

UNIVERSITÉ DE LIMOGES

École doctorale

Sciences et Ingénierie pour l'Information, Mathématiques

FACULTÉ DES SCIENCES ET TECHNIQUES

Habilitation à diriger des recherches

Discipline : Informatique et applications

présentée et soutenue par

Damien SAUVERON

le 6 décembre 2014

Sécurité et interactions des « smart secure devices » et des « réseaux mobiles »

JURY :

Samia BOUZEFRANE	MCF HDR	Conservatoire National des Arts et Métier	Rapporteur
Keith MAYES	Professeur	Royal Holloway, University of London	Rapporteur
Mohamed MOSBAH	Professeur	Institut Polytechnique de Bordeaux	Rapporteur, Président
Serge CHAUMETTE	Professeur	Université de Bordeaux	Examineur
Maryline LAURENT	Professeur	Telecom SudParis	Examinatrice
Pascal URIEN	Professeur	Telecom ParisTech	Examineur
Philippe GABORIT	Professeur	Université de Limoges	Chargé du suivi

Aux trois femmes de ma vie : Clara, ma fille, Anaïs, ma femme et Joëlle, ma mère.

Remerciements

Table des matières

Introduction	7
Avant-propos	7
Positionnement scientifique	8
Production scientifique	10
 I Smart secure devices	 11
1 Sécurité et application des cartes multiapplicatives	13
1.1 Contributions	13
1.2 Perspectives	16
2 Sécurité et application de systèmes RFID	17
2.1 Contributions	17
2.1.1 Notation	18
2.1.2 Schéma général du jeu de protocoles d'authentification	18
2.1.3 Schéma pour le protocole d'authentification utilisant g_1	18
2.1.4 Comparatif avec l'état de l'art	20
2.1.5 Autres contributions	21
2.2 Perspectives	22
3 Évaluation et certification sécuritaires	23
3.1 Contributions	24
3.2 Perspectives	25
 II Réseaux mobiles	 27
4 Du « grid computing » à la mobilité	29
4.1 Contributions	29
4.2 Perspectives	31
5 Les réseaux de capteurs	33
5.1 Contributions	33
5.2 Perspectives	33
6 Les flottes de drones	35
6.1 Contributions	36
6.2 Perspectives	36
 Conclusion	 39

Bibliographie	44
Annexes	45
A Cartes multiapplicatives	
A.1 Collaborative and Ubiquitous Consumer Oriented Trusted Service Manager	
A.2 A Novel Consumer-Centric Card Management Architecture and Potential Security Issues	
A.3 Feature Interaction Problems in Smart Cards with Dynamic Application Lifecycle and their Countermeasures	
A.4 Recovering from a Lost Digital Wallet : A Smart Cards Perspective Extended Abstract	
A.5 Some security problems raised by open multiapplication smart cards . . .	
A.6 Multiapplication Smart Card : Towards an Open Smart Card ?	
B Protocoles RFID	
B.1 A Set of Efficient Privacy Protection Enforcing Lightweight Authentication Protocols for Low-cost RFID Tags	
C Évaluation sécuritaire	
C.1 An efficient and simple way to test the security of Java Cards	
D Du Grid à la Mobilité	
D.1 A Grid of Java Cards to Deal with Security Demanding Application Domains	
D.2 The Software Infrastructure of a Java Card Based Security Platform for Distributed Applications	
D.3 Secure Collaborative and Distributed Services in the Java Card Grid Platform	
D.4 Smart cards and remote computing : Interaction or convergence ?	
D.5 MANETS : An Exclusive Choice Between Use And Security ?	
E Réseaux de capteurs	
E.1 Wireless Sensor Nodes	
F Flottes de drones	
F.1 Improving Security of Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements. A Position Paper	
G CV, projet scientifique, liste complète des publications et rapport d'activités 2009-2014	

Table des figures

1	Vue schématique de mes activités de recherche.	9
1.1	Le modèle ICOM.	14
1.2	Le modèle UCOM.	14
1.3	Architecture générique de déploiement de TSM.	15
1.4	Vue générique du modèle CO-TSM.	15
1.5	Vue générique du mécanisme de migration d'application.	16
2.1	Schéma général du jeu de protocoles d'authentification proposé.	19
2.2	Le protocole d'authentification utilisant g_1	20
3.1	Trace d'une exécution normale vue au travers des différentes couches. . .	24
3.2	Trace d'une exécution <i>glitchée</i> vue au travers des différentes couches. . .	24
4.1	Grille de calcul sécurisée basée sur Java Card.	30
4.2	Grille de calcul sécurisée et mobile basée sur Java Card.	31
4.3	Réseau mobile ad hoc classique.	32
4.4	Réseau mobile ad hoc sécurisé avec les cartes.	32
6.1	Flotte de drones.	35
6.2	Proposition de Secure Element : ARFSSD.	36
6.3	Flotte de drones sécurisée avec les dispositifs ARFSSD.	37

Liste des tableaux

1	Résumé de la production scientifique après l'obtention du doctorat (à partir de 2005)	10
2.1	Notation utilisée dans la description des protocoles.	18
2.2	Comparaison des coûts avec les autres protocoles.	21
2.3	Comparatif sécuritaire avec les autres protocoles.	21

Introduction

« Il n'est point de bonheur sans liberté, ni de liberté sans courage. » (Périclès)

Avant-propos

Ce mémoire d'habilitation à diriger des recherches (HDR) reprend l'ensemble de mes contributions scientifiques depuis l'obtention de mon doctorat d'Informatique de l'Université Bordeaux 1 il y a dix ans (le 3 décembre 2004). Je montrerai tout d'abord lors de cette introduction, comment et pourquoi mes travaux de recherches ont évolué en un projet scientifique cohérent me permettant d'acquérir mon autonomie scientifique tout en restant dans les thématiques du laboratoire XLIM.

Chaque chapitre présentera une des facettes de mes activités de recherche. Ainsi, tout au long du document, pour chacun des chapitres, je résumerai la ou les problématiques scientifiques abordées, je déclinerais mes contributions et je proposerai des perspectives.

Toutefois, avant de rentrer véritablement dans le vif de la Science, je souhaite aborder ma vision de ce que représente une habilitation à diriger des recherches. Ce point est capital dans un contexte où le candidat que je suis n'a pas eu la chance de pouvoir encadrer de doctorant. Pour moi, l'obtention de l'HDR doit avant tout être la preuve que le candidat est capable de mener une recherche originale et de haut niveau, tout en ouvrant des pistes de recherches nouvelles et fructueuses. Si la rédaction et la soutenance de l'HDR sont bien des épreuves individuelles, l'objectif étant à terme de diriger des recherches, il est évident que le candidat doit pouvoir montrer ses aptitudes tant à fédérer des collègues autour de lui afin que chacun d'eux s'épanouisse dans la recherche qu'à collaborer avec des chercheurs internationaux afin d'atteindre des résultats de haut-niveau dans un contexte scientifique très compétitif.

De par la qualité des résultats que je vais décliner par la suite, dont l'obtention de la Prime d'Excellence Scientifique pour la période 2011-2015 est une confirmation, mais aussi pour avoir su travailler en équipe avec les collègues du laboratoire qui le souhaitent ainsi qu'avec de très nombreux collègues à l'international, je pense répondre à la quasi-totalité des critères énoncés de cette vision de l'HDR. Il ne manquerait à mon profil que la direction de la recherche et l'animation scientifique si je n'avais pas accompli de telles tâches à l'international : tout d'abord en tant que vice-président du groupe de travail de l'IFIP¹ Pervasive Systems Security (2007-2013) puis récemment en tant que président depuis 2014. En décembre 2013, en reconnaissance du travail accompli, l'assemblée générale de l'IFIP m'a décerné le « Silver Core Award » qu'aucun chercheur français n'a reçu depuis 2010. Mes activités de direction de la recherche et d'animation scientifique

1. L'IFIP (International Federation for Information Processing) créée en 1960 sous les auspices de l'UNESCO est la société savante pour l'informatique (elle peut être comparée à IEEE). Elle est reconnue par l'ONU et rassemble plus de 56 sociétés savantes du domaine du traitement de l'information réparties sur les 5 continents et représentant plus d'un demi million de membres. Elle comprend plus de 3500 scientifiques venant du monde académique et de l'industrie. Elle est organisée en 13 comités techniques, eux-même divisés en 101 groupes de travail.

se sont aussi traduites et renforcées par la publication de plusieurs numéros spéciaux sur des thématiques scientifiques importantes dans différents journaux ayant de bons facteurs d'impact. Enfin, si je ne devais citer qu'un seul événement majeur auquel j'ai pu apporter ma vision scientifique parmi les dizaines dans lesquels j'ai été impliqués (conférences, workshops, séminaires), il s'agirait sans conteste de WISTP (Workshop in Information Security Theory and Practice). Alors que j'ai créé WISTP en 2007 et que je me suis toujours fortement impliqué dans sa réussite, sa 8^{ème} édition vient de se terminer avec un taux d'acceptation de 24%. Face aux différents indicateurs positifs que recueille ce workshop (le taux d'acceptation moyen sur 8 ans est inférieur à 30%), il va devenir une conférence en 2015.

Positionnement scientifique et organisation du mémoire

L'avant-propos concernant ce mémoire étant terminé, voici le contexte scientifique dans lequel se sont inscrits mes travaux. Comme il n'est pas fréquent d'utiliser une terminologie anglo-saxonne, il me faut préciser pourquoi je l'ai fait dans le titre et à plusieurs reprises dans ce mémoire. En effet, j'ai conservé le terme « smart secure devices » car il recouvre une pluralité de « dispositifs sécurisés intelligents » (traduction littérale de l'expression anglaise) que sont les cartes à puce, les étiquettes radio-fréquences (tag RFID), les capteurs, etc. Il est aussi à noter les guillemets dans le titre de ce mémoire autour du néologisme « réseaux mobiles » utilisé pour définir le concept d'objets (au sens matériel du terme) et de systèmes (au sens logiciel) distribués *mobiles* (que l'on pourrait qualifier de nœuds) connectés essentiellement via des *réseaux* sans fil. Ces deux expressions atypiques constitueront les fils conducteurs de la présentation de mes travaux et chacune d'elles sera l'objet d'une partie de ce manuscrit. Elles seront dorénavant utilisées sans guillemet et présentées sommairement dans les introductions des deux premières parties.

La figure 1 illustre parfaitement les évolutions tant thématiques que temporelles de mes activités de recherche pour former mon projet scientifique : « Sécurité et interactions des smart secure devices et des réseaux mobiles ». Celui-ci consiste à sécuriser les smart secure devices mais aussi à les utiliser pour sécuriser les réseaux mobiles tant au niveau des nœuds que des échanges entre eux. La numérotation sur la figure indique la chronologie de mes différentes activités de recherches. Bien sûr, celles-ci n'ont pas été réalisées dans un séquençement aussi caricatural et elles ont souvent été entremêlées. Cet ordonnancement offre toutefois une bonne vision des évolutions de ma recherche. Si dans la suite de cette section, mes activités de recherche sont présentées de façon chronologique, pour la clarté du mémoire et pour permettre au lecteur de se rendre directement aux résultats qui l'intéressent, ces activités seront replacées dans les deux grandes parties introduites précédemment : smart secure devices et réseaux mobiles.

Ainsi après la fin de ma thèse de doctorat [43] dans laquelle je m'étais intéressé à la sécurité et aux applications des cartes à puce (en particulier de la technologie Java Card), j'ai poursuivi mes travaux sur les cartes multiapplicatives pendant plusieurs années. Sur ce sujet, j'ai récemment obtenu de beaux résultats que l'on retrouvera au chapitre 1.

