'une transaction de paiements lorsqu'un code PIN n'est pas vérifié (cas d'attaque). Dans le cas contraire, les transactions de paiement sont autorisées. Ainsi, uniquement lorsque l'utilisateur est authentifié, il est autorisé à effectuer le paiement NFC avec le GAB. Pour prouver la sécurité, la convivialité et les performances de notre méthode, nous avons fixé les objectifs suivants :

- Étudier la résistance de notre solution et prouver qu'elle est simple et qu'elle est protégée contre les treize attaques citées auparavant.
- Calculer le temps moyen d'authentification de l'utilisateur par l'expérimentation et prouver qu'il est réduit.
- Comparer notre méthode avec plusieurs techniques importantes.

4.2.3 Présentation du protocole DAP

Dans ce paragraphe, nous présentons notre protocole nommé Dynamic Array PIN (DAP) où le but est de renforcer la sécurité de la saisie du code PIN par l'ATM. Ce protocole utilise uniquement le code PIN comme secret partagé entre l'utilisateur et le serveur bancaire. Lorsque l'utilisateur rapproche son smartphone du lecteur NFC de l'ATM, ce dernier affiche deux tableaux de 10 chiffres chacun et qui sont aléatoires et numérotés de 0 à 9. L'utilisateur peut faire glisser les chiffres du deuxième tableau à droite ou à gauche afin de faire correspondre un chiffre de ce tableau à un chiffre qui représente une référence dans le premier tableau.

Notre protocole est utilisé pour sécuriser un paiement électronique effectué avec le GAB à l'aide d'un smartphone. Il se caractérise par un temps d'authentification court, un faible taux d'erreur et une protection du paiement NFC contre treize attaques. Notre solution permet à l'utilisateur de sélectionner une carte de crédit à partir d'une liste de cartes intégrées dans le smartphone. Les principales phases de notre solution sont les suivantes :

4.2.3.1 Phase d'enregistrement

Dans la base de données du serveur bancaire, les informations suivantes sont enregistrées :

- Le code PIN de l'utilisateur ;
- L'ID : l'UUID (Universally Unique Identifier) utilisé pour identifier l'élément sécurisé ;
- Le numéro de téléphone ;
- L'identifiant de la carte bancaire qui fait référence au nom de la banque, à l'affiliation de l'utilisateur, au numéro de compte utilisateur, à son montant, à l'historique de ses transactions, etc.

4.2.3.1 Phase d'authentification

Pour s'authentifier, l'utilisateur applique les étapes suivantes :

- Mémoriser le numéro dans le deuxième tableau qui correspond au premier chiffre du code PIN dans le premier tableau (voir figure 4.5). La position de ce chiffre dans le premier tableau est appelée la référence.
- Par exemple, comme le montre la figure 4.5, pour introduire le code PIN '8642', l'utilisateur recherche son premier chiffre 8 dans le tableau supérieur et lit le chiffre qui lui correspond dans le tableau inférieur. Il s'agit du chiffre 4 dans cet exemple. Ensuite, il

cherche la position de 4 dans le premier tableau (qui est le troisième à partir de la gauche) et la considère comme référence. Ensuite, à l'aide d'un petit pavé tactile installé sur le GAB et recouvert d'une cachette pour cacher le doigt de l'utilisateur, l'utilisateur fait glisser le deuxième tableau horizontalement vers la gauche ou vers la droite et l'arrête en libérant son doigt chaque fois qu'un chiffre du code PIN dans le second tableau correspond à la référence dans le premier. La barre de défilement de l'axe X de la figure 4.5 est utilisée dans une interface de notre implémentation pour simuler le pavé tactile de l'ATM. Pour indiquer la fin de la saisie du code PIN, l'utilisateur appuie sur le bouton 'Validate'.

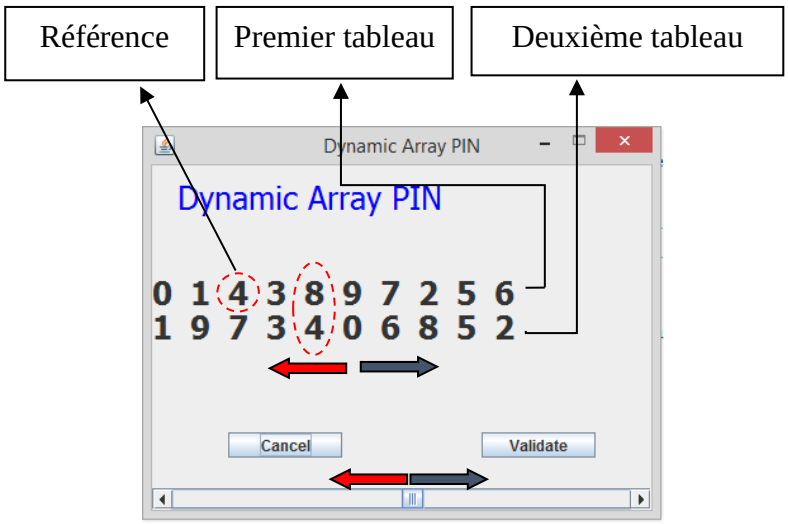

Figure 4.5 : Interface du protocole DAP [Chabbi 2020b]

L'idée de base de ce protocole est que l'attaquant peut voir la saisie de l'utilisateur, mais il ne peut pas révéler le code PIN car il ne peut pas détecter le chiffre qui représente la référence et qui est référencée par l'utilisateur pour saisir les chiffres du code PIN. Cette référence modifiable à chaque session d'authentification est obtenue à partir du premier chiffre du code PIN inconnu pour l'attaquant.

4.2.3.1 Phase de confirmation par SMS

Après une saisie réussie du code PIN, la transaction de paiement est exécutée. Le serveur envoie au smartphone une confirmation SMS (considérée comme sécurisée par TLS) indiquant les détails de la transaction (le numéro de compte utilisateur, le montant retiré, le solde, la date et l'heure de la transaction, etc.). Ce message peut être utilisé comme un test d'intrusion.

4.2.4 Etapes du protocole DAP

Comme le montre le diagramme de la figure 4.6, les étapes de notre protocole sont les suivantes :

- L'utilisateur rapproche son smartphone du lecteur NFC de l'ATM ;
- L'ATM récupère les informations stockées sur la carte bancaire du smartphone et les transmet au serveur bancaire. Cette transmission est cryptée à l'aide de l'algorithme de cryptage AES (Advanced Encryptions Standard) car il est meilleur en termes de confidentialité et d'intégrité que les autres algorithmes comme DES (Data Encryptions Standard), 3DES (Triple DES), ou BLOWFISH [Wahid et al. 2018]. Concernant la sécurité du numéro de compte (pas du code PIN), le processus de tokenisation peut être utilisé conjointement avec notre proposition qui se limite à une technique éprouvée sûre contre de multiples attaques, utilisée pour saisir un code PIN via l'ATM. Cette sécurité est assurée au niveau de l'ATM. Concernant le transfert sécurisé des informations bancaires enregistrées sur la carte bancaire embarquée dans le smartphone (comme le numéro de compte), elles sont transmises avant l'introduction du PIN réalisée par notre technique, le numéro de compte peut être transféré du smartphone au GAB après application du processus de tokenisation.
- Le serveur récupère le code PIN utilisateur de sa base de données, génère deux tableaux d'indices aléatoires de 0 à 9 et les transmet à l'ATM ;
- L'ATM affiche à l'écran les deux tableaux avec les boutons « Cancel » et « Validate ». Les chiffres du deuxième tableau peuvent être déplacés par l'utilisateur vers la droite ou vers la gauche à l'aide d'un pavé tactile ;
- Pour s'authentifier, l'utilisateur doit faire glisser le deuxième tableau et relâcher le doigt à chaque fois qu'un chiffre du code PIN du deuxième tableau coïncide avec le chiffre de la référence dans le premier tableau. Enfin, il appuie sur le bouton « Validate » pour indiquer la fin de la saisie du code PIN ;

- Lorsque le bouton « Validate » est appuyé, le GAB envoie la saisie de l'utilisateur au serveur ;
- Le serveur compare le code PIN saisi à celui extrait de la base de données.

