OPENTRUST™

OpenTrust WhitePaper

Trusted Ecosystems ou la sécurité de proche en proche

Sherley Brothier, Directeur du département Recherche et Développement d'OpenTrust

Paris, 15 mai 2008

SOMMAIRE

1 DE NOUVEAUX DEFIS POUR LES DSI

La nécessité d'adapter son Système d'Information (SI) aux impératifs métiers, la migration des réseaux privés vers l'Internet et le besoin de dématérialiser les processus d'entreprise pour plus de réactivité et de productivité posent de nouveaux défis de plus en plus complexes à résoudre :

- Comment allier la flexibilité du SI (réorganisations, nouvelles offres ou acquisitions) avec des exigences de sécurité chaque jour plus présentes ?
- Comment opérer un réseau en toute sécurité et disponibilité alors qu'il est de plus ouvert à Internet ?
- Comment contrôler l'accès de mon système d'information en toute sécurité par mes clients, mes fournisseurs, mes partenaires qui peuvent être aussi mes concurrents ?
- Comment gérer la mobilité indispensable aux salariés, et concilier convivialité et sécurité pour les VIP de l'entreprise ?
- Comment gérer et contrôler de nouveaux moyens d'accès incontrôlables (pda, smart phones, pc du domicile, etc…) ?
- Comment recruter et motiver des jeunes diplômés sans leur donner un environnement de travail qui intègre toutes les « nouvelles » technologies qui ne sont pour eux qu'un environnement naturel (web 2.0, skype, wifi, etc..) ?
- Pourquoi avoir investi des dizaines/centaines de millions d'euros pour mettre en œuvre un ERP SAP ou Oracle et continuer à envoyer à un autre utilisateur d'ERP SAP ou Oracle des factures et des bons de commandes papier par la Poste ?

Face à toutes ces transformations liées à l'ouverture, le travail en réseau, le changement de « consommation » du SI, chaque entreprise doit continuer à garantir un niveau de sécurité élevé quel que soit le terminal utilisé (poste de travail, laptop, PDA, poste « public », etc.), quelle que soit la localisation de l'utilisateur (à son poste de travail, en mobilité au sein d'un site de l'entreprise, depuis l'extérieur de son entreprise, etc.), quel que soit le réseau informatique utilisé (LAN, LS, xDSL, 3G, WIFI, Internet, etc.) et potentiellement, quelle que soit la ressource adressée (application métier interne au SI, application B2B, messagerie, téléphone, imprimante, réseau, partenaire, fournisseur, etc.).

Parallèlement, la plupart des nouveaux besoins fonctionnels applicatifs doivent prendre en compte des fonctions de sécurité : la dématérialisation des processus, des transactions et des échanges, qui sont aujourd'hui au coeur des processus métiers de chaque entreprise, nécessitent plus que jamais des fonctions d'authentification, de traçabilité, d'intégrité, d'audit, de confidentialité ou encore de non répudiation.

La sécurisation et la confiance accordée à son SI sont donc au cœur des enjeux métiers et, sans remettre en cause la nécessité de la défense d'un « périmètre », nécessitent une approche complémentaire mais incontournable basée sur la mise en place de multiples écosystèmes de confiance au sein et à l'extérieur de l'entreprise.

2 LES LIMITES DE L'APPROCHE ACTUELLE DE LA SECURITE : LES QUESTIONS DE CONFIANCE

L'époque où le rôle des équipes sécurité se réduisait à protéger le système d'information en ajoutant « machinalement » en périphérie du réseau informatique d'entreprise (ie. généralement à la frontière du réseau d'entreprise et de l'interconnexion Internet) un nouvel équipement de sécurité (Firewall, proxy filtrant/authentifiant, anti-SPAM, anti-virus, système de détection d'intrusion, etc.) en regard de chaque nouvelle vulnérabilité est bel et bien révolue.

Aujourd'hui la majorité des architectures réseau est basée sur de l'authentification MAC et IP sur des déploiements de solutions IPSec ou VPN SSL ainsi que sur de la gestion de règles de routage ou de filtrage relativement complexes à administrer et à suivre dans le temps (syndrome du « je ne sais pas forcément à quoi sert cette règle dans mon Firewall, mais je préfère ne pas y toucher par crainte d'un dommage collatéral non prévu »).