De façon parallèle, j'ai poursuivi mes travaux, initiés en thèse, dans le domaine de la sécurisation des grilles de calcul à l'aide de cartes à puce. Comme je le montrerai au chapitre 4, ces travaux fondateurs ont ouvert la piste à de nombreuses recherches fructueuses qu'a pu poursuivre mon ancien directeur de thèse avec deux doctorants ayant soutenu avec succès leur thèse. De mon côté, si j'ai continué à collaborer avec lui sur cette thématique, j'ai préféré mettre l'accent sur l'aspect mobilité en travaillant sur les réseaux mobiles ad hoc (principalement les Mobile Ad hoc Networks – MANETs). Ces travaux

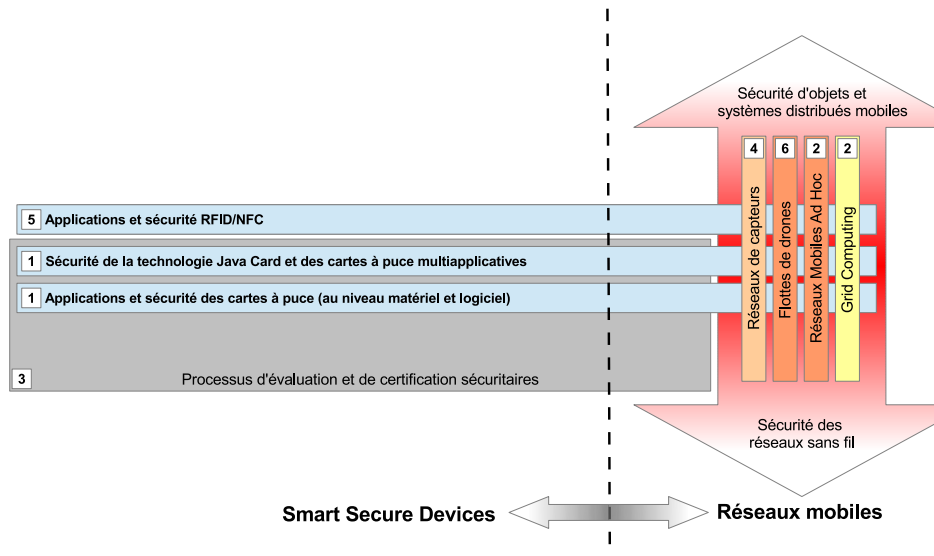


FIGURE 1 – Vue schématique de mes activités de recherche.

seront aussi présentés dans le chapitre 4, car ils constituent ma « conversion », au sens sacré du terme, à la « mobilité » en passant d'activités de sécurisation du « grid computing » (c'est-à-dire des systèmes fondamentalement fixes) vers des activités similaires sur le « wireless mobile computing » (c'est-à-dire des systèmes particulièrement mobiles et volatiles).

Ayant travaillé lors de ma thèse CIFRE, dans un Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI), je souhaitais faciliter l'évaluation de produits basés sur la technologie Java Card et montrer les limites de l'application de ces méthodologies d'établissement de la confiance, en particulier dans le cadre des cartes à puce. Ces travaux seront présentés au chapitre 3.

Ensuite, je me suis intéressé aux réseaux de capteurs qui par bien des aspects se rapprochent des problématiques des MANETs et des cartes à puce. En un sens, ce type de réseaux est à l'interface des activités smart secure devices et réseaux mobiles ; pour leur présentation dans ce mémoire, ces travaux pourraient se trouver indifféremment dans l'une ou l'autre des deux parties. J'ai choisi de les placer dans le chapitre 5 au sein de la partie II car même si mes contributions actuelles sont mineures, elle établissent le lien avec les travaux les plus récents sur les flottes de drones.

Plus récemment, avec plusieurs collègues, nous nous sommes intéressés à offrir des solutions innovantes utilisant la technologie RFID. Elles seront présentées au chapitre 2. Au travers de la technologie Near-Field Communication (NFC), un sous-ensemble de la technologie RFID, de nouvelles passerelles de communication entre les smart secure devices et les nœuds des réseaux mobiles sont possibles. Comme actuellement peu de travaux ont été menés tant sur la sécurité des tags RFID actifs que sur leurs utilisations pour sécuriser des réseaux mobiles, je proposerai une perspective en lien avec le chapitre présenté ci-dessous sur les flottes de drones.

Ainsi, si mes derniers travaux sur les flottes de drones, développés au chapitre 6, pour-

raient paraître complètement déconnectés du reste de mes activités, ils sont en réalité très enchevêtrés avec les points précédents puisqu'ils consistent en l'utilisation d'un smart secure device radio-fréquence actif embarqué sur chaque drone pour sécuriser tant le nœud lui-même que l'essaim dans sa globalité.

Ce mémoire se terminera par des annexes reprenant plusieurs travaux que je référence dans les différents chapitres et qui me semblent importants pour comprendre et juger de mon activité de recherche.

Production scientifique

Depuis l'obtention de mon doctorat, l'ensemble de mes travaux s'est traduit par la production scientifique décrites dans la table 1.

	Revue	Chapitre	SI	Actes	CI	CN	Projets	Distinctions	Soumis	ECdF
1 - Cartes à puce		4	2	4	1					
1 - Cartes multiapplicatives	1				3				3+1MI	1
5 - RFID/NFC					1		2			1
3 - Evaluation/Certification	1				1					
2 - Grid Computing	1		3	1	7	1		ABIT, PI		
2 - Réseaux Mobiles Ad Hoc	1				3		1			
4 - Réseaux de capteurs		2								
6 - Flottes de drones					1					1
Autres			5			1				
Total	4	6	10	5	17	2	3	ISCA	4	3

Légende – SI : Numéro spécial de revue (en anglais Special Issue) ; CI : Conférences internationales

CN : Conférences nationales ; ECdF : En cours de finalisation ; MI : Révision mineure

PI : Papier invité ; ABIT : Award of best innovative technology ; ISCA : IFIP silver core award

TABLE 1 – Résumé de la production scientifique après l'obtention du doctorat (à partir de 2005)

En parallèle de ces activités de productions scientifiques, j'ai été impliqué dans plus d'une centaine d'événements scientifiques à différents niveaux (PC chairs, General Chair, Publicity Chair, Editor, Steering Committee member, Program Committee member, etc.).

J'ai aussi participé à la direction de la recherche avec des collègues prestigieux au travers de plus d'une dizaine de numéros spéciaux de journaux [31, 32, 38, 37, 40, 41, 42, 46, 49, 50]. J'y participe encore au travers de certains numéros à paraître en 2016 [36, 3, 30] et qui ne figurent donc pas dans la table 1.

Première partie

Smart secure devices

Au sein de cette première partie du mémoire, je vais présenter plusieurs travaux que j'ai pu mener avec différents collègues concernant les cartes à puce, et en particulier les cartes multiapplicatives, les tags RFID et les méthodologies d'établissement de la confiance qui sont appliquées à ces dispositifs. Il est à noter que beaucoup des travaux présentés dans cette partie pourraient avoir un impact pratique car ils reposent souvent sur des standards existants et ils pourraient permettre de les améliorer.

Chapitre 1

Sécurité et application des cartes multiapplicatives

Si depuis les années 80 les cartes à puce sont des objets de notre quotidien, depuis la fin des années 90, certaines d'entre elles sont multiapplicatives et sont de plus en plus utilisées. Ainsi, dans l'industrie des télécommunications, la plupart des cartes SIM utilisées sont des cartes multiapplicatives. Deux grandes technologies concurrentes, Java Card et Multos, tendent à maîtriser ce marché sur lequel sont émises plusieurs milliards de cartes chaque année. Si ces cartes rencontrent un certain succès auprès des décideurs, grâce à la possibilité de charger des applications après l'émission de la carte (c'est-à-dire après sa remise au porteur), l'utilisation de cette caractéristique reste encore confidentielle en regard des possibilités offertes quand ces cartes sont utilisées couplées avec des technologies comme Near-Field Communication (NFC). En effet, l'industrie de la carte à puce fonctionne depuis presque 40 ans sur un modèle fermé, centré sur l'émetteur, qui bien qu'il ait eu ses avantages (comme celui non négligeable d'offrir une certaine confiance aux utilisateurs), n'est plus adapté au monde actuel, connecté et ouvert. Pour que les cartes multiapplicatives s'imposent comme des périphériques sécurisés et flexibles capables d'offrir un haut degré de confiance, un nouveau modèle de fonctionnement impliquant l'utilisateur est nécessaire.

Ce chapitre reprend mes principales contributions et perspectives dans ce domaine.

1.1 Contributions

Après mes travaux de thèse [43] dans lesquels j'avais introduit le concept de pré-persistance [19] tout en révélant différents problèmes dans les spécifications Java Card pouvant conduire à des implémentations incompatibles et disposant de niveaux de sécurité très différents – problèmes qui ont été corrigés dans la version 3.0 des spécifications Java Card en reprenant les idées sous-jacentes du concept de pré-persistance au travers de la notion d'« atteignabilité » (reachability) –, j'ai décidé de m'abstraire des caractéristiques spécifiques des technologies pour proposer des modèles applicables à toutes.

Ma première contribution importante a été d'introduire la notion de cartes à puce multiapplicatives ouvertes [45], c'est-à-dire permettant au porteur de la carte de charger des applications après l'émission, d'en lister les défis à résoudre [21] et de proposer des méthodes pour tester leur sécurité [20] (en particulier dans le cadre de l'évaluation sécuritaire qui sera décrite au chapitre 3). De façon pragmatique, j'avais aussi proposé un modèle de cartes semi-ouvertes pour lesquelles seuls des tiers de confiance pourraient installer des applications après l'émission. Assez étonnamment, sans que je puisse mesurer l'influence

de mes travaux, ce modèle a trouvé sa traduction dans la technologie NFC au travers des Trusted Service Managers (TSM).

Au delà du crédit (difficilement mesurable) qui m'est attribuable pour le concept de TSM, mes travaux ont intéressé des collègues du Royal Holloway University of London et en particulier Raja Naeem Akram qui a brillamment étendu ceux-ci lors de sa thèse de doctorat « A User Centric Security Model for Tamper-Resistant Devices » dont j'ai eu la chance d'être rapporteur. En effet, en opposition au modèle classique ICOM (Issuer Centric Smart Card Ownership Model – c'est-à-dire un modèle centré sur l'émetteur) présenté en figure 1.1, Raja a proposé le modèle UCOM (User Centric Smart Card Ownership Model – c'est-à-dire un modèle centré sur l'utilisateur) présenté en figure 1.2.

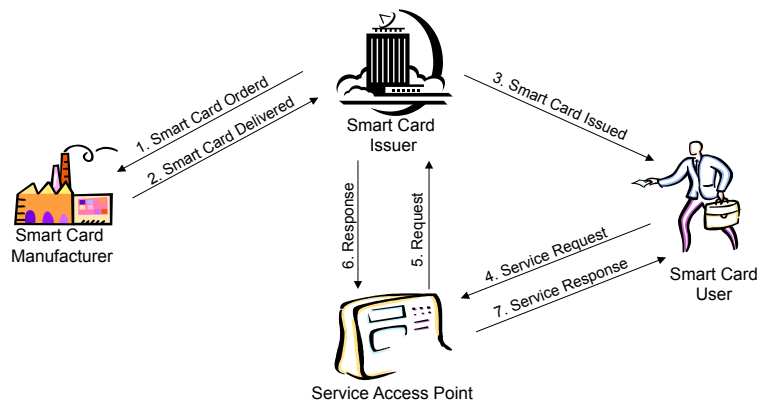


FIGURE 1.1 – Le modèle ICOM.

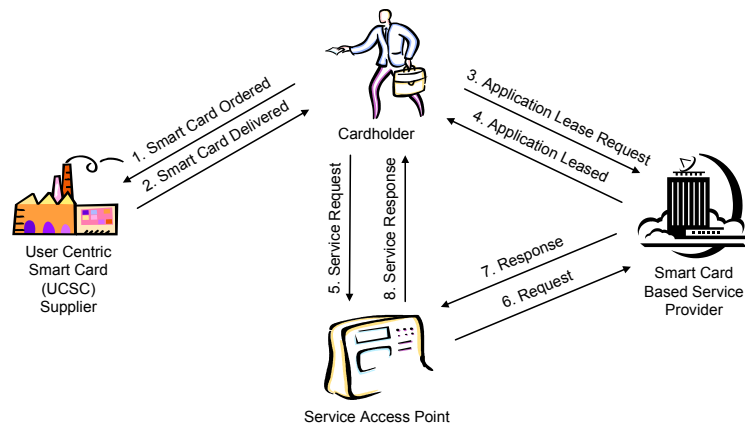


FIGURE 1.2 – Le modèle UCOM.

À l'issue de sa soutenance de thèse, Raja et moi avons échangé plusieurs idées dont certaines ont pris corps aujourd'hui au travers de plusieurs publications. Par exemple, nous avons étendu le concept de TSM classique (illustré en figure 1.3), très fermé et contraignant puisque seules les applications de fournisseurs associés au TSM peuvent être installées sur la carte, en celui de TSM collaboratif et ubiquitaire (Consumer Oriented Trusted Service Manager – CO-TSM) [4] (illustré en figure 1.4) qui est lui à la fois flexible, ouvert et orienté utilisateur. Il est essentiel de noter que nos propositions sont applicables aussi bien dans le modèle ICOM que UCOM, même s'il est certain qu'elles se prêtent mieux à ce dernier.

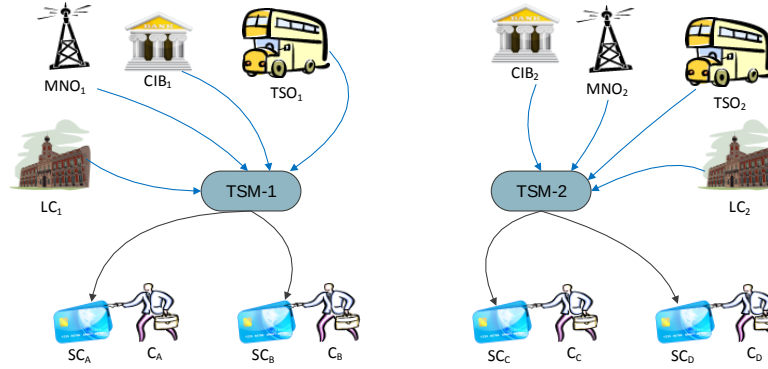


FIGURE 1.3 – Architecture générique de déploiement de TSM.

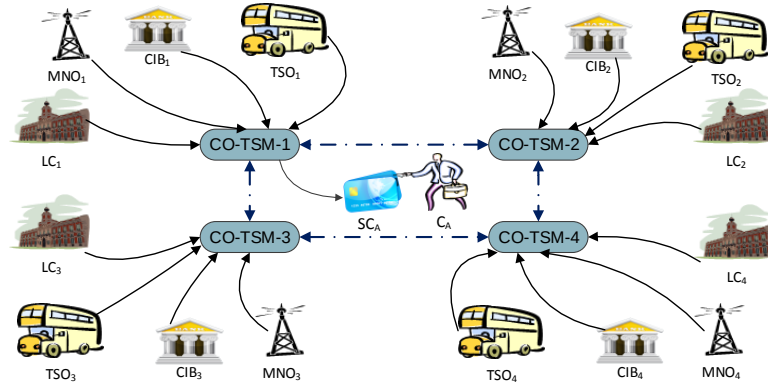


FIGURE 1.4 – Vue générique du modèle CO-TSM.

Devant l'attrait de mes travaux avec Raja et des collègues du Royal Holloway ainsi que face à l'engouement suscité par la technologie NFC, le consortium GlobalPlatform, un des acteurs majeurs du monde de la multiapplication sur cartes à puce, s'est positionné en publiant en 2012 un « white paper » définissant les grandes lignes d'un modèle centré sur le consommateur (GP-CCM). Nos propositions de CO-TSM sont bien évidemment aussi applicable à ce modèle.

Afin d'asseoir nos propositions, nous nous sommes penchés sur les menaces potentielles [5] qui pourraient découler de notre proposition d'une nouvelle architecture pour la gestion des applications sur des cartes ayant un modèle orienté utilisateur (UCOM ou GP-CCM). Pour lutter contre les FIP (Feature Interaction Problem)¹ liés à la suppression d'une application, et comme GlobalPlatform et Java Card ne permettent pas de résoudre ces problèmes (Multos n'y est pas sensible lorsqu'il s'agit de l'effacement d'une application), nous avons proposé un framework [6] permettant d'en minimiser les conséquences. Si ces problèmes sont peu probables dans le modèle ICOM, dans un modèle orienté utilisateur, UCOM ou GP-CCM, il est absolument nécessaire de les prendre en compte afin d'éviter qu'une application dépendante d'autres applications ne dysfonctionne en raison de la suppression d'une de ces dernières.

Les détails relatifs à ces travaux sont disponibles dans les publications [4, 5, 6] jointes en annexe A de ce mémoire.

1. De façon simpliste, lorsque plusieurs fonctionnalités (fonctions, applications, et/ou APIs) sont liées au point que le changement, la modification ou l'interruption de l'une d'elles nuit à la stabilité globale et/ou à l'exécution fiable des autres alors il y a un FIP, c'est-à-dire un problème d'interaction des fonctionnalités.

Assez classiquement, j'ai aussi contribué à de nombreux ouvrages scientifiques [14, 34, 44, 48] et à des travaux connexes comme l'évaluation de la qualité de générateurs de nombres aléatoires de Java Cards [25], une mémoire étendue pour Java Card [26], etc.

1.2 Perspectives

Les perspectives concernant les travaux entrepris avec Raja concernant les cartes multiapplicatives sont de plusieurs ordres. Tout d'abord nous entendons lever les freins psychologiques des utilisateurs à l'utilisation potentielle de telles cartes au travers de solutions de sauvegarde [7] sur un serveur sécurisé pour pouvoir restaurer les applications en cas de perte ou de changement de cartes pour un modèle plus récent (tout en respectant les politiques d'utilisation associées à chaque application et définies par les fournisseurs d'applications). Comme illustré en figure 1.5, nous avons également développé un mécanisme de migration du contenu de la carte vers une autre carte qui nous servira pour des travaux de la seconde partie de ce mémoire (en particulier pour les flottes de drones et les réseaux mobiles ad hoc).

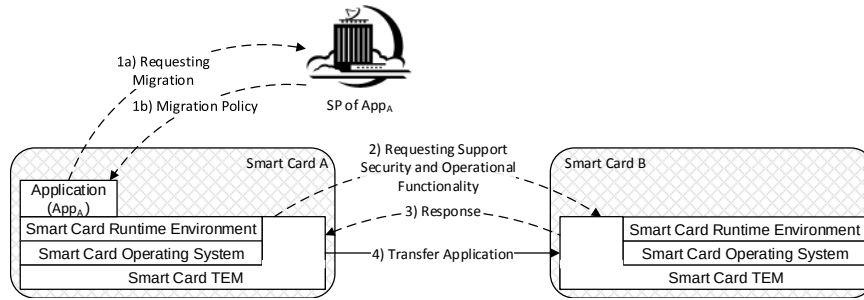


FIGURE 1.5 – Vue générique du mécanisme de migration d'application.

Nous nous intéressons également à montrer que le composant « Trusted Environment & Execution Manager » (TEM) est suffisant pour contrer les menaces d'une plate-forme ouverte et assurer la confiance aussi bien du point de vue du porteur de carte, que de celui des TSMs et des fournisseurs d'applications. Nous étudions aussi d'autres problématiques de FIP dans les cartes suivant un modèle orienté utilisateur (UCOM ou GP-CCM). Plus globalement, nous développons actuellement toutes les parties de l'écosystème en vue de l'adoption de nouveaux modèles orientés utilisateurs par l'industrie de la carte. En effet, disposer d'éléments sécurisés compatibles UCOM permettraient de sécuriser de multiples systèmes distribués.

Chapitre 2

Sécurité et application de systèmes RFID

Les étiquettes radio-fréquences, aussi appelées tags RFID, sont les codes-barres d'aujourd'hui et de demain. Afin de ne pas augmenter le prix des produits auxquels ils sont attachés, il est indispensable que leur coût de production reste faible. Ces contraintes économiques obligent à imaginer des tags et des protocoles cryptographiques dit bas-coûts (« low cost »). Bien sûr, tous les systèmes RFID ne sont pas destinés à être bas-coûts. Ainsi dans les industries des transports publics ou du bancaire dans lesquelles le NFC est utilisé (par exemple pour le paiement sans contact via NFC depuis son téléphone), les systèmes cryptographiques reposent sur des primitives souvent bien étudiées et plus sécurisées. Les quelques industriels qui ont utilisé des algorithmes propriétaires et le principe de la sécurité par l'obscurité (comme la société NXP pour le Mifare) s'en sont mordus les doigts.

Si les systèmes RFID peuvent faciliter la vie quotidienne des utilisateurs (passage plus rapide en caisse, etc.), ils sont aussi sources de menaces pour leur vie privée. Il est possible de les utiliser à l'encontre des utilisateurs pour tracer leurs déplacements, pour collecter des informations sur eux en vue d'un profilage publicitaire, etc. C'est pourquoi les protocoles visant à renforcer la vie privée au niveau des intermédiaires (par exemple le dispositif de lecture qui va effectuer une action telle que l'ouverture ou non d'une porte) en protégeant l'identité des tags (et donc des porteurs) sont nécessaires.

2.1 Contributions

En dehors de l'étude des menaces contre les cartes sans contact dans l'industrie des transports publics [33], ma contribution la plus significative, en partenariat avec plusieurs collègues, est la proposition pour des tags RFID bas-coûts d'un jeu de protocoles d'authentification légers et efficaces permettant de protéger la vie privée [2]. Ces protocoles opèrent en $O(1)$ en nombre d'opérations du côté de la base de données contre $O(n)$, n étant le nombre de tags dans la base, pour les protocoles de l'état de l'art. Outre la description de nos propositions, l'article [2] disponible en annexe B présente de nombreuses attaques, dont certaines nouvelles, sur des protocoles de l'état de l'art. Afin d'être complet, nos protocoles, comme ceux de l'état de l'art, reposent sur l'hypothèse de l'existence d'un PRNG « lightweight ». Pour ne pas alourdir inutilement le mémoire, je ne présente ci-après que la construction générale et une instance de celle-ci.

2.1.1 Notation

La table 2.1 présente la notation utilisée dans la description des protocoles.

TABLE 2.1 – Notation utilisée dans la description des protocoles.

DB	:	Désigne la base de données
R	:	Désigne le lecteur
T	:	Désigne le tag
SID	:	Désigne l'ID sécurisé du tag
hkSID	:	Désigne la clé associée au SID du tag dans la table de hachage de DB
K	:	Désigne la clé partagée entre le tag et la base de données
R ₁	:	Un nombre aléatoire généré par le lecteur
R ₂	:	Un nombre aléatoire généré par le tag
X _[i..j]	:	Désigne la séquence de bits de X du i^{me} au j^{me} bit avec $i > j$
A → B	:	Message envoyé par l'entité A à l'entité B
X ⊕ Y	:	XOR binaire des opérandes X, Y
X ∧ Y	:	ET binaire des opérandes X, Y
X ≪ Y	:	Décalage binaire à gauche sur X de Y bits
X ≫ Y	:	Décalage binaire à droite sur X de Y bits
X Y	:	Concaténation des opérandes X, Y
X = Y	:	Affecte la valeur Y à X
X $\stackrel{?}{=}$ Y	:	Compare l'égalité de X avec Y
Query	:	Message pour débiter la procédure d'authentification
Auth _{DB}	:	Ticket authentifiant la base de données
Auth _T	:	Ticket authentifiant le tag
OK	:	Message confirmant une authentification réussie
NOK	:	Message confirmant un échec de l'authentification

$Left(X)$ et $Right(X)$ sont deux fonctions d'extraction qui retournent respectivement la moitié des bits de X les plus significatifs et les moins significatifs.

$$\begin{aligned}
 Left : \quad \mathbb{F}_2^{2m} &\rightarrow \mathbb{F}_2^m \\
 X &\mapsto Left(X) = X_{[2m-1..m]} \\
 Right : \quad \mathbb{F}_2^{2m} &\rightarrow \mathbb{F}_2^m \\
 X &\mapsto Right(X) = X_{[m-1..0]}
 \end{aligned}$$

2.1.2 Schéma général du jeu de protocoles d'authentification

Afin de simplifier la présentation du protocole, nous allons faire l'hypothèse que SID , $hkSID$ et $K \in \mathbb{F}_2^l$ et que $R_1, R_2 \in \mathbb{F}_2^{l/2}$ et nous allons poser $2m = l$.