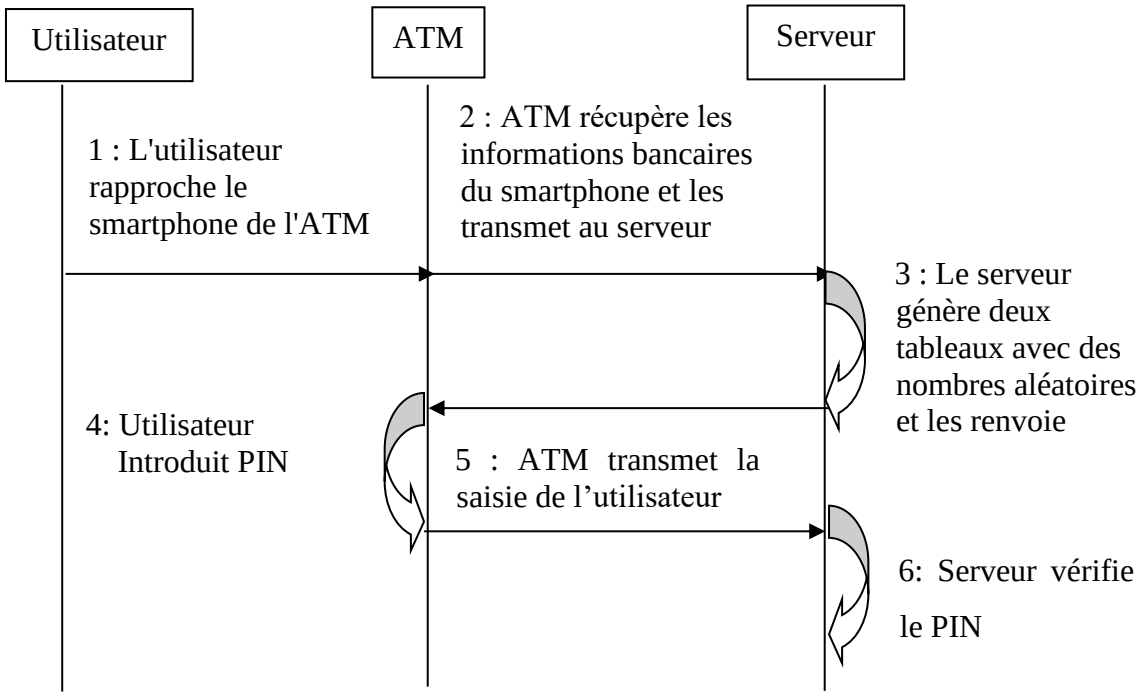

Figure 4.6 : Le protocole DAP [Chabbi 2020b]

4.3 Analyse de la sécurité

Dans cette section, nous analysons la sécurité de notre protocole contre treize attaques. Cette analyse montre que notre protocole résiste mieux aux attaques suivantes :

4.3.1 Attaque force brute

Le principe de cette attaque est d'essayer toutes les combinaisons de caractères possibles jusqu'à ce que le code PIN soit trouvé. Dans la technique proposée, la randomisation des nombres dans les deux tableaux générés par le serveur pour chaque session d'authentification conduit l'utilisateur à relâcher son doigt à une nouvelle position de la référence générée à chaque tentative d'authentification qui précède une opération de paiement. Pour trouver le code PIN, il existe une probabilité de 1 sur 10^{N*2} (N = nombre de chiffres dans le code PIN) car les tableaux contiennent chacun 10 chiffres, ce qui implique que la probabilité de trouver le vrai code PIN est trop faible. Pour une telle attaque et en utilisant la technique DAP, il est difficile de parcourir tout l'espace du code PIN. De plus, le GAB peut bloquer le processus de paiement après trois tentatives infructueuses.

Si l'attaquant applique une attaque de surf à l'épaule, il est pratiquement impossible de voir quand l'utilisateur relâche son doigt qui est protégé par la cachette et il est également impossible de mémoriser les images d'écran correspondant aux chiffres du code PIN.

Dans le cas d'une attaque utilisant la capture d'écran par caméra, l'attaquant ne peut pas détecter le vrai code PIN pour deux raisons : la première est que l'utilisateur peut dépasser un chiffre du mot de passe et dans ce cas, il doit s'arrêter sans relâcher son doigt et faire défiler les chiffres dans la direction inverse pour atteindre son chiffre. La seconde est que l'utilisateur peut le faire exprès (c'est-à-dire faire glisser le chiffre à droite ou à gauche sans relâcher son doigt) pour confondre davantage l'attaquant. Pour plus de sécurité, on peut ajouter une source lumineuse au-dessus du GAB pour diffuser de la lumière dans toutes les directions devant les caméras qui peuvent être installées autour du GAB. Cette lumière peut être un obstacle à la lisibilité de l'image enregistrée par la caméra ou par un attaquant.

4.3.2 Attaque par canal auxiliaire

Ce type d'attaque utilise des logiciels espions qui tentent de capturer les frappes de l'utilisateur en utilisant plusieurs types de ressources telles que l'accéléromètre, le microphone, la caméra, etc.

La solution proposée est robuste contre ce type d'attaque grâce à la randomisation des nombres qui remplissent les deux tableaux générés par le serveur à chaque session d'authentification. De plus, en relâchant son doigt sous la cachette, l'utilisateur ne donne aucune possibilité à l'attaquant de connaître les chiffres du code PIN car le Spyware ne peut pas deviner le numéro de référence généré à partir du premier chiffre du code PIN et qu'il n'est connu que par l'utilisateur seulement.

4.3.3 Attaque par clonage

Dans ce type d'attaque, l'attaquant peut installer auprès du GAB, des appareils qui enregistrent les données privées de l'utilisateur stockées dans la carte bancaire intégrée dans le smartphone, puis cloner les informations volées sur une nouvelle carte bancaire intégrée dans un autre smartphone pour l'utiliser pour un paiement NFC. Dans notre système, l'attaque de clonage n'a aucune chance d'aboutir car notre protocole nécessite l'introduction du code PIN pour effectuer la transaction de paiement et l'attaque de clonage ne permet pas de restaurer le code PIN qui est stocké en toute sécurité dans l'élément sécurisé au lieu de la carte bancaire.

4.3.4 Attaque par enregistrement d'écran

Ce type d'attaque est fourni par des logiciels malveillants qui peuvent être installés sur le GAB et qui permettent l'enregistrement de tout l'écran pendant la session d'authentification. Avec notre protocole, cette attaque ne donne aucun résultat par rapport au chiffre du code PIN. En fait, à chaque instant, la capture d'écran ne montre que deux tableaux contenant des chiffres et cette image ne donne aucune information sur le numéro de code PIN qui a été sélectionné par l'utilisateur uniquement en manipulant la barre de défilement.

4.3.5 Attaque par rejeu

Cette attaque suppose que le téléphone mobile est authentifié avec le lecteur NFC de l'ATM en envoyant un identifiant secret. Ainsi, l'attaquant écoute indiscrètement la communication entre le téléphone et le lecteur de l'ATM, reçoit l'identifiant et renvoie ou rejoue cet identifiant depuis son propre téléphone dans une autre session d'authentification [Merkus 2018]. En raison de la randomisation des deux tableaux générés par le serveur, notre protocole est résistant à ce type d'attaque car à chaque session d'authentification, le numéro de référence dans le premier tableau sera modifié et l'utilisateur mémorisera une nouvelle référence pour valider les chiffres du code PIN.

4.3.6 Attaque par enregistrement caméra

L'attaquant peut installer une caméra sur le GAB pour enregistrer l'entrée du code PIN. Avec notre protocole, l'enregistrement d'écran ATM par une caméra ne peut donner aucune information sur les chiffres du code PIN car la caméra ne peut enregistrer que deux tableaux affichés sur l'écran ATM et une barre de défilement se déplaçant à gauche ou à droite. L'enregistrement de la caméra ne donne donc aucune information sur le chiffre du code PIN. Notre protocole est donc sécurisé contre ce type d'attaque.

4.3.7 Attaque surf à l'épaule (*Shoulder surfing*)

Dans cette attaque, l'attaquant se positionne derrière l'utilisateur pour voir et mémoriser ses frappes lors de la saisie du code PIN. Avec notre solution, un attaquant qui visualise un utilisateur saisissant son code PIN ne peut avoir aucune idée sur les chiffres du code PIN comme dans le cas de la caméra, car notre utilisateur n'introduit pas des chiffres d'une manière directe. Nous pouvons conclure que notre protocole est résistant aux attaques de surf à l'épaule.

4.3.8 Attaque de tache (*Smudge attack*)

Le principe de cette attaque est de suivre les traces des doigts de l'utilisateur laissés sur l'écran de l'ATM pour pouvoir détecter le schéma d'authentification. Notre protocole est protégé contre ce type d'attaque car il n'y a pas de schéma d'authentification dessiné et l'utilisateur ne touche pas l'écran de l'ATM, il ne fait que glisser son doigt sur le petit pavé tactile, le relâche dans le temps nécessaire et enfin il appuie sur le bouton 'Validate ', il ne donne donc aucune information sur le code PIN.

4.3.9 Attaque de Spyware

Un logiciel espion est un code malveillant qui capture les coordonnées des touches de l'utilisateur sur l'écran de l'appareil (l'ATM dans notre étude), ou enregistre la totalité de l'écran pendant la phase d'authentification. En utilisant notre protocole, l'utilisateur n'a rien à craindre concernant le spyware qui essaye de capturer ses coordonnées parce qu'il ne trouve que des glissements des chiffres du second tableau vers la droite ou vers la gauche et la pression du bouton 'Validate'. De cette façon, le spyware ne pourra jamais détecter les chiffres du code PIN. Le résultat est le même si le logiciel espion enregistre la totalité de l'écran pendant la phase d'authentification.

4.3.10 Attaque par enregistrements multiples

L'attaquant peut utiliser l'intersection de plusieurs enregistrements de données, d'écran ou de caméra pour découvrir le code PIN. Cependant, notre protocole est protégé contre ce type d'attaque car le fait d'acquérir plusieurs enregistrements ne donne aucune information sur les chiffres du code PIN car l'utilisateur ne reprend que deux gestes en faisant glisser le deuxième tableau et en appuyant sur le bouton 'Validate'. D'un autre côté, les chiffres dans les deux tableaux changent également de manière aléatoire et par conséquent le chiffre représentant la référence change à chaque session d'authentification, ce qui rend les attaques d'enregistrement multiples sans aucun effet.

