SECURITE DES SYSTEMES EMBARQUES

Animateurs : Marie Lise Flottes, LIRMM, Giorgio Di Natale, LIRMM, Guy Gogniat, Lab-STICC

Contributeurs : Lilian Bossuet, LaHC, Jean-Luc Danger, Télécom ParisTech, Giorgio Di Natale, LIRMM, Jean-Max Dutertre, ENSMSE, Viktor Fischer, LaHC, Marie-Lise Flottes, LIRMM, Guy Gogniat, Lab-STICC, Sylvain Guilley, Télécom ParisTech, David Hely, LCIS, Philippe Maurine, LIRMM, Renaud Pacalet, Télécom ParisTech, Bruno Robisson, CEA, Arnaud Tisserand, IRISA, Lionel Torres, LIRMM.

A. DESCRIPTION

1. Définition

La sécurité des systèmes embarqués couvre de nombreuses problématiques liées à la protection des circuits et des données qu'ils manipulent. Il s'agit i) d'optimiser l'implémentation d'algorithmes cryptographiques afin de dépasser les limites actuelles en termes de débit, surface, consommation et résistance aux attaques ; ii) de développer des bancs d'évaluation sécuritaire afin d'approfondir la compréhension des mécanismes d'attaques matérielles et des contremesures associées ; iii) de développer de nouvelles briques sécuritaires matérielles (TRNG[1], PUF[2]) en prenant en compte les différents supports d'exécution (ASIC, FPGA, RFID,…), iv) de développer des outils d'aide à la conception afin de rendre systématique la réalisation d'architecture matérielle intégrant des mécanismes de protection, v) de développer des solutions permettant au niveau matériel de protéger la propriété intellectuelle et la contrefaçon de circuits électroniques, et vi) d'avoir une approche globale de la sécurité depuis le niveau technologique jusqu'au niveau système. Les mesures visant à renforcer la sécurité ont pour point commun la nécessité de leurs mises en œuvre au sein de composants matériels ayant de fortes contraintes d'implémentation.

2. Périmètre

La volonté au sein du thème « Sécurité des systèmes embarqués » est d'adresser les différentes facettes de la problématique sécuritaire des composants matériels. Cette problématique est par essence pluridisciplinaire ; le développement de solutions faisant appel à des compétences multiples : cryptographie, informatique, électronique, physique. Aujourd'hui, les solutions purement informatiques, souvent qualifiées de logicielles, montrent leurs limites dans le cadre des systèmes embarqués où les contraintes de surface, vitesse, consommation,… sont particulièrement fortes. De même, les réponses purement mathématiques (cryptographie) sont menacées par la mise en œuvre des algorithmes proposés sur des cibles technologiques logicielle ou matérielle. Enfin, la physique apporte des avantages (sources d'aléa) et des inconvénients (fuite d'information) qui doivent être pris en compte lors de la conception de systèmes protégés. Il est donc nécessaire d'appréhender la dimension matérielle lors du développement des mécanismes de protection des systèmes électronique. C'est clairement cette dimension qui est adressée dans le thème « Sécurité des systèmes embarqués ». Des focus sur les bancs d'évaluation sécuritaires, sur les contremesures matérielles, sur les briques cryptographiques, sur les architectures de système sur puce,… sont au cœur des problématiques adressées.

3. Mots clés

Attaques par canaux auxiliaires, attaques par injection de fautes, bancs d'évaluation sécuritaire, contremesures, crypto-processeur, opérateurs cryptographiques, architecture matérielle et logicielle sécurisée, TRNG, PUF, outils de conception, RFID, modélisation, caractérisation et preuve des attaques et des contremesures, sécurité des FPGA, Test et sécurité, contrefaçon

[1] *True Random Number Generator*

[2] *Physically Unclonable Function*

4. 2020 : The Big Picture

Les systèmes embarqués se déploient chaque jour davantage dans notre quotidien et sont de plus en plus caractérisés par des capacités à communiquer avec leur environnement comme l'illustre la Figure 1. Par ailleurs, ces systèmes contiennent de façon croissante des informations critiques ou sont amenés à gérer des systèmes critiques. Leur protection devient donc un enjeu de société majeur.