Avant la distribution d'un tag à son utilisateur, une phase d'enregistrement du tag dans la base est nécessaire. Elle n'est pas décrite ici mais elle est expliquée dans [2]. Le schéma général du jeu de protocoles d'authentification est alors celui présenté sur la figure 2.1

2.1.3 Schéma pour le protocole d'authentification utilisant g_1

Parmi les différents protocoles proposés, la figure 2.2 présente le protocole 1 utilisant le PRNG $g_1(X)$

$$\begin{aligned}
 g_1 : \quad \mathbb{F}_2^l &\rightarrow \mathbb{F}_2^l \\
 X &\mapsto g_1(X) \text{ où le résultat est un pseudo-aléa.}
 \end{aligned}$$

Les fonctions du schéma général se raffine alors ainsi :

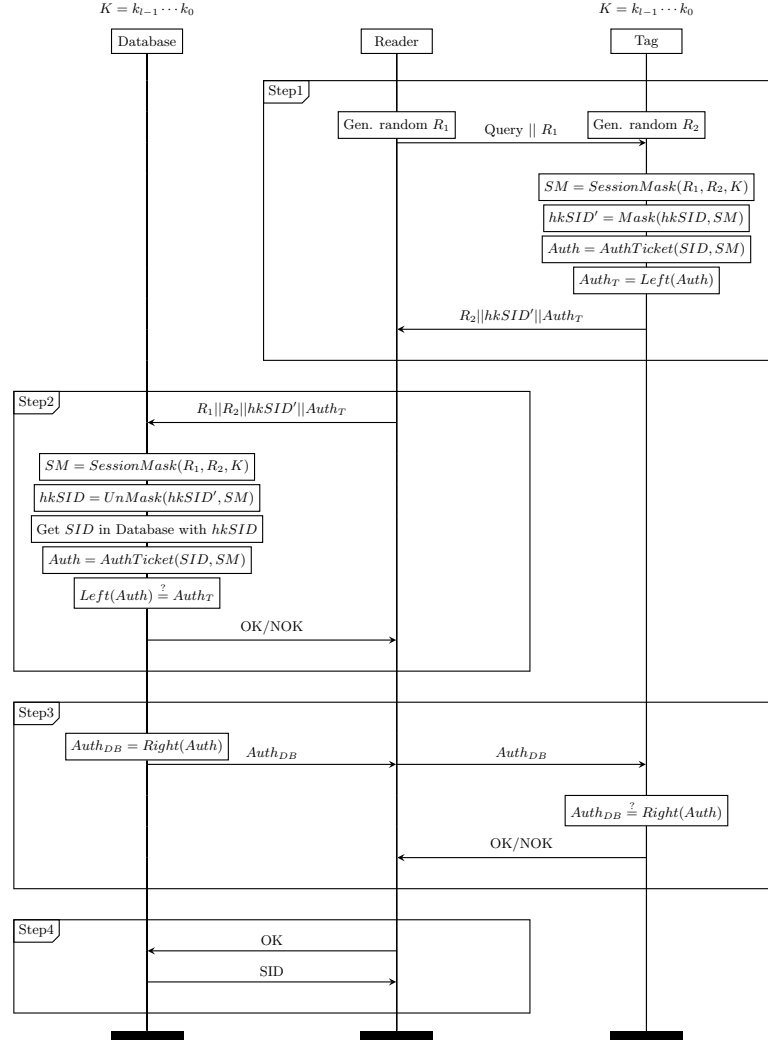
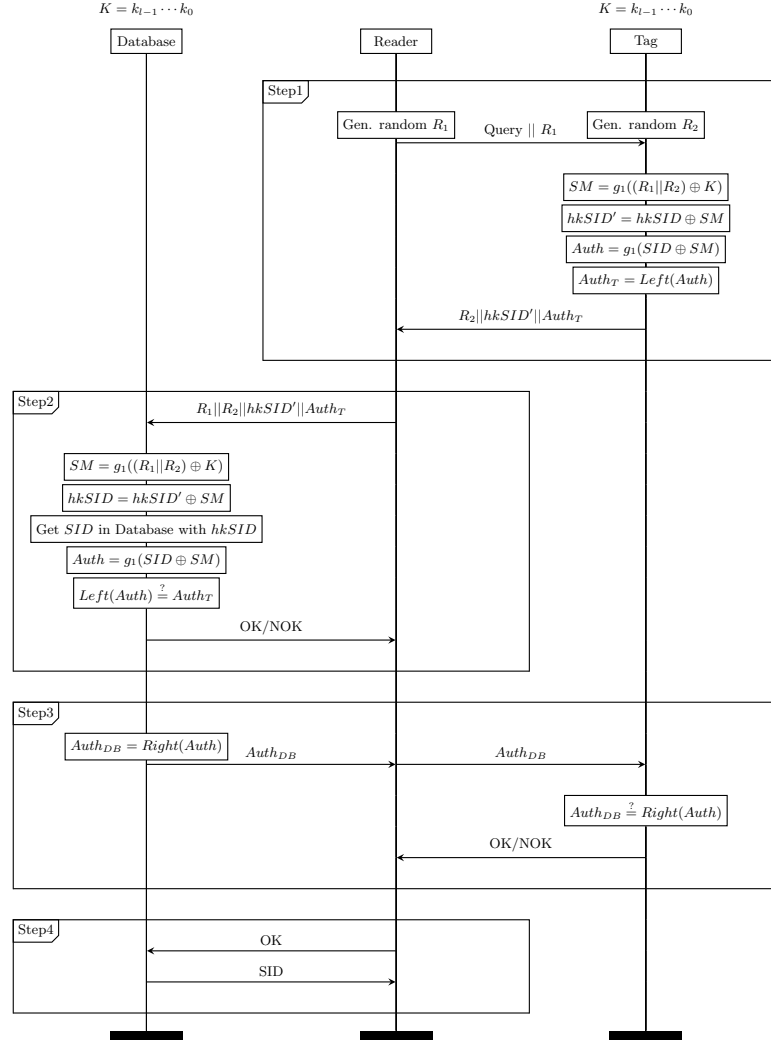


FIGURE 2.1 – Schéma général du jeu de protocoles d'authentification proposé.

- $SessionMask(R_1, R_2, K) = g_1((R_1 \parallel R_2) \oplus K)$
- $Mask(hkSID, SM) = hkSID \oplus SM$
- $AuthTicket(SID, SM) = g_1(SID \oplus SM)$
- $UnMask(hkSID', SM) = hkSID' \oplus SM$.

FIGURE 2.2 – Le protocole d'authentification utilisant g_1 .

2.1.4 Comparatif avec l'état de l'art

Il faut noter que certains résultats de la table 2.2 sont différents de ceux présentés dans les travaux d'origine car afin d'avoir le comparatif le plus juste nous avons pris en compte tous les messages (comme la Query, l'aléa envoyé par le lecteur et d'autres informations). Dans la table 2.2, le protocole Gossamer est mis de « ultralightweight » à « lightweight » et

	Song <i>et al.</i> [47]	Chien <i>et al.</i> [27]	Gossamer [39]	Nos propositions [2]	
				Classiques	Étendues
Communication $R \rightarrow T$	$40 + 2l$	$40 + l + l/2$	$40 + 3l$	$40 + l$	$40 + l + l/2$
Communication $T \rightarrow R$	$2l$	$1 + 2l + l/2$	$2l$	$1 + 2l$	$1 + 2l + l/2$
Total sur l'interface RF	$41 + 4l$	$41 + 4l$	$40 + 5l$	$41 + 3l$	$41 + 4l$
Taille mémoire sur le tag	l	$3l$	$7l$	$3l$	$3l$
Taille mémoire sur la base	$4l$	$5l$	$4l$	$2l$	$2l$
Coût de calcul sur la base	$O(n)$	$O(n)$	$O(n)$	$O(1)$	$O(1)$
Classification du coût de calcul sur le tag	Lightweight	Lightweight	Ultralightweight to Lightweight	Lightweight	Lightweight
Durée de vie du tag (en nombre d'authentifications)	10^5 or 10^{12}	10^5 or 10^{12}	10^9 or 10^{12}	∞	∞

TABLE 2.2 – Comparaison des coûts avec les autres protocoles.

pas seulement à « ultralightweight » comme dans Peris *et al.* [39] car la fonction *MixBit* utilise la fonction *add* (d'addition) que l'on considère plus coûteuse qu'un $\oplus$.

La table 2.3 fournit un comparatif de la résistance de nos protocoles et de ceux de l'état de l'art contre les attaques étudiées dans l'article [2] disponible en annexe B.

	Song <i>et al.</i> [47]	Chien <i>et al.</i> [27]	Gossamer [39]	Our Proposals [2]
Untraceability	No	Yes	Yes	Yes
Mutual authentication	No	Yes	Yes	Yes
Algebraic Attack Resistant	No	Yes	Yes	Yes
Desynchronization & DoS Attacks Resistant	No	No	No	N/A (Yes)
Database Entry Collision Resistant	N/A (Yes)	No	No	N/A (Yes)
Chosen Value Attack Resistant	∇	Yes	partial (cf (AT4) in [2])	Yes
Timing Attack Resistant	∇	partial (cf (AT8) in [2])	partial (cf (AT8) in [2])	N/A (Yes)
Random Authentication Attack Resistant	∇	Yes	Yes	Yes
Database impersonation Attack Resistant	No	Yes	Yes	Yes
Man-in-the-middle Attack Resistant	No	Yes	∇	Yes
Replay Attack Resistant	No	Yes	No	Yes

∇ : La résistance contre cette attaque est inutile car il existe une attaque plus facile avec une probabilité de réussite plus élevée

N/A : Non Applicable (donc le protocole est résistant)

TABLE 2.3 – Comparatif sécuritaire avec les autres protocoles.

On constate clairement au travers des tables 2.2 et 2.3 que notre jeu de protocoles est intéressant.

2.1.5 Autres contributions

Dans le domaine des RFID, un autre résultat, que je ne considère pas comme une contribution significative, est issu du projet, dont j'étais porteur, SoRFID (Security of RFID) de la fédération de recherche MIREs (Mathématiques & leurs Interactions, Images & information numérique, Réseaux et Sécurité – fédération labellisée FR 3423 par le CNRS de laboratoires du PRES Limousin-Poitou-Charentes). En effet, nous avons réalisé, à base de matériel sur étagère (Arduino), plusieurs prototypes permettant de réaliser avec succès des attaques sur des systèmes RFID connus pour être peu (ou pas) sécurisé et qui sont pourtant encore largement utilisés dans des secteurs sensibles (paiement, alarme, contrôle d'accès, etc.). L'intérêt du projet était avant tout de faire collaborer des chercheurs de différentes équipes du laboratoire XLIM : DMI (Département Mathématiques-Informatique),

OSA (Ondes et Systèmes Associés) et C2S2 (Composants Circuits Signaux et Systèmes hautes fréquences).

Dans le domaine applicatif autour du NFC, j'ai contribué de façon mineure au projet DIL (Détection Innovation Laboratoire) porté par Pierre Dusart et qui a également impliqué Pierre-François Bonnefoi. Ce projet intitulé « Limousin Autonomie & Médiation Sécurisée » s'est déroulé de 2010 à 2012. Il portait sur la thématique du maintien à domicile et il reposait sur l'utilisation de tags RFID associés à des actions prédéfinies. Via l'utilisation de la technologie NFC, le patient prouvait qu'il avait effectué des actions (prise de médicaments, etc.). L'objet du projet était de renverser le paradigme en faisant du patient un acteur de son autonomie qui consent à transmettre des informations aux professionnels de santé via les actions qu'il effectue et non un spectateur de sa fin de vie dans un logement truffé de capteurs en charge de contrôler (« espionner » est ce que ressent le patient) la moindre de ses actions. Évidemment le projet comprenait bien plus qu'un simple déploiement de tags RFID et de lecteurs. Une plate-forme de médiation pour les professionnels de santé en charge de suivre le patient y était également associée.

2.2 Perspectives

Sur la base des travaux présentés sommairement ci-dessus, nous sommes en cours de rédaction d'un nouvel article permettant de proposer des tags encore plus bas-coûts sous certaines hypothèses (mémoire non volatile de type FRAM à la place de Flash ou EEPROM). Une autre perspective consiste à s'intéresser à la sécurité des tags RFID actifs qui sont pour l'instant peu étudiés et qui seront utiles dans le cadre des flottes de drones présentées au chapitre 6. Enfin, il y a des convergences évidentes à développer entre le chapitre sur les cartes multiapplicatives et celui-ci au travers de l'utilisation de la technologie NFC. Par exemple, la migration d'applications d'une carte SIM UCOM à une autre, illustrée au chapitre 1 en figure 1.5, pourrait se faire en mode pair-à-pair entre deux téléphones disposant de la technologie NFC.