4.3.11 Attaque vol du smartphone

En utilisant notre technique DAP, le vol du smartphone ne permet jamais au voleur d'effectuer un paiement NFC avec l'ATM car le DAP nécessite l'introduction du code PIN

inconnu pour l'attaquant et il n'y a aucun moyen de le savoir puisqu'il est sauvegardé en toute sécurité dans la base de données du serveur et dans l'élément sécurisé du smartphone. Ainsi, notre approche est protégée contre les attaques de vol du smartphone.

4.3.12 Attaque shoulder surfing suivi du vol du smartphone

Si l'attaquant effectue une attaque Shoulder-Surfing en premier, puis vole le smartphone, il ne peut pas effectuer de paiement qui nécessite la connaissance du code PIN. Sachant que l'attaque de surf sur l'épaule ne lui permet pas de connaître le mot de passe en utilisant le protocole proposé, le vol du smartphone n'aura aucun effet après l'attaque Shoulder-surfing.

4.3.13 Attaque enregistrement par caméra suivi du vol du smartphone

Si l'attaquant utilise une attaque d'enregistrement par caméra et éventuellement une attaque du vol du smartphone, il ne peut pas effectuer de paiement NFC devant le GAB qui nécessite la connaissance du code PIN, et comme c'est prouvé précédemment, L'attaque par enregistrement caméra ne permet pas à l'attaquant de connaître le code PIN, et à cet effet, l'attaque vol du smartphone qui a suivi l'attaque d'enregistrement par caméra n'aura aucun effet.

4.4 Expérimentation et évaluation

Dans cette section, nous évaluons l'utilisabilité et la mémorisation car ces deux paramètres représentent les facteurs d'évaluation de toute méthode d'authentification.

4.4.1 Outillage

Pour aboutir aux résultats de notre protocole DAP ; nous avons conçu une application à installer sur l'ATM. Les outils de développement étaient : Eclipse Neon.2 Release (4.6.2) et Java 1.8.0. L'équipement de développement est un ordinateur Toshiba Core i5 (Intel 5) qui simule l'ATM.

4.4.2 Test d'utilisabilité

Nous avons choisi un échantillon de 30 personnes d'âges différents de 15 à 72 ans pour tester notre méthode. L'âge inférieur à 60 ans représente la plupart des personnes qui peuvent utiliser pour le paiement, un smartphone et des distributeurs automatiques de billets dans notre société. Après avoir expliqué le principe de la méthode aux participants, chacun doit tester l'application seule plusieurs fois pour se familiariser avec elle. Ensuite, chaque participant effectuera neuf tentatives d'authentification en suivant la procédure de saisie détaillée précédemment et en utilisant notre application Java sur le même ordinateur mentionné ci-dessus. Les résultats expérimentaux seront donc obtenus à partir de 30 * 9 = 270 sessions d'authentification pour chaque PIN (4, 6 et 8 chiffres). Le temps d'authentification de chaque session est calculé à partir du moment où l'utilisateur commence à déplacer son doigt sur le pavé tactile de l'ATM pour faire glisser la barre de défilement utilisée pour déplacer les chiffres du deuxième tableau jusqu'au moment où il appuie sur le bouton ‘Validate’.

4.4.3 Evaluation

Les résultats obtenus des expériences et représentés dans le tableau 4.1 montrent les temps d’authentification y compris le temps moyen et le taux d’erreur pour chaque participant et pour chaque longueur de PIN. En prenant par exemple le code PIN de 4 chiffres, on remarque que le temps d'authentification moyen est égal à 5.20 ms, et le taux d'erreur est égal à 4,07%, ce qui signifie que notre protocole est caractérisé par un temps d'authentification réduit et un taux d'erreur faible.

Age	Temps d'authentification moyen (Seconde)			Taux d'erreur		
	PIN 4 chiffres	PIN 6 chiffres	PIN 8 chiffres	PIN (chiffres)		
				4	6	8
19	3.12	6.70	8.92	0/9	0/9	1/9
19	2.40	7.11	8.96	0/9	1/9	0/9
50	5,71	11.36	14.34	1/9	1/9	2/9
20	3.53	7.81	10.26	0/9	0/9	1/9
19	3.76	8.33	11.67	0/9	0/9	0/9
49	5,09	10.14	13.80	1/9	1/9	2/9
20	4.05	6.35	7.77	0/9	0/9	0/9
15	3.19	7.34	10.31	0/9	0/9	1/9
19	4.16	7.22	12.11	0/9	0/9	0/9
38	4.29	8.79	14.18	1/9	1/9	1/9
15	4.35	8.76	11.24	0/9	0/9	0/9
35	4.37	10.78	13.11	0/9	0/9	1/9
25	4.41	7.20	9.26	0/9	1/9	0/9
20	4.52	8.58	12.70	0/9	0/9	0/9
31	4.92	10.59	14.77	0/9	1/9	2/9
28	3.84	8.46	11.75	0/9	0/9	1/9
33	5.15	12.34	15.42	1/9	1/9	1/9
18	3.00	6.37	10.90	0/9	0/9	0/9
47	5.22	11.58	14.91	1/9	0/9	1/9
34	5.22	10.58	13.34	0/9	0/9	0/9
20	3.41	6.33	7.86	0/9	0/9	0/9
32	4.29	8.62	12.25	1/9	0/9	1/9
20	2.31	8.27	10.45	0/9	0/9	0/9
17	3.29	7.06	12.32	0/9	0/9	0/9
41	5.56	9.12	13.86	1/9	1/9	2/9
44	5.87	12.98	15.79	0/9	0/9	0/9
16	7.24	10.48	13.78	0/9	0/9	1/9
15	9.25	11.03	12.58	0/9	1/9	1/9
48	7.72	14.60	19.80	1/9	2/9	2/9
72	21.17	25.67	38.34	3/9	4/9	5/9
Moyenne						
29	5.20	9.69	13.23	4.07	5.56	9.63

Tableau 4.1 : Temps d'authentification du protocole DAP [Chabbi 2020b].

4.5 Comparaison de sécurité et de performance

Nous allons maintenant comparer notre technique avec plusieurs méthodes importantes en effectuant deux types de comparaison : l'une de sécurité et l'autre de performance.

4.5.1 Comparaison de sécurité

Dans cette section, nous comparons notre solution avec plusieurs solutions existantes importantes. Nous vérifions les attaques qui pourraient compromettre les méthodes ou les protocoles mentionnés. Les résultats sont obtenus par la logique de l'analyse de l'attaque vers la méthode ou le protocole.

Le tableau 4.2 présente les résultats de la comparaison où 'V' respectivement 'R' signifie que la technique est vulnérable ou résistante à l'attaque.

Attaque/ Méthode	FakeP	PassW	Capp	Bpass	DAP
Vol de la carte ou du smartphone	R	R	R	R	R
Shoulder-surfing	R	R	/	/	R
Enregistrement multiple	V	V	R	R	R
Canal auxiliaire	R	R	R	R	R
Force brute	V	V	R	R	R
Spyware	R	R	R	R	R
Enregistrement d'écran	R	R	R	R	R
Clonage de carte	R	R	R	R	R
Enregistrement par Caméra	R	R	/	/	R
Smudge	R	R	R	R	R
Rejeu	R	R	R	R	R
Enregistrement caméra et vol du smartphone	R	R	V	V	R
Shoulder-surfing et vol du smartphone	R	R	V	V	R

Tableau 4.2 : Limites de sécurité de quelques méthodes [Chabbi 2020b].

Les méthodes FakePIN et PassWindow malgré qu'elles soient résistantes contre l'attaque Shoulder-Surfing et enregistrement par caméra, elles sont vulnérables à l'attaque d'intersection des enregistrements multiples.

Les méthodes BrightPass et Cappcha sont vulnérables aux attaques de Shoulder-surfing et d'enregistrement par caméra suivies de l'attaque du vol de smartphone, car un attaquant ou une caméra peut utiliser une observation directe en regardant ou en filmant l'entrée directe du code PIN. Dans la technique BrightPass, un attaquant qui connaît le principe de fonctionnement, enregistre dans sa mémoire les nombres entrés dans les cercles ayant une luminosité élevée. Si par la suite l'attaquant peut voler ou emprunter le smartphone, il peut

effectuer une transaction de paiement avec le GAB en suivant les indications de l'élément sécurisé.

Selon le tableau 4.2, nous pouvons calculer pour chaque méthode, le nombre d'attaques qui la franchissent. Les résultats sont mentionnés dans le tableau 4.3. Nous pouvons voir dans ce tableau que notre solution est la plus sécuritaire car elle lutte contre toutes les attaques répertoriées.

Méthode	Nombre d'attaques
FakeP	2
PassW	2
Capp	2
Bpass	2
DAP	0

Tableau 4.3 : Comparaison entre méthodes par le nombre d'attaques qui les franchissent [Chabbi 2020b].

Nous pouvons maintenant présenter les points forts de notre solution en matière de sécurité qui se sont révélés :

- Le type d'élément sécurisé utilisé offre un haut niveau de sécurité.
- Dans le pire des cas, si une nouvelle attaque supplémentaire est découverte et casse notre protocole, un SMS de confirmation est envoyé au smartphone du propriétaire. Le SMS représente un message d'alarme car il informe l'utilisateur que le montant de son compte bancaire est modifié. Cela signifie que le protocole utilise une technique de détection d'intrusion.
- Le protocole n'utilise aucune méthode biométrique. Ainsi, les caractéristiques biométriques de l'utilisateur ne sont pas exposées aux attaques associées.

4.5.2 Comparaison de performance

L'objet de cette comparaison est de montrer que la solution proposée est économique en termes de matériel et de temps d'authentification et qu'elle est efficace. Les mesures de temps obtenues avec un code PIN à 6 et à 8 chiffres sont légèrement supérieures par rapport aux temps obtenus avec un code PIN à 4 chiffres. Le temps d'authentification de notre méthode est linéairement évolutif avec le nombre de chiffres du code PIN. Les autres propositions comme [Guerar 2017] n'ont pris en compte que des codes PIN à 4 chiffres. La figure 4.7 présente le résultat d'une session d'authentification utilisant le protocole DAP.

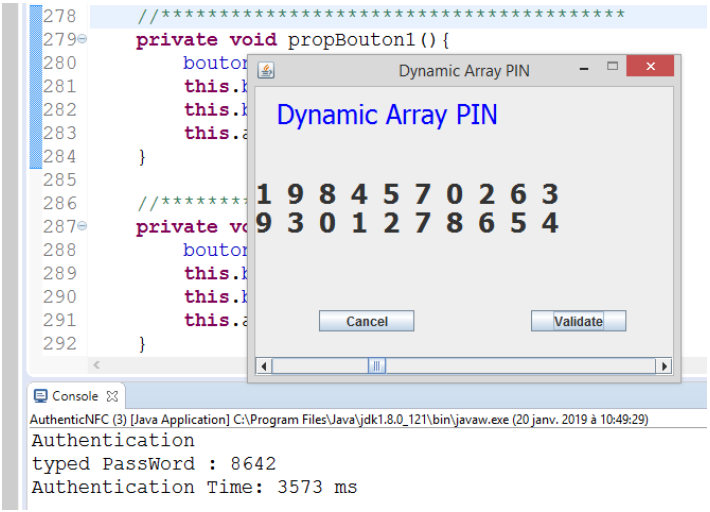

Figure 4.7 : Session d'authentification avec le protocole DAP [Chabbi 2020b].

Nous présentons dans le tableau 4.4 les temps d'authentification des méthodes FakeP, PassW, Capp, Bpass et CWPIN (Color Weel PIN) [Guerar 2017], et notre protocole (DAP) obtenu par l'expérimentation, comme mentionné précédemment. Bien que le temps d'authentification de CWPIN soit inférieur à DAP, nous pouvons dire que le temps d'authentification estimé pour notre protocole est meilleur. En fait, le maximum d'âge de personne participante dans la méthode CWPIN est de 58 ans. Cependant, DAP a pris en compte le personnage le plus âgé qui a atteint 72 ans. Cela pourrait influencer différentes mesures telles que le temps d'authentification et le taux d'erreur.

Méthode	**Temps d'authentification (s)**
FakeP	10.90
PassW	18.12
Capp	4.12
Bpass	8.20
CWPIN	4.55
DAP	5.20

Tableau 4.4 : Comparaison de temps d'authentification des méthodes [Chabbi 2020b].

Le tableau 4.5 donne une comparaison entre DAP et CWPIN, qui est la plus sécuritaire et la plus récente parmi les autres solutions mentionnées. Le taux d'erreur CWPIN est obtenu par [Guerar 2017]. L'analyse montre que le DAP est le plus économique.

CWPIN	DAP
Utilise QR code	Pas d'utilisation de QR code
Temps nécessaire pour scanner QR code	Pas de temps pour scanner QR code
Stockage du PIN et le tableau de couleurs dans SE	Stockage du PIN seulement dans SE
Deux applications : Une sur le smartphone et l'autre sur le GAB	Une seule application installée sur le GAB
Méthode non utilisable si le nombre de chiffres du PIN est impair.	Utilisable si le nombre de chiffres du PIN est pair ou impair.
La fin de saisie du code PIN est indéterminée.	La fin de saisie du PIN est déterminée par la sélection du bouton « Validate »

Tableau 4.5 : DAP vs CWPIN [Chabbi 2020b].

Le tableau 4.6 indique la difficulté que les utilisateurs les plus âgés peuvent rencontrer lors de l'opération d'authentification avec un GAB en utilisant l'une des cinq méthodes (FakePIN, Passwindow, Cappcha, BrightPass et CWPIN) et notre solution. Nous supposons que chaque difficulté a un score d'un point.

Méthode	Difficultés	Degré de difficulté
FakeP	▪ Mémoriser deux mots de passe : l'un est alphanumérique et l'autre est une direction. ▪ Clavier virtuel qui peut être modifié à chaque tentative d'authentification. ▪ La lettre à presser est la combinaison de la lettre du mot de passe et de la direction.	4
PassW	▪ Mémoriser deux mots de passe : code PIN et une icône présélectionnée. ▪ Mémoriser l'emplacement de l'icône présélectionnée dans une grille modifiable pour chaque opération d'authentification et contenant d'autres icônes aléatoires. ▪ Afficher un clavier virtuel et une grille sans icônes. ▪ Incliner le téléphone pour déplacer la grille sur le clavier virtuel afin d'entrer le chiffre PIN à l'emplacement de l'icône présélectionnée. ▪ Masquer l'entrée de la caméra.	6
Capp	▪ Mémoriser le code PIN. ▪ Incliner le téléphone mobile à un degré spécifique affiché sur l'écran et maintenez-le dans une telle position pendant une seconde pour avoir accès au code PIN.	2
Bpass	▪ Mémoriser le code PIN. ▪ Affichez un ensemble de petits cercles qui prennent la position des numéros de mot de passe. Dans un cercle de faible luminosité, l'utilisateur entre un faux chiffre. En haute luminosité, il entre un vrai chiffre.	2

CWPIN	▪ Mémoriser le code PIN. ▪ Scanner le code QR ▪ Afficher une roue des couleurs et glisser une barre de recherche selon le principe déjà énoncé	3
DAP	▪ Enregistrer le code PIN. ▪ Afficher deux tableaux et l'utilisateur fait glisser le deuxième tableau pour faire correspondre un chiffre du code PIN existant dans le deuxième tableau avec le chiffre de référence existant dans le premier tableau	2

Tableau 4.6 : Comparaison des degrés de difficultés [Chabbi 2020b].

Les résultats présentés dans le tableau 4.6 indiquent que la méthode DAP proposée présente moins de difficultés pour les utilisateurs plus âgés.

Le tableau 4.7 présente une comparaison entre le DAP et le protocole Secure Crédit Card Protocol (SCCP), avec des caractéristiques importantes en faveur de notre proposition.

SCCP	**DAP**
Utilise uniquement carte de crédit	Utilise smartphone. Utilisateur peut sélectionner une carte bancaire à partir d'une liste
Vulnérable contre l'attaque vol de carte crédit	Résistante à l'attaque vol du smartphone
Pas de code PIN utilisé	Utilisation de code PIN
Pas de message de confirmation après paiement	Message de confirmation après paiement indiquant les détails de la transaction et qui peut être utilisé comme un test d'intrusion
Pas d'élément sécurisé utilisé	Utilisation d'élément sécurisé

Tableau 4.7 : DAP vs SCCP [Chabbi 2020].

La comparaison de notre solution avec celle de Nana et al., présentée dans le tableau 4.8, indique que notre solution est plus sécuritaire et plus économique.

Attaque / Solution	**Solution Nana et al.**	**DAP**
Faux lecteur d'empreinte	V	R
Enregistrement par caméra (si mot de passe est utilisé)	V	R
Shoulder-Surfing (si mot de passe est utilisé)	V	R

Tableau 4.8 : DAP vs la solution Nana et al. [Chabbi 2020b].

4.6 Conclusion

Dans ce chapitre, nous avons proposé une nouvelle technique d'authentification des utilisateurs pour sécuriser le paiement NFC dans un système composé de : un serveur, un guichet automatique et un smartphone NFC. Cette technique est une nouvelle méthode sécurisée pour introduire un code PIN appelée DAP. Cette méthode représente un protocole qui active ou désactive le paiement NFC. Nous avons évalué le protocole proposé DAP par analyse et nous avons prouvé son efficacité. Nous avons proposé un test d'intrusion afin d'indiquer à l'utilisateur que son solde du compte est modifié après chaque transaction. De plus, nous avons comparé notre solution avec plusieurs protocoles et méthodes de sécurité existants importants et nous avons prouvé qu'elle est la meilleure et qu'elle résiste à treize attaques. De plus, nous avons prouvé qu'elle n'était pas coûteuse car elle ne nécessitait pas de périphériques matériels complexes.

De plus, la solution proposée présente les caractéristiques intéressantes suivantes :

- L'utilisation d'un smartphone qui remplace la carte bancaire ou la carte de crédit qui peut être sélectionnée par l'utilisateur.
- Le type d'élément sécurisé utilisé est conforme à EMV, Globalplatfrom et Javacard. Il a une capacité de mémoire importante et il est mobile. Ainsi, il pourrait être placé avec ses applications NFC et son code PIN dans un nouveau smartphone.
- La proposition est économique en termes de ressources matérielles car elle ne nécessite que l'ajout d'un composant de base qui est un petit pavé tactile avec sa cachette de protection.

Conclusions et perspectives

1. Conclusions

Au cours de ces dernières années, il y a eu une orientation d'une tranche de la population vers l'utilisation des nouveaux outils technologiques pour accomplir des services nécessaires dans la vie courante de l'utilisateur. Cette orientation a engendré des inventions ou des améliorations des technologies et des instruments utilisés pour rendre service aux utilisateurs tels que les cartes intelligentes, les smartphones, les ATM, les points de vente etc. Cette situation a renforcé la commercialisation de ces dispositifs et de leurs technologies associées. Parmi les nouvelles technologies, la NFC qui a bien prouvé son émergence dans la société et son influence dans la vie courante de tous les jours. Elle est aujourd'hui utilisée dans plusieurs domaines rendant plusieurs services à l'utilisateur comme le paiement, le transport public, le contrôle d'accès, la billetterie etc.

Toutefois, comme toute autre technologie, la NFC est cible d'un ensemble de menaces et d'attaques qui peuvent violer la sécurité des entités dotées de cette technologie pendant une communication sans contact, cette violation peut atteindre la vie privée de l'utilisateur en restituant ses données confidentielles utilisées à des fins sensibles comme la manipulation d'un compte bancaire. La sécurité des données confidentielles des utilisateurs durant un échange NFC important comme le paiement constitue le point critique dans l'utilisation de cette technologie, et elle a motivée une grande partie des problématiques de recherche dans ce domaine.

Cette thèse a porté sur la sécurisation des données sensibles des utilisateurs en protégeant les donnes de la carte bancaire, la carte de crédit, le smartphone et l'ATM contre des attaques. L'objectif principal était de sécuriser le dispositif et l'application (service) NFC tout en économisant le temps de transfert de messages, le temps d'authentification et l'espace de stockage dans l'élément sécurisé et en utilisant une technique non complexe et non coûteuse.

Après analyse de quelques nouvelles méthodes proposées dans ce contexte, nous avons constaté que chacune, soit elle souffre d'un certain type d'attaque, soit elle est très coûteuse en ressources utilisées, de temps de transfert de messages, de temps d'authentification, d'espace de stockage ou de complexité. Nous nous sommes alors intéressés à la satisfaction de ces

arguments. Pour y parvenir, nous avons proposé une première méthode qui consiste à envoyer un mot de passe crypté avec l'identificateur de l'élément sécurisé avec une fonction de hachage proposée. Le mot de passe envoyé sera vérifié dans une mémoire cache du serveur. Cette méthode est renforcée aussi par un protocole d'authentification simple et efficace qui a pu montrer son efficacité de point de vue de la sécurité de la communication NFC et ses performances en matière de réduction du temps d'authentification, du transfert de messages et d'espace de stockage par rapport à des méthodes de l'état de l'art. En sus, un test d'intrusion a été proposé pour le renforcement de la sécurité. Les démonstrations basées sur la logique de l'analyse et les résultats fournis dans cette thèse à partir des expérimentations de la fonction de hachage et de la simulation menées sur le protocole proposé ont révélé que la méthode est plus sûre avec des économies significatives sur les arguments déjà cités.

Nous avons également proposé une deuxième méthode qui représente une nouvelle technique de saisie de mot de passe. Cette technique a été implémentée en langage Java. Pour montrer l'efficacité de notre implémentation, nous l'avons évaluée sur un échantillon d'utilisateurs de différents âges. Les résultats obtenus ont montré clairement la supériorité (performance et l'efficacité) de notre méthode sur les méthodes connexes existantes.

2. Perspectives

Avec les résultats évocateurs présentés dans cette thèse, nos travaux de recherche ont fait des progrès importants dans la sécurité des dispositifs et applications NFC et spécifiquement le paiement électronique NFC en utilisant le smartphone et le guichet automatique bancaire.

Toutefois, il existe encore de nombreuses directions de recherche qui méritent d'être explorées pour compléter ces travaux. Nous envisagerons à l'avenir de sécuriser les flux d'informations entre le contrôleur hôte, le contrôleur NFC et l'élément sécurisé en créant des tunnels de sécurité. Nous structurons les directions de recherche comme suit :

- L'utilisation de capteurs capables d'acquérir l'iris de l'utilisateur en plus des caractéristiques physiologiques en temps réel pour éviter les attaques à l'aide d'images d'iris.
- L'utilisation de caméras sophistiquées associées à l'ATM capables de prendre l'image 3D (3 Dimensions) du visage de l'utilisateur en temps réel et de désactiver tous les canaux d'entrée de l'image à l'exception du canal de l'élément sécurisé pendant l'opération de paiement.

Sur le plan de conception et implémentation matérielle, nous préconisons que :

- L’utilisateur doit maintenir la confidentialité de son mot de passe.
- L'utilisateur ne doit pas emprunter son smartphone et doit le déclarer rapidement lors d’une perte.
- Ces solutions doivent être mises en œuvre par des spécialistes et des techniciens capables d'installer le matériel et les logiciels nécessaires tout en les contrôlant et les vérifiant à des instants précis.

Liste des publications

Liste des publications

Revues internationales avec comité de lecture

- Chabbi S., Boudour R., Semchedine F.: *A Secure Cloud Password and Secure Authentication Protocol for Electronic NFC Payment Between ATM and Smartphone.* Ingénierie des systèmes d'information (2020).
- Chabbi S., Boudour R., Semchedine F., Chefrour D.: *Dynamic Array PIN: A novel Approach to Secure NFC electronic payment between ATM and Smartphone.* Information security journal (2020).

Conférences internationales avec comité de lecture

- Chabbi S., Boudour R., Semchedine F.: A secure protocol, based on iris technology, for NFC phone applications. In : *International Conference on Mathematics and Information Technology (ICMIT)*. IEEE, Adrar, Algeria. p. 78-83 (2017).
- Chabbi S., Boudour R.: *Securing NFC applications embedded in a NFC phone.* In: International Conference on Automatic Control, Telecommunications and Signals (ICATS), Annaba, Algeria. (2015).
- Chabbi S., Boudour R.: *Adaptation d'un protocole d'authentification RFID-Biométrique.* In: International Conference on Embedded Systems in Telecommunications and Instrumentation (ICESTI), Annaba, Algeria. (2014).

Références

A

[Agarwal et al. 2007] Agarwal, Shivani, et al. "Security issues in mobile payment systems." Proceedings of ICEG 2007: The 5th International Conference on E-Governance 2007.

[Ahamad et al. 2016] Ahamad, Shaik Shakeel, Ibrahim Al-Shourbaji, and Samaher Al-Janabi. "A secure NFC mobile payment protocol based on biometrics with formal verification." International Journal of Internet Technology and Secured Transactions 6.2: 103-132. 2016

[Akman 2015] Akman, Özgen. "Near Field Communication Applications." 2015.

[Akrout 2012] Akrout, Rim. "Analyse de vulnérabilités et évaluation de systèmes de détection d'intrusions pour les applications Web. " Diss 2012.

[Albert 2010] Albert, Jérémie. "Modèle de calcul, primitives, et applications de référence, pour le domaine des réseaux ad hoc fortement mobiles. " Diss. Bordeaux 1, 2010.

[Alcime et al. 2013] Alcime Matthieu,Ghartouchent Malek, Rached Nihad. "NFC technology: Study report." 2013.

[Ali 2015] Ali, D. A. G. A. A. "Near-field communication technology and its impact in smart university and digital library: comprehensive study." Journal of Library and Information Sciences 3.2. 43-77 2015.

[Aljuaied 2001] Aljuaied, Ali M. "Bluetooth technology and its implementation in sensing devices. ". Naval Postgraduate School Monterey CA, 2001.

[Aman 2014] Aman, Frederic. "Reconnaissance automatique de la parole de personnes agées pour les services d'assistance à domicile." Diss. 2014.

[Anand et al. 2013] Anand, Duvey Anurag, Goyal Dinesh, and Hemrajani Dr Naveen. "A Reliable ATM Protocol and Comparative Analysis on Various Parameters with other ATM Protocols." International Jouranl of Communication and Computer Technologies (IJCCT), ISSN: 2278 9723.01-56. 2013

[Arun 2020] Arun Thomas. "Logical and Physical attacks on ATM Machines. " 2020

[Aste et al. 2017] Aste, T., Tasca, P., & Di Matteo, T. "Blockchain technologies: The foreseeable impact on society and industry. Computer" 50(9), 18-28. 2017
https://doi.org/10.1109/MC.2017.3571064

[ATMIA 2014] ATMIA. "Best Practices for Preventing ATM Gas and Explosive Attacks. " 2014

[ATMSWG 2009] ATMSWG, “Best Practice For Physical ATM Security,” ATM Security Working Group. 2009.

http://www.link.co.uk/SiteCollectionDocuments/Best_practice_for_physical_ATM_security.pdf. [Accessed:14-Nov-2016].

B

[Benchennane 2015] Benchennane, Ibtissam. "Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus". Diss. University of sciences and technology in Oran, 2015.

[Benecke and Ellermann 1998] C. Benecke and U. Ellermann, "Securing Classical IP over ATM Networks," in Proceedings of the 7th conference on usenix security symposium (SSYM '98), Berkeley, CA, US, pp. 1–11.1998.

[Bloomberg 2018] J. Bloomberg, "ATM 'Jackpotting' Attacks Reveal Deeper Problems," 12 02 2018. [Online]. Available: https://www.forbes.com/sites/jasonbloomberg/2018/02/12/atm-jackpotting-attacks-reveal-deeper-problems/#5b1147ee6fc3. [Accessed 10 04 2018].

