Proposition d'article pour SAR'2002

TITRE

SIM-IP, un module de sécurité pour les applications de l'internet.

AUTEURS

Pascal Urien, Pascal.Urien@ louveciennes.sema.slb.com
Adel Tizraoui, Adel.Tizraoui@ louveciennes.sema.slb.com
Marc Loutrel, Marc.Loutrel@ louveciennes.sema.slb.com
Hayder Saleh, Hayder.Saleh@ louveciennes.sema.slb.com

SchlumbergerSema,36-38 rue de la Princesse
BP45
78431 Louveciennes Cedex
France

Téléphone 33 1 30 08 46 89
Fax 33 1 30 08 45 24

Résumé.

Dans ce papier nous décrivons une architecture de modules de sécurité SIM-IP, à base de cartes à puce, répondant aux besoins croissant de sécurité de l'économie de réseau. Après une introduction soulignant l'importance de la sécurité dans l'internet de nouvelle génération, nous décrivons brièvement la technologie des puces sécurisées (SPOM) et nous exposons l'évolution prévisible de leurs performances au cours des cinq prochaines années. Nous présentons ensuite une technologie émergente de carte à puce internet, qui a reçu plusieurs prix industriels et dont le protocole de base SmartTP fait l'objet d'un internet draft. Enfin nous analysons l'introduction de ces composants dans les applications de l'internet, et à titre d'illustration nous décrivons un logiciel expérimental de téléphonie H323 fonctionnant avec un module SIM-IP.

Mots clés.

Sécurité, internet, carte à puce.

SIM-IP,
un module de sécurité pour les applications de l'internet.

[1]Pascal Urien, [2]Adel Tizraoui, [3]Marc Loutrel, [4]Hayder Saleh

SchlumbergerSema Smartcard Research center, 36 rue de la Princesse,
BP 45, 78431 Louveciennes Cedex France
Pascal.Urien@louveciennes.sema.slb.com

Résumé.

Dans ce papier nous décrivons une architecture de modules de sécurité SIM-IP, à base de cartes à puce, répondant aux besoins croissant de sécurité de l'économie de réseau. Après une introduction soulignant l'importance de la sécurité dans l'internet de nouvelle génération, nous décrivons brièvement la technologie des puces sécurisées (SPOM) et nous exposons l'évolution prévisible de leurs performances au cours des cinq prochaines années. Nous présentons ensuite une technologie émergente de carte à puce internet, qui a reçu plusieurs prix industriels et dont le protocole de base SmartTP fait l'objet d'un internet draft. Enfin nous analysons l'introduction de ces composants dans les applications de l'internet, et à titre d'illustration nous décrivons un logiciel expérimental de téléphonie H323 fonctionnant avec un module SIM-IP.

Mots clés.

Sécurité, internet, carte à puce.

Introduction.

On assiste aujourd'hui à la convergence de plusieurs facteurs technologiques et économiques qui tendent à introduire la notion d'objet communiquant, intégrant un système informatique et muni de ressources de communication (filaires ou sans fils) permettant l'échange de données avec le réseau internet.

L'omniprésence des ordinateurs (*ubiguitous computing*), l'accès universel à la toile d'araignée mondiale (*ubiguitous internet*), et l'intégration de ces fonctions dans des surfaces de silicium de plus en plus réduites (parfois appelées SOC - System On Chip [1]) sont autant de facteurs favorisant l'apparition massive d'objets divers ou de terminaux multimédia reliés à internet. En particulier les communications IP en mode sans fils, qui permettent l'accès à des services depuis un réseau d'accès [2], ou les interactions entre objets communiquant impliquent la mise en place d'une architecture sécurisée de bout en bout. Ces impératifs de sécurité sont proches de la problématique des AAA (*Authentication, Authorization, Accounting* [3]) étudiée par l'IETF.

L'authentification de l'utilisateur est un problème clé tant pour la connexion à un réseau d'accès, que pour l'obtention du service auquel il a souscrit. Cette opération nécessite la connaissance de divers paramètres dont certains sont publiques (adresse de serveur, identifiant d'abonné..), et d'autres confidentiels (clés d'authentification…). L'ensemble de ces

[1] SchlumbergerSema, Smartcard Research Center.
[2] Doctorant cifre, LIP6.
[3] Doctorant cifre, UTC.
[4] Doctorant cifre, UVSQ-PRISM.