Chapitre 3

Évaluation et certification sécuritaires

Les processus d'évaluation et de certification sécuritaires sont parmi les techniques d'assurance les plus répandues pour établir la confiance dans la sécurité d'un produit des technologies de l'information. Sans aller jusqu'à tenir une discussion philosophique sur la question de la « confiance », il est naturel de s'interroger sur « Qu'est que la confiance dans la sécurité ? », « Le niveau de confiance est-il graduable ? », « Sur quels critères la confiance est-elle établie ? », etc. Depuis le milieu des années 1980, des experts internationaux se sont penchés sur ces questions et ont convergé dans le domaine de la sécurité sur une méthodologie et un ensemble de critères dit « Critères Communs » à partir de 1995. En 1999, la version 2.1 a été normalisée sous l'intitulé ISO15408. Depuis, ces critères et la méthodologie ont continué à évoluer puisque la version finale 3.1 devrait bientôt être publiée.

En pratique, afin de s'assurer de la sécurité de différents produits sensibles, issus des technologies de l'information, utilisés sur leur territoire (comme par exemple les cartes bancaires), certains états, dont la France, ont mis en place un schéma de certification sécuritaire s'appuyant sur ces critères et méthodologies. En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est l'autorité chargée de mettre en place le schéma d'évaluation et de certification sécuritaires. Dans le schéma tri-partite classique, un commanditaire (par exemple le développeur d'un produit nécessitant une certification) soumet son produit à un Centre d'Évaluation de la Sécurité des Systèmes d'Information (CESTI) qui se charge de vérifier la sécurité de celui-ci en regard de la conception, du cahier des charges, du développement, et de multiples autres aspects, le tout sous le regard attentif et vigilant de l'ANSSI qui peut exiger que des tâches particulières soient plus approfondies. Afin d'éviter toute collusion entre le CESTI et le commanditaire, l'organisme qui délivre un certificat est l'ANSSI. Le niveau de certification est fonction des objectifs du commanditaire, du temps passé à vérifier les mécanismes sécuritaires du produit et de la connaissance de ceux-ci par le CESTI. Un produit avec certificat de niveau EAL1 peut être considéré comme ayant subi de simples tests de sécurité avec une connaissance « boîte noire » du produit alors qu'un produit avec un certificat de niveau EAL7 aura été vérifié en totalité, avec des preuves formelles du bon fonctionnement des mécanismes sécuritaires et des preuves de leur bonne implémentation, avec des vérifications de la sécurité des environnements de production, etc.

3.1 Contributions

Dans ce contexte, ma première contribution, même si elle est dans la continuité de mes travaux de thèse, est une méthodologie facilitant l'évaluation de la sécurité de cartes multiapplicatives basées sur la technologie Java Card [20, 21]. En effet, en utilisant la méthodologie proposée permettant d'isoler physiquement un motif à observer (par exemple un algorithme de chiffrement particulier) dans une trace d'exécution via l'ajout de motifs connus (ou le déclenchement d'événements connus et observables depuis l'extérieur - par exemple via envoi de données sur l'I/O) proche du motif ciblé, les centres d'évaluation gagnent un temps précieux pour conduire leurs évaluations sécuritaires de cartes à puce Java Card. Comme on le constate sur les figures 3.1 et 3.2, une fois le motif isolé, les évaluateurs peuvent effectivement appliquer plus facilement (c'est-à-dire avec une meilleure précision puisqu'ils peuvent se synchroniser sur le motif ou l'événement connu inséré dans la trace), et avec des équipements moins puissants (par exemple l'oscilloscope a besoin de moins de mémoire ou à taille mémoire équivalente il peut faire un meilleur échantillonnage), les attaques classiques de l'état de l'art (Simple Power Analysis, Differential Power Analysis, Fault Attack, Timing Attack, etc.). Si cette méthodologie est principalement proposée pour Java Card, elle peut aussi s'adapter à d'autres technologies (par exemple Multos). Pour de plus amples détails l'article [20] est disponible en annexe C.

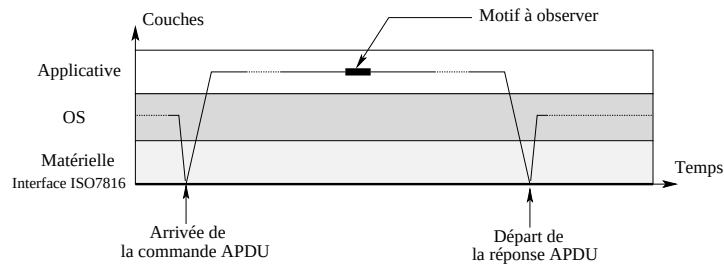


FIGURE 3.1 – Trace d'une exécution normale vue au travers des différentes couches.

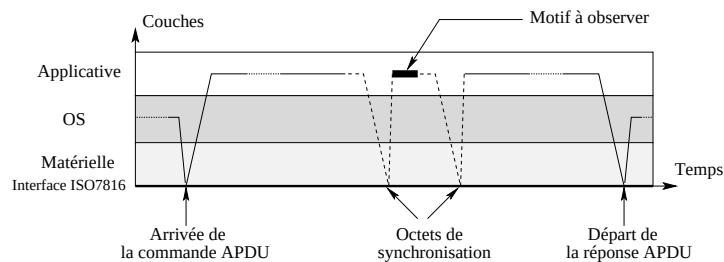


FIGURE 3.2 – Trace d'une exécution *glitchée* vue au travers des différentes couches.

L'objectif de cette méthodologie était également de construire un dictionnaire de bytécodes Java Card afin de pouvoir faire la rétro-conception d'une trace d'exécution capturée via l'observation de la consommation en courant ou des émissions électromagnétiques d'une carte Java Card. Sur ce point, je n'ai malheureusement pas abouti par manque de temps et surtout d'équipements. Pourtant ces travaux [20, 21] ont inspiré des chercheurs de la société Riscure qui ont réussi cette prouesse dans un article publié et primé à WISTP2007.

Mes autres contributions [29, 28] ont été de montrer les limites de ces processus d'évaluation et certification avec en particulier l'impossibilité pour un utilisateur final de s'assurer que le produit qu'il possède a été ou non certifié. Pour cela, en 2007, avec Pierre Dusart, nous avons proposé un certain nombre de pistes pour étendre la confiance jusqu'à l'utilisateur final. Ces travaux recoupent ceux sur les cartes multiapplicatives car il est important d'avoir confiance dans la carte dans les modèles orientés utilisateurs (UCOM et GP-CCM) où le porteur de celle-ci peut décider de son contenu.

3.2 Perspectives

Avec le développement des Physical Unclonable Functions (PUF), certaines des suggestions [29, 28] que nous avons émises deviennent possibles. En particulier comme indiqué en section 1.2, dans le cas d'une plate-forme ouverte, le composant « Trusted Environment & Execution Manager » (TEM) étant la pierre angulaire permettant d'offrir le niveau de confiance nécessaire à tous les acteurs, nous proposerons qu'il s'appuie sur les « preuves » de confiance numériques¹ apportées par les méthodologies d'évaluation et de certification sécuritaires et sur des techniques complémentaires comme celles que nous avons imaginées dans [28, 29].

Enfin, si les processus d'évaluation et de certification sécuritaires se sont longtemps cantonnés à quelques périphériques comme la carte à puce, des travaux sont en cours pour l'étendre aux capteurs dont je parlerai au chapitre 5.

1. Ces preuves numériques n'existent actuellement pas.

Seconde partie

Réseaux mobiles

Les travaux présentés dans cette seconde partie du mémoire sont à la croisée de deux termes à la mode (que j'aurai pu utiliser par facilité) : l'Internet des objets (« Internet of Things ») et les systèmes cyber-physiques (« cyber-physical systems »). Toutefois, en ce sens qu'ils interfacent les smart secure devices, vus dans la première partie, entre eux ou dans des infrastructures, j'ai préféré les définir sous le néologisme de « réseaux mobiles » présenté dans l'introduction de ce mémoire.

Mon parcours a consisté dans un premier temps à sécuriser des systèmes fixes, comme les grilles, pour aller vers des systèmes distribués, puis vers des systèmes distribués faiblement mobiles connectés sans fil (les réseaux de capteurs, les réseaux mobiles ad hoc) et enfin vers des systèmes distribués mobiles avec une connectivité sans fil pouvant être instable (les flottes de drones).

Chapitre 4

Du « grid computing » à la mobilité

Ce chapitre va introduire trois domaines connexes sur lesquels j’ai travaillé et qui illustrent ma « conversion » à la mobilité dans les systèmes distribués.

Le grid computing. Avec l’ouverture des plates-formes de calcul, le développement des réseaux et en particulier des réseaux sans fil, les besoins de sécurisation de ces plates-formes et systèmes n’ont cessé de croître. En une vingtaine d’années, de nouveaux paradigmes pour les grilles de calcul sont apparus. Ainsi les ressources de calcul, classiquement centralisées dans des grilles situées en des lieux bien définis, sont devenues, grâce aux réseaux, distribuées sur des ordinateurs situés en des lieux potentiellement inconnus. Dans ce contexte, il est difficile de faire confiance à ces nouvelles ressources de calcul, pourtant si intéressantes car gracieusement mis à disposition par leurs propriétaires.

La mobilité avec infrastructure. En parallèle, les ordinateurs sont devenus plus petits, plus portables et plus mobiles de sorte que les utilisateurs les gardent en permanence avec eux. Certains vont même jusqu’à utiliser ces ressources personnelles dans leur vie professionnelle. C’est le concept du « bring your own device » qui met parfois en danger la sécurité des organisations acceptant cette politique. En effet, dans ce contexte, les périphériques utilisés sont généralement connectés à l’infrastructure de l’entreprise et par effet de ricochet ils peuvent la mettre en péril.

La mobilité sans infrastructure. Essentiellement prévus pour les situations où aucune infrastructure n’est disponible, les réseaux mobiles ad hoc sont un concept très séduisant mais difficile à sécuriser. Bien qu’intéressants les chercheurs depuis plus de 20 ans, aujourd’hui ces réseaux ne sont quasiment jamais réellement déployés.

4.1 Contributions

Lors de ma thèse, dans le contexte d’une équipe travaillant sur les systèmes et objets distribués, j’avais proposé le développement d’une grille de calcul totalement sécurisée et dont les ressources de calcul seraient des cartes à puce [15]. Nous ne visions certes pas le domaine du calcul haute-performance et nous souhaitions simplement proposer une plate-forme prototype capable de traiter des problèmes de sécurité [17, 18, 22], de simuler un réseau mobile ad hoc (en retirant des nœuds simulés par les cartes, en les déplaçant ce qui correspond à une nouvelle topologie, etc.), etc. Ces travaux dont l’illustration se trouve en

figure 4.1 ont fait l'objet de plusieurs publications dont une [11] a été récompensée après l'obtention de mon doctorat par le seul prix attribué à eSmart2005 : celui de la meilleure technologie innovante.

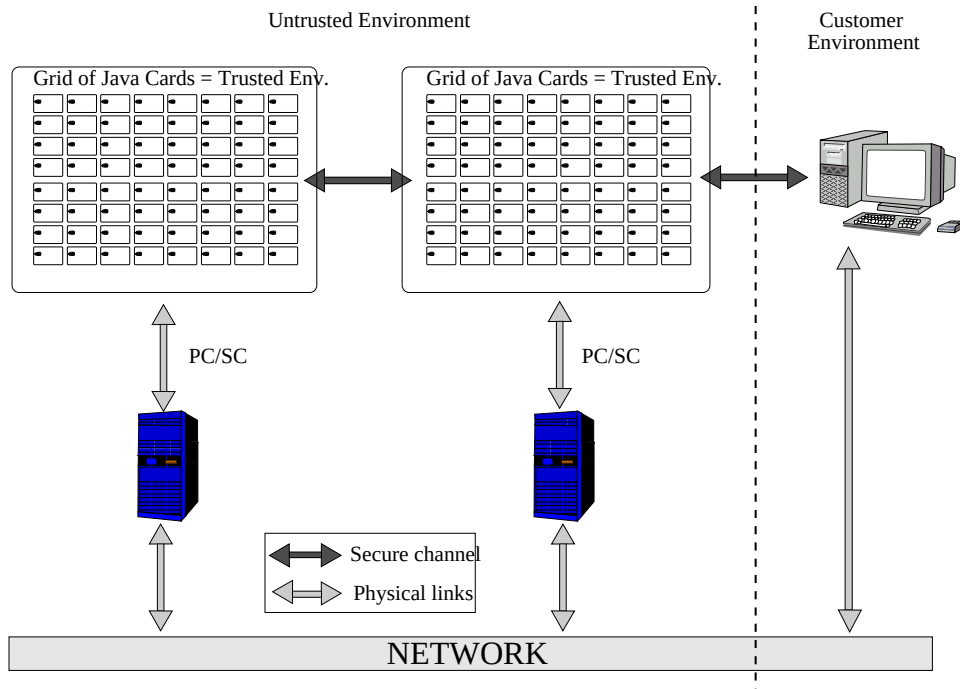


FIGURE 4.1 – Grille de calcul sécurisée basée sur Java Card.