[Blythe 2004] Blythe, Philip T. "Improving public transport ticketing through smart cards." Proceedings of the Institution of Civil Engineers-Municipal Engineer. Vol. 157. No. 1. Thomas Telford Ltd, 2004.

[Bolhuis 2014] Bolhuis, Martijn. "Using an NFC-equipped mobile phone as a token in physical access control. " MS thesis. University of Twente, 2014.

[Bouazzouni 2017] Bouazzouni, M. A. "Processus sécurisés de dématérialisation de cartes sans contact". Doctoral dissertation. https://oatao.univ-toulouse.fr/19488/ 2017.

[Braeuer et al. 2016] Braeuer, Johannes, Bernadette Gmeiner, and Johannes Sametinger. "A risk assessment of logical attacks on a CEN/XFS-based ATM platform." International Journal on Advances in Security Volume 9, Number 3 & 4, 2016.

[BCV 2017] BCV. "Encaisser simplement sans argent liquide, à moindre frais. " 2017.

[Business Insider 2018] Business Insider. "Here are 3 things that make cardless ATMs secure." 2018.

[Bosamia et Dharmendra 2019] Bosamia, Mansi, and Dharmendra Patel. "Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures." 2019.

C

[Caldwell 2012] Caldwell, Tracey. "Locking down the e-wallet."Computer Fraud & Security 2012.4 5-8. 2012.

[Ceipidor et al. 2013] Ceipidor U.B., Medaglia C., Marino A., Morena M., Sposato S., Moroni A., Di Rollo P. & La Morgia M. "Mobile ticketing with NFC management for transport companies. Problems and solutions." 2013 5th International Workshop on Near Field Communication (NFC), IEEE, 1-6. 2013

[Chabbi 2015] Chabbi, Samir. "Sécurité des applications NFC. " Mémoire de Magister. 2015

[Chabbi 2020a] Chabbi S., Boudour R., Semchedine F.: "A Secure Cloud Password and Secure Authentication Protocol for Electronic NFC Payment Between ATM and Smartphone. " Ingénierie des systèmes d'information 2020.

[Chabbi 2020b] Chabbi S., Boudour R., Semchedine F., Chefrour D.: "Dynamic Array PIN: A novel Approach to Secure NFC electronic payment between ATM and Smartphone. " Information security journal 2020.

[Chen et al. 2014] Chen C.H., Lin I.C. & Yang C.C. "NFC Attacks Analysis and Survey. " 2014 Eigth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 458-462. 2014

[Chikouche et al. 2012] Chikouche, Noureddine, Foudil Cherif, and Mohamed Benmohammed. "An authentication protocol based on combined RFID-biometric system RFID-biometric system." arXiv preprint arXiv:1207.5627 2012.

[Committee on Payments and Market Infrastructures 2020] Committee on Payments and Market Infrastructures. "Payment aspects of financial inclusion in the fintech era." Bank for International Settlements 2020.

[Cornelia et al. 2017] Cornelia, Ana-Maria, and Angela Repanovici. "Legal Information Management Using QR Codes." Qualitative and Quantitative Methods in Libraries 4.2 : 381-397. 2017.

[Coskun et al. 2012] Coskun, V.; Ok, K.; Ozdenizci, B. "Near Field Communication (NFC): From Theory to Practice." 1st ed.; John Wiley and Sons: London, UK, 2012.

[Coskun et al. 2013] Coskun, V.; Ok, K.; Ozdenizci, B. "Professional NFC Application Development for Android" 1st ed.; John Wiley Sons, Wrox: London, UK, 2013.

[Coskun et al. 2015] Coskun, Vedat, Busra Ozdenizci, and Kerem Ok. "The survey on near field communication." Sensors 15.6: 13348-13405. 2015

[Cremers et al. 2012] Cremers, Cas, et al. "Distance hijacking attacks on distance bounding protocols." Symposium on Security and Privacy. IEEE, 2012.

[CNA 2018] CNA. "Singapore rolls out unified payment QR code SGQR in latest cashless push. " 2018.

[Cnet France 2019] Cnet France. "Smartphone vole, ligne et téléphone bloqués, que faire ? " 2019.

D

[Dave 2013] Dave, Konark Truptiben. "Brute-force Attack "Seeking but Distressing"." International Journal of Innovations in Engineering and Technology (IJIET) 2.3 2013.

[David 2020] David Cramer. "What’s the difference between IT security vulnerability, threat & risk?. " 2020

[De Luna et al. 2019] De Luna, Iviane Ramos, et al. "Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied." Technological Forecasting and Social Change 146 : 931-944. 2019

[Dhaouadi 2014] Dhaouadi, Mondher. "Conception et optimisation des antennes RFID UHF en vue d'améliorer la fiabilité des systèmes RFID." Communications. Tunis: Ecole Supérieure des Communications de Tunis, 2014.

[Di Pietro et al. 2018] Di Pietro, Roberto, et al. "N-Guard: a Solution to Secure Access to NFC tags." Conference on Communications and Network Security (CNS). IEEE, 2018.

[Diebold 2012] Diebold, "ATM Fraud and Security", 2012. Available: http://securens.in/pdfs/KnowledgeCenter/5_ATM%20Fraud%20and%20Security.pdf. (Accessed: 14-Nov-2016).

[Digital munition 2013] Digital munition, "Identification and authentication-Information security Lesson 2.", 2013.

[Dominic 2014] Dominic. "Broom.Global Payments 2020" Transformation and Convergence. BNY Mellon, 2014.

[Drimer and Murdoch 2007] S. Drimer and S. J. Murdoch. "Keep your enemies close: Distance bounding against smartcard relay attacks." In USENIX Security: Proceedings of the 19th USENIX Security Symposium, 2007.

[Datalogic 2020] Datalogic. "Datalogic products.", 2020.

[Download.zone 2020] Download.zone. "RFID Technology and everyday use of this innovative system in our life Technology and everyday use of this innovative system in our life. ", 2020.

[Dreamstim 2018] Dreamstim. "La carte de métro est un système d'étiquetage sans contact de carte à puce pour des services de transport en commun dans la régio. Paiement, illustration. ", 2018.

[Daily Mirror 2019] Daily Mirror. "Be aware on ATM skimming attacks: " Fincsirt, 2019.

[Davidzou.com 2016] Davidzou.com. "NFC Security - Armourcard Active Jammer", 2016.

[Diakos et al. 2013] Diakos, Thomas P., et al. "Eavesdropping near-field contactless payments: a quantitative analysis." The Journal of Engineering 2013.10 : 48-54. 2013

E

[Economic and Social Council 2020] Economic and Social Council. "Report of the Partnership on Measuring Information and Communication Technology for Development. ", 2020

[El Gajoui and Fadoua 2014] EL GAJOUI, Khadija, and Fadoua ATAA ALLAH. "Vers un système de reconnaissance optique des caractères dans des documents multilingues: Français-Amazighe.", 2014.

[Elbahri 2015] ELBAHRI, Mohamed. "A highly efficient algorithm for fast motion detection and estimation using parallel processing. " Diss. 2015.

[El Madhoun 2019] El Madhoun, Nour, Emmanuel Bertin, and Guy Pujolle. "The EMV Payment System: Is It Reliable?." 3rd Cyber Security in Networking Conference (CSNet). IEEE, 2019.

[EMVCO 2014] EMVCO. "A Guide to EMV Chip Technology. ", November 2014

[Enisa 2016] Enisa. "Security of Mobile Payments and Digital Wallets. ", December 2016

[Emerj 2019] Emerj. "Machine Vision in Banking – Facial Recognition and OCR. ", 2019.

[ENSICAEN 2020] ENSICAEN. "Le piratage informatique. Techniques d'attaques. ", 2020.

F

[FinCoNet 2016] FinCoNet. "Online and mobile payments: Supervisory challenges to mitigate security risks. " September 2016.

G

[Gaddam et al. 2018] Gaddam, Ajit, Selim Aissi, and Sekhar Nagasundaram. "Tokenization revocation list." U.S. Patent No. 9,978,094. 22 May 2018.

[Ghag and Saket 2012] Ghag, Omkar, and Saket Hegde. "A comprehensive study of google wallet as an NFC application." International Journal of Computer Applications 58.16, 2012.

[Global Cyber Security Center 2016] Global Cyber Security Center. "ATM. A look at the future and emerging security threats landscape. ", 2016.

[GMV 2011] GMV, "Protect your automatic teller machines against logical fraud," 2011. Available: http://www. gmv.com/export/sites/gmv/DocumentosPDF/checker/ WhitePaper_checker.pdf. [Accessed: 14-Nov-2016].

[Goudelis et al. 2008] Goudelis, Georgios, Anastasios Tefas, and Ioannis Pitas. "Emerging biometric modalities: a survey." Journal on Multimodal User Interfaces 2.3-4 : 217, 2008.

[Guerar 2017] Guerar, M. "Security problems in embedded systems". (PhD thesis from the University of Oran-Algeria). 2017

[Guerar et al (a). 2016] Guerar, Meriem, et al. "Using screen brightness to improve security in mobile social network access." IEEE Transactions on Dependable and Secure Computing 15.4 : 621-632, 2016.

[Guerar et al. 2018] Guerar, Meriem, Alessio Merlo, and Mauro Migliardi. "Completely automated public physical test to tell computers and humans apart: a usability study on mobile devices." Future Generation Computer Systems 82 : 617-630, 2018.

[Guerar et al (b). 2016] Guerar, Meriem, Mohamed Benmohammed, and Vincent Alimi. "Color wheel pin: Usable and resilient ATM authentication." Journal of High Speed Networks 22.3 : 231-240, 2016.

[Guerfi 2008] Guerfi, Souhila. "Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D. " Diss. 2008.

[Grossi 2019] Grossi, Marco. "A sensor-centric survey on the development of smartphone measurement and sensing systems." Measurement 135 : 572-592, 2019.

H

[Hancke et al. 2009] Hancke, G., Mayes, K., Markantonakis, K. "Confidence in smart token proximity: Relay attacks revisited. " Computers & Security 28(7) 615–627, 2009.

[Hiyadi 2016] Hiyadi, Hajar. "Reconnaissance 3D de gestes pour l'interaction homme-système. " Diss. 2016.

[Hyderabad studio N 2018] Hyderabad studio N. "Robbery attack in ICICI bank ATM" at serilingampally. 2018.

[Hervé 2012] Hervé. "Présentation de la communication en champ proche (ou NFC pour les intimes) ", 2012.

I

[ICT Lounge 2020] ICT Lounge. "Types of computer Networks. " Acceded 2020

[IdTechEx 2018] IdTechEx. "Cardless, facial recognition ATMs." Artificial Intelligence Research. 2018.

[Industry ARC 2020] Industry ARC. "Near Field Communication (NFC) Chips Market" Research Report, 2020.

[Istock 2019] Istock. "Fille chauffeur payer à la place de stationnement par smartphone. " 2019.

[Insight Vault-co-op Financial services 2017] Insight Vault-co-op Financial services. "ATM trends Focus on user Experience. " 2017.

[INETCO 2019] INETCO. "UK Transaction Reversal Fraud | Security Update | INETCO Blog. " 2019.

J

[Jadla 2018] Jadla, Marwen. "L'authentification sécurisée utilisant le trusted computing. " Diss. École Polytechnique de Montréal, 2018.

[Jdaida 2016] Jdaida, S. "Analyse de sécurité des applications d'authentification par NFC". (Doctoral dissertation, École Polytechnique de Montréal). https://publications.polymtl.ca/2149/. 2016.

[Jensen et al. 2016] Jensen, Oliver, Mohamed Gouda, and Lili Qiu. "A secure credit card protocol over NFC." Proceedings of the 17th International Conference on Distributed Computing and Networking. 2016.

[Junaidu 2011] Junaidu Bello Marshall and Mua'zu Abdullahi Saulawa. "Cyber-Attacks: The Legal Response. ", 2011.

[Jayasinghe et al. 2016] Jayasinghe, Danushka, et al. "Extending emv tokenised payments to offline-environments." Trustcom/BigDataSE/ISPA. IEEE, 2016.

K

[Kaltschmid 2016] T. Kaltschmid, "95 Prozent aller Geldautomaten laufenmit Windows XP, " heise online. Available: http://www.heise.de/newsticker/meldung/95-Prozentaller-Geldautomaten-laufen-mit-Windows-XP- 2088583.html. [Accessed: 14-Nov-2016].

[Kasanda and Jackson 2018] Kasanda, Ella Nsonta, and Jackson Phiri. "ATM Security: A case study of Emerging Threats." International Journal of Advanced Studies in Computers, Science and Engineering 7.10, 2018.

[Kaspersky 2019] Kaspersky. "Kaspersky Security Bulletin 2019. Statistics", 2019.

[Kaspersky 2020] Kaspersky. "A look at the ATM/PoS malware landscape from 2017-2019. ", 2020.

[Kim et al. 2014] Kim, Siwan, Hyunyi Yi, and Jeong Hyun Yi. "FakePIN: "Dummy key based mobile user authentication scheme." Ubiquitous Information Technologies and Applications. Springer, Berlin, Heidelberg, 157-164, 2014.

[Kolaki 2017] Kolaki, Maria. "Mobile Payment Use and Mobile Payment Transactions by Older Adults: A Qualitative Study." 2017.

[Ku et al. 2019] Ku, Yeeun, et al. "Draw It As Shown: Behavioral Pattern Lock for Mobile User Authentication." IEEE Access 7 : 69363-69378, 2019.

[Kuhn et al. 2010] M. Kuhn, H. Luecken, and N. O. Tippenhauer. "UWB impulse radio based distance bounding." In Proceedings of the Workshop on Positioning, Navigation and Communication (WPNC), 2010.

[Kumar 2016] Kumar, Gulshan. "Denial of service attacks–an updated perspective." Systems science & control engineering 4.1: 285-294, 2016.

L

[Lacmanovié and Izabela 2011] Lacmanović, Dejan, and Izabela Lacmanović. "Contactless payments based on Near Field Communication Technology." E-society Journal: 75, 2011.

[Levy et al. 2016] Levy, Koby, et al. "Multiple NFC card applications in multiple execution environments." U.S. Patent No. 9,439,220. 6 Sep. 2016.

[Li 2011] Li, Haoyue. "Wi-Fi data transmission employing microcontroller and Wi-Fi CompactFlash Card. " Diss. University of Toledo, 2011.

[Lifchitz 2012] Lifchitz, R. "Hacking the NFC credit cards for fun and debit, " Hackito Ergo Sum conference, 2012.

[Ling et al. 2017] Ling, J., Wang, Y., & Chen, W. "An Improved Privacy Protection Security Protocol Based on NFC. " IJ Network Security, 19(1), 39-46, 2017.

[Litayem 2014] Litayem Nabil. "Contributions méthodologiques à la conception et optimisation de systèmes embarqués. " Thèse de doctorat, 2014.

[Lowe 2010] F. Lowe, "ATM community promotes jitter technology to combat ATM skimming, " ATM Marketplace, 2010. Available: http://www.atmmarketplace.com/ article/178496/ATMcommunity-promotes-jitter-technology-to-combat-ATM-skimming. [Accessed: 14-Nov-2016].

[Luca 2006] Viganò, Luca. "Automated security protocol analysis with the AVISPA tool." Electronic Notes in Theoretical Computer Science 155 : 61-86, 2006.

[Lekic 2013] Lekic, Nedjeljko, and Zoran Mijanovic. "NFC identification system for fuel dispensing control on petrol station." Eurocon, IEEE, 2013.

M

[Martin 2009] Martin Drašar. "Password based authentication. " Thése de Master. 2009.

[Mehallel 2019] MEHALLEL, Elhadi. "Contribution au Traitement des Signaux en Communication Ultra Large Bande (ULB). " Diss. 2019.

[Merkus 2018] Merkus, J. "Security evaluation of the NFC contactless payment protocol using Model Based testing" (Master's thesis, Open University Nederland), 2018.

[Michael 2001] Michael S. Scott. "Robbery at Automated Teller Machines. " 2001

[Mouser Electronics 2020] Mouser Electronics. "An introduction to Near Field Communication. " 2020.

[Malwarebytes labs 2019] Malwarebytes labs. "Everything you need to know about ATM attacks and fraud: part 1. " 2019.

[Maxfield Chen 2020] Maxfield Chen. "Attacking NFC and RFID. ", 2020.

[Moreno 2001] Moreno. "La Carte à puce. Histoire secrète. ", 2001

N

[Nambord and Emil 2017] Nambord, Magnus, and Emil Hansson. "NFC collision avoidance with controllable NFC transmission delay timing." U.S. Patent No. 9,723,635. 1 Aug. 2017.

[Nti 2017] Nti, Isaac Kofi. "Improving security levels in Automatic Teller Machines (ATM) using multifactor authentication. " Diss. 2017.

[NovaCard 2013] NovaCard. "NFC, simply about complicated. ", 2013.

[NFC Forum 2020] NFC Forum. "About the technology. ", 2020.

O

[Ok et al. 2010] Ok, K.; Coskun, V.; Aydin, M.N.; Ozdenizci, B. "Current Benefits and Future Directions of NFC Services. " In Proceedings of the IEEE International Conference on Education and Management Technology, Cairo, Egypt, 2–4 ; pp. 334–338. November 2010.

[Okereke and Mary 2017] Okereke, Daniel, and Mary Hedderman. "Factors Driving Mobile Payment Adoption: Benefits, Challenges & Opportunities." 2017.

[Orasanu 2015] Orosanu, Luiza. "Reconnaissance de la parole pour l'aide à la communication pour les sourds et malentendants. " Diss. 2015.

[Otterbein et al. 2017] Otterbein, F., Ohlendorf, T., & Margraf, M. "The German eID as an Authentication Token on Android Devices", 2017. Available: https://arxiv.org/ftp/arxiv/papers/1701/1701.04013.pdf. 2017.

[Owen 2016] Owen Wild, "Cash Trapping. Type 1. Attacks in Spain,", December 2016. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/brochures/ncr_security_alert_-_2016-14_cash_trapping_in_spain_0.pdf. [Accessed 7 October 2018].

[Owen 2018] Owen Wild, "Transaction Reversal Fraud - Global," 09 July 2018. [Online]. Available: https://www.ncr.com/content/dam/ncrcom/content-type/brochures/NCR%20Security%20Alert%20-%202018-06%20Transaction%20Reversal%20Fraud.pdf. [Accessed 7 October 2018].

P

[Pasquet et al. 2008] Pasquet, Marc, Joan Reynaud, and Christophe Rosenberger. "Secure payment with NFC mobile phone in the Smart Touch project." International Symposium on Collaborative Technologies and Systems. IEEE, 2008.

