Composant cryptographique TPM
Retours d'expériences et perspectives

Frédéric Rémi, Goulven Guiheux

Laboratoire d'évaluation d'AMOSSYS
Espace performance Bât M1 35760 SAINT GREGOIRE
{frederic.remi,goulven.guiheux}@amossys.fr

Résumé Cet article à vocation didactique présente les fonctionnalités mises à disposition des applications par un composant cryptographique TPM. Les services de haut-niveaux (attestation locale et distante, stockage sécurisé, ...) utilisant le composant TPM sont détaillés. Un retour d'expérience sur la conformité et l'efficacité des services et des principales applications (notamment la virtualisation) est effectué via le déroulement d'un plan de tests sur deux puces représentatives du marché. Pour conclure, nous présentons les principales perspectives et problématiques offertes par cette technologie pour la sécurisation des architectures de type PC.

Mots-Clé : TPM, TSS, TCG, Trusted Computing, PCR, SRK, EK, CRTM, vTPM, Local attestation, Remote attestation.

1 Introduction

Le manque de confiance dans la sécurité des architectures de plateformes ouvertes de type PC a poussé en octobre 1999, IBM, Intel, Microsoft, Compaq et HP à se regrouper au sein de « La Trusted Computing Platform Alliance » ou littéralement « alliance pour une informatique de confiance ». Aujourd'hui, ce sont plus de 130 sociétés qui ont rejoint l'alliance devenue depuis avril 2003 le TCG ou « Trusted Computing Group ».
Le TCG spécifie notamment l'architecture du composant cryptographique TPM (Trusted Platform Module) dont l'objectif principal est d'améliorer la sécurité des plateformes de type PC. Cette amélioration sécuritaire repose sur la spécification de services de sécurité haut-niveaux utilisant les propriétés du TPM (attestation locale et distante de la plateforme, stockage sécurisé dépendant de l'état de la plateforme).
Le principe de base du TPM est d'offrir aux utilisateurs un composant physique de confiance sur le poste client. Ce composant met à disposition de l'utilisateur des fonctions cryptographiques de base (génération d'aléa, de clés, de signatures électroniques, de hachage), de stockage sécurisé et d'agrégation de mesures. La confiance affichée provient alors de la nature matérielle du composant. Le pilotage du composant TPM est quant à lui réalisé via une architecture logicielle dédiée, la TSS pour TCG Software Stack.

L'objectif du TCG est de fournir un service attestant de l'intégrité d'une plateforme reposant sur cette architecture matérielle et logicielle. Cette architecture permet de mesurer les informations jugées sensibles (fichiers exécutables, librairies, pilotes, noyau du système, clés d'activation, fichiers de configurations, données personnelles, ...). Ce service d'attestation est soit local, soit distant. Dans le second cas, les mesures effectuées sont communiquées via un protocole spécifique à un tiers de confiance qui valide ou non ces mesures. Pour cette raison, le TCG est perçu par ses détracteurs comme une menace sérieuse pour les libertés individuelles. En effet, le fait que chaque programme soit accompagné d'une signature validée par un tiers restreint l'utilisation de logiciels libres. En trame de fond se cache la possibilité pour les promoteurs du TCG d'empêcher toute concurrence sur leur plateforme sécurisée en bloquant l'installation de logiciels tiers. Cette caractéristique leur a d'ailleurs valu le surnom de Treacherous Computing (Informatique déloyale), en opposition au nom officiel Trusted Computing (Informatique de confiance).

2 Présentation du composant TPM

2.1 Architecture matérielle

Le TPM est un composant passif de type carte à puce interagissant avec sa pile utilisatrice selon un modèle challenge-réponse. Le composant est de préférence soudé à la carte mère et possède un accès bidirectionnel avec le CPU. L'accès se fait par le biais d'un port bas débit LPC d'une bande passante variant de 256 Mo/s à 1 Go/s selon les modèles, géré par le « South Bridge ». Le TPM est composé de plusieurs modules décrits fonctionnellement dans les paragraphes suivants.

Module Input/Output (I/O). Le module I/O gère le flux d'information véhiculé par le bus de communication. Il met en oeuvre le protocole de codage/décodage des flux entrants et sortants et route les données vers les modules appropriés. Le composant TPM est relié à un port bas débit LPC (Low Pin Count). Par son positionnement, ce composant se distingue naturellement des cartes à puces ou autres clés USB qui interagissent avec la plateforme matérielle après le chargement de l'OS.

Module Non-Volatile Storage. Le module de mémoire non-volatile permet d'assurer le stockage permanent des données suivantes en mémoire.

- Endorsement Key (EK). Paire de clés asymétriques générée par le fabriquant de la puce TPM pour son identification en phase de personnalisation du composant. Au premier démarrage du composant, un protocole d'activation du composant est initié entre le fabriquant et le poste client. La bonne exécution de ce protocole entraîne la certification par le fabriquant de la partie publique de la clé EK. Ce certificat devient la carte

d'identité du composant TPM, il fournit la preuve que le TPM est authentique, i.e. que ce n'est pas une contrefaçon ou une virtualisation logicielle du composant matériel ;
- Storage Root Key (SRK). Paire de clé asymétrique générée à l'exécution de la commande `TPM_TakeOwnership` (cf ci-dessous). Elle joue le rôle de clé maître ou racine dans un système de hiérarchie des clés classique. Seule sa partie privée est stockée dans une partie protégée de la mémoire non volatile. La partie publique de la clé est utilisée pour le chiffrement de données ou de clés filles.
- Owner Authorization Data. A l'exécution de la commande `TPM_TakeOwnership` par le propriétaire du poste client, un condensé de 160 bits est créé et stocké en mémoire. Cette valeur constitue un mot de passe commun entre le composant et le propriétaire de la plateforme. Il permet d'assurer au propriétaire l'usage exclusif de capacités de sécurité du composant TPM. Malgré l'usage du terme `Authorization Data`, ce mot de passe partagé est utilisé pour assurer un usage exclusif du composant par le propriétaire légitime.

Module Volatile Storage. Le module de mémoire volatile permet d'assurer le stockage des données temporaires.

Module Plateform Configuration Register. Les mémoires PCR sont des registres de 160 bits permettant de stocker l'état d'une plateforme. Ils sont utilisés pour agréger les mesures dans le processus d'attestation locale du poste client. Le TCG spécifie un minimum de 16 registres dont les 8 premiers (0-7) sont réservés à un usage interne du TPM. Les autres registres, soit 8 au minimum (8-15), sont réservés aux applications (*i.e.* chargeur d'amorce, noyau, librairies système, drivers, applications).

Module Attestation Identity Keys (AIKs). Ce module optionnel permet le stockage des clés AIK. Les clés AIK sont des bi-clés utilisées lors du protocole d'attestation de la plateforme. Nous décrivons leur utilité dans le paragraphe Les AIK peuvent être tout aussi bien stockées sur un système de stockage externe au TPM.

Modules Program code and Execution Engine. Le module Program code contient le firmware du composant TPM. Le module Execution engine constitue le CPU du TPM et à ce titre exécute les commandes envoyées par le module I/O en interprétant le micro code du firmware.

Module Random Generator (RNG). Ce module implémente un générateur d'aléa physique. Cet aléa est utilisé pour la génération des clés, des vecteurs d'initialisation et des challenges aléatoires pour les protocoles cryptographiques.

Module SHA-Engine. Ce module implémente la fonction de hachage cryptographique SHA-1. Le TCG étant un centre de normalisation, ce module devrait évoluer dès la standardisation par le NIST d'un nouvel algorithme de hachage cryptographique en remplacement de SHA-1.

Module HMAC Engine. Ce module implémente la fonction de hachage à clé HMAC. La taille des clés est de 20 octets et la taille des blocs est de 64 octets. La fonction supporte le calcul du HMAC selon la RFC 2104.

Module Key Generation. Le module de génération de clés permet de créer des clés symétriques et asymétriques. Le module de génération supporte des clés RSA jusqu'à 2048 bits (512 à 2048 bits).

Module RSA Engine. L'algorithme RSA est utilisé à la fois en mode signature et en mode chiffrement. Le TCG respecte le standard PKCS#1 qui fournit les détails des spécifications pour la signature, le chiffrement et le formatage des données RSA.

Module Opt-In. Le module Opt-in implémente la politique de configuration du composant TPM. Plusieurs états sont définis « Enabled/Disabled » , « Active/Inactive » et « Owned/Unowned » .

Module Power Detection. Ce module permet de gérer les états d'alimentation du TPM en conjonction de ceux de la plateforme. À tout moment, le TPM doit connaître les changements d'état de la plateforme. Certaines commandes du TPM peuvent être restreintes selon la valeur de ces états.

Module de chiffrement symétrique. Le TCG spécifie le générateur de pseudo-aléa MGF1 de PKCS#1v2.1 en mode chiffrement par flot pour le service de confidentialité des sessions d'authentification et de transport. Concernant le service de confidentialté des données internes, le composant TPM peut également utiliser un algorithme de chiffrement symétrique mais le choix revient au constructeur. On remarquera que le TCG ne spécifie aucun algorithme symétrique par flot ou par bloc pour le chiffrement de données utilisateur.

2.2 Services intrinsèques au composant

Les services offerts nativement par le composant sont les suivants :

- *Unicité de la plateforme.* Chaque TPM est associé à une clé RSA unique appelée Endorsement Key (EK). Cette clé est générée par le constructeur en phase de personnalisation du TPM. La partie publique de cette clé est certifiée par une AC associant à chaque TPM un certificat unique. Cette clé ne doit jamais être communiquée à l'extérieur du TPM ;

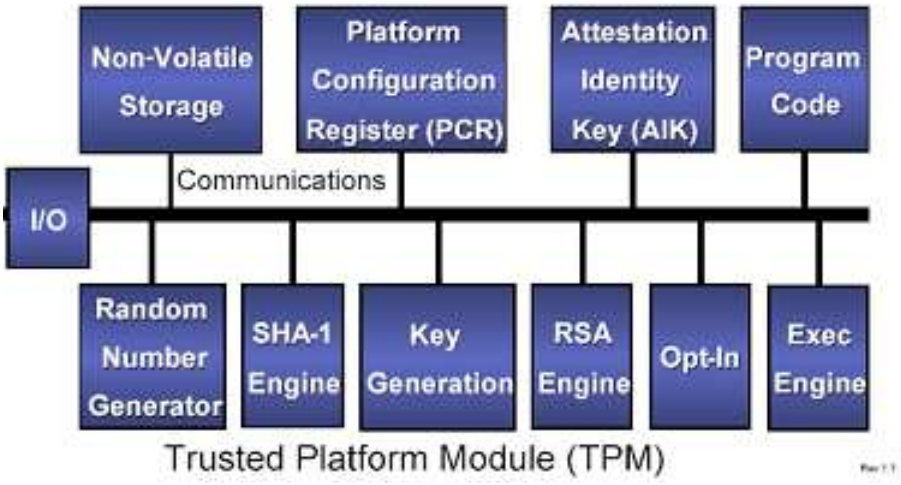

Fig. 1. Architecture matérielle du composant TPM

- *Stockage sécurisé.* Le TPM intègre un service de protection des données en confidentialité. Ce service repose sur une hiérarchie de clés. Chaque clé est protégée par une clé de niveau supérieur. La racine de cette hiérarchie est constituée par la clé SRK (Storage Root Key). Cette clé est stockée à l'intérieur du TPM, tandis que les autres clés sont stockées sur un support externe (disque dur par exemple). La clé SRK est générée par le TPM lors de la prise de possession du TPM en utilisant la commande `TPM_TakeOwnership`.
- *Scellement de données.* Ce service est un mécanisme de stockage sécurisé dépendant de l'état de la plateforme. Le « descellement » d'une donnée n'est possible que si l'état des registres PCR au moment du scellement est identique à l'état des registres PCR au moment du descellement. Ce mécanisme est utilisé pour le service d'attestation locale.
- *Opérations cryptographiques.* Le TPM met à disposition de l'utilisateur les fonctions cryptographiques suivantes :
  - Fonction de hachage SHA-1 ;
  - Génération de clés, chiffrement et signature RSA bits conforment aux travaux du groupe de standardisation de l'IEEE P1363 ;
  - Génération d'aléa.
- *Extension des registres PCR.* Ce mécanisme est utilisé pour le service d'attestation locale et distante du poste client. Il permet d'agréger des mesures réalisées par des logiciels tiers dans les registres PCR du TPM. Le processus d'extension est une opération cryptographique simple consistant à concaténer la valeur courante du registre PCR avec la nouvelle mesure

puis à hacher le tout :

$$PCR_{t+1}[i] = \text{SHA-1}\Big(PCR_t[i]||M\Big) \quad (1)$$

M désigne la mesure réalisée par une application logicielle. Selon le concept de mesure définit par le TCG, $M = \text{SHA-1}(\text{DATA})$. La variable i désigne l'index du registre concerné par l'extension. Cette opération offre plusieurs avantages :

- Il est calculatoirement impossible de trouver des collisions sur la valeur des registres pour deux mesures différentes ;
- La mesure n'est pas commutative, i.e. deux mesures déséquencées produisent des résultats différents ;
- L'opération permet de stocker un nombre illimité de mesures dans les registres PCR puisque le résultat est toujours une empreinte de 160 bits.

2.3 Architecture logicielle et services associés

La TSS constitue une spécification logicielle fournissant un standard d'API permettant d'accéder aux fonctions de la puce TPM. Elle établit le lien entre les programmes ou le système d'exploitation et la puce. Les développeurs peuvent l'utiliser pour créer des applications interopérables fonctionnant avec le TPM. La version actuelle de la spécification de la TSS est en version 1.2 datant de mars 2007.
Les objectifs de l'API TSS sont :

- d'apporter un point d'entrée pour les applications aux fonctionnalités du TPM ;
- de gérer les services du TPM ;
- d'assurer la gestion du composant (synchronisation, contrôle de flux, audit des requêtes, ...)

La figure 2 illustre l'architecture logicielle associée au TPM.

- Au niveau le plus bas, le composant TPM est accessible via le driver TPM (TDD) situé au même niveau que le noyau du système d'exploitation (ring 0). Ces drivers fournis par les constructeurs ne sont pas inclus dans la TSS ;
- Au niveau utilisateur, la TSS est composée de ;
  - Un module de gestion de driver TPM (**TDDL**) qui constitue une couche d'abstraction aux drivers TPM permettant de développer des composants logiciels indépendants du driver TPM considéré. Il permet en outre le passage du mode utilisateur au mode noyau (TPM Device Driver). Le TPM est associé à un seul module TDDL. Ce module est initié et fournit par le fabriquant du TPM.
  - La couche des services principaux (**TCS**) fournit toutes les primitives du TPM et l'ensemble des services communs :
    - Synchronisation des requêtes envoyées au TPM[1] ;

[1] Le TPM traite les requêtes séquentiellement et n'est pas conçu pour un environnement multithread

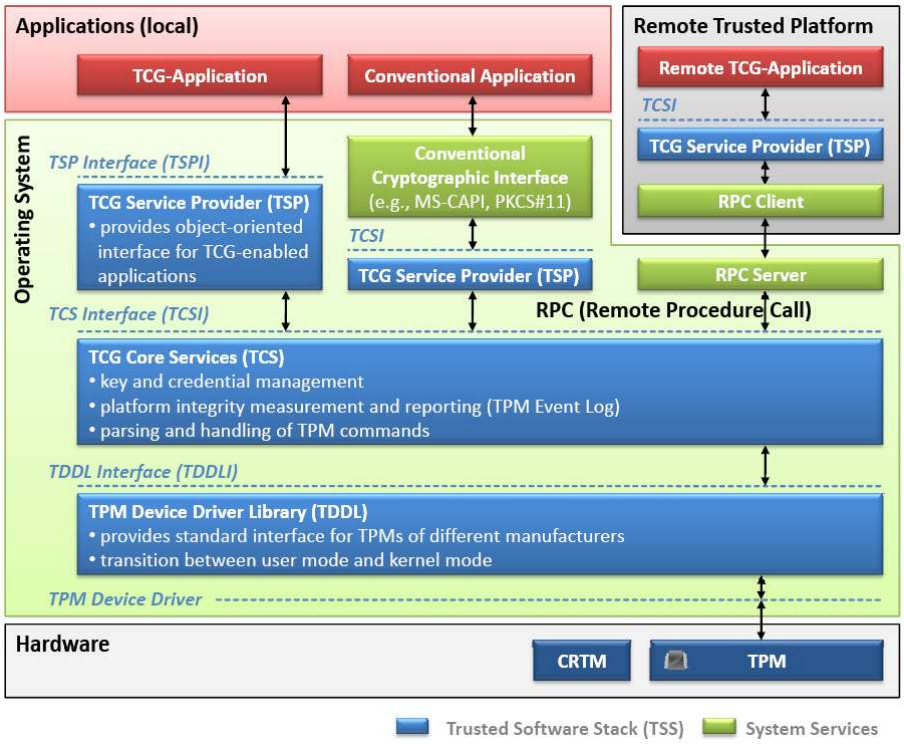

Fig. 2. Diagramme de la TSS

- Journalisation des évènements et des opérations ;
- Audit des évènements qui ont fait l'objet d'une mesure via le processus d'extension des registres ;
- Gestion des certificats de la plate-forme ;
- Gestion des informations d'authentification et d'identification.

Le TPM est associé à un seul module TCS. Ce module est exécuté comme un service système en mode utilisateur (daemon) et est utilisé par des applications de bas-niveaux implémentant des services spécifiques (middleware ou composant d'OS).

- Une couche de services de haut-niveau, la (**TSP**), utilisée par les applications souhaitant utiliser le TPM. Elle met à disposition de ces applications les services de la TCS en masquant les contraintes de gestion.

3 Services haut-niveaux

3.1 Attestation locale

L'attestation locale est un service permettant le contrôle de l'intégrité du poste client. L'objectif de ce contrôle est de conditionner l'accès à certaines

données, ressources ou applications. En pratique, l'intégrité de la plateforme est vérifiée par l'établissement d'une chaîne de confiance liant tous les éléments critiques de la configuration. Depuis le boot du poste client, chaque élément logiciel réalise une mesure de l'élément suivant avant de l'exécuter. En pratique, les éléments logiciels sont les suivants :

- Le BIOS ;
- Le gestionnaire de démarrage (Grub) ;
- Le système d'exploitation ;
- Les applications.

La mesure d'une donnée ou d'une application est constituée par un motif d'intégrité SHA-1. Cette mesure est à l'initiative des applications. L'ensemble des mesures successives forment une chaîne de confiance initiée par le CRTM (Core Root Trusted Measurement). Ce code est exécuté en premier sur le poste client au démarrage. L'objectif du CRTM est de réaliser une mesure de soi-même et de l'élément logiciel suivant. Concrètement, sur un poste client, le CRTM représente l'ensemble des premiers octets du BIOS qui vont s'auto-mesurer puis mesurer le reste du BIOS.

Le processus de mesure se déroule de la manière suivante : Soient A et B deux entités telles que A execute B :

- A mesure B (un exécutable ou un autre fichier). Le résultat est un condensé de B ;
- Ce condensé est écrit dans un fichier log Stored Measurement Log (SML) stocké en mémoire.
- A écrit le condensé de B dans un registre PCR via l'opération d'extension des registres PCR ;
- Le contrôle est donné à B.

L'attestation locale fait intervenir deux éléments cruciaux :

- Le fichier SML. Il s'agit d'un fichier de journalisation des mesures géré par l'application initiatrice de la mesure. Ce fichier contient le triplet suivant :
  - Le registre PCR utilisé pour la mesure ;
  - Le condensé SHA-1 ;
  - Le nom de l'élément mesuré.
- Les registres PCR. Leur fonction est de garantir l'intégrité du fichier SML. Le processus de vérification de l'intégrité du fichier SML se déroule en deux étapes :
  - Rejeu logiciel du processus d'extension des registres(Cf. formule 1) sur la base des mesures du fichier SML ;
  - Comparaison du résultat avec l'état courant des registres PCR du TPM.

  L'intégrité est valide si les résultats sont identiques. Cette opération doit être initiée par une application tierce de confiance. Le synoptique 3 décrit le déroulement du processus d'attestation d'une plateforme.

3.2 Attestation distante

L'attestation distante offre l'opportunité à un tiers de confiance de vérifier l'état dans lequel se trouve une plate-forme et d'en déduire si cet état est de

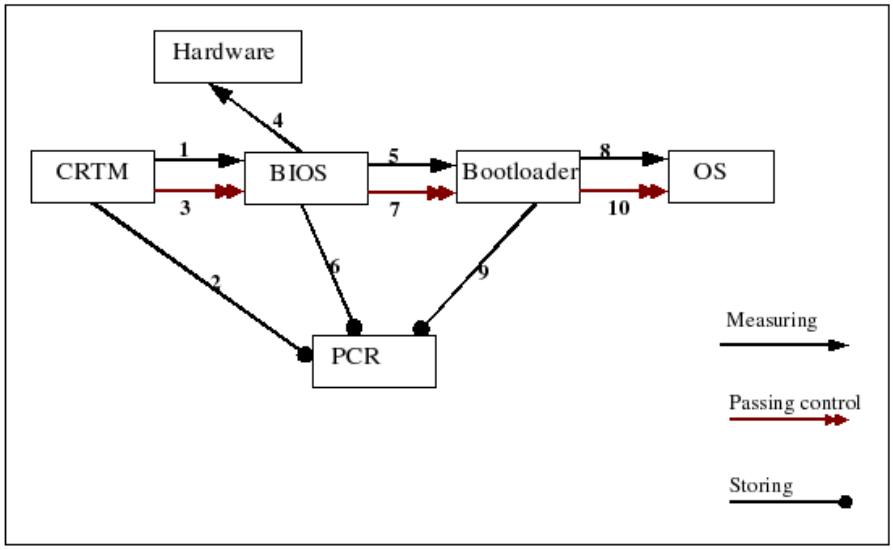

Fig. 3. Déroulement du processus de mesure

confiance ou non. Lorsque la chaîne de confiance couvre le système d'exploitation et les applications, le demandeur d'une attestation peut conditionner la délivrance d'un contenu sensible à la valeur des registres PCR.
L'attestation distante est le prolongement de l'attestation locale. L'attestation distante d'un poste client se fait par l'envoi de ses registres PCR et de son fichier SML au tiers de confiance qui va se charger de vérifier les informations. La sécurité du schéma d'attestation distante repose sur l'établissement d'un canal de communication sécurisé entre le tiers de confiance et le TPM.

3.3 Stockage sécurisé de clés

Le service de stockage de clés découle directement de la fonction de stockage sécurisé du TPM. L'utilisation de la TSS est requise.

3.4 Signature de certificats

Le service de signature de certificats découle directement de la fonction de signature du TPM. L'utilisation de la TSS est requise.

4 Retour d'expériences

Cette partie présente les résultats des tests de conformité et d'efficacité réalisés en temps contraint dans le cadre du marché DGA Postes Clients et Interconnexions Multiniveaux (PCIM).

4.1 Stratégie de Tests

La stratégie de tests s'est inspirée du schéma d'évaluation/certification CSPN de la DCSSI. Ce schéma permet de tester des produits de sécurité en temps contraint selon une méthodologie privilégiant l'expertise technique à la complétude méthodologique. Les grandes phases de la stratégie de tests sont :

- Identification de l'évaluation ;
- Identification du produit évalué ;
- Fonctionnalités, environnement d'utilisation et de sécurité ;
- Installation du produit ;
- Analyse de la conformité ;
- Analyse de la résistance des fonctions et des mécanismes ;
- Analyse des vulnérabilités (intrinsèques, de construction, d'exploitation) ;
- Analyse de la facilité d'emploi ;
- Synthèse et avis d'expert.

4.2 Synthèse de l'analyse des composants

Les deux puces concernées par les tests sont des composants TPM compatibles avec les spécifications 1.2 du TCG. Les puces proviennent des constructeurs Broadcom et ATMEL.

4.3 Synthèse de l'analyse des applications

Portée des tests. Les expérimentations sur les TPM ont porté sur les quatre applications suivantes :

- Trusted Grub ;
- Integrity Measurement Architecture (IMA) ;
- Trousers ;
- TPM-TOOLS.

Trusted Grub. Trusted Grub est un patch à appliquer sur le chargeur de démarrage de Grub. Il mesure les éléments suivants lors du démarrage du poste :

- Le stage 1.5 de Grub[2] ;
- Le stage 2 de Grub ;
- Le fichier de configuration de Grub ;
- Le noyau Linux ;
- L'image du système minimal (`initrd`).

Les tests effectués se sont concentrés sur l'analyse de la conformité des mesures et ont consisté à :

- Modifier un élément ;
- Redémarrer la plateforme ;
- Consulter le fichier SML afin de vérifier des changements dans les mesures.