Après ma thèse, j'ai contribué à proposer différentes évolutions de cette plate-forme. Tout d'abord, nous l'avons utilisé comme plate-forme de médiation pour faire du PIR (Private Information Retrieval) entre des entités n'ayant à priori pas confiance entre elles [16]. Nous avons ensuite fait évoluer cette plate-forme avec des collègues du Royal Holloway University of London vers la mobilité [35] en utilisant les cartes SIM embarquées sur des téléphones portables communicants via le réseau GSM comme l'illustre la figure 4.2.

C'est à ce stade que se sont arrêtés, me concernant, les travaux sur la grille. Son développement s'est toutefois poursuivie en une version multi-niveaux qui a donné lieu à plusieurs publications et à deux thèses soutenues (« Conception, mise en œuvre et validation d'un environnement logiciel pour le calcul sécurisé sur une grille de cartes à puce de type Java » pour Achraf Karray en 2008 et « Communications multi-niveaux sécurisées dans une flotte de terminaux mobiles » pour Jonathan Ouoba en 2013) sous la direction du Professeur Serge Chaumette.

Pour ma part j'ai souhaité me consacrer au domaine proche et tout aussi séduisant qu'est celui des réseaux mobiles ad hoc. Dans le type de réseaux illustré figure 4.3, lorsque l'application 1 (située sur le nœud A) souhaite communiquer avec l'application 3 (située sur le nœud C), au niveau de la couche réseau, l'échange se fait via le nœud intermédiaire B car A et C ne sont pas à portée radio. Il faut alors s'assurer que le nœud B n'est pas malveillant (par exemple qu'il n'est pas égoïste et qu'il ne cherchera pas à minimiser sa consommation en énergie en ne retransmettant pas les messages s'il n'a rien à y gagner).

Pour s'assurer de la bonne collaboration de tous les nœuds participants au réseau, nous avons introduit avec Pierre-François Bonnefoi un tiers de confiance, prenant la forme d'une carte à puce, embarqué sur chacun d'eux afin de créer un réseau de contrôle au sein

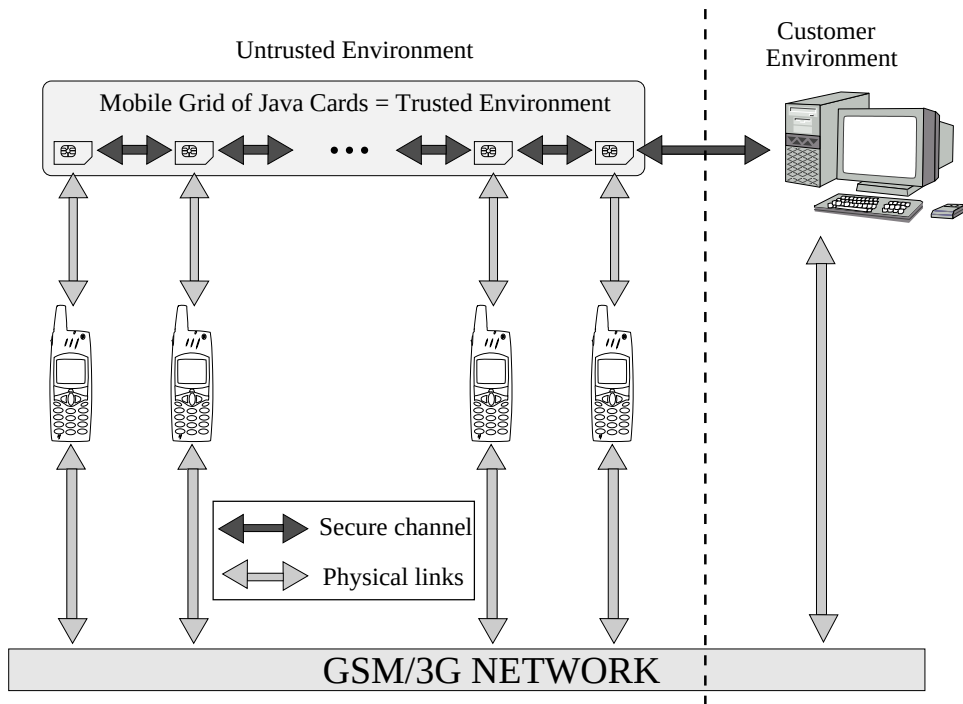


FIGURE 4.2 – Grille de calcul sécurisée et mobile basée sur Java Card.

de la plate-forme MADNESS (Mobile AD hoc Network with Embedded Secure System) [12, 10] illustrée sur la figure 4.4.

De par le projet que je développe dans ce mémoire, c'est tout naturellement que j'ai aussi contribué à un état de l'art sur les interactions entre le domaine de la carte à puce et celui du calcul distribué [23]. De manière plus anecdotique, j'ai également contribué à un protocole d'établissement de clés dans un réseau mobile ad hoc [9].

Plusieurs des travaux présentés dans ce chapitre sont disponibles en annexe D.

4.2 Perspectives

Suite à l'état de l'art [13] que nous avons rédigé sur l'opposition existant entre « sécurité » et « utilisabilité » dans les réseaux mobiles ad hoc, nous avons commencé des travaux sur une nouvelle méthode d'authentification pour permettre la création dynamique de réseaux mobiles ad hoc dans le cadre de la plate-forme MADNESS. Je suis persuadé que notre solution permettra de contribuer à leur popularisation et à une utilisation réelle de ce type de réseaux. Il est à noter que si l'utilisation de périphériques (par exemple des cartes à puce) basés sur le modèle UCOM présenté en section 1.1 n'est pas nécessaire, elle facilitera grandement l'adoption par les utilisateurs finaux de nos propositions.

Une autre perspective intéressante est développée au chapitre 6 puisque l'on peut voir ces travaux comme une instanciation « volante » de la plate-forme MADNESS. Cependant dans ce contexte, les modèles de mobilités seront différents. Les nœuds y sont plus mobiles géographiquement mais aussi plus rapides dans leurs déplacements ce qui pourra engendrer une connectivité peut être plus erratique si les nœuds ne restent pas dans une topologie d'essaim.

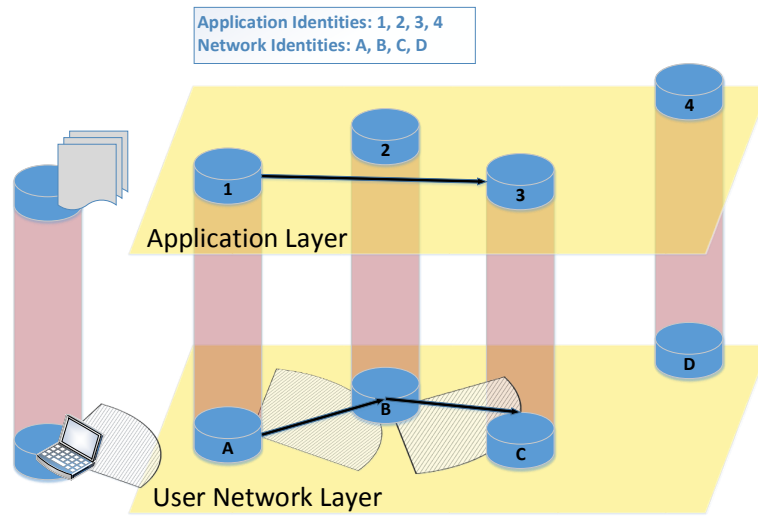


FIGURE 4.3 – Réseau mobile ad hoc classique.

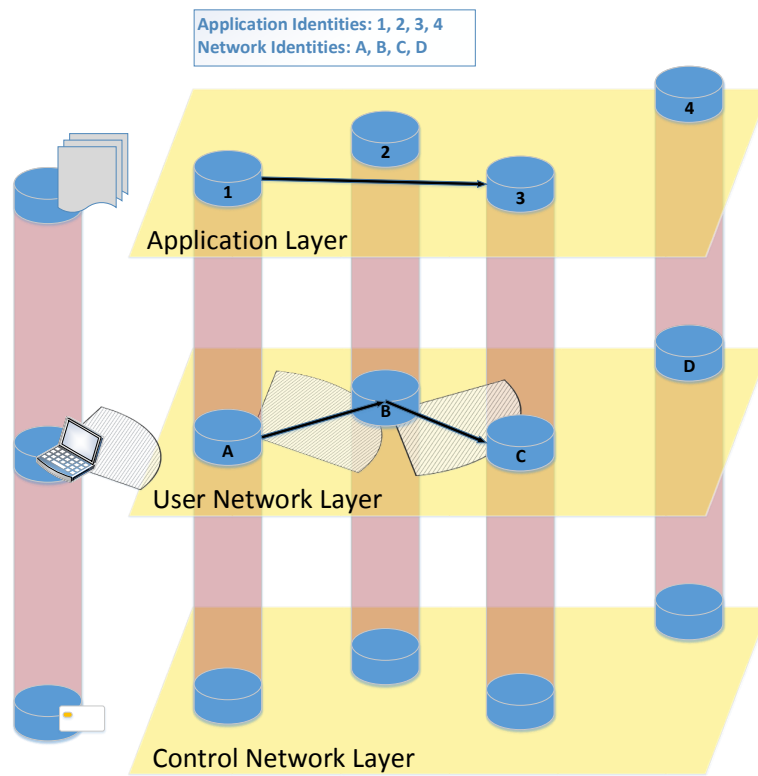


FIGURE 4.4 – Réseau mobile ad hoc sécurisé avec les cartes.

Chapitre 5

Les réseaux de capteurs

Les réseaux de capteurs (et d'actionneurs) sont un sujet en plein essor car ils permettent d'interfacer le monde physique et le monde informatique (ce sont des systèmes cyber-physiques). Les nouvelles technologies de communications sans fil, les nouvelles méthodes pour économiser et récupérer l'énergie mais également les différents capteurs possible grâce aux développements des MEMS (MicroElectroMechanical Systems) font des réseaux de capteurs un domaine pouvant s'appliquer aussi bien à des applications civiles (par exemple la domotique dans laquelle ils peuvent servir à déclencher des scénarii, l'industrie dans laquelle ils peuvent faire des mesures de concentration de polluant) que militaires.

5.1 Contributions

Mes contributions dans ce domaine sont pour l'instant mineures puisqu'elles se résument à deux chapitres de livre. Le premier [24], disponible en annexe E, présente un état de l'art des réseaux de capteurs, en particulier en terme de sécurité, alors que le second [8] explique comment prendre en main des plates-formes pour former un réseau capteurs/actionneurs. Je contribue également au domaine par un pilotage de la recherche au travers de numéros spéciaux de journaux.

5.2 Perspectives

Si ce domaine m'intéresse depuis peu (fin 2013), il est situé à la croisée des chemins des smart secure devices et des réseaux mobiles. Aussi je vois la possibilité de déployer une plate-forme assez semblable à MADNESS pour sécuriser un réseau de capteurs. En outre, je suis convaincu qu'une plate-forme pour capteurs disposant d'une architecture adoptant le modèle UCOM permettrait d'atteindre un haut niveau de sécurité. Enfin, je pense que mon expérience du monde de l'évaluation et de la certification sécuritaires me permettra de contribuer aux travaux qui commencent tout juste à émerger concernant la certification sécuritaire des capteurs.

