

INTERVIEW

“Sécurité : IP VPN est maintenant devenu la norme”

La gestion de sites distants réclame pour se déployer et se généraliser des réseaux à la fois sécurisés et performants. La migration vers IP (Internet Protocol) impose ainsi de nouvelles réponses en matière de sécurité, notamment pour l'utilisation de la technologie KVM (clavier, écran et souris déportés).



Jean-Michel Craye
SCE/GC Sécurité



François Dufour
DGC/Banque assurance

France Telecom

■ Où en est-on des déploiements IP dans le secteur bancaire ?

Les technologies IP sont, aujourd'hui, largement déployées dans les banques pour établir les liaisons entre les sièges, les sites informatiques et les agences, et entre les agences. Voilà trois ans que la migration suit son chemin, que les lignes spécialisées (Frame Relay) ou les accès Numéris sont petit à petit remplacés, les PABX supprimés (de simples téléphones les remplacent) et que la convergence voix-données se concrétise avec la généralisation des accès DSL, de plus en plus SDSL d'ailleurs [1].

■ Comment les questions de sécurité sont-elles résolues dans ce nouvel environnement ?

Ce mouvement de migration vers les technologies IP a engendré une “virtualisation” des accès – la sécurité n'est plus assurée par les seuls liens physiques classiques – qui a imposé des réponses nouvelles en matière de sécurité. Depuis fin 2002, la technologie MPLS (Multiple Protocol Label Switching) a joué un grand rôle dans la généralisation de l'IP sécurisé. Elle permet d'assurer une étanchéité des flux IP qui est à la base de nos réseaux VPN (Virtual Private Network). Ces derniers sont aujourd'hui la norme, en particulier dans le bancaire. Notre réseau IP VPN a, d'ailleurs, été le premier à rece-

voir, en 2001, la certification EAL1+ du DCSSI [2]. Notre solution permet d'assurer, en plus de cette capacité à distinguer et à cloisonner des flux, que l'administration de ces réseaux est elle-même sécurisée. Cela signifie que les accès des routeurs d'entreprise sont contrôlés, et que l'intégrité de leurs tables de routage est garantie. La technologie MPLS/VPN assure également une sélection appropriée des flux qui sont prioritaires (entre la voix qui réclame du temps réel, et les données dont les paquets peuvent être réassemblés sans ces contraintes de temps, par exemple) de façon à garantir la qualité du service.

■ La disponibilité offerte par les réseaux IP est-elle désormais la même que sur les réseaux classiques ?

Le niveau de disponibilité est sensiblement le même que celui qui était atteint avec les lignes spécialisées. Mais le rapport prix/performance a changé d'unité de mesure. À prix égal, le volume de données échangées a été multiplié par des facteurs qui varient de 10 à 100.

■ Votre offre IP VPN peut-elle se décliner pour répondre à des besoins spécifiques en matière de sécurité ou de performances ?

Le domaine de la banque et de la finance, celui des grandes administrations et de cer-

taines industries sont, en effet, plus sensibles que d'autres aux questions touchant à la sécurité, mais nous n'avons pas à proprement parler d'offres très différentes à proposer aux uns et autres. Les besoins restent assez similaires. Par contre, nous négocions avec chacun de nos clients des engagements de niveau de service (SLA) qui portent sur le niveau de disponibilité ou sur des interruptions minimales de services, par exemple. Et, pour assurer une surveillance et une analyse du réseau conformes à des impératifs réglementaires de reporting et de tracking – c'est le cas avec de grandes banques –, nous pouvons mettre à disposition de nos clients un responsable sécurité qui sera chargé de consolider toutes les informations recueillies pour les diffuser au client auquel il est rattaché.

■ L'IP favorise le déploiement de nouvelles générations de KVM [3] et de nouveaux usages dans la gestion de sites distants. L'IP change-t-il la donne en termes de sécurité ?

La sécurité des KVM est, en effet, une vraie question. Il faut que les flux d'administration ou de gestion ne puissent pas être écoutés, et que le canal d'accès ne devienne pas une porte ouverte vers les systèmes d'information. Mais les solutions ne sont pas purement techniques (IP VPN, authentification forte, confidentialité), elles ont un aspect évidemment lié au management des personnes et aux procédures qu'il est impératif de respecter et de faire respecter. ■

Propos recueillis par Y. A.

[1] Symmetric Digital Subscriber Line. Le même débit est garanti dans les deux sens (montant et descendant).