paramètres, dont les propriétaires peuvent être multiples (réseau, service, client…), sont les composants d'un profil, nécessaire à la réalisation du service.
Ainsi le protocole WEP [4] réalise l'authentification d'un client dans un réseau sans fil 802.11. Il utilise un jeu de une à quatre clés fixes RC4 de 40 bits (cette taille étant une conséquence de la législation Américaine) ; une séquence d'octets pseudo aléatoire (*key stream*) dont la longueur est identique à celle des données à chiffrer, est déduite d'un nombre de 24 bits IV (soit 16 millions de possibilités). Un classique algorithme de Vernam effectue le chiffrement (ou exclusif des données et de la suite d'octets pseudo aléatoire). William Arbaugh, de l'université du Maryland, a montré, lors d'une présentation à l'IEEE en mai 2001 [5] qu'il était possible de casser cette procédure en moins de 48 heures. Cet exemple illustre le rôle critique de la sécurité dans l'introduction de nouvelles technologies de communication.
Au terme de la procédure d'authentification le réseau ou le service affecte à l'utilisateur des droits, généralement déduits de la consultation d'une base de données ; il devient alors possible de facturer l'internaute pour les ressources qu'il consomme. Jusqu'à présent la plupart des utilisateurs d'un réseau télématique sont authentifiés par des mots de passes. L'introduction de mécanismes à clés publiques (tels que SSL) permet d'authentifier le côté serveur dont l'environnement informatique est considéré sûr et loge des clés RSA privées. Côté client, le système hôte ne mémorise aucune clé, ou encore stocke une valeur de clé chiffrée à l'aide d'un mot de passe (*passphrase*), en raison du manque de sûreté de fonctionnement de ces systèmes (ordinateurs personnels …).
Une approche permettant l'amélioration de la sécurité côté client, consiste à conduire le processus d'authentification à l'aide de classiques cartes SIM [6], dans des infrastructures sans fils de type OWLAN [7] (*Operator Wireless Local Area Network*). Dans la solution proposée par Nokia [8] un terminal sans fil obtient une adresse IP délivrée par un contrôleur d'accès (AC), avec lequel il initialise un processus d'authentification, au cours duquel il transmet son identifiant *IMSI. AC* communique avec un serveur d'authentification (AS) grâce au protocole RADIUS (*Remote Authentication Dial In User Service* – RFC 2865, 2486). Ce dernier élément, obtient du réseau opérateur (HLR), un vecteur (*RAND, SRES*) permettant à AC de mener à bien la procédure d'authentification.
Depuis plusieurs années nous avons introduit le concept de carte à puce internet (lauréat de plusieurs prix industriels [9,10]. Dans ce papier nous présentons l'introduction de cette technologie pour la réalisation de module de sécurité (modules SIM-IP [11]) adaptés aux besoins émergeant des réseaux. A titre d'exemple nous décrivons succinctement un logiciel de téléphonie mettant en œuvre de tels composants.

Carte à puces classiques.

La carte à puce à microprocesseur, encore nommée SPOM [12] (Self Programmable One Chip Microcomputer) est une pastille de silicium dont la surface n'excède pas 25 mm^2 en raison des contraintes de flexion induites par le support en PVC sur lequel elle est collée. Ce composant apparu au début des années 80 s'est historiquement développé dans un contexte bancaire, afin de renforcer la sécurité des opérations de paiement (*off line* et *on line*), la puce réalise la signature d'une transaction ou l'authentification du porteur à l'aide d'une clé DES embarquée.
Un SPOM (cf. figure 1) comporte un CPU dont la puissance de traitement varie de quelques MIPS (pour les classiques processeurs 8 bits) à 33 MIPS [13] (dans le cas des nouvelles architectures RISC 32 bits). L'unité centrale occupe environ 25% du composant, la surface restante est allouée aux différents types de mémoire, c'est à dire la ROM (de 128 à 256 Ko, avec une surface relative 1), l'E^2PROM (64 à 128 Ko et une surface relative de 4) et la RAM

(quelques Ko avec une surface relative de 16). A l'horizon 2005 les fondeurs de silicium envisagent une réduction de surface du CPU aux alentours de 10 % de la puce sécurisée, des ressources RAM de l'ordre de 128 ko et l'introduction de technologie de mémoire non volatile (FeRAM ou FLASH) autorisant des capacités de stockage comprises entre 1 et 2 Mo. On considère généralement que les technologies mémoires évolueront plus lentement que celle des processeurs embarqués dont la puissance de traitement devrait suivre la loi de Moore, soit un accroissement de 64 en neuf ans (soit environ 2000 MIPS en 2010). Remarquons également qu'en l'état de l'art une puce sécurisée intègre un million de transistor, c'est à dire autant que les processeurs DX486 au début des années 90.

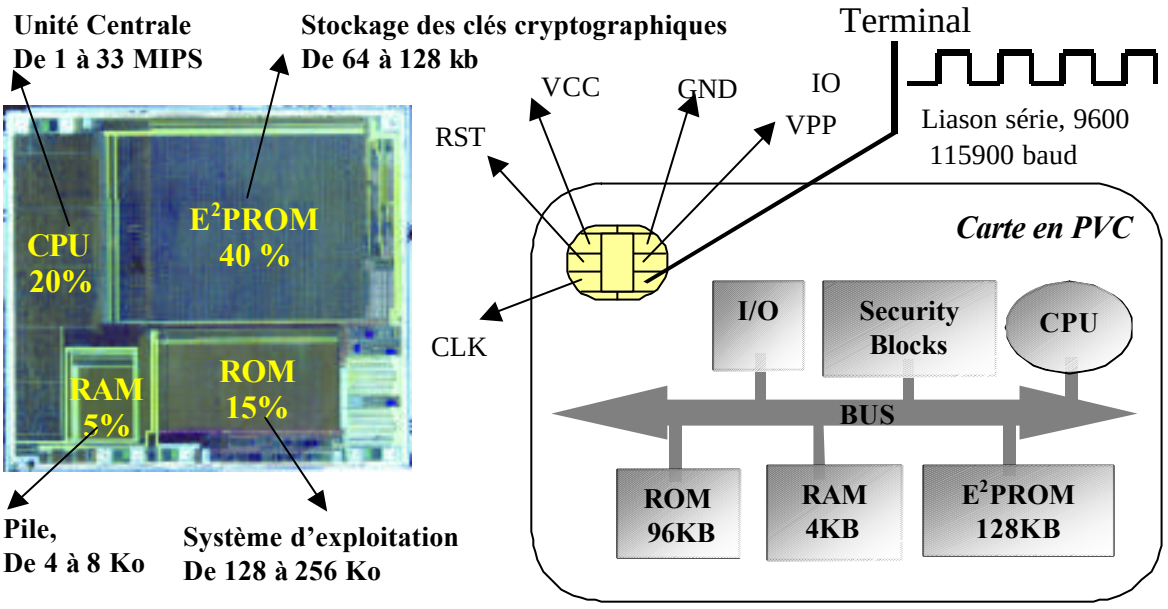

Figure 1. SPOM et carte à puce.

La principale qualité d'un SPOM est d'être *tamper resistant* c'est à dire de résister à des attaques dont le but est de lire des données secrètes (clés cryptographiques …) stockées dans la mémoire non volatile. Schématiquement on peut classer ces attaques en quatre catégories distinctes [14],

- *les attaques par intrusion* (à l'aide de microsondes…), ont pour objectifs l'acquisition d'informations sur le *design* de la puce (*reverse engineering*) ou sur la structure de son système d'exploitation (lecture optique du contenu de la ROM). L'enregistrement des signaux qui transitent sur le bus d'interconnexion peut permettre de capturer des clés ou de rejouer certaines séquences de commandes du CPU.
- *les attaques logicielles*, exploitent les failles de sécurité des protocoles, des algorithmes cryptographiques, et de leur implémentation.
- *les attaques par écoutes*, consistent en l'enregistrement et l'analyse de tous les signaux physiques produits par le processeur au cours de son fonctionnement. Par exemple l'analyse statistique des puissances consommées ([15] DPA – Differential Power Analysis) pendant l'exécution d'une suite connue d'instructions réalisant un algorithme DES, permet de déduire par corrélation (puissance consommée / clé) la valeur de la clé.
- *les attaques hardware* tentent de générer des défauts de fonctionnements inconnus du concepteur de la puce, à l'aide de mécanismes physiques tels que défauts d'alimentation en énergie, en horloge, ou au moyen de sources de rayonnement externes. Typiquement l'attaquant espère modifier une instruction de test ou de branchement conditionnel dans

certaines phases de fonctionnement de la puce, afin de lire tout ou partie de la NVM (mémoire non volatile).

Les contre-mesures tentent d'interdire les attaques par intrusion (par exemple en déposant un treillis métallique sur la puce ou en embrouillant les signaux du bus d'interconnexion), détectent les attaques hardwares à l'aide de différents capteurs (fréquence d'horloge, alimentation, température, ..) ou insèrent des délais aléatoires dans le système d'exploitation. L'implémentation des algorithmes cryptographiques tels que DES peut être adaptée pour offrir une plus grande résistance aux attaques DPA.
Une puce sécurisée émet et reçoit des messages à l'aide d'une liaison série *half duplex* (une seule patte d'entrée sortie est disponible), dont le débit est compris entre 9600 et 115,200 bauds. Le dialogue obéit à un paradigme de type question réponse, la norme ISO 7816 [16] décrit le format des commandes échangées (nommées APDU – Application Protocol Data Unit) ; la requête comporte au moins cinq octets (CLA INS P1 P2 P3) et des données optionnelles dont la longueur *Lc* est précisée par la valeur de l'octet P3. La carte délivre un message de réponse qui comprend des octets optionnels d'information (dont la longueur *Le* est spécifiée par l'octet P3) et un mot de status large de deux octets. (SW1 SW2, 9000 notifiant le succès d'une opération) Lorsque la longueur de la réponse n'est pas connue à priori un mot de status «61 Le» indique la longueur du message de réponse. Une fois ce paramètre connu le terminal obtient l'information au moyen de la commande *GET RESPONSE* (CLA C0 00 00 Le). La norme ISO7816 décrit par ailleurs un système hiérarchique de fichiers comportant un répertoire racine (MF, Master File), des sous répertoires (DF, Dedicated files) et des fichiers (EF, Elementary Files) ces différents composants étant identifiés par seulement deux octets.

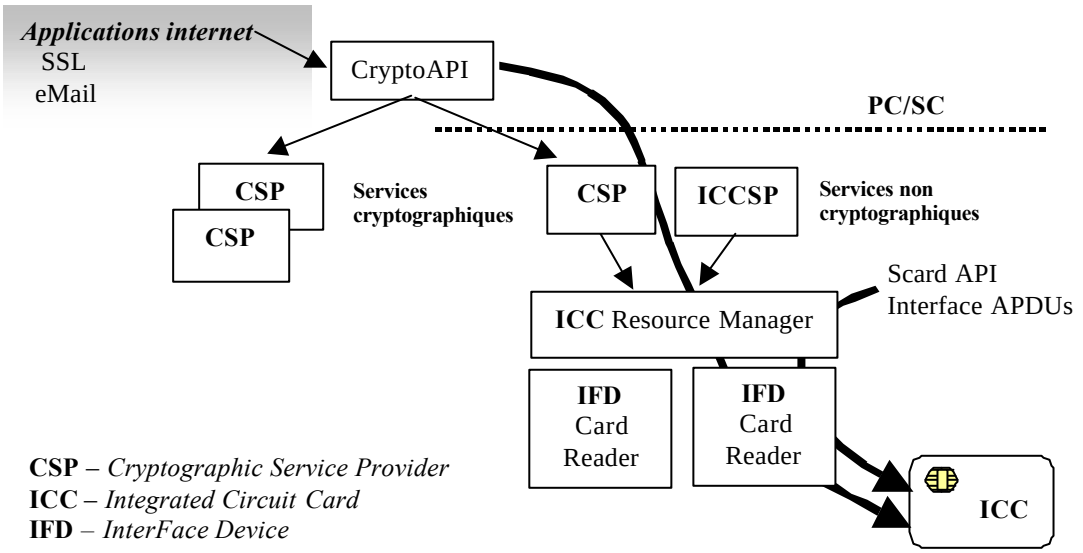

Figure 2. Exemple de middleware associé à une carte à puce.

Les opérations classiques supportées par une carte à puce sont la lecture ou l'écriture de données dans la mémoire non volatile et l'invocation de fonctions cryptographiques [12]. La mise en œuvre de ces ressources sécurisées depuis un logiciel implique la génération d'APDUs à l'aide d'une architecture adaptée. A titre d'exemple la figure 2 présente l'architecture des systèmes win32 permettant l'appel de fonctions cryptographiques logées dans des cartes à puces. Une application utilise les services offerts par une *CryptoAPI* qui implémente une interface avec des ressources cryptographiques (chiffrement, déchiffrement,

génération de clés) fournies par des *cryptographic service provider* (CSP). Ces composants réalisent les procédures cryptographiques par voie logicielle (fichiers DLLs), ou à l'aide de cartes à puces (SCSP – Smartcard CSP). Dans ce dernier cas la pile PC/SC [17] permet l'échange de messages entre une puce sécurisée et la *CryptoAPI*. Il devient ainsi possible de mettre en œuvre de manière transparente, depuis un navigateur ou une messagerie électronique, des services cryptographiques embarqués dans une puce.
Un bref examen des applications de l'internet montre que, malgré le besoin grandissant de sécurité de l'économie de réseau, pratiquement aucune d'entre elles ne mettent à profit les ressources sécurisées des cartes à puce. Puisque le protocole IP est devenu le standard de facto de communication entre applications, nous avons introduit un nouveau protocole, SmartTP (Smart Transfer Protocol) , décrit par un internet draft [18] permettant d'utiliser une puce comme un nœud internet ordinaire (et donc d'échanger des messages transportés par des paquets TCP/IP).

De la puce internet à l'objet communicant.