Chapitre 6

Les flottes de drones

Les drones sont de plus en plus utilisés dans des applications militaires et civiles. Dans les applications civiles, ils peuvent, par exemple être utilisés pour la surveillance des incendies de forêts, la recherche de personnes disparues dans des avalanches. Cependant, la plupart des drones étant petits, ils ne peuvent pas transporter d'équipements lourds (par exemple, des capteurs lourds ou plusieurs petits capteurs en même temps). Par conséquent, les drones intègrent souvent seulement quelques capteurs dédiés et c'est en collaborant ensemble qu'ils forment un essaim de drones simples capable d'offrir des fonctionnalités complexes. De plus, voler en essaim est utile et permet de couvrir des zones géographiques plus étendues. Comme ces vols nécessitent une collaboration entre les drones, ceux-ci communiquent d'une manière similaire à celle des nœuds d'un réseau mobile ad hoc (MANET) ou d'un Delay/Disruptive Tolerant Network (DTN) à cause de la connectivité potentiellement erratique. Par conséquent, comme on peut le constater sur la figure 6.1, les drones sont exposés à des problèmes de sécurité similaires à ceux adressés dans le chapitre 4 avec la plate-forme MADNESS.

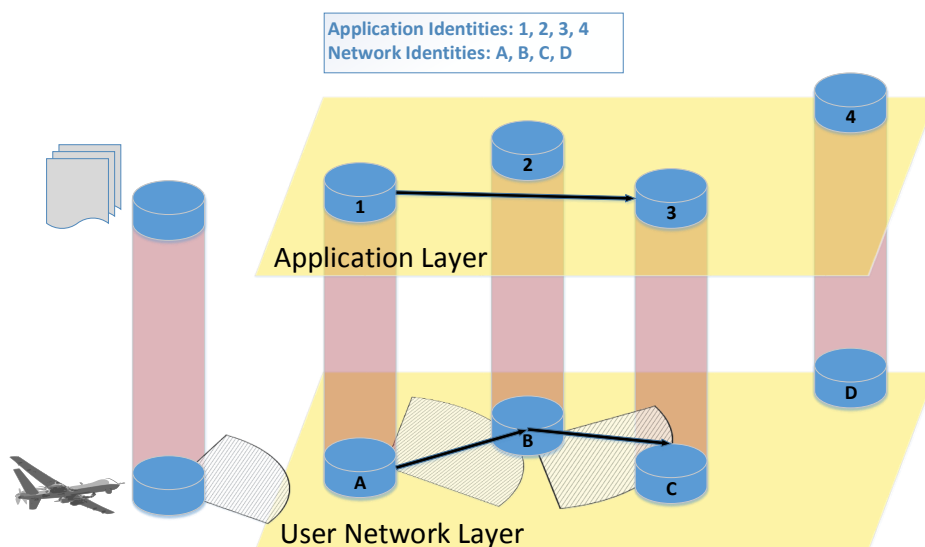


FIGURE 6.1 – Flotte de drones.

S'il est vrai que dans certains contextes (comme les applications civiles) les problématiques de sécurité pourraient sembler insignifiantes (ou tout du moins une attaque pourrait ne pas avoir un impact majeur), dans les applications militaires, il est essentiel d'y répondre. En effet, dans ce contexte, les drones ont besoin de stocker de façon sécurisée des données comme le plan de vol pour la mission, des photos, les coordonnées des points d'intérêt (positions ennemis ou alliés). Ce sont là des données précieuses pour l'adversaire sur les champs de bataille modernes.

6.1 Contributions

Dans nos travaux de positionnement [1] (disponible en annexe F) j'ai introduit un modèle de l'adversaire dans lequel ce dernier dispose d'un potentiel d'attaque élevé. J'ai montré que ce modèle qui prend en compte la capture d'un drone pour lui faire subir des attaques (Simple Power Analysis, Differential Power Analysis, Fault Attack, Timing Attack, etc.) visant à révéler les secrets qu'il contient, est justifié et que pour résister à ces menaces il faut que les drones embarquent un élément de sécurité tamper-resistant. Il ressort de l'analyse que nous avons conduite qu'il serait intéressant de disposer d'un élément de sécurité mêlant les caractéristiques des cartes à puce suivant le modèle UCOM et des RFID actifs. Ceci m'a conduit à proposer un « Active Radio Frequency Smart Secure Device » (ARFSSD) actuellement en cours de développement et illustré figure 6.2.

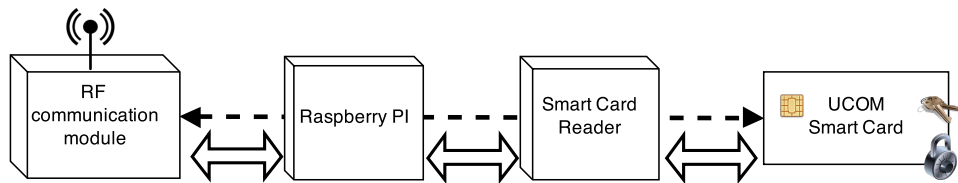


FIGURE 6.2 – Proposition de Secure Element : ARFSSD.

Une fois munis des dispositifs ARFSSD, les drones devraient former une plate-forme volante sécurisée permettant d'offrir les garanties nécessaires. Cette plate-forme, présentée figure 6.3 sera déployée dès que les dispositifs seront prêts.

6.2 Perspectives

Je suis actuellement en train de rédiger un état de l'art très complet des différentes menaces de sécurité dans une flotte de drone. J'ai également entamé une collaboration afin de mettre au point un algorithme d'inondation multi-sauts adapté à ce type de réseau.

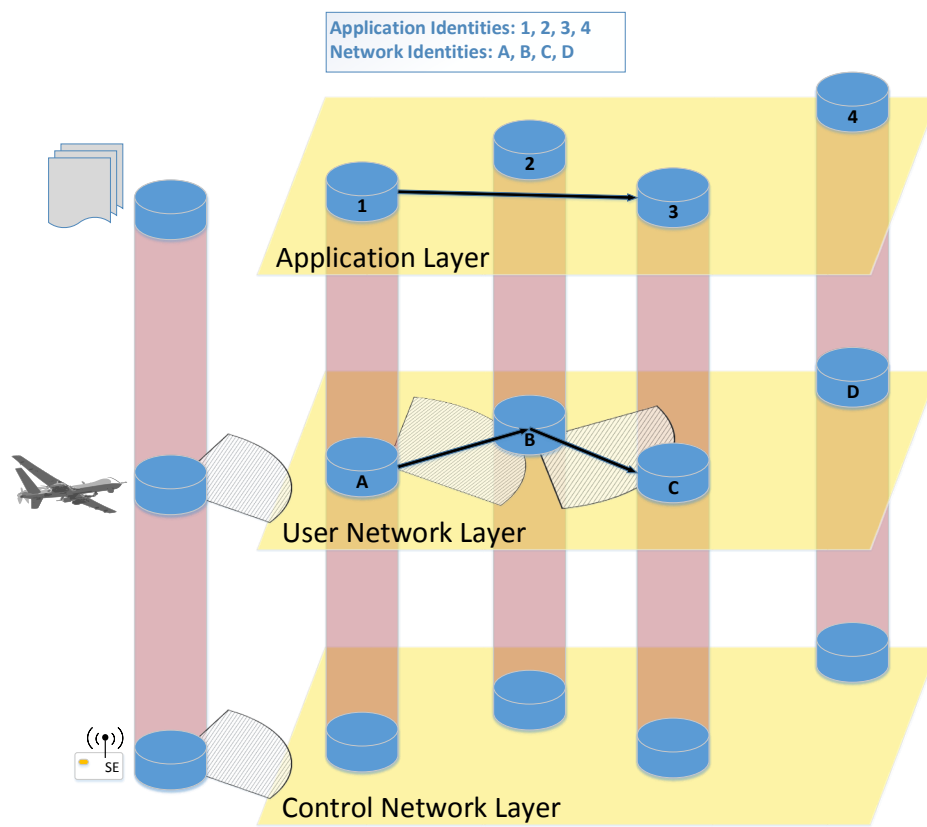


FIGURE 6.3 – Flotte de drones sécurisée avec les dispositifs ARFSSD.

Conclusion

Comme je pense l'avoir montré à chaque chapitre de ce mémoire, de nombreuses perspectives de recherche existent dans mon projet *Sécurité et interactions des « smart secure devices » et des « réseaux mobiles »*. Ces perspectives sont souvent imbriquées et l'aboutissement de l'une d'elles sera un pas en avant sur le chemin menant à la résolution des autres.

J'ai commencé ce mémoire par une citation de ce grand homme qu'était Périclès : « *Il n'est point de bonheur sans liberté, ni de liberté sans courage.* ». Elle mérite quelques explications.

La rédaction d'un mémoire d'habilitation à diriger des recherches est avant tout une épreuve personnelle. Elle exige rigueur et courage. Rigueur dans la présentation d'une décennie des travaux de recherche. Courage, car l'écriture est certes faite de moments de satisfaction, mais aussi de moments de doutes, de moments où l'on se sent coupable des trop nombreuses heures passées loin de sa famille. En somme, c'est une épreuve sur la vie quotidienne pour gagner en liberté scientifique, en liberté d'esprit, voire même en liberté administrative. En un mot une épreuve pour se rapprocher du bonheur qu'évoque Périclès.

J'aurai certes pu me limiter à concaténer mes travaux, mais cela n'aurait été que très peu satisfaisant pour moi. Je pense sincèrement que cette épreuve était nécessaire, tant d'un point de vue personnel pour faire un bilan, que d'un point de vue collectif en raison de la dimension symbolique que revêt l'obtention du diplôme d'habilitation à diriger des recherches. J'espère au terme de cette conclusion franchir avec succès la ligne d'arrivée qui me sépare de cette liberté et de ce bonheur tant désiré afin de poursuivre librement ma recherche en collaborant avec les personnes que j'apprécie.

Bibliographie

- [1] Raja Naeem Akram, Pierre-François Bonnefoi, Serge Chaumette, Konstantinos Markantonakis, and Damien Sauveron. Improving Security of Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements - A Position Paper. In *2nd AE-TOS international conference on "Research challenges for future RPAS/UAV systems"*, Bordeaux, France, September 2014.
- [2] Raja Naeem Akram, Pierre-François Bonnefoi, Pierre Dusart, Konstantinos Markantonakis, and Damien Sauveron. A Set of Efficient Privacy Protection Enforcing Lightweight Authentication Protocols for Low-cost RFID Tags. *Information Sciences*, Submitted.
- [3] Raja Naeem Akram, Hsiao-Hwa Chen, Javier Lopez, Damien Sauveron, and Laurence T. Yang. Security, Privacy and Trust of the User-centric Solutions. *Future Generation Computer Systems*, 2016.
- [4] Raja Naeem Akram, Konstantinos Markantonakis, and Damien Sauveron. Collaborative and Ubiquitous Consumer Oriented Trusted Service Manager. In *13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-14)*, Beijing, China, September 2014. IEEE Computer Society.
- [5] Raja Naeem Akram, Konstantinos Markantonakis, and Damien Sauveron. A Novel Consumer-Centric Card Management Architecture and Potential Security Issues. *Information Sciences*, (Special Issue on Security and Privacy Information Technologies and Applications for Wireless pervasive Computing Environments), Minor Revision.
- [6] Raja Naeem Akram, Konstantinos Markantonakis, and Damien Sauveron. Feature Interaction Problems in Smart Cards with Dynamic Application Lifecycle and their Countermeasures. In *11th International Conference on Information Security Practice and Experience (ISPEC 2015)*, Submitted.
- [7] Raja Naeem Akram, Konstantinos Markantonakis, and Damien Sauveron. Recovering from a Lost Wallet - A Smart Card's Perspective. *Pervasive and Mobile Computing*, Submitted.
- [8] Jérémie Albert, Lionel Barrère, Serge Chaumette, and Damien Sauveron. Wireless Sensors (Languages/Programming/Developments Tools/Examples). In Konstantinos Markantonakis and Keith Mayes, editors, *Secure Smart Embedded Devices, Platforms and Applications*, chapter 24, pages 541–564. Springer, 2014.
- [9] Ioannis G. Askoxylakis, Damien Sauveron, Konstantinos Markantonakis, Theodore Tryfonas, and Apostolos Traganitis. A Body-Centered Cubic Method for Key Agreement in Dynamic Mobile Ad Hoc Networks. In *Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08. Second International Conference on*, pages 193–202, Cap Esterel, France, August 2008. IEEE.
- [10] Ève Atallah, Pierre-François Bonnefoi, Céline Burgod, and Damien Sauveron. Mobile Ad Hoc Network with Embedded Secure System. In *Ambient Intelligence Developments Conference*, Nice - Sophia-Antipolis, France, September 2006.