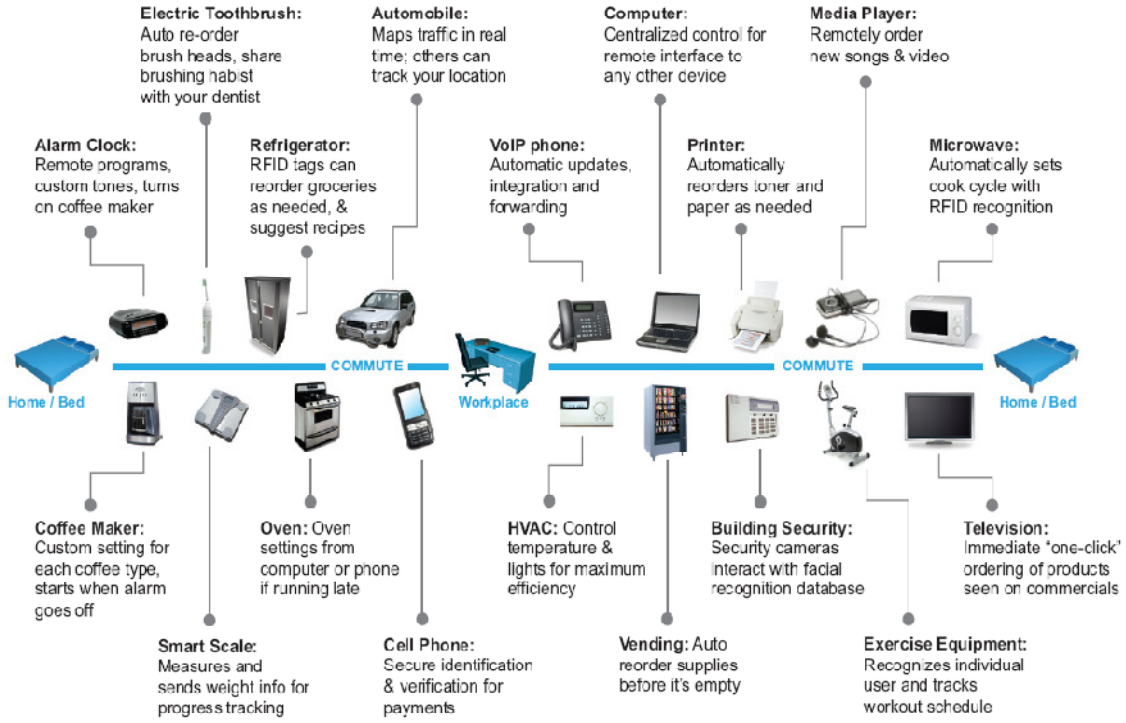

Figure 1 : Multiplication des systèmes embarqués communicants (source : Attacks on Mobile and Embedded Systems – Five important trends, June 20, 2011, Mocana Corporation https://www.mocana.com/)

Cette dernière décennie a vu se multiplier les attaques contre les systèmes embarqués compromettant ainsi leur potentielle diffusion à plus grande échelle. En parallèle, de nombreuses protections ont été développées par exemple pour les attaques en faute et par observation et à tous les niveaux d'abstraction et pour différents types de circuits (FPGA, ASIC, GPP,...). Il existe également, ici et là, des bribes d'outils aidant à la conception de circuits sécurisés. Même si l'ensemble de ces travaux ont permis l'introduction sur le marché de circuits très sécurisés (généralement par combinaison de contremesures), on est encore très loin de l'optimal. Il est donc indispensable de réfléchir et de proposer des méthodologies, des technologies et des outils permettant de mieux mesurer la dimension sécuritaire des systèmes embarqués. Au niveau des mécanismes de protection, même s'il existe des tentatives éparses, il n'y a pas de consensus autour d'outils et de métriques permettant de caractériser aussi « scientifiquement » que possible leur intégration dans les systèmes. Aujourd'hui, cette intégration reste sous optimale. Au niveau des outils de conception de circuits sécurisés, très peu de travaux existent et il n'y a pas d'outils reconnus (en dehors de la mise en œuvre de quelques techniques intéressantes comme la logique asynchrone). Au niveau des bancs d'évaluation sécuritaire, l'approche actuelle est encore très empirique. Il existe quelques plateformes commerciales (CRI, Rescure, Secure-IC,…) mais il reste encore très difficile d'évaluer les menaces réelles. La prochaine décennie correspond donc à un tournant au niveau de la diffusion des systèmes embarqués. Les évènements récents montrent qu'il existe encore de nombreux défis afin de pouvoir garantir la protection des systèmes, des données qu'ils véhiculent et des échanges d'informations qui y sont associés. La dimension matérielle des systèmes électronique ne peut être ignorée et doit au contraire être renforcée pour offrir aux utilisateurs un environnement de confiance performant.

B. ACTEURS

1. Acteurs européens hors France

Université de Cambridge en Angleterre, Université Catholique de Louvain en Belgique, Katholieke Universiteit Leuven en Belgique, Ruhr-Universität Bochum en Allemagne, Université de Lugano en Suisse, Université de Graz en Autriche, …

2. Acteurs internationaux hors Europe

Université du Massachusetts, Amherst aux Etats-Unis, Université George Mason, Fairfax aux Etats-Unis, Virginia Tech, Blacksburg aux Etats-Unis, National Institute of Advanced Industrial Science and Technology au Japon, …

3. Acteurs académiques français

Laboratoires avec leurs points forts :

- Attaques par canaux auxiliaires
- Attaques par injection de fautes
- Contremesures
- Bancs d'évaluation sécuritaire
- Cryptoprocesseurs
- Opérateurs cryptographiques
- Architecture matérielle et logicielle sécurisée
- TRNG, PUF, RFID
- Sécurité des FPGA
- Test et sécurité
- Contrefacon, clonage

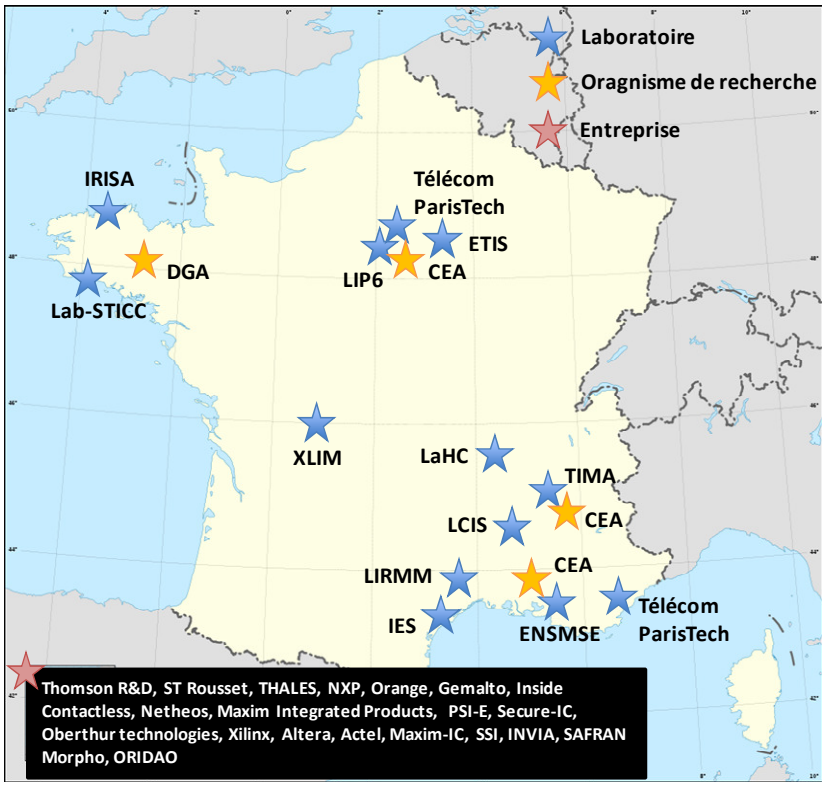

Figure 2 : Acteurs au niveau national

Laboratoires : LIRMM, IES, LCIS, ENSMSE, TIMA, Télécom ParisTech, LaHC, XLIM, LIP6, ETIS, IRISA, Lab-STICC, …

Organismes de recherche : CEA (LIST, LETI), DGA, …

Entreprises : Thomson R&D, ST Rousset, THALES, NXP, Orange, Gemalto, Inside Contactless, Netheos, Maxim Integrated Products, PSI-E, Secure-IC, Oberthur technologies, Xilinx, Altera, Actel, Maxim-IC, SSI, INVIA, SAFRAN Morpho, ORIDAO, …

4. Taille de la communauté académique française

- Nombre d'équipes académiques en France : environ une quinzaine, de tailles variées
- Nombre total de chercheurs et enseignant-chercheurs dans ces équipes : entre 30 et 40
- Nombre total de doctorants dans ces équipes : entre 50 à 60

C. DEFIS

1. DEFIS 1 : Attaques par canaux auxiliaires, par injection de fautes et contremesures

Les attaques par canaux auxiliaires et par injection de fautes correspondent à des menaces critiques contre les systèmes embarqués étant donné leur très fort potentiel d'extraction d'informations secrètes et critiques. Aujourd'hui, beaucoup de travaux restent relativement « empiriques » et il devient essentiel de mieux comprendre et surtout formaliser les mécanismes d'attaques et de contremesures. Plusieurs points importants apparaissent clairement aujourd'hui :

A) Développer un environnement de conception de circuits sécurisés

- Cet environnement doit être constitué d'outils de conception assistée par ordinateur (« CAD ») standards mais équipés (avec des « add ons ») pour simuler les phénomènes

physiques qui permettent les attaques, pour tester formellement des propriétés sécuritaires (preuve) et pour ajouter (semi)-automatiquement des protections au circuit. Ces outils devront être appliqués à tous les niveaux d'abstraction (physique, logique, architectural, algorithmique,…). Notons que dans le cas particulier des attaques en fautes, les contremesures à mettre en œuvre au niveau porte, architectural et opérationnel s'apparentent aux techniques développées dans le cadre du thème « test et Fiabilité » mais doivent être adaptées au contexte de la sécurité matérielle pour tenir compte de phénomènes d'erreurs liés à des fautes induites par l'attaquant et non « naturelles ».

- Cet environnement s'articule autour de bancs de « caractérisation » permettant de modifier le comportement du circuit ou de mesurer les modifications de l'environnement créées par ce dernier lorsqu'il fonctionne (comme le ferait un attaquant). Il est également important de définir une configuration de bancs « consensuelle » afin de mieux partager les informations et les avancées obtenues.
- Cet environnement doit posséder des outils d'« extraction d'information » qui, à partir des données obtenues par mesure ou simulation, extraient (par exemple, à l'aide de techniques cryptanalytiques) les informations susceptibles d'être obtenues par les attaquants. Il est également important de proposer à partir de ces outils des « métriques » de la sécurité d'un composant. Dans le même esprit que précédemment une réflexion doit être menée afin d'aboutir à la définition d'outils d'extraction d'information « consensuelle ».

B) Mettre en place une méthodologie de conception basée sur cet environnement

- Il est important d'affiner les modèles de phénomènes physiques qui permettent les attaques (ou syndromes). Pour cela, il faudra spécifier, concevoir, fabriquer et caractériser (grâce aux bancs) des circuits dédiés de très faible complexité (typiquement plusieurs centaines de portes).
- Il est essentiel de pouvoir estimer l'efficacité des contre-mesures. Pour cela, il faudra spécifier, concevoir (grâce aux outils de CAD intégrant les modèles de syndromes), fabriquer et caractériser (grâce aux bancs et aux outils d'extraction d'information) des circuits dédiés dont la complexité est faible (typiquement plusieurs milliers de portes).
- Il est également nécessaire d'intégrer les contre-mesures validées à l'étape précédente dans des fonctions cryptographiques. Pour cela, il faudra spécifier, concevoir, fabriquer et caractériser des circuits dont la complexité est moyenne (typiquement plusieurs dizaines de milliers de porte).
- Enfin, il faut intégrer dans des systèmes complexes ces fonctions cryptographiques de façon optimale. De nouvelles architectures HW/SW pourront, à cet effet, être proposées pour gérer au mieux le compromis performance/sécurité/coût mais également disponibilité. Pour cela il est indispensable de créer un lien très fort avec des industriels pour adapter ces solutions au mieux de la menace réelle.

Objectifs scientifiques

Bancs d'évaluation sécuritaire, modélisation, caractérisation, preuve, architecture, outil de conception

Acteurs académiques français

Télécom ParisTech, LIRMM, LaHC, IRISA, LIP6, TIMA, ENSMSE, CEA, DGA, …

2. DEFIS 2 : TRNG, PUF

La génération de nombres réellement aléatoires est cruciale en cryptographie (génération de clés confidentielles, de nonces, de vecteurs d'initialisation, protocoles d'authentification). Les PUF sur silicium sont des primitives cryptographiques récentes qui utilisent les différences physiques entre des circuits d'architecture identique pour générer un code spécifique à chaque circuit (empreinte digitale du circuit). Leurs mises en œuvre soulèvent de nombreux points critiques :

A) Caractérisation des sources d'aléa et extraction d'entropie pour les TRNG

- Pour générer de tels nombres dans les circuits logiques, il est indispensable de caractériser les sources d'aléa disponibles dans les circuits logiques comme par exemple la métastabilité, l'instabilité de la phase d'un signal d'horloge (jitter), le chaos. Par caractérisation, on entend un modèle stochastique de la source selon les recommandations données par la méthodologie d'évaluation AIS31. Une fois que la source est caractérisée, il convient d'extraire le maximum d'entropie de celle-ci en proposant un principe d'extraction implantable dans les circuits logiques.
- Cette extraction doit être couplée avec un principe de mesure temps réel de l'aléa extrait pour d'une part garantir que les nombres générés sont réellement aléatoires et qu'il n'y a pas de tentative de manipulation de la source d'aléa. Cette dernière partie, cruciale, est très peu étudiée dans l'état de l'art actuel qui se consacre uniquement à faire passer une batterie de tests statistiques aux nombres générés. C'est un défi majeur qu'il faut relever pour mieux comprendre et caractériser les nombres générés et pour pouvoir les qualifier de nombres réellement aléatoires.

B) Caractérisation de la source d'aléa pour les PUF

- Les différences entre les circuits de même architecture apparaissent lors de la phase de production et sont dues à des mécanismes physiques incontrôlables. Les PUF peuvent être utilisées pour authentifier le matériel (lutte contre la contrefaçon), ou pour générer une clé cryptographique unique (spécifique au circuit). Comme pour les générateurs de nombre réellement aléatoires, le besoin de caractérisation de la source d'aléa est nécessaire pour la maîtrise des PUF.

C) Attaques et contremesures dédiés aux TRNG et aux PUF

- De nombreuses attaques ciblant les cœurs de chiffrement peuvent potentiellement viser les générateurs d'aléa qui délivrent le secret aux cœurs de chiffrement et les PUF qui permettent l'authentification des circuits. Il convient donc d'étudier leur faisabilité et éventuellement de développer les contre-mesures permettant aux TRNG et aux PUF de résister. Parmi les attaques envisagées, les attaques passives (par analyse de canaux auxiliaires) et les attaques actives (telles que les attaques en fautes) sont de bons candidats. Le canal électromagnétique par exemple (pour les attaques passives et actives) pourrait être un canal privilégié car son action peut être localisée ce qui semble être une condition nécessaire à l'analyse du générateur d'aléa. Le phénomène de verrouillage (locking) des générateurs basés sur des oscillateurs en anneau doit être étudié et modélisé car celui-ci peut être mis à profit lors d'attaques actives.

Objectifs scientifiques

Modélisation, caractérisation, métriques, architecture, outil de conception, augmentation et évaluation de la robustesse, preuve de sécurité, tests statistiques embarqués, contrefacon, clonage

Acteurs académiques français

LaHC, Télécom ParisTech, IRISA, TIMA, ENSMSE, CEA, DGA, LIRMM…

3. DEFIS 3 : Architecture matérielle et logicielle sécurisée

La protection des systèmes sur puce devient extrêmement complexe en situation réelle étant donné les nombreuses sources possibles d'attaques et le nombre croissant de fonctionnalités devant être intégrées au sein de l'architecture. Il est essentiel d'avoir une approche verticale de la sécurité afin d'appréhender les nombreuses couches mises en œuvre, depuis le niveau applicatif jusqu'au niveau portes. Plusieurs points doivent être considérés :

A) Attaques sur les réseaux de communication

- Les attaques par sondage (espionnage) des bus de communication entre composants discrets et les attaques par perturbation de ces mêmes bus (injection, substitutions spatiales ou

temporelles) peuvent être critiques pour le système, il est donc indispensable de développer des solutions systématiques visant à renforcer le niveau de protection du système.

B) Mise au point d'une architecture matérielle et logicielle pour sécuriser l'ensemble d'un système à partir d'un noyau de confiance

- Le noyau de confiance est composé d'un circuit intégré considéré comme enceinte sécurisée et comportant un micro-processeur, ses périphériques classiques et un co-processeur cryptographique destiné à protéger les accès à la mémoire externe (confidentialité et intégrité). Il est également composé d'un gestionnaire logiciel de sécurité, sorte d'hyperviseur de virtualisation spécialisé dans la gestion du co-processeur cryptographique et dans l'extension de la sécurité à l'ensemble des communications et des composants du système ; ce noyau logiciel est compact, conçu de la façon la plus fiable qui soit et, si possible, avec l'aide de techniques formelles et de preuve. Un ou plusieurs OS conventionnels tournent au dessus du gestionnaire de sécurité. Le gestionnaire de sécurité est protégé par le co-processeur cryptographique. Les OS hôtes bénéficient de services de sécurité exportés par le gestionnaire et garantis par le co-processeur (protection de pages mémoire en confidentialité et/ou en intégrité). Développer un tel système respectant les contraintes des systèmes embarqués reste un défi majeur aujourd'hui.

C) Modélisation, conception, génération automatique et validation par simulation et par analyse statique. Preuves de sécurité et de sûreté

- Il est essentiel de développer des approches théoriques de la sécurité des systèmes embarqués. Aujourd'hui l'essentiel des travaux propose des solutions ad hoc. Il est nécessaire de proposer des approches systématiques, prouvées permettant de garantir par construction la sécurité d'un système embarqué en fonction du périmètre de sécurité choisi et du modèle de menace considéré et cela en tenant compte de tous les niveaux d'abstraction (approche en profondeur de la sécurité).

D) Architecture de cryptoprocesseurs pour des applications embarquées

- Les systèmes embarqués voient une convergence forte d'applications hétérogènes sur un même matériel. Chacune de ces applications a des besoins propres en termes de sécurité auxquels il convient de répondre par des moyens logiciels et matériels vus comme un service homogène par les couches système et applicative. Il est donc impératif de fournir des moyens de cryptographie agile et à haute performance qui permettent à différentes entités de bénéficier au sein du système, de manière efficace, sécurisée et isolée, des services nécessaires à la réalisation de leurs fonctions. Les principaux verrous à lever sont la réalisation d'un système cryptographique hétérogène sur puce regroupant des crypto-processeurs pour le chiffrement asymétrique (chiffrement à clé publique), pour le chiffrement symétrique (chiffrement à clé secrète) et pour le hachage, le partage de ressources mémoires de façon sécurisé au sein du système, la gestion sécurisée matérielle et logicielle des clés de chiffrement et des certificats de sécurité et le déploiement sécurisé de services adaptatifs de cryptographie.

E) Opérateurs et algorithmes arithmétiques pour la cryptographie

- Un point essentiel lors du développement de cryptoprocesseur concerne l'étude et la conception d'opérateurs arithmétiques notamment pour la cryptographie asymétrique (ECC et RSA) avec plusieurs objectifs : hauts débits, faible consommation d'énergie, et grande robustesse aux attaques par canaux cachés. Les approches utilisant des représentations évoluées des nombres combinées à des algorithmes arithmétiques particuliers sont prometteuses et doivent être encore davantage étudiées. Il serait judicieux de développer au niveau de la communauté une bibliothèque logicielle de calcul arithmétique pour la cryptographie asymétrique pour des processeurs généralistes ainsi qu'une bibliothèque de blocs matériels de calcul arithmétique évolués pour la cryptographie.

Objectifs scientifiques

Cryptoprocesseur, opérateurs cryptographiques, hyperviseur, virtualisation, API de sécurité, moniteur, capteurs, preuve de sécurité, sécurité intra et inter couches, test du matériel, gestion de la personnalisation et du cycle de vie, séparation rouge/noire, gestion sécurisée des clés

Acteurs académiques français

LIRMM, LaHC, IRISA, Lab-STICC, LIP6, Télécom ParisTech, ENSMSE, CEA, DGA, LCIS, …

4. DEFIS 4 : RFID

Les technologies sans contact sont désormais utilisées dans de nombreuses applications sécurisées (contrôle d'identité, paiement, logistique, lutte contre la contrefaçon,…). Cependant la sécurité reste le principal frein à une large adoption de cette technologie.

Plusieurs contraintes rendent la sécurisation des systèmes RFID complexe. D'abord les tags passifs disposent de peu de ressource, il est donc difficile d'utiliser des protocoles complexes mettant en œuvre des calculs cryptographiques complexes.

A) Accroissement de la robustesse des systèmes RFID

- Les systèmes RFID sont particulièrement sensibles aux perturbations liées à l'environnement, il est donc nécessaire de mettre en œuvre des méthodes augmentant la robustesse de ces systèmes. Toutefois il s'agit de systèmes communicants complexes et très hétérogènes dont les performances sont étroitement liées à l'environnement (perturbations, protocole, nombres de tags dans le champ du lecteur…), il est donc difficile d'évaluer les effets des contre-mesures proposées lors de la phase de conception.
- Des travaux sur la mise en œuvre de simulateur permettant la modélisation et la simulation de systèmes RFID complexes (middleware, lecteurs et tags) et aussi la réalisation de plateforme de prototypage rapide permettant la validation de nouvelles architectures de tags RFID sécurisés dans un environnement physique réel sont nécessaires. Ces outils sont essentiels pour évaluer des scénarios d'attaque mais aussi les contre-mesures logicielles et matérielles.

B) Primitives cryptographiques dédiées pour les systèmes RFID

- Les systèmes RFID sont caractérisés par des contraintes en surface et consommation extrêmement sévères. Il est donc indispensable de développer des briques matérielles cryptographiques respectant des contraintes de très faible consommation et de très faible surface. Ce travail doit être couplé au développement de cryptographie légère. Il est donc fondamental de : réduire la surface (mutualisation de ressources entre co-processeurs), éventuellement développer de la cryptographie légère (lightweight cryptographie) propriétaire, de développer des contremesures légères (en s'appuyant éventuellement sur le point précédent, un nouvel algorithme peut certainement être spécifié pour résister mieux ou à moindre coût aux attaques), et enfin définir des protocoles sécurisés qui marchent en environnement contraint (e.g. accès en lecture mais non en écriture d'une mémoire non volatile à budget restreint).

Objectifs scientifiques

Modélisation, caractérisation, preuve, architecture, réduction de la surface, cryptographie légère, contremesures légères, protocoles sécurisés, très faible consommation, outils de validation

Acteurs académiques français

LCIS, Télécom ParisTech

5. DEFIS 5 : Formation à la sécurité des systèmes embarqués

Face aux enjeux développés à travers les quatre défis précédents, il apparaît indispensable de renforcer les aspects formation à la sécurité des systèmes embarqués. Un travail doit être mené dans ce sens afin de renforcer la lisibilité des formations existantes au niveau national. Le thème Sécurité des systèmes embarqués » se propose de mener ce travail et de promouvoir les supports pédagogiques actuellement utilisés au sein de la communauté.

Objectifs scientifiques

Attaques par canaux auxiliaires, Attaques par injection de fautes, Contremesures, Bancs d'évaluation sécuritaire, Cryptoprocesseurs, Opérateurs cryptographiques, Architecture matérielle et logicielle sécurisée, TRNG, PUF, RFID, Sécurité des FPGA, Test et sécurité, Contrefacon, clonage

Acteurs académiques français

En cours de recensement