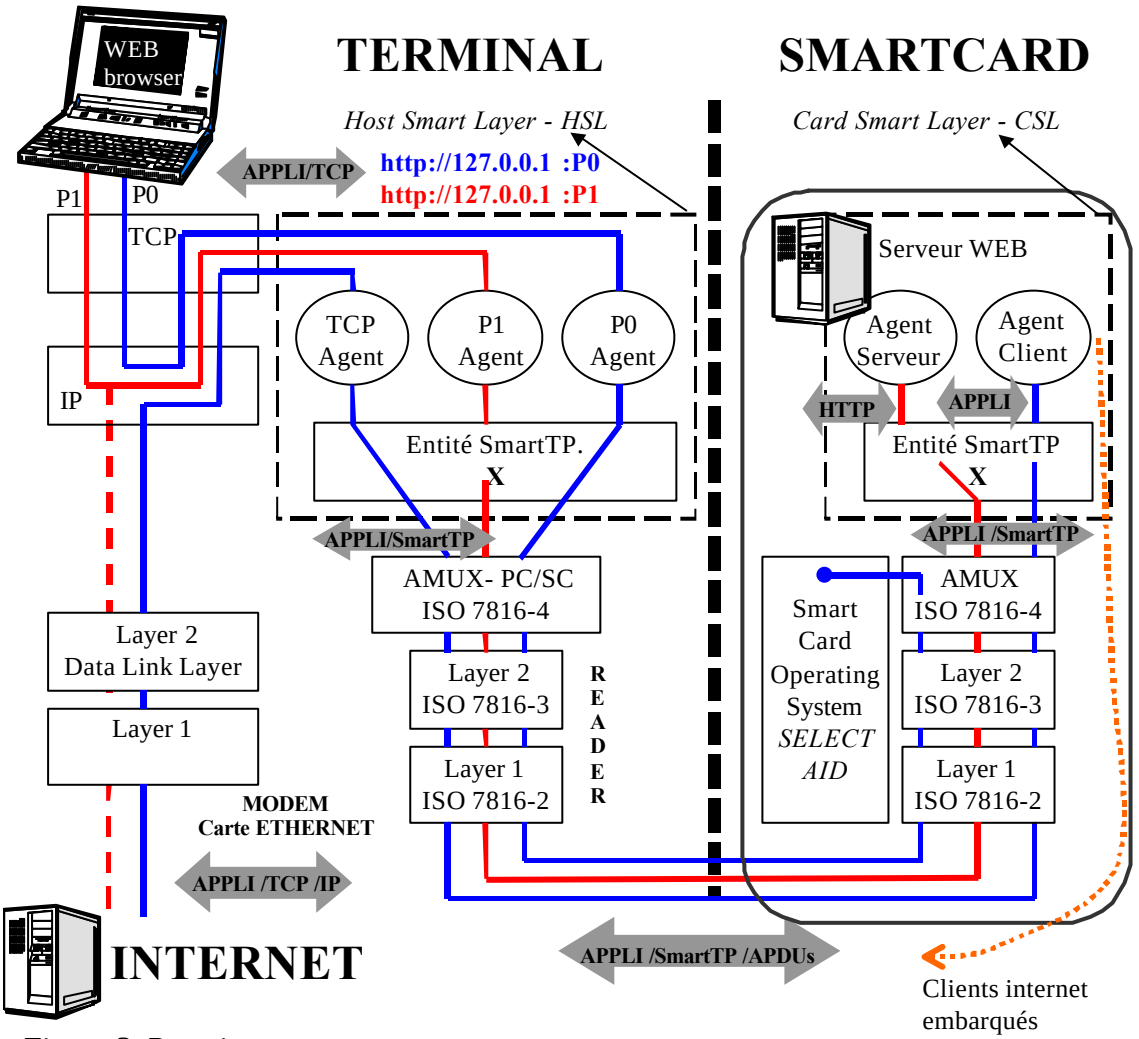

Figure 3. Puce internet.

L'approche puce internet consiste à loger dans la puce des applications internet clients ou serveurs. Dans l'état actuel de l'art il n'est pas possible d'intégrer une ressource de communication dans la surface réduite du SPOM (remarquons toutefois que ce verrou

pourrait disparaître avec l'intégration de la technologie *bluetooth*). En conséquence il est nécessaire d'utiliser les facilités de communication offertes par le terminal. Une autre contrainte résulte des protocoles d'échange de données de type half duplex entre terminal et carte. Cependant, bien que TCP présente des aspects *full duplex* induit par les paquets d'acquittement, les applications traditionnelles de l'internet (HTTP, LDAP, …) suivent un paradigme de type question/réponse compatible avec les restrictions citées précédemment. La particularité du modèle de communication des cartes à puce est donc la répartition des couches protocolaires entre terminal et carte. Les différentes options ont été décrites dans [19,22], schématiquement trois alternatives se présentent

- Utiliser une adresse IPv4 fixe [20], ce qui impose une mobilité restreinte à un réseau (ou sous réseau) IP particulier, et pose le problème de la disponibilité massive de ces adresses (1 milliard de puces sont produites par an).
- Partager l'adresse IP du terminal [21] et affecter à la puce un ou plusieurs ports TCP.
- Affecter une adresse IPv6 à chaque application embarquée [19]. Cet dernier choix est attractif en raison du nombre important d'adresses disponibles (2^{128}), cependant il est lié au déploiement massif des réseaux IPv6.

L'architecture que nous présentons permet le partage de la pile TCP/IP du terminal auquel la carte est connectée. Des entités logicielles autonomes (dénommées agents) sont implémentées dans le système hôte et la puce sécurisée, et dialoguent à l'aide du protocole SmartTP, transporté par des APDUs. Côté terminal des agents réseaux accèdent à la pile de communication et réalisent une conversion de protocole entre SmartTP et TCP. Côté carte des agents réalisent des protocoles serveurs (HTTP) ou client (LDAP, SIP, …) ; ces entités logicielles communiquent avec le réseau au moyen de sessions avec les agents réseaux échangeant des unités protocolaires SmartTP. Un paquet SmartTP est constitué d'un en tête de cinq octets et d'un champ optionnel de données de 240 octets au plus. Un en tête SmartTP comporte des références (2 octets) source et destination (équivalentes aux ports TCP) et un champ *FLAG* permettant la gestion des événements d'une session (ouverture, fermeture, échange de données bloquant, acquittement, …). Trois agents principaux assurent la gestion de la carte internet.

- L'agent P0 (associé au port TCP P0=8082) transforme une requête HTTP en une suite d'APDUs, destinée par exemple à instancier une application embarquée. Ainsi l'URL

  http://127.0.0.1:8082/?write=00A40400054A54455354

  sélectionne l'applet JTEST (Application Identifier = 5A 54 45 53 54 = JTEST), en cas de succès on obtient un fichier image de 1 pixel, dans le cas contraire un statut d'erreur HTTP est délivré (c'est une technique que nous nommons *CardBug* [23,24]).
- L'agent P1 (associé au port TCP P1=8080) ouvre une session avec le serveur WEB embarqué dans la puce. Ainsi l'URL,

  http://127.0.0.1:8080/Key1?x=69DA379EF99580A8

  réalise un chiffrement DES du mot 69DA379EF99580A8 à l'aide d'une clé Key1.
- L'agent *client TCP* permet aux agents cartes client d'ouvrir des sessions TCP et d'échanger des informations avec des serveurs internet distants.

Intégration des puces dans l'internet de nouvelle génération.

Nous classifierons succinctement (cf. tableau 1) l'usage des puces internet en trois catégories en fonction de la complexité des opérations conduites par la puce sécurisée,

- *Le mode mémoire*. La mémoire non volatile stocke des données identifiées par des URLs. Le terminal supposé sûre, lit ces informations (par exemple des identifiants ou des clés de chiffrement) mais réalise tous les calculs cryptographiques. La puce se comporte comme

un serveur portable qui embarque les données critiques d'un internaute (adresse de serveur, login, mot de passe …).