- [11] Ève Atallah, Franck Darrigade, Serge Chaumette, Achraf Karray, and Damien Sauveron. A Grid of Java Cards to Deal with Security Demanding Application Domains. In *Proceedings of the 6th e-Smart International Conference (e-Smart 2005)*, Nice - Sophia-Antipolis, France, September 2005.
- [12] Pierre-François Bonnefoi, Patrick Pouligeas, and Damien Sauveron. MADNESS : A Framework Proposal for Securing Work in Ad Hoc Networks. In HW Chu, MJ Savoie, and B Sanchez, editors, *3rd International Conference on Computing, Communications and Control Technologies, Vol 1, Proceedings*, pages 96–100, Austin, Texas, USA, July 2005.
- [13] Pierre-François Bonnefoi, Damien Sauveron, and Jong Hyuk Park. MANETS : AN EXCLUSIVE CHOICE BETWEEN USE AND SECURITY? *Computing and Informatics*, 27(5) :799–821, 2008.
- [14] Samia Bouzeffrane, Damien Sauveron, Julien Cordry, and Khaled Garri. Mise en œuvre d’une application, choix de solutions, performances. *Les cartes à puce*, pages 201–254, 2013.
- [15] Serge Chaumette, Pascal Grange, Achraf Karray, Damien Sauveron, and Pierre Vignéras. Secure distributed computing on a Java Card Grid. In *Proceedings - 19th IEEE International Parallel and Distributed Processing Symposium, IPDPS 2005. 7th International Workshop on Java for Parallel and Distributed Computing*, volume 2005, Denver, Colorado, USA, April 2005. IEEE.
- [16] Serge Chaumette, Achraf Karray, and Damien Sauveron. Gestion de la Sécurité pour l’Extraction Parallèle Distribuée des Connaissances. In *Proceedings of the 6èmes Journées Francophones Extraction et Gestion de Connaissances - EGC 2006*, pages 31–40, Lille, France, January 2006.
- [17] Serge Chaumette, Achraf Karray, and Damien Sauveron. Secure Collaborative and Distributed Services in the Java Card Grid Platform. In Waleed W Smari and William K McQuay, editors, *Proceedings of the 2006 International Symposium on Collaborative Technologies and Systems, CTS 2006. Workshop on Collaboration and Security (COLSEC’06)*, volume 2006, pages 56–63, Las Vegas, NV, USA, May 2006. IEEE.
- [18] Serge Chaumette, Achraf Karray, and Damien Sauveron. The Software Infrastructure of a Java Card Based Security Platform for Distributed Applications. *Security in Information Systems, Proceedings of the 4th International Workshop on Security in Information Systems, WOSIS 2006, In conjunction with ICEIS 2006, Paphos, Cyprus, May 2006*, pages 101–114, May 2006.
- [19] Serge Chaumette and Damien Sauveron. Modèles de mémoire en Java Card. Introduction du concept de pré-persistance. In *MAJECSTIC’04 (MANifestation des JEunes Chercheurs STIC)*., page 8p., Calais, France, October 2004.
- [20] Serge Chaumette and Damien Sauveron. An efficient and simple way to test the security of java cards. *Security in Information Systems, Proceedings of the 3rd International Workshop on Security in Information Systems, WOSIS 2005, In conjunction with ICEIS2005, Miami, USA, May 2005*, pages 331–341, May 2005.
- [21] Serge Chaumette and Damien Sauveron. Some security problems raised by open multiapplication smart cards. In *Proceedings of the 10th Nordic Workshop on Secure IT-systems (NordSec 2005)*, pages 1–12, Tartu, Estonia, October 2005.
- [22] Serge Chaumette and Damien Sauveron. A High Level Security Framework for the Grid : the Java Card Grid Testbed. *20th European Conference on Modelling and Simulation : Modelling Methodologies and Simulation Key Technologies in Academia and Industry, ECMS 2006. The 2006 High Performance Computing & Simulation (HPC&S) Conference*, pages 740–743, May 2006.

- [23] Serge Chaumette and Damien Sauveron. Smart cards and remote computing : Interaction or convergence ? *Information Security Technical Report*, 14(2) :101–110, May 2009.
- [24] Serge Chaumette and Damien Sauveron. Wireless Sensor Nodes. In Konstantinos Markantonakis and Keith Mayes, editors, *Secure Smart Embedded Devices, Platforms and Applications*, chapter 14, pages 335–350. Springer, 2014.
- [25] Serge Chaumette, Damien Sauveron, Stéphanie Eonet, and Jonathan Gimenez. Evaluation and comparison of the PRNG of different brands of Java Cards. - Framework and first results. In *Proceedings of the 8th e-Smart International Conference (e-Smart 2007)*, Sophia Antipolis, France, September 2007.
- [26] Serge Chaumette, Damien Sauveron, and Achraf Karray. Extended Secure Memory for a Java Card in the Context of the Java Card Grid project. In *Proceedings of the 11th Nordic Workshop on Secure IT-systems (NordSec 2006)*, pages 1–13, Linköping, Sweden, October 2006.
- [27] Hung-Yu Chien and Chen-Wei Huang. A Lightweight Authentication Protocol for Low-Cost RFID. *Journal of Signal Processing Systems*, 59(1) :95–102, 2010.
- [28] Pierre Dusart and Damien Sauveron. Which Trust Can Be Expected of the Common Criteria Certification at End-User Level ? In *Future Generation Communication and Networking (FGCN 2007)*, volume 2, pages 423–428, Jeju Island, Kora, December 2007. IEEE.
- [29] Pierre Dusart, Damien Sauveron, and Tai-hoon Kim. Some limits of Common Criteria certification. *International Journal of Security and Its Applications*, 2(4) :11–20, 2008.
- [30] Gerhard Hancke, Aikaterini Mitrokotsa, Reihaneh Safavi-Nain, and Damien Sauveron. Recent Advances in Physical-Layer Security. *Computer Networks*, 2016.
- [31] Young-Sik Jeong, Hamid Reza Arabnia, James J. Park, Han-Chieh Chao, Se Dong Min, and Damien Sauveron. Wellness Technologies and Services for Future Life Care. *The Scientific World Journal*, 2015.
- [32] Young-Sik Jeong, Damien Sauveron, and Jong Hyuk Park. Advanced security technologies and services for future computing environments. *Computer Journal*, 56(10) :1151–1153, August 2013.
- [33] Konstantinos Markantonakis, Keith Mayes, Damien Sauveron, and Ioannis G. Askoxyllakis. Overview of Security Threats for Smart Cards in the Public Transport Industry. In *e-Business Engineering (ICEBE), 2008 IEEE International Conference on*, pages 506–513, Xi'an, China, October 2008. IEEE.
- [34] Konstantinos Markantonakis, Keith Mayes, Michael Tunstall, Damien Sauveron, and Fred Piper. Smart Card Security. *Computational Intelligence in Information Assurance and Security*, 57 :201–233, 2007.
- [35] Keith Mayes, Serge Chaumette, Konstantinos Markantonakis, and Damien Sauveron. The Mobile Java Card Grid Project. In *Proceedings of 7th e-Smart International Conference (e-smart 2006)*, Nice - Sophia-Antipolis, France, September 2006.
- [36] Nele Mentens, Damien Sauveron, Shiuh-Jeng Wang, and Isaac Woungang. Lightweight and Energy-Efficient Security Solutions for Mobile Computing Devices. *IET Information Security*, 2016.
- [37] James J.(Jong Hyuk) Park, Shiuh-Jeng Wang, and Damien Sauveron. Security technologies and applications for convergence environments. *Security and Communication Networks*, 5(3) :249–251, March 2012.
- [38] Jong Hyuk Park, Han-Chieh Chao, Damien Sauveron, and Yang Xiang. Intelligent Internet Computing : Applications and Security Systems. *Journal of Internet Technology*, 11(3) :297–298, May 2010.

- [39] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. Advances in Ultralightweight Cryptography for Low-Cost RFID Tags : Gossamer Protocol. In Kyo-Il Chung, Kiwook Sohn, and Moti Yung, editors, *Information Security Applications*, volume 5379 of *Lecture Notes in Computer Science*, pages 56–68. Springer Berlin Heidelberg, Jeju Island, Korea, September 2009.
- [40] Bart Preneel, Jongsung Kim, and Damien Sauveron. Advanced theory and practice for cryptography and future security. *Mathematical and Computer Modelling*, 55(1-2) :1–2, January 2012.
- [41] Seungmin Rho, Damien Sauveron, and Weifeng Chen. Advanced signal processing and HCI issues for interactive multimedia services. *Multimedia Tools and Applications*, pages 1–5, September 2013.
- [42] Seungmin Rho, Damien Sauveron, and Konstantinos Markantonakis. Advanced semantic and social multimedia technologies for future computing environment. *Multimedia Tools and Applications*, 64(2) :219–225, 2013.
- [43] Damien Sauveron. *Étude et réalisation d'un environnement d'expérimentation et de modélisation pour la technologie Java Card. Application à la sécurité*. Thèse de doctorat - phd thesis, LaBRI, Université Bordeaux 1, December 2004.
- [44] Damien Sauveron. Smart Card Reader APIS. In Keith E. Mayes and Konstantinos Markantonakis, editors, *Smart Cards, Tokens, Security and Applications*, chapter 12 and App, pages 277–293. Springer, 2008.
- [45] Damien Sauveron. Multiapplication smart card : Towards an open smart card ? *Information Security Technical Report*, 14(2) :70–78, May 2009.
- [46] Damien Sauveron, Konstantinos Markantonakis, and Christos Verikoukis. Security and resilience for smart devices and applications. *EURASIP Journal on Wireless Communications and Networking*, 2014(1) :123, July 2014.
- [47] Boyeon Song and Chris J. Mitchell. RFID Authentication Protocol for Low-cost Tags. In *Proceedings of the First ACM Conference on Wireless Network Security*, WiSec '08, pages 140–147, New York, NY, USA, 2008. ACM.
- [48] Michael Tunstall, Konstantinos Markantonakis, Damien Sauveron, and Keith Mayes. Smart Cards : Communication Protocols and Applications. *Handbook of Computer Networks*, 3 :251–268, 2007.
- [49] Sang-Soo Yeo, Hangbae Chang, Weifeng Chen, Naveen K. Chilamkurti, Seungmin Rho, and Damien Sauveron. Advanced Service Technology and Application in Smart Sensor Networks. *International Journal of Distributed Sensor Networks*, 2015.
- [50] Sang-Soo Yeo, Jong Hyuk Park, Kirk P. Arnett, Kim Keung Lai, Damien Sauveron, and Toshihiro Tabata. Advances and Challenges of Security in Web and Pervasive Computing Environments. *International Journal of Security and Its Applications*, 2008.

Annexes

Annexe A

Cartes multiapplicatives

A.1 Collaborative and Ubiquitous Consumer Oriented Trusted Service Manager

ANNEXE A. CARTES MULTIAPPLICATIVES

A.2 A Novel Consumer-Centric Card Management Architecture and Potential Security Issues

A.3 Feature Interaction Problems in Smart Cards with Dynamic Application Lifecycle and their Counter-measures

A.4 Recovering from a Lost Digital Wallet : A Smart Cards Perspective Extended Abstract

A.5 Some security problems raised by open multiapplication smart cards

A.6 Multiapplication Smart Card : Towards an Open Smart Card ?

Annexe B

Protocoles RFID

B.1 A Set of Efficient Privacy Protection Enforcing Lightweight Authentication Protocols for Low- cost RFID Tags

ANNEXE B. PROTOCOLES RFID

Annexe C

Évaluation sécuritaire

C.1 An efficient and simple way to test the security of Java Cards

ANNEXE C. ÉVALUATION SÉCURITAIRE

Annexe D

Du Grid à la Mobilité

D.1 A Grid of Java Cards to Deal with Security Demanding Application Domains

ANNEXE D. DU GRID À LA MOBILITÉ

D.2 The Software Infrastructure of a Java Card Based Security Platform for Distributed Applications

D.3 Secure Collaborative and Distributed Services in the Java Card Grid Platform

D.4 Smart cards and remote computing : Interaction or convergence ?

D.5 MANETS : An Exclusive Choice Between Use And Security?

Annexe E

Réseaux de capteurs

E.1 Wireless Sensor Nodes

ANNEXE E. RÉSEAUX DE CAPTEURS

Annexe F

Flottes de drones

F.1 Improving Security of Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements. A Position Paper

ANNEXE F. FLOTTES DE DRONES

Annexe G

**CV, projet scientifique, liste
complète des publications et
rapport d'activités 2009-2014**