[2] Direction centrale de la sécurité des systèmes d'informations. Elle est placée sous l'autorité du secrétaire général de la Défense nationale. EAL1+ (Evaluation Assurance Level) correspond au premier niveau de certification des critères communs (standard en matière de sécurité).

Le “+” signifie que ce niveau est “augmenté.”

[3] Keyboard, Video, Mouse: clavier, écran et souris déportés pour mutualiser l'accès à des serveurs distants et assurer leur contrôle.

ENQUÊTE GLOBAL INSIGHT

Le volume des transactions électroniques de paiement va doubler en 2010 par rapport à 2004

■ Le nombre de transactions électroniques de paiement devrait connaître dans le monde une croissance moyenne annuelle de 12,9 % sur la période 2004-2009 pour atteindre un volume de 384,2 milliards d'opérations en 2009 et, du coup, doubler au cours de l'année 2010 par rapport volume observé en 2004 (209,8 milliards de transactions). C'est l'un des résultats d'une étude conduite par **Global Insight** récemment publiée (mai 2006) pour le compte d'ACI Worldwide. Elle constate, en outre, que le

volume global des transactions électroniques de paiement est, à quelques exceptions près [1], directement lié à l'importance du PIB. Cette évolution du volume des transactions est également, selon les moyens de paiement utilisés [2], plus ou moins liée à celle de la consommation des ménages ou des technologies.

L'étude montre, par ailleurs, un mouvement d'accélération qui se confirme au détriment des transactions réalisées en espèces et en chèques. L'utilisation de ces derniers, par

exemple, ne cesse de décliner depuis 1999, puisque sa part dans le volume des transactions électroniques passe de 35 % il y a sept ans, à 20 % en 2004, et à 10 % en 2009. Dans le même temps, la part des paiements électroniques réalisés chez les commerçants passe de 43 % en 1999, à 54 % en 2004 et 61 % en 2009.

Cette évolution ne touche pas de la même façon tous les pays ni toutes les régions du monde. La Chine et l'Inde progressent plus vite que la moyenne : la première devrait doubler le nombre

de ses transactions en trois ans, la seconde en quatre ans. L'Asie-Pacifique et l'Europe de l'Est, de leurs côtés, devraient respectivement connaître des croissances annuelles moyennes de 19,2 % et 21,6 %.

[1] Le Canada et le Brésil, avec une part mondiale de leur PIB respectif assez faible (1,9 % et 2,3 %), talonnent la France (4,1 %) au 5^e et 6^e rang, tandis que le Japon avec un fort PIB (14 % du PIB mondial) ne figure qu'au 10^e rang avec un faible niveau de transactions (deux fois moins que le Canada).

[2] Il s'agit des transactions "non-cash" réalisées sous différentes formes (paiements par chèques, transferts et paiements chez les commerçants), et paiement de gros montants de types LVTS, ACH, RTGS, etc.

Forte croissance du nombre d'ATM en Europe de l'Est et centrale

■ Selon Retail Banking Research, le nombre d'ATM en Europe de l'Est et centrale, a connu l'an dernier une croissance de 26 % pour approcher les 70 000 unités, réalisant ainsi la progression la plus importante des régions du monde. Dans le même temps, les volumes des retraits d'argent liquide via les ATM ont augmenté de 20 % pour atteindre 2,4 milliards transactions, cor-

respondant à un total de 175 milliards d'euros (+33 % par rapport à 2004). Le montant moyen de ces retraits est de 121 euros en Hongrie et de 37 euros en Ukraine. NCR reste le principal fournisseur de ces équipements avec une part de marché de 45 %, et Windows NT remplace petit à petit OS/2 et s'impose comme le système d'exploitation le plus utilisé dans ces machines.

Les livraisons mondiales de cartes à puce bancaires devraient encore croître de 20 % cette année

■ Selon **Eurosmart**, l'association qui regroupe plus de 80 % des industriels de la carte à puce dans le monde, 400 millions de cartes à puce bancaires devraient être livrées cette année dans le monde. Ce chiffre représente une croissance de 19 % par rapport à l'an passé (336 millions) qui est principalement due à la poursuite de la migration EMV à un rythme assez similaire à celui enregistré en 2005 (+20 %), et, pour une part encore réduite, à la confirmation de la maturité du marché du paiement sans contact aux États-Unis (entre

10 et 12 millions de cartes en 2005, 30 millions prévus cette année) et à son démarrage en Asie.