Pour pallier certaines limitations, les entreprises ont largement déployé des projets de gestion d'identités constitués le plus souvent d'un annuaire d'entreprise, d'un outil de « Enterprise Single Sign-On » (eSSO) ou de WebSSO, afin de faciliter la gestion du cycle de vie des identités basé sur des mots de passe dans le SI.

Mais l'existant et les solutions de sécurité défensive actuellement mises en place ne permettent toujours pas de répondre aux trois questions simples mais sur lesquelles repose toute la confiance qu'on accorde à son SI :

- Ai-je l'assurance de l'identité de la personne ou de l'équipement avec lequel je communique ?
- Ai-je la certitude que ma donnée ou ma transaction est intègre, n'a pas été altérée et qu'elle est bien protégée en cas de perte ou de vol ?
- Ai-je l'assurance que je peux adapter rapidement mon SI à des impératifs métiers et ce sans créer de nouvelles failles de sécurité ?

Cette confiance repose en fait sur trois piliers :

- Un réseau et une infrastructure « de confiance »
- Une identité numérique sécurisée
- Des transactions électroniques protégées

3 PASSER DE LA SECURITE PERIMETRIQUE A LA SECURITE PAR LA CONFIANCE OU COMMENT CREER LA CONFIANCE ELECTRONIQUE TELLE QU'ELLE EXISTE DANS L'ENVIRONNEMENT DES AFFAIRES ?

3.1 UNE INFRASTRUCTURE RESEAU DE CONFIANCE : L'IDENTITE AU CŒUR DES RESEAUX

Internet est aujourd'hui devenu le moyen privilégié pour interconnecter différents sites physiques d'une entreprise: les VPN MPLS proposés par les opérateurs offrent à présent une garantie de sécurité importante tout en assurant le support de fonctionnalités à haute valeur ajoutée telle que la qualité de service sur les WAN (y compris en multi opérateurs). Il en est de même concernant les besoins de mobilité qui se sont accrus avec l'arrivée de l'Internet et des téléphones mobiles hauts débits ou des différentes cartes/clés 3G+: Internet est également devenu le moyen d'accès distant au système d'information.

Ainsi combien de dirigeants de grand groupe vont préférer se connecter au réseau via leur carte 3G car ils n'ont pas accès, ou ne savent pas accéder au réseau en dehors de leur bureau !

Dans le même temps, ces nouveaux moyens de communication ont entraîné nombre de fraudes électroniques, de déni de service applicatif, de vol d'information, de destruction de données, ou encore de déploiement de virus ou logiciels espion: les diverses techniques liées au « phising » et à l'usurpation d'identité sont notamment à l'origine de nombreux vols d'information privée et de dommages financiers considérables.

Jusqu'à présent l'approche actuelle de la sécurité a consisté d'un côté à empiler des couches de sécurité périphérique (addition permanente de boîtiers à la périphérie du réseau) principalement administrée au travers des règles de filtrages (adresse IP, adresse MAC, ports TCP/UDP , NAT, etc.) et de l'autre à concevoir des logiciels et des applications toujours plus sûrs et basés sur les concepts de « sécurité par design », de « sécurité par défaut » et de « sécurité de déploiement ».

Le principe de réalité entraînant systématiquement la victoire de l'arme sur l'armure, les choses sont différentes dans la réalité : typiquement la « sécurité par design » tel qu'on la conçue jusqu'à maintenant se trouve systématiquement confrontée au nombre toujours croissant de vulnérabilités découvertes chaque jour, la « sécurité par défaut » même si elle est indispensable ne suffit plus à assurer les besoins légitimes des utilisateurs toujours avides de nouvelles facilités de travail (ouvrant au passage les portes à de nouvelles vulnérabilités). Enfin la « sécurité de déploiement » se trouve devoir affronter le monde réel où chaque correctif (système ou applicatif) fait l'objet de « reverse-engineering » afin d'être exploité puis utilisé comme faille de sécurité.

Parallèlement à cela, ce modèle n'est plus adapté à la nouvelle donne : des environnements hétérogènes et complexes massivement déployés dans les entreprises où différents systèmes, applications et réseaux doivent interopérer et où la plupart du temps pour installer un composant applicatif, une élévation de privilège système est nécessaire, constituant potentiellement une nouvelle porte ouverte aux vulnérabilités.