[2] On notera que le stage 1 de Grub est mesuré par le BIOS.

À l'issu des tests, nous avons constaté la conformité de la mise à jour du fichier SML. Néanmoins, l'étape de reproduction du processus d'extension des registres PCR a mis en exergue une non conformité fonctionnelle. Une analyse du code nous a permis de constater que la fonction d'extension a été omise.

Integrity Measurement Architecture. IMA est un module noyau permettant au système d'exploitation de mesurer l'intégrité des binaires chargés en mémoire : pilotes, librairies et exécutables. IMA est développé par le groupe de recherche d'IBM sur le TCG([IMA]). Il se présente sous la forme d'un patch du noyau Linux. Le fonctionnement d'IMA est transparent pour l'utilisateur. Lors du chargement du binaire en mémoire, IMA le mesure. Si le binaire a déjà été utilisé, IMA vérifie le motif d'intégrité du binaire avec celui du fichier SML. Quelque soit le résultat de ce test, IMA n'empêche pas l'utilisation des binaires. En revanche, il incrémente des compteurs reflétant les résultats de ces mesures :

- Nombre de fichiers mesurés ;
- Nombre de changement d'intégrité ;
- Nombre de violations ;
- ...

De plus, IMA offre également aux applications la possibilité de mesurer un fichier en lecture seule.
Les tests se sont concentrés sur la conformité du produit. Nous avons étudié les mesures de binaires et l'interface de mesure des fichiers en lecture seule. Le produit s'est montré conforme. IMA reste néanmoins plus proche d'un prototype expérimental que d'un produit finalisé. Une application tierce interprétant les mesures d'IMA afin de réagir aux changements d'intégrité est notamment très attendue.
L'association d'IMA avec Trusted Grub est un exemple d'implémentation du service d'attestation locale du poste. Malheureusement, le manque de synergie entre les spécifications des deux produits affaiblit la chaîne de confiance. En effet, IMA utilise les premiers registres PCR pour initialiser ses mesures alors que les paramètres par défaut de Trusted Grub prévoient une mesure du noyau Linux (et donc d'IMA) sur les registres suivants.

Trousers. Trousers est un projet Linux visant à développer une pile logicielle TSS de source libre. Elle permet à des applications comme Tpm-tools d'utiliser le TPM. A l'heure actuelle, Trousers est compatible intégralement avec les spécifications 1.1 du TCG mais partiellement avec la version 1.2. Néanmoins le projet en est à un stade très avancé et la pile est aujourd'hui fonctionnellement quasi complète. Par ailleurs, une analyse en temps contraint de la pile a été effectuée selon une métrique d'analyse d'API cryptographique comprenant des critères tels que :

- L'indépendance vis à vis des algorithmes et des applications ;
- L'indépendance vis à vis du module cryptographiques ;
- Le degré d'expertise cryptographiques (prises en compte des attaques de la littérature, conception sécurisée) ;

- Les services auxiliaires (cycle de vie des clés, audit des requêtes, authentification du module, ...) ;
- Le partage de charge, gestion de l'asynchronisme ;
- Le contrôle de flux ;
- ...

Il ressort de cette expertise que l'API TSS manque de maturité notamment en termes de mécanismes d'auto protection permettant de résister aux attaques de la littérature (API hooking, attaques cryptographiques ...).

TPM-TOOLS. TPM-TOOLS constitue une boîte à outils permettant d'utiliser le TPM. Son fonctionnement requiert l'utilisation de Trousers. Les services proposés par TPM-TOOLS :

- Scellement de données ;
- Activation du TPM ;
- Mise à zéro du TPM ;
- Obtention de la partie publique de l'EK ;
- Prise de possession du TPM (génération d'une nouvelle clé SRK et révocation de l'ancienne).

Nos analyses se sont concentrées sur une étude de la conformité fonctionnelle de l'outil.

4.4 Virtualisation TPM

Présentation de la virtualisation. La virtualisation TPM a pour objectif de fournir les services du composant matériel aux machines virtuelles. À l'heure actuelle, trois solutions liées au concept de virtualisation sont présentes sur le marché :

- Une solution utilisant les technologies VT d'INTEL et PACIFICA d'AMD ;
- Une solution logicielle reposant sur la solution de virtualisation XEN ;
- Une solution d'IBM reposant sur un support matériel mettant à disposition un composant TPM physique virtualisable.

Solution reposant sur XEN. La solution reposant sur XEN consiste à émuler logiciellement un composant TPM au niveau de l'hyperviseur. Il s'agit d'une implémentation logicielle où l'utilisation du TPM physique est très limitée.
Les avantages et inconvénients d'une telle solution sont liés du fait qu'une instance virtuelle, logicielle, de TPM (vTPM) est clairement différenciée d'une implémentation matérielle et les propriétés de sécurité sont différentes :

- Les hiérarchies de clés sont indépendantes : chaque vTPM possède sa propre hiérarchie de clés, sans lien avec la hiérarchie des clés du TPM physique (notamment les *storage root key* et *endorsement key*) ;
- La génération des clés d'un vTPM est exécutée en logiciel par le processus et ne fait pas intervenir le TPM matériel ;
- Les fonctions des vTPM sont indépendantes des fonctions du TPM : un appel à un vTPM ne se matérialise pas par un appel au TPM.

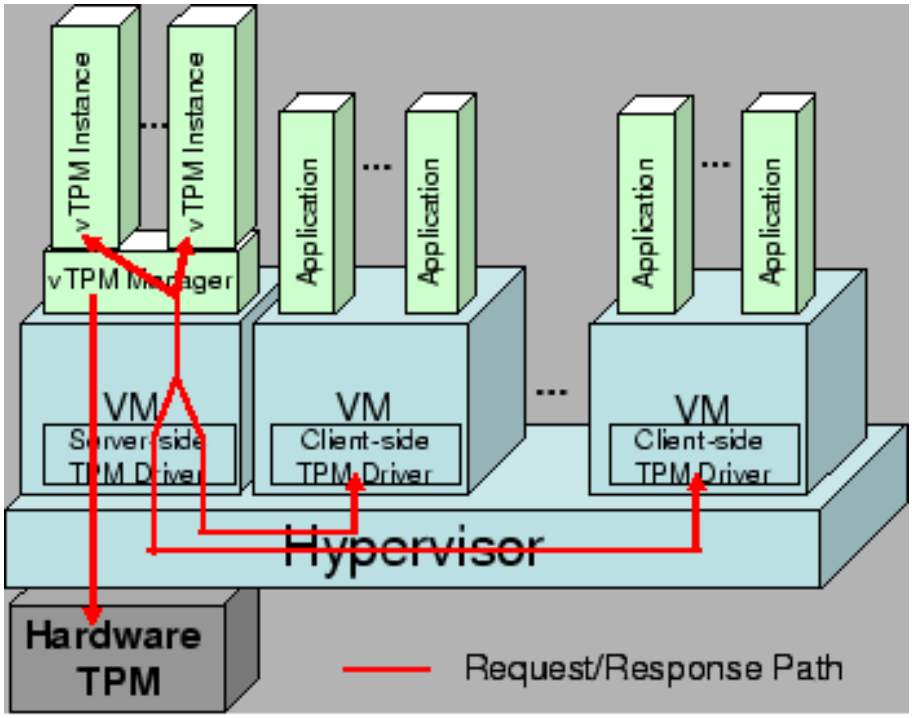

Fig. 4. Virtualisation de TPM : solution de XEN

Nos tests sur ce produit se sont cantonnés à :

- Vérifier la possibilité d'utiliser le vTPM dans une machine virtuelle ;
- Vérifier la continuité de la chaîne de confiance (propagation des mesures de l'attestation locale).

Les expérimentations ont montré que :

- La solution de XEN correspond fonctionnellement à ses spécifications : les machines virtuelles utilisent bien les services des vTPM ;
- La continuité de la chaîne de confiance n'est pas réalisée puisque l'initialisation d'un vTPM ne fait pas intervenir l'état de la machine hôte. Selon nous, une solution aurait été d'initialiser les registres PCR du vTPM avec une mesure de XEN et des registres PCR du TPM matériel.

Solution d'IBM. L'initiative d'IBM part de la constatation que les TPM n'ont pas été spécifiés pour être employés par plusieurs systèmes à la fois. Par conséquent, IBM a étendu les spécifications du TPM permettant un usage multi-système simultané. Cette solution fait l'objet d'une extension au standard TPM

1.2, définissant de nouvelles commandes dédiées à la virtualisation d'un TPM. Le support matériel (IBM PCI-X Cryptographic Processor, carte PCIXCC) met

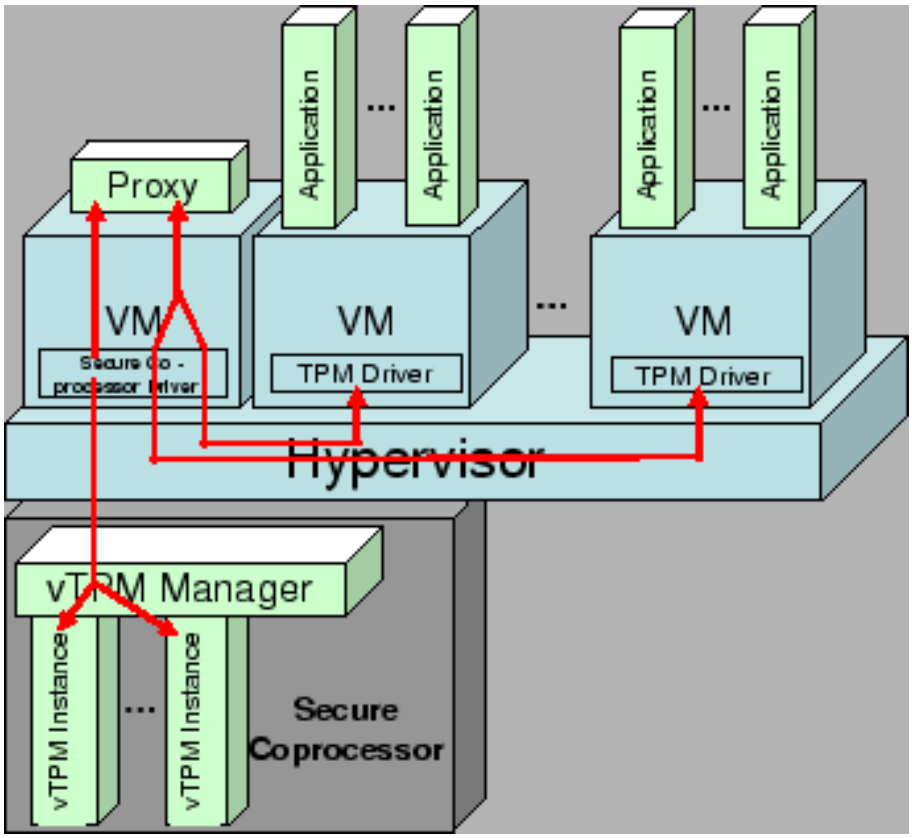

Fig. 5. Virtualisation de TPM : solution d'IBM

à disposition un composant TPM physique aux machines virtuelles. Les TPM virtualisés sont indépendants les uns des autres, ne partagent pas d'informations et ne communiquent pas. Chaque machine virtuelle a accès uniquement à son TPM virtuel à travers le proxy et est cloisonnée des autres TPM virtuels. La seule possibilité de partage d'informations entre instances est d'utiliser les fonctions de sauvegarde et restauration d'instance pour créer des clones d'un même TPM virtuel. Il faut toutefois remarquer que la gestion de l'isolation entre les vTPM est en partie logicielle : c'est au proxy, qui concentre toutes les requêtes des machines virtuelles, d'assurer l'aiguillage des commandes en fonction des associations machine virtuelle / vTPM.
De plus, le système prévoit qu'une machine virtuelle puisse virtualiser elle même un composant TPM virtuel. Dans ce cas, le TPM virtuel associé à cette ma-

chine virtuelle est lui-même virtualisé pour les machines virtuelles filles (ceci se traduit en pratique par le fait qu'une commande transite deux fois par le proxy avant d'atteindre la carte). Ceci conduit à une arborescence de TPM virtuels, qui peuvent s'appuyer soit sur le TPM physique soit sur un autre TPM virtuel. Cette fonctionnalité traduit le caractère modulaire et avancé de la solution.

5 Conclusion

La technologie TPM constitue une avancée indéniable pour la sécurisation des architectures de postes clients. Elle offre nativement des services cryptographiques implémentés matériellement à moindre coût et permet la spécification de services de sécurité haut-niveaux tels que l'attestation locale ou distante.
Nos expérimentations sur le composant TPM, sa pile logicielle et les différentes applications utilisatrices ont montré que certains problèmes de conformité fonctionnelle et d'efficacité subsistent. On citera notamment :

- Le manque de maturité, l'absence de prise en compte de la sécurité dans la pile TSS ;
- Le problème de compatibilité matérielle avec certains composants du marché (BROADCOM).

Toutefois, ces problèmes sont à relativiser compte tenu de la jeunesse de cette technologie et des nombreux développements en cours de réalisation.
Par ailleurs, notre confiance dans cette technologie est ternie par la relative opacité des spécifications du TCG. En effet, ces dernières sont très volumineuses mais malheureusement peu explicites et trop adaptables par les constructeurs sur certains aspects (mesure du boot, protocole d'activation, attestation locale et distante, ...). Elles s'apparentent plus à des documents de conception détaillés destinés aux développeurs. Il manque clairement un niveau de spécification formelle ou au moins pseudo-formelle des principaux protocoles et services cryptographiques. Il conviendra donc de suivre attentivement les futures évolutions de cette technologie, notamment en termes d'évaluation de sécurité, afin d'en garder une certaine maîtrise garantissant la confiance dans son utilisation.

Références

[TPM1] TPM Main Part 1 Design Principles Specification Version 1.2 Revision 94 29 March 2006

[TPM2] TPM Main Part 2 TPM Structures Specification Version 1.2 Revision 94 29 March 2006

[TPM3] TPM Main Part 3 Commands Specification Version 1.2 Level 2 Revision 94 29 March 2006

[TSS1] TCG Specification Architecture Overview Specification Revision 1.3 28 March 2007

[TSS2] TCG Software Stack (TSS) Specfication Version 1.2 Level 1 Errata A Part1 : Commands and Structures 7 March 2007

[IMA] Reiner Sailer and Xiaolan Zhang and Trent Jaeger and Leendert van Doorn, Design and Implementation of a TCG-based Integrity Measurement Architecture

[VTPM-IBM1] Stefant Berger, Ramon Caceres, Kenneth A. Goldman, Ronald Perez, Reiner Sailer, Leendert Van Doort, vTPM : Virtualizing the Trusted Platform Module

[VTPM-XEN1] Virtual Trusted Platform Module http ://domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_vtpm.index.html

[VTPM-IBM2] TPM Main Part 3 IBM Commands Specification Version 1.2 Revision 10 25 April 2005 http ://domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_vtpm.index.html/$ FILE/mainP3IBMCommandsrev10.pdf