La migration EMV marque le pas cette année en Grande-Bretagne où elle est pratiquement achevée, mais elle connaît ses premiers déploiements en Turquie, au Canada, en Chine, en Ukraine et en Thaïlande. La part en volume des cartes bancaires dans les marchés de la carte à puce, dominés par la carte SIM pour la téléphonie mobile (73,6 %), reste stable autour de 17,7 %.

Combiner la gestion commerciale et la vente mobile

■ Le terminal de paiement développé sous le nom de MobiPos par MoneyLine annonce une nouvelle génération d'ordinateurs portables "tout-en-un" capables de rassembler des fonctions jusque-là séparées dans des machines différentes et peu intégrées (PC de bureau et terminal de paiement). Cet ordinateur, bâti sur une plateforme Windows CE – un gage d'ouverture indispensable pour assurer les fonctions de prise de commande, de saisie d'articles, de consultation, et de facturation –, intègre aussi les fonctions sécurisées d'un terminal

de paiement avec lecteur de cartes à puce (EMV Level 1) et quatre SAM (Security Access Module). Il est équipé d'une imprimante, d'un lecteur de codes barre, dispose de ports USB et RS 232, et d'un clavier 20 touches. En embarquant le logiciel de monétique intégré C3 Axis de MoneyLine, il assure la gestion des différents contrôles de cartes dans le terminal. Enfin, il peut accéder à la base de données monétique open source Archicube du constructeur via une liaison Wi-Fi ou GPRS.



Contrôle KVM sur IP optimisé

La technologie KVM sur IP permettant de vous déplacer sans bouger. Vous cherchez une solution pour accéder à vos serveurs quand et où vous le souhaitez. Raritan vous propose la solution :

Dominion® KX

- Cryptage SSL 128 bits
- Chiffrement de toutes les données – notamment la vidéo
- Sécurité additionnelle offerte par la fonctionnalité "server and client shared key"
- Fonctionnalité IP-ACL (Access Control List)
- Accès local et distant avec authentification externe
- Profils de sécurité utilisateur personnalisés



Contactez nous ou visitez: Raritan.fr

Raritan France

120 Rue Jean Jaurès, 92300 Levallois-Perret
Tél: 01.47.56.20.39 sales.france@raritan.com

 **Raritan®**
When you're ready to take control®

En bref

■ Transaction Systems

Architects Inc (TSA), fournisseur des solutions de paiement électroniques du groupe ACI Worldwide, va acquérir la société Electronic Payment Systems AG (eps), un fournisseur de systèmes de paiement électronique en Allemagne et Suisse. TSA a publié récemment une étude qui montre que l'Allemagne est le troisième marché mondial derrière les États-Unis et le Royaume-Uni, pour le nombre des transactions électroniques de paiement.

■ **Axalto** a livré près de 18 millions de cartes à puce bancaires au cours du premier trimestre 2006. Son activité Services Financiers a réalisé un chiffre d'affaires de 42 millions de dollars, en progression de 2 % à taux de change constants. L'activité est restée globalement stable dans la région Europe, Moyen-Orient et Afrique, avec une bonne progression du Moyen-Orient, de l'Europe centrale et de l'Europe du Sud et un recul au Royaume-Uni. L'activité en Asie est également restée stable. La progression du chiffre d'affaires est surtout due aux marchés américains qui progressent grâce à la migration EMV en Amérique latine et au déploiement des cartes de paiement sans contact aux États-Unis.

■ **Gemplus** a enregistré pour son premier trimestre une croissance de ses livraisons de cartes à puce bancaires de 75 % à 22 millions d'unités, et réalisé un chiffre d'affaires en progression de 55 % à 56,4 millions d'euros.

■ Oberthur Card Systems

a livré au cours du premier trimestre 2006, 16 millions de cartes à puce bancaires contre 19,6 millions au cours du premier trimestre 2005, et réalisé pour cette activité un chiffre d'affaires de 24,7 millions d'euros en baisse de 23,4 % en tendance annuelle.

■ **Multiratings**, une société d'informations financières dans le secteur de la gestion d'actifs à destination des professionnels (investisseurs institutionnels) vient de reprendre l'activité de stockage et de diffusion de données OPCVM de Logicinvest, et d'acquérir le logiciel Logicinvest. Ce dernier, primé par l'Anvar en 2002, est un logiciel de capture et de mise à jour automatique de données qui a permis à Logicinvest de développer une base de données de 26000 fonds d'investissement.

■ **BEA Systems**, un leader mondial des logiciels d'infrastructure d'entreprise, publie un Livre Blanc entièrement dédié à la MiFID de la Commission européenne apportant des changements fondamentaux aux marchés des instruments financiers dans l'Union européenne et dont l'objectif est d'introduire des règles et définitions communes interdisant aux pays membres de mettre en place des barrières compliquant artificiellement les opérations transfrontalières.

Paiement sans contact avec le téléphone mobile : le Mobey Forum identifie trois scénarios

■ Le **Mobey Forum** qui réunit de grandes banques [1], des intégrateurs, des fabricants de téléphones mobiles et des fournisseurs de technologies, travaille depuis quelques années sur les perspectives ouvertes par l'utilisation du téléphone mobile dans le domaine de la banque (paiement, banque en ligne, opérations de courtage). Il a identifié trois scénarios possibles pour assurer le succès du déploiement du téléphone mobile comme moyen de paiement sans contact. Ces scénarios correspondent à des modèles de développement (*business ecosystem*) dans lesquels les acteurs dominants baptisés *platform managers* changent selon le rôle qu'ils jouent vis-à-vis de l'élément sécurisé (circuit embarqué dans le téléphone qui peut être une carte SIM, un TPM, ou un circuit NFC associé au téléphone) [2] chargé de stocker les éléments de confiance réclamés par les transactions de paiement. Dans le cas d'application d'envergure internationale, le Mobey Forum voit des sociétés chargées de personna-

liser le circuit sécurisé jouer le rôle de *platform manager*, tandis que ce rôle revient à des opérateurs télécoms pour des applications d'envergure nationale, ces opérateurs choisissant d'utiliser la carte SIM, établie déjà comme le lien privilégié avec leurs abonnés, pour stocker les applications de paiement. Enfin, les banques et les fournisseurs de service de paiement apparaissent dans un troisième scénario, comme les acteurs principaux dans un modèle de marchés de niche, avec le risque toutefois d'une fragmentation excessive de ce type de marchés. Pour le Mobey Forum, ces scénarios sont tout aussi valables pour des applications d'authentification en ligne.

[1] ABN AMRO, Bank of Ireland, HSBC, The Royal Bank of Scotland, Accenture, Nokia, HP entre autres.

[2] TPM pour Trusted Platform Module. Un type de circuit que l'on trouve déjà dans certains PC et qui, dans le cas présent, permet de stocker des secrets et l'application associés aux opérateurs de paiement. NFC pour Near Field Communication, le circuit radiofréquence qui permet d'assurer la transaction sans contact aux niveaux des couches basses.

Sécurité et maintenance : Intel réinvente le PC pour l'entreprise

■ **Intel** vient de dévoiler une technologie qui servira de plateforme matérielle et logicielle à une nouvelle génération de PC d'entreprise qui devraient apparaître sur le marché au cours du second semestre de cette année. Baptisée vPro, cette technologie apporte des réponses inédites en matière de sécurité, mais également des solutions nouvelles pour améliorer la gestion à dis-

tance et la maintenance des parcs d'ordinateurs dans une entreprise. À ces deux objectifs qui visent à réduire le TCO (*Total Cost of Ownership*) de cette nouvelle génération de PC et d'accroître sa sécurité, s'y ajoute un troisième : celui offrir des gains en termes de consommation électrique et de dissipation thermique grâce au développement d'une architecture et de techniques

dédiées à la gestion de l'énergie*. Une petite révolution qui doit se marier l'heure venue avec le futur système d'exploitation Vista de Microsoft, lui aussi conçu pour apporter des réponses nouvelles en termes de sécurité. Mais pas seulement. Cette plateforme est également conçue pour faciliter l'utilisation de systèmes d'exploitation différents (Linux, XP, 2000), et en particulier de sys-

tèmes d'exploitation dits légers (*thin embedded OS*), pour démarrer en dehors et en parallèle du système d'exploitation principal, sur une partition protégée, des applications spécifiques de sécurité (anti-virus, pare-feu) ou de maintenance.

*Issues des développements pour les PC portables, ces technologies qui permettent "d'éteindre" certaines zones des processeurs ou des mémoires, vont permettre des gains jusqu'à 40 % d'énergie.