[Patel et al. 2018] Patel, S., Shah, V., & Kansara, M. "Comparative Study of 2G, 3G and 4G. " International Journal of Scientific Research in Computer Science, Engineering and Information Technology (Volume 3 , 2456-3307), 2018.

[PCI 2009] PCI Security Standards Council. "Skimming Prevention: Overview of Best Practices for Merchants. ", 2009.

[Pourghomi 2014] Pourghomi, P. "Managing near field communication (NFC) payment applications through cloud computing" (Doctoral dissertation, Brunel University, School of Information Systems, Computing and Mathematics), 2014.

[Promontory 2017] Promontory an IBM Company. "Biometric authentication in payments. Considerations for Policymakers. ", https://app.ranenetwork.com/article/8001000008492/, 2017

[PNGEgg 2020] PNGEgg."Paiement sans contact terminal de paiement communication en champ proche. ", 2020.

[PNG wing 2016] PNG wing. "Point of sale system architecture organization, gazelle, computer. ", 2016.

[Panasonic Industry 2019] Panasonic Industry."NFC smartphone technology and applications driving Near Field Communications. ", 2019.

[PSR 2018] PSR. "Payment System Regulator (PSR). Contactless mobile payments. " A PSR report. 2018.

R

[Rasmussen and apkun 2010] K. B. Rasmussen and S. Cˇ apkun. "Realization of RF distance bounding. In USENIX Security" Proceedings of the 19th USENIX Security Symposium. USENIX, 2010.

[Rajewski 2017] Rajewski Fran. "Coup de projecteur sur les rançongiciels : les modes de chiffrement. ", Emsisoft 2017.

[RBC Royal bank 2020] RBC Royal bank. "Contactless payment. " 2020.

[Roland 2013] Roland, Michael, Josef Langer, and Josef Scharinger. "Applying relay attacks to Google Wallet." 5th International Workshop on Near Field Communication (NFC). IEEE, 2013.

[Research gate 2013] Research gate. "Coils inductive coupling". Download scientific diagram. 2013.

[Rohde & schwarz 2013] Rohde & schwarz. "Near Field Communication (NFC) Technology and Measurements" White paper. 2013.

[Researchgate 2015] Researchgate. "Eavesdropping attack". Download scientific Diagram, 2015.

[Rodrigues 2014] Rodrigues, Helena, et al. "MobiPag: Integrated mobile payment, ticketing and couponing solution based on NFC." Sensors 14.8 : 13389-13415. 2014.

[Roland and Langer 2013] Roland, Michael, and Josef Langer. "Cloning Credit Cards: A Combined Pre-play and Downgrade Attack on {EMV} Contactless." 7th {USENIX} Workshop on Offensive Technologies ({WOOT} 13). 2013.

[Ryx 2017] Ryx. "Les fonctions de hachage cryptographiques. " Zeste de savoir 2017.

S

[Saha et Geetha 2017] Saha, R., & Geetha, G. "Symmetric random function generator (SRFG): A novel cryptographic primitive for designing fast and robust algorithms. " Chaos, Solitons & Fractals, 104, 371-377. https://doi.org/10.1016/j.chaos.2017.08.020, 2017.

[Saket et al. 2012] Saket, R. K., Bharat Bhushan Sagar, and Gurmit Singh. "ATM reliability and risk assessment issues based on fraud, security and safety." International Journal of Computer Aided Engineering and Technology 4.3 : 279-293, 2012.

[Salvador 2018] Salvador Mendoza. "NFC Payments: The Art of Relay &
Replay Attacks. ", August 14, 2018.

[Science ABC 2019] Science ABC. "Why Are ATM Card PINs Usually Just 4-Digit Long? " 2019.

[Secure technology Alliance 2017] Secure Technology Alliance. "Mobile Identity Authentication. " March 2017.

[Siddiqui 2013] Siddiqui, Ahmad Tasnim, and Mohd Muntjir. "A study of possible biometric solution to curb frauds in ATM transaction." IJASCSE, November 2013.

[Singh et al. 2018] Singh, Manmeet Mahinderjit, Ku Aina Afiqah Ku Adzman, and Rohail Hassan. "Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures." International Journal of Engineering & Technology 7.4.31: 298-305, 2018.

[Singha and Manoj 2019] Singha, Sur Chandra, and Manoj Kumar Verma. "Integration of AIDC Technology in Mobile via QR Code for Enhancing the Library Services: A Case Study of Don Bosco College Central Library, Arunachal Pradesh." Indian Journal of Information Sources and Services 9.2 : 44-48, 2019.

[Schmidt 2020] Stéphanie Schmidt. "Jackpotting : des logiciels malveillants font cracher des billets aux distributeurs automatiques. ", 2020.

[Srinivasan 2018] Srinivasan, Rajarajan. "DragPIN: A secured PIN entry scheme to avert attacks." Int. Arab J. Inf. Technol. 15.2 : 213-223, 2018.

[Security Magazine 2011] Security Magazine. "Get smart about access control. ", 2011.

[Security solutions Media 2012] Security solutions Media. "Ram Raiding : The biggest threat to ATM security. ", 2012.

[State bank of Lincoln 2018] State bank of Lincoln. "Security information. ", 2018.

[Salvador Mendoza 2018] Salvador Mendoza. "Intro to NFC Payment Relay Attacks. ", 2018.

[Security Affairs 2017] Security Affairs. "Europol arrested 27 for jackpotting attacks on ATM" 2017.

[SlideShare 2015] SlideShare. "Near Field Communication (NFC Architecture and Operating Modes)." 2015.

[Sullivan 2013] Sullivan, Richard J. "The US adoption of computer-chip payment cards: implications for payment fraud." Economic Review-Federal Reserve Bank of Kansas City : 59. 2013.

T

[Taleby et al. 2020] Taleby Ahvanooey, Milad, et al. "A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks." arXiv : arXiv-2001, 2020.

[Thevenon 2011] Thevenon, Pierre-Henri. "Sécurisation de la couche physique des communications sans contact de type RFID et NFC". Diss. 2011.

[Tornambé 2016] Tornambé, Anthony. "Modélisation système et développement d'antennes multistandards pour objets de paiement sans contact et de communication NFC". Diss. Aix-Marseille, 2016.

[The RFIP Blog-Wordpress.com 2016] The RFIP Blog-Wordpress.com. "NFC for Beginners-A short introduction. " 2016.

[The straits times 2016] The straits times. "Pay for bus, train rides by tapping your phone", transport News. 2016.

[TechJury 2020] TechJury. "What Is Brute Force and How to Stay Safe". Master Guide 2020.

[The Balance 2019] The Balance. "How to Set Up Google Wallet App for Android and iOS", 2019.

[TypesnUses.com 2019] TypesnUses.com. "Different Types of Wireless Communication Technologies", 2019

U

[U.S. Payments Forum 2019] U.S. Payments Forum. "Guidelines for Contactless ATM Transactions – A Guide for ATM Owners and Operators. ", 2019.

V

[Vila and Ricardo 2015] Vila, José, and Ricardo J. Rodríguez. "Practical experiences on NFC relay attacks with android." International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer, Cham, 2015.

[Vincent 2012] Vincent, A. M. "Contribution to the deployment of mobile services and to the analysis of transaction security" (PhD thesis, University of Caen Basse- Normandie), 2012.

[Vietnam Investment Review 2018] Vietnam Investment Review. "Recent Agribank thefts may have featured skimming devices. ", 2018.

[Villeroy 2018] Villeroy. "Rapport annuel 2018 de l'Observatoire de la sécurité des moyens de paiement. ", 2018.

W

[Wahid et al. 2018] Wahid, M. N. A., Ali, A., Esparham, B., & Marwan, M. "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. " Journal Computer Science Applications and Information Technology, 3, 1-7. 2018

[Wang et al. 2006] Wang, Xun, et al. "On the effectiveness of secure overlay forwarding systems under intelligent distributed DoS attacks." IEEE Transactions on Parallel and Distributed Systems 17.7: 619-632, 2006.

[Wu et al. 2014] Wu, T. S., Lee, M. L., Lin, H. Y., and Wang, C. Y. "Shoulder-surfing-proof graphical password authentication scheme". International Journal of Information Security, 13(3), 245-254, 2014.

[WikiHow 2019] WikiHow. "How to dispose of a credit card ? ", 2019.

[Www.grandviewresearch.com 2020] Www.grandviewresearch.com. "Contactless Payment Market Size, Share & Trends Analysis Report By Device (Smartphones & Wearables, Point-of-Sales Terminals, Smart Cards), By Solution, By Application, By Region, And Segment Forecasts, [2020 – 2027]. 2020.

Y

[Yende 2018] Yende, Raphael. "Support de cours de sécurité informatique et crypto.", 2018.

[Yi et al. 2012] Yi, J.H., Ma, G., Yi, H., Kim, S.: "Method and Apparatus for Authenticating Password of User Device. ", 10-1175042, Korea 2012.

[Yi et al. 2014] Yi, H., Piao, Y., & Yi, J. H. "Touch logger resistant mobile authentication scheme using multimodal sensors. " In Advances in Computer Science and its Applications (pp. 19-26). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-41674-3_4, 2014.

Z

[Zheng et al. 2018] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. "Blockchain challenges and opportunities: A survey. " International Journal of Web and Grid Services, 14(4), 352-375, 2018.