La véritable transformation sur laquelle OpenTrust travaille depuis plus de 3 ans propose de passer d'une sécurité périphérique à une sécurité de proche en proche (« Trusted Ecosystem », «Trusted Stack », « End to End Trust[1] » selon les éditeurs) où chaque composant (routeur, réseau, machines, serveurs, utilisateurs, système, applications, transactions, etc.) doit faire confiance au composant appelant et/ou à celui qu'il appelle pour s'exécuter (et ainsi de suite).

Cette approche visant à placer l'identité numérique (et par conséquent l'authentification forte) au coeur de tout système est reprise par de nombreuses initiatives. Typiquement chez CISCO, on parle de plus en plus de « CISCO Trusted Security[2] » (aussi appelé « TrustSec » par CISCO) dont un des objectifs consiste à utiliser le modèle RBAC[3] (Role Based Access Control) pour reconnaître les données associées au rôle d'un utilisateur et ainsi réguler ce qui est autorisé et ce qui ne l'est pas, basé sur ce rôle. Dans la majeure partie des cas, le protocole 802.1x et l'utilisation de certificats X509 sont les principaux composants mis en oeuvre pour authentifier les équipements. Par exemple, la décision de connecter un équipement dans un VLAN plutôt qu'un autre se base sur l'authentification forte, la posture, la conformité du poste qui cherche à se connecter à certaines règles de sécurité (« antivirus » ou « anti-malware » à jour par exemple, etc.) ainsi que sur la localisation physique de l'équipement. Il en est de même pour les postes téléphoniques TOIP avec l'utilisation de certificat X509 au sein même des postes IP pour authentifier et chiffrer les communications.

L'approche OpenTrust : « Trusted Network and Devices » qui consiste à donner une identité numérique et permettre l'authentification forte des serveurs, routeurs, postes de travail, téléphones IP et des smartphones permet donc de mettre fin à une approche uniquement basée sur la ségrégation réseau physique en créant de véritables « domaines de confiance » ou « bulles de sécurité » logiques au sein de son réseau.

Cette approche permet de passer d'un réseau physiquement compartimenté (et donc difficile à faire évoluer et coûteux à maintenir) à un réseau logique organisé sur des critères basés sur le rôle et les privilèges des machines ou des utilisateurs.

[1] http://www.microsoft.com/mscorp/twc/endtoendtrust

[2] http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns147/ns774/net_implementation_white_paper0900aecd80716abd.html

[3] http://csrc.nist.gov/rbac/sandhu-ferraiolo-kuhn-00.pdf

3.2 AUTHENTIFICATION FORTE ET CARTE A PUCE : UNE IDENTITE NUMERIQUE SECURISEE

Depuis quelques années, les entreprises ont largement déployé les solutions IAM (« Identity and Access Management ») des leaders du domaine (tels que IBM/Tivoli IAM[4], Sun IdM[5], Oracle IAM[6], Microsoft[7], etc.) en utilisant des annuaires LDAP ou ActiveDirectory, des solutions de « Provisioning » (Identity Management), des méta-annuaires ou encore des fonctions de eSSO/WebSSO pour gérer leurs utilisateurs et/ou employés, voire leurs partenaires.

Jusqu'à présent la gestion des identités et des accès était vue comme un système de gestion du cycle de vie des habilitations dans les différents référentiels du SI d'une entreprise. La sécurisation ou la « matérialisation » de cette identité reposait sur une authentification de type login/mot de passe avec les risques (usurpation d'identité) et la complexité pour l'utilisateur.

Le véritable enjeu pour répondre par l'affirmative à la question « Ai-je l'assurance de l'identité de la personne avec laquel je communique ? » est l'intégration des solutions de gestion de l'identité existantes avec l'état de l'art en matière d'authentification forte et de support lié à l'identité, la carte à puce.

Les habilitations deviennent alors nativement intégrées dans une infrastructure de confiance basée sur un badge unique d'entreprise et sur l'authentification forte qui permettent non seulement de sécuriser l'identité mais de gérer le cycle de vie complet de ces différents moyens d'accès qu'ils soient physiques (accès aux locaux, paiement du restaurant d'entreprise, etc.) ou logiques (credentials).

La plupart des fournisseurs de cartes ou tokens cryptographiques sont aujourd'hui capables d'embarquer sur un même support les « secrets » nécessaires aux différents types d'authentification logique (certificat X509, Seed OTP, secrets liés au eSSO, etc.) tout en incluant sur le même support des pistes magnétiques, du RFID, du MIFARE, du HID, ou autre.

Tout en réduisant les coûts d'exploitation et de Help Desk, cette approche qui consiste à élever, de façon importante, le niveau de sécurité (physique et logique) des identités est appelée par OpenTrust: « Trusted Identity ». Elle permet de matérialiser et sécuriser l'identité et donc :

- Une gestion de bout en bout de l'identité,
- Un « guichet unique » de gestion de l'identité numérique source de gain de productivité,
- L'Authentification forte,
- Un badge unique permettant accès physique et logique,
- Une simplification drastique pour l'utilisateur de la gestion de sa propre identité.

[4] http://www.ibm.com/software/tivoli/

[5] http://www.sun.com/software/products/identity/index.jsp

[6] http://www.oracle.com/products/middleware/identity-management/identity-management.html

[7] http://www.microsoft.com/windowsserver2003/technologies/idm/ilm.mspx

3.3 APPLICATIONS ET WEBSERVICES : DES TRANSACTIONS SECURISEES

Dans le domaine applicatif, la prochaine évolution est l'entrée progressive dans un monde dématérialisé à l'image des « hoobies » de nos enfants qui passent par l'usage des réseaux sociaux (« Facebook », « MySpace », et « Second Life », en tête) à l'intérieur desquels ils échangent avec des « amis virtuels » qu'ils ne voient et qu'ils ne verront certainement jamais. L'analogie dans le monde professionnel est relativement simple : vidéoconférence, webinar, messagerie instantanée, messagerie électronique, process dématérialisés, facture électronique, etc.

Du côté des applications métier, la tendance est également à la dématérialisation, même s'il reste encore du chemin à parcourir : quoi de plus illogique qu'un processus de commande fournisseur au sein d'une entreprise où la plupart du temps, le responsable du projet effectue une demande d'achat dans son ERP (ou passe par son assistante pour effectuer la demande), la valide, la fait valider par le n+1 voire le n+2 du demandeur, l'imprime pour être envoyée par Fax puis par courrier postal au fournisseur, qui la ressaisit dans son propre ERP pour la valider ? Lorsque l'on sait que la mise en place de chaque ERP d'entreprise coûte en moyenne plusieurs dizaines/centaines de millions d'euro, on peut être en mesure de se demander pourquoi un processus a priori simple comme celui de l'émission d'une commande continue à utiliser du papier et la voie postale / fax.

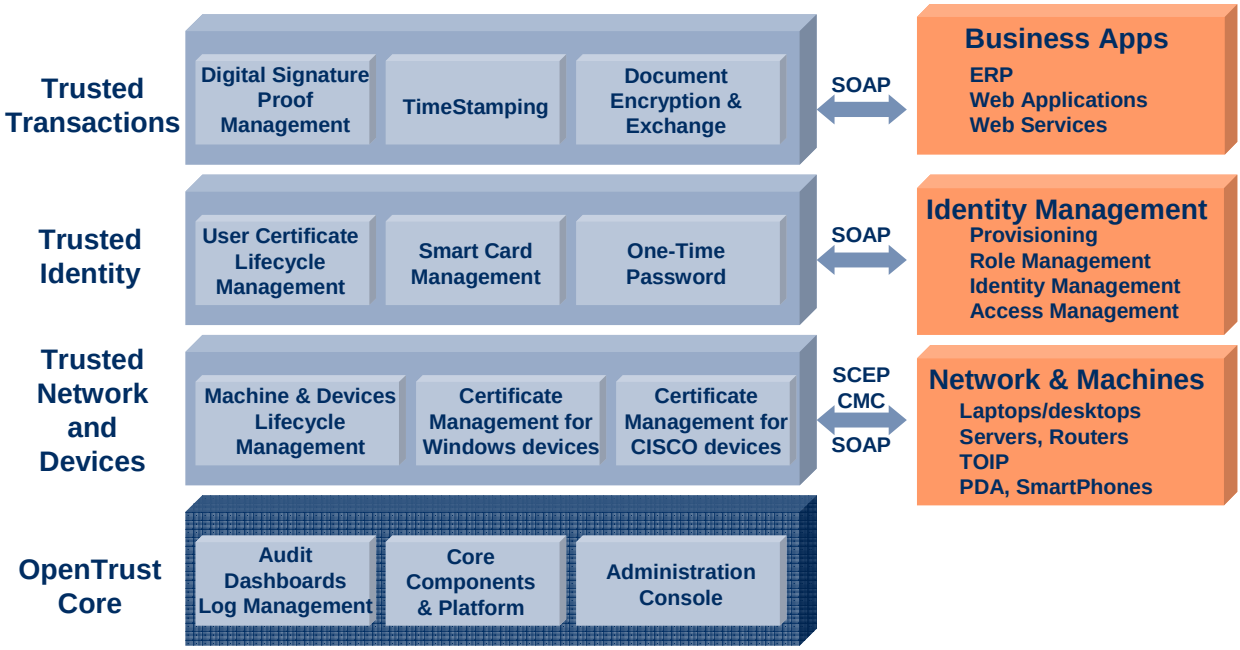
Le véritable enjeu est à nouveau de « dématérialiser » ces transactions mais aussi et surtout d'en s'assurer l'intégrité entre applications.

Pour adresser de façon fiable, simple et sécurisée ce type de besoin ainsi que tout ce qui concerne les échanges sécurisés, OpenTrust a introduit l'approche « Trusted Transaction », positionnant l'identité digitale, les moyens de signatures électroniques et de gestion de la preuve (c'est à dire, la capacité à démontrer a posteriori qu'un document ou qu'une transaction a parfaitement suivi les règles/processus en vigueur) comme éléments de base aux processus de dématérialisation.

4 OPENTRUST 3.0 : *TRUSTED ECOSYSTEMS* OU LA SECURITE DE PROCHE EN PROCHE

Pour répondre à ces enjeux, OpenTrust a donc développé OpenTrust 3.0 une offre unique autour des trois piliers de la confiance numérique :

- Un réseau et une infrastructure « de confiance » : Trusted Network and Devices,
- Une identité numérique sécurisée : Trusted Identity,
- Des transactions électroniques protégées : Trusted Transactions.



Cette suite logicielle, entièrement orientée service (SOA), a été conçue dès l'origine dans un souci de simplicité, de respect des standards et d'intégration dans un système d'information hétérogène afin de garantir une mise en œuvre et un retour sur investissement très rapide. Elle permet notamment :

- Une gestion de bout en bout de l'identité pour l'ensemble des acteurs du SI (personnes, machines et applications),
- Un « guichet unique » de gestion de l'identité numérique source de gain de productivité,
- Authentification forte et donc sécurité,
- La mise en place de badge unique permettant accès physique et logique,
- Une simplification drastique pour l'utilisateur de la gestion de sa propre identité,
- La mise en place d'une sécurité logique du réseau et donc une plus grande adaptabilité de son réseau,
- Des réductions de coûts au niveau administration du réseau et help desk utilisateur,
- Des gains de productivité (mobilité) et de sécurité.

Avec cette initiative, OpenTrust, éditeur de logiciel spécialisé dans les écosystèmes de confiance, positionne l'identité numérique au coeur de chaque composant du système d'information que ce soit le réseau et chacun des équipements actifs qui le constituent (routers, concentrateurs, etc.), le terminal ou le poste de travail (PC, Laptop, Smartphone, etc.), l'utilisateur (ou plus exactement son identité digitale qui sera utilisé par les systèmes et les applications), les systèmes et les applications eux-mêmes qui nécessitent authentification, traçabilité, confidentialité.

Au même titre que le « Trusted Computing Group[8] » (TCG), fondé par AMD, Hewlett-Packard, IBM, Infineon, Intel, Lenovo, Microsoft et Sun Microsystems entre autre, qui embarque dans chaque carte mère, une puce sécurisée, les solutions matérielles et logicielles du marché ont dans les dernières années intégrées nativement le support de l'identité numérique rendant possible un déploiement massif de la sécurité par la confiance.

A ce jour, l'offre OpenTrust a permis à plus de 50 grandes entreprises françaises et européennes de mettre en place très rapidement leurs écosystèmes de confiance utilisant les bases de la sécurité de proche en proche où l'identité numérique se comporte comme une véritable clé de voûte. La sécurité par la confiance est aujourd'hui une réalité quotidienne pour plus d'un million d'utilisateurs OpenTrust dans le monde[9].

8 https://www.trustedcomputinggroup.org

9 Nous consulter (sales@opentrust.com) pour mise à disposition des cas clients les plus représentatifs (sécurisation d'un réseau de 100 000 concessionnaires automobiles, badge unique pour 70 000 utilisateurs et identité numérique plus de 100 000 machines pour un grand groupe pétrolier, etc…)