- *Le mode appel de procédure*. Les fonctions cryptographiques, sont exécutées par le processeur du SPOM et sont identifiées par des URLs de manière analogue aux processus démarrés depuis un serveur WEB à l'aide d'une interface de type Common Gateway Interface (CGI).
- *Le mode proxy de confiance*. Un protocole client incorporant des composants sécurisés (SSL, mot de passe jetable, …) est entièrement réalisé par la puce sécurisée. Typiquement une application embarquée est activée à l'aide d'une requête HTTP, elle se connecte à un serveur distant, conduit une authentification simple ou mutuelle et en cas de succès calcule une ou plusieurs clés de session qui seront utilisées par le terminal pour assurer des services de confidentialité ou d'intégrité de données.

Mode opératoire	Données.	Procédures.	Protocoles.
Mémoire	Puce	Terminal	Terminal
Appel de procédure	Puce	Puce	Terminal
Proxy de confiance	Puce	Puce	Puce

Tableau 1. Classification des modes opératoires d'une puce internet.

Les informations, procédures et protocoles stockés dans la puce internet sont identifiés par des URLs et accessibles à l'aide d'un schéma d'organisation de données qui peut être un parseur XML [26] ou une base de donnée [25]. Ce bloc fonctionnel utilise les services d'une interface sécurisée d'accès aux méthodes et données embarquées. Par exemple [26] lors d'une tentative d'accès à un objet protégé cette entité produit un formulaire HTML qui comporte un champ password et un pointeur sur un processus d'authentification.
Les principaux bénéfices de l'introduction de technologie XML dans les cartes internet sont la description des ressources embarquées à l'aide de DTD bien connues, et la compatibilité avec les procédures d'appels d'objets basées sur des dialectes dérivés de XML, telles que SOAP. Nous remarquerons également qu'un document XML est composé de divers entités transportées par le protocole HTTP, qui peuvent être stockées dans la puce internet [24].

SIM-IP.

De manière analogue aux terminaux de téléphonie mobile qui sont personnalisés, authentifiés et facturés à l'aide de cartes SIM, nous proposons de définir des modules de sécurité SIM-IP pour la personnalisation de logiciels multimédia (VoIP…) et la facturation de la qualité de service (QoS…) requise en particulier pour le transport de flux multimédia à travers le réseau internet.
L'architecture logicielle de notre module SIM-IP (cf. figure 4) comporte une ou plusieurs piles de communication, un daemon HTTP, un schéma d'organisation de donnée (parseur XML), une interface de sécurité supervisant les accès aux données, procédures (cryptographiques), et protocoles embarqués.
Un profil utilisateur contient un jeu de paramètres nécessaire à la réalisation d'un service, en voici une liste non exhaustive,

- Des clés (et des procédures) authentifiant le bénéficiaire d'un service particulier, ou assurant la confidentialité ou l'intégrité des informations échangées. Ainsi les messages des protocoles RSVP (rfc 2205) ou COPS (rfc 2748) sont identifiés par un *integrity object* [27], qui délivre la signature des données (*keyed message digest*) à l'aide d'une fonction

d'empreinte MD5 et d'une clé d'identification (*key identifier*). Certaines clés sont détenues par le prestataire du service, et d'autres par le porteur de la carte SIM-IP.

- Des données nécessaires au service délivré, par exemple des identifiants d'utilisateur (Network Access Identifier [31], adresses SIP [28], h323_ID [29], …), des adresses de serveurs divers (authentification, annuaires, politiques de QoS…), des clés de session, des informations personnelles (carnets d'adresses …).
- Des protocoles réalisant des opérations sécurisées telles que le classique SSL, des enregistrements à des serveurs de localisation (LDAP, SIP…), des appels SIP authentifiés (INVITE…).

Nous avons développé un premier prototype qui comprend un logiciel de téléphonie H323 sous win32 (une adaptation du code public *openH323*) muni d'une interface carte à puce (PC/SC), et une carte SIM-IP (cf. tableau 2) mettant en œuvre un paradigme de type mémoire. Les paramètres de personnalisation du logiciel sont,

- un identifiant (h323_ID) figurant dans le message *setup* du paquet d'appel Q.931 du protocole H323.
- un carnet d'adresse qui comporte une liste de h323_ID visualisée par le logiciel à l'aide d'une liste déroulante . Le premier élément de la liste fournit l'identifiant du porteur de la carte.

Le logiciel détecte l'insertion d'une carte SIM-IP, sélectionne une application carte embarquée JTEST, et lit le carnet d'adresse. Chaque élément du carnet d'adresse est associé à une clé DES d'authentification (KEYx), et à une adresse IP (ADRx). Une prochaine version comportera pour chaque correspondant le nom de l'annuaire LDAP ou l'on peut obtenir son adresse IP (ILSx).

Afin de prévenir les appels indésirables le logiciel authentifie un appel sortant en ajoutant au h323_ID local un préfixe de 8 octets chiffré par la clé KEYx du correspondant (identifié par son adresse IP ADRx ou son annuaire ILSx), qui inclut les champs suivants,

- un nombre aléatoire de 2 octets (r2) étendu de manière symétrique à 4 octets ($r4=2^{16}.r2 + r2$).
- l'heure GMT exprimée en format UNIX (4 octets, représentant le nombre de secondes écoulées depuis le 1° janvier 1970).

Le logiciel destinataire de l'appel extrait le h323_ID du message *setup* de l'appelant, en déduit sa clé KEYx, et déchiffre le préfixe. Il vérifie que le nombre r4 comporte deux parties symétriques et que l'heure d'émission de l'appel est cohérente (par exemple le délai de transit est inférieur à une minute…)..

Ressource embarquée	URL SIM-IP
Application JTEST	http ://127.0.0.1 :8082/ ?write=00A40400054A54455354
Carnet d'adresses	http ://127.0.0.1 :8080/name
clé DES pour l'index x	http ://127.0.0.1 :8080/KEYx
Adresse IP pour l'index x	http ://127.0.0.1 :8080/ADRx
Nom de l'annuaire pour l'index x	http ://127.0.0.1 :8080/ILSx

Tableau 2, un exemple de contenu de module SIM-IP

Une version améliorée du module de sécurité intégrera la fonction de génération du h323_ID du destinataire, ainsi qu'une procédure de vérification du h323_ID entrant, et calculera des clés de session destinées au chiffrement et au contrôle d'intégrité du flux multimédia transporté par le protocole RTP. La gestion de la qualité de service pourra également être

prise en compte à l'aide d'un protocole tel que RSVP ou COPS logé dans la carte SIM-IP, réalisant le calcul des *integrity object* à l'aide de clés prépayées.

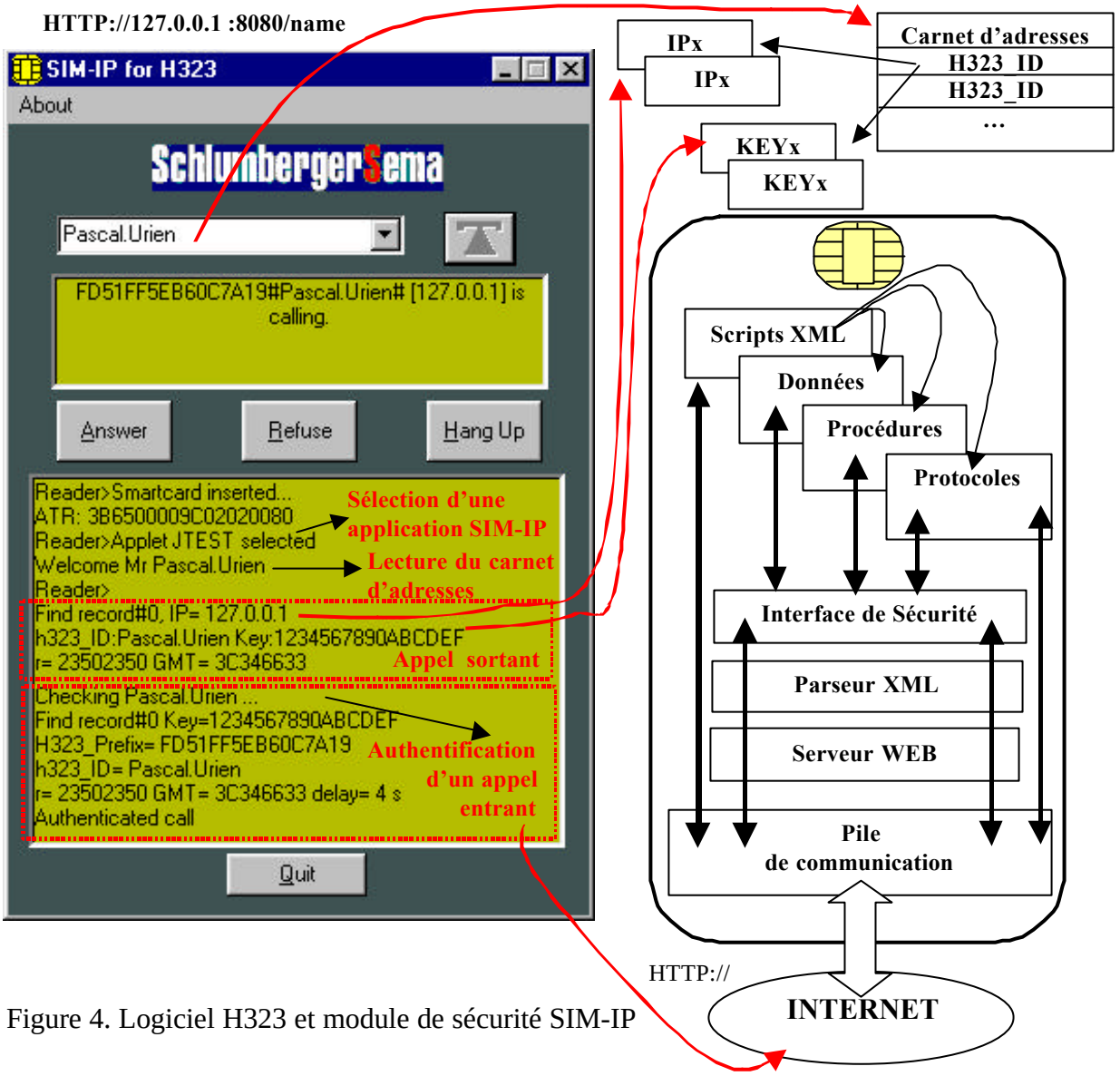

Figure 4. Logiciel H323 et module de sécurité SIM-IP

Conclusion.

Dans ce papier vous avons introduit un concept de puce internet et son application à des modules de sécurité destinés à personnaliser et à gérer les aspects sécuritaires des applications internet, plus particulièrement multimédia. Cette approche fera l'objet d'études plus approfondies dans le cadre du projet MMQoS (*Maîtrise de la Mobilité et de la Qualité de service dans la 4° génération de mobile*) labelisé en mai 2001 par le RNRT [32] . Nous espérons promouvoir l'introduction des puces sécurisées dans les protocoles de l'internet, par exemple en standardisant un ou plusieurs TCP dédiés. Nous envisageons également, à moyenne échéance, l'introduction de cartes supportant des communications sans fils afin de permettre la personnalisation de logiciels par simple présence d'un utilisateur.

Références.

[1] SOC'2001 – Séminaire des Objets Communicants, SEE RNRT, Grenoble 17,18 octobre 2001

[2] J.Zuidweg, "Software architectures for next generation networks", Protocols for Multimedia Systems PROMS 2000 pp 513,527, ISBN 83-88309-05-6.

[3] de Laat, C., et al., "Generic AAA Architecture", RFC 2903, August 2000.

[4] W. Arbaugh, N. Shankar, and Y. Wan, Your 802.11 « Wireless Network has No Clothes. http://www.cs.umd.edu/~waa/wireless.pdf .

[5] William A.Arbaugh, "An Inductive Chosen Plaintext Attack against WEP/WEP2", mai 2001, http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-230.zip

[6] ETSI - GSM 11.11 "Digital cellular telecommunications system(Phase2+); Specification of the Subscriber Interface Identity Module – Mobile Equipment (SIM_ME)interface".

[7] http://www.nokia.com/networks/wireless_lan/solution_faq.html

[8] J.Ala-Laurila, J.Mikkonen, J.Rinnemaa "Wireless LAN Access Network Architecture for Mobile Operators", IEEE Communications Magazine November 2001 pp 82,89

[9] Sésame 2000, "Meilleure innovation technologique", cartes'2000 octobre 2000, Paris.

[10] Advanced Award 2001, "Most Innovative Product of the Year", février 2001, Londres.

[11] Pascal Urien "SIM-IP, Smartcard benefits for wireless applications", Application and Services in Wireless Networks ASW'2001 25th-27th July 2001, INT Evry France, Hermès Sciences publications ISBN 2-7462-0305-7.

[12] Guillou, L.C. and Ugon, M. and Quisquater, J.J.(1992), "The smard card: A standardized security device dedicated to public cryptology", *Contemporary cryptology - The science of information integrity , G. J. Simmons, Ed., IEEE Press*, pp. 561-613.

[13] Tual, J.P. (1999) "MASSC : A Generic Architecture for Multi application Smart Cards", *IEEE Micro journal,* N°0272-1739/99.

[14] Kommerling, 0. and Kuhn, M.G. (1999) "Design Principles for Tamper-Resistant smartcard Processors" Proceedings of the USENIX Workshop on Smartcard Technology Smartcard'99, pp 9-20.

[15] Kocher, P.and Jaffe, J.and Jun,B. (1999) "Differential Power Analysis" Proceedings of CRYPTO'99, Springer-Verlag, pp 388-397.

[16] ISO/IEC 7816, "Identification cards - Integrated circuit(s) card with contact". *International Organization for Standardization.*

[17] PC/SC (1996) "Interoperability Specification for ICCs and Personal Computer Systems", *© 1996 CP8 Transac, HP, Microsoft, Schlumberger, Siemens Nixdorf.*

[18] SmartTP (2001) "SmartTP, smart transfer protocol" *internet draft, draft-urien-SmartTP-00.txt.*

[19] Pascal Urien, Guy Pujolle «IP benefits for smartcards use in wireless networks » ETSI Project Smartcard Platform (EP SCP) Tdoc SCP-010189, Turku-Finland 26,29 june 2001.

[20] Rees, J. and Honeyman, P. (2000),"Webcard: a Java Card web server". *Proceeding of Smart Card Research and Advanced Application Conference CARDIS'2000.*

[21] Urien, P. (2000) " Internet Card, a smart card as a true Internet node", *Computer Communication*, volume 23, issue 17.

[22] Pascal Urien, Hayder Saleh, Adel Tizraoui « Carte à puce internet, état de l'art et perpectives » Actes du congrès JRES'2001, Quatrièmes Journées Réseaux 2001 pp 353,364, Lyon 10-14 décembre 2001.

[23] Pascal Urien - Hayder Saleh - Adel Tizraoui. "Authentification dynamique par carte à puce internet, une possible alternative à l'usage polémique des cookies et des WebBugs". Infosec'Com 2001 – 29,30,31 mai 2001 la défense.

[24] Pascal Urien, Hayder Saleh, Adel Tizraoui , "XML Smartcards", *LNCS 2093* IEEE International Conference on Networking, ICN'01, July 11-13, 2001 - CREF, Colmar, France.

[25] Christophe Bobineau, Luc Bouganim, Philippe Pucheral, Patrick Valduriez, "PicoDBMS: Scaling down Database Techniques for the Smartcard" VLDB'2000 26th International Conference on Very Large Database

[26] Urien, P. (2001) "Programming internet smartcard with XML scripts", *LNCS 2140*, e-Smart 2001.

[27] « RSVP Cryptographic Authentication » RFC 2747 January 2000.

[28] « SIP: Session Initiation Protocol » RFC 2543 March 1999.

[29] International Telecommunication Union (ITU) Recommendation H323, "Packet-based multimedia communication systems", October 1997.

[30] International Telecommunication Union (ITU) H.235 "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals" Version 2 November 2000.

[31] « The Network Access Identifier » RFC 2486, January 1999.

[32] http://www.telecom.gouv.fr/rnrt/projets/res_01_52.htm