Architecture pour un Extranet Adaptatif

Pierre VANNEL[1] , Yves ROUDIER[2], Olivier Fouache[2] et Refik MOLVA[2]
[1]*Gemplus Labs, av. du Jujubier, Z.I. Athélia IV, B.P. 90, 13702 La Ciotat CEDEX, France*
[2]*Institut Eurécom, 2229 route des Crêtes, B.P. 193, 06904 Sophia-Antipolis, France*
E-mail: pierre.vannel@gemplus.com

Résumé. Un extranet permet à une organisation de partager une partie de son système d'information (documents, services, ordinateurs, etc.) de manière sécurisée sur l'Internet. La sécurité est cruciale mais ne doit en rien gêner l'établissement de relations commerciales. Cet article examine comment concevoir un tel extranet. Il présente une solution automatisant la définition et la mise en oeuvre du contrôle d'accès ainsi que l'administration à grande échelle des utilisateurs en utilisant un modèle à base de capacités. L'article décrit un prototype utilisant une infrastructure SPKI et offrant une authentification forte grâce aux cartes à puce.

Mots Clés : extranet, pare-feu, authentification, SPKI, Handle System, carte à puce, agent

1. Introduction

Le développement du commerce électronique interentreprises conduit celles-ci à ouvrir de plus en plus leurs systèmes d'information à des tierces parties autorisées tout en assurant, si nécessaire, la confidentialité des transactions. En fournissant une infrastructure de communication sécurisée, les extranets sont un élément essentiel des solutions proposées. Aujourd'hui, la constitution d'un extranet demeure une tâche complexe nécessitant une forte collaboration entre les partenaires : définitions des autorisations, des ressources partagées et de leurs sémantiques, etc. Cette complexité conduit souvent à une organisation verticale d'un extranet [ENX]. De plus, les architectures actuelles d'extranets répondent difficilement aux exigences du commerce électronique telles que la réactivité, l'adaptabilité et la mise à l'échelle.
La réactivité est l'un des fondements du commerce électronique : il s'agit d'établir une nouvelle relation commerciale de manière quasi-instantanée pour une durée limitée.
L'adaptabilité est aussi très importante : par exemple, la mise à disposition de nouvelles ressources, éventuellement d'un nouveau type, la définition de nouvelles autorisations, le tout sans retard, sont autant de services que devrait permettre un extranet.
Enfin, la mise à l'échelle est la capacité pour une petite organisation de servir le plus grand nombre sans mettre en place une infrastructure à un coût prohibitif.
Cet article propose un nouveau paradigme appelé *extranet adaptatif*, permettant de satisfaire ces nouvelles exigences, sans sacrifier la sécurité. Il a été développé dans le cadre du projet en partenariat SEVA.

2. Etat de l'art

Un extranet peut être défini comme le partage sécurisé d'une partie de leurs systèmes d'information entre les organisations le constituant ou avec des utilisateurs externes, par l'intermédiaire de l'Internet. Les technologies « pair à pair » – peer-to-peer – semblent prometteuses [S-Peer] pour accomplir ce partage, mais elles n'ont pas encore la maturité nécessaire pour séduire les entreprises. Actuellement, le partage d'une ressource est fortement liée à sa nature et à son implémentation : par exemple, le partage d'un document HTML fera appel à un serveur Web et à

un contrôle d'accès spécifique. Dans ce chapitre, différentes technologies pour sécuriser le partage dans un extranet sont examinées.

2.1 Extranet et Réseau Privé Virtuel

Lorsqu'il s'agit d'interconnecter de façon sécurisée des réseaux d'entreprises, la solution privilégiée est d'utiliser des réseaux privés virtuels. Classiquement, un réseau privé virtuel est utilisé par une entreprise pour interconnecter des sites distants. Les communications transitent par l'Internet et sont protégées au niveau réseau par des moyens cryptographiques, par exemple en utilisant le protocole IPSec [KeAt98a][KeAt98b]. Un réseau privé virtuel peut être considéré par une entreprise comme un moyen d'étendre son réseau au delà de son pare-feu, vers un autre site ou le poste d'un télétravailleur par exemple. En contrepartie, il en importe aussi les risques.
Un extranet recouvre une notion plus large : il ne s'agit pas seulement d'établir un canal de communication sécurisé entre des partenaires mais aussi de définir les services offerts et les ressources partagées entre les membres de l'extranet. Un accord le décrivant est nécessaire.

2.2 Pare-feu

Le principal reproche adressé à l'architecture actuelle des pare-feux est qu'elle est généralement statique : un administrateur humain est nécessaire pour adapter les règles de filtrage. D'autre part, une grande part de la sécurité dépend de la disponibilité de cet opérateur, qui doit détecter et déjouer une attaque en mettant à jour en conséquence les règles du pare-feu. De plus, la complexité de l'écriture des règles n'immunise pas l'intranet contre des erreurs de programmation.
Les pare-feux dynamiques ou adaptatifs sont une tentative de réponse à ce problème. Par exemple, le pare-feu SunScreen [SUN] introduit des règles dites «time of day», qui sont activées à un instant programmé. D'autres pare-feux peuvent être couplés à des systèmes de détection d'intrusion : lors d'une attaque détectée, ils peuvent fermer la connexion responsable. Malheureusement, ils ne satisfont pas encore le besoin de configuration dynamique d'un extranet.
Dans les réseaux d'entreprises, les pare-feux sont couramment associés avec des serveurs d'authentification : le pare-feu intervient au niveau réseau pour filtrer le trafic, puis les utilisateurs sont authentifiés au niveau applicatif sur la base de listes de contrôle d'accès. Généralement, des annuaires d'entreprises de type LDAP centralisent ces listes et les partagent avec les pare-feux. Dans ce type d'architecture, un pare-feu ne définit plus un périmètre de sécurité : son rôle se limite à bloquer les trafics malveillants. Malheureusement, aucune information en provenance du contrôle d'accès applicatif ne lui est transmise : il ne lui est pas possible d'adapter son filtrage.

2.3 SOCKS

SOCKS [LGL96] est un protocole proxy générique, approuvé par l'IETF, permettant à des clients d'accéder à des serveurs sans nécessiter une connexion IP directe. SOCKS intègre des mécanismes d'authentification négociables et peut être une bonne solution pour s'authentifier auprès d'un pare-feu. Cependant, SOCKS nécessite de modifier l'application cliente. Malheureusement, dans une entreprise, le code source des applications est rarement disponible.
Une solution commerciale [eBorder] a été récemment introduite sur le marché afin de remédier à ce problème.
Toutefois, les mécanismes d'authentification de SOCKS sont encore rudimentaires comparés aux besoins d'un extranet.

3. Vers un extranet adaptatif

La problématique du contrôle d'accès de ressources partagées entre différentes organisations a fait l'objet d'une revue détaillée [ClLy98] et a permis d'en déduire différentes conditions à remplir par un extranet, dont certaines peuvent sembler contradictoires.

Tout d'abord un extranet doit être facile à utiliser, à administrer et à déployer. Il doit minimiser les interactions avec l'utilisateur et lui présenter les ressources disponibles de façon conviviale. Un administrateur doit être capable de gérer une vaste communauté d'utilisateurs de nature très changeante et un large éventail de ressources hétérogènes. Le support aux utilisateurs doit être aisé, couvrant par exemple le renouvellement d'autorisations.
Le contrôle d'accès doit avoir une granularité fine : limiter l'accès à certaines ressources à un nombre limité d'utilisateurs pour une période donnée. La sécurité doit être suffisamment forte pour que l'accès compromis d'un utilisateur ne remette pas en cause la sécurité de l'extranet tout entier.
La collection de données par l'opérateur des ressources ne doit pas se faire au détriment de la protection de la vie privée, c'est à dire enregistrer des informations personnelles à l'insu de l'utilisateur. Une telle violation ne soulève pas seulement un problème éthique, mais peut avoir de sérieuses conséquences économiques.
Un extranet fait l'objet d'un accord entre différentes parties et en particulier de l'acceptation de règles communes. En cas de non-respect de l'accord détecté par l'un des partenaires, il doit être possible d'établir les responsabilités des uns et des autres et pour les parties concernées d'agir en conséquence et sans retard.
L'architecture d'extranet adaptatif que nous décrivons se propose de répondre à ces exigences.
Elle se décompose en trois modules, chacun prenant en charge sa part de la complexité de la sécurisation des échanges interentreprises : gestion des services, gestion des utilisateurs et administration de l'extranet pour configurer tous les composants de sécurité.

3.1 Gestion des Services

Un extranet consiste en un ensemble de partenaires, certains offrant des services, d'autres les consommant, et chacun pouvant jouer les deux rôles. Construire un extranet signifie s'accorder sur quels services sont offerts à quel partenaire et être capable de mettre à jour cet offre. La granularité du contrôle d'accès doit être au niveau du service et doit pouvoir prendre en compte son hétérogénéité (page Web, document multimédia, application…). Un système d'identification universelle fournit une partie de la réponse. L'organisme américain Corporation for National Research Initiatives (CNRI) a proposé le Handle System comme un service nommage universel offrant une résolution sécurisée de nom sur l'Internet [SRL01]. Ce système a fait l'objet de propositions à l'IRTF. Le Handle System crée un espace de nommage global identifiant de manière unique des ressources numériques sur l'Internet. Une autorité de nommage centrale – autorité « racine » – référence toutes les sous-autorités de nommage dans le monde. Un identifiant d'une ressource numérique est appelé un handle et peut être résolu en une ressource, par exemple une URL HTTP ou une adresse FTP.
Les handles fournissent à un opérateur de ressources une identification persistante des ressources, mais, plus important encore, une granularité très fine du contrôle d'accès aux ressources qu'il offre. Les droits d'accès peuvent être définis sur chaque handle, indépendamment du serveur applicatif de la ressource et sans le modifier. Nous considérons le Handle System comme une infrastructure pour enregistrer des informations de contrôle d'accès et en cela, il est parfaitement approprié pour stocker des droits d'accès applicatifs pluripartites.
Toutefois, l'architecture actuelle du Handle System, avec un espace de nommage public et unique, n'est pas satisfaisant dans le contexte d'un extranet adaptatif. Le projet SEVA a modifié le Handle System dans le but de pouvoir créer un espace de nommage privé par extranet. Un partenaire de l'extranet administre l'autorité de nommage centrale de l'extranet, référençant toutes les autorités de nommage des autres participants. Chaque partenaire gère localement un serveur LHS – Local Handle Server – stockant les identifiants des ressources qu'il partage. Un handle d'une ressource de l'extranet ne peut être résolu que par un participant de l'extranet, les utilisateurs étant authentifiés grâce à leurs cartes à puce.

3.2 Gestion des Utilisateurs

L'objectif ultime d'un système d'authentification et de contrôle d'accès est de déterminer si un droit a été accordé à un utilisateur. Par comparaison avec un intranet, le réaliser avec un extranet est autrement plus ardu. En effet, il s'agit de contrôler des utilisateurs d'autres entreprises que la sienne. Ils peuvent être en plus grand nombre, plus volatiles : des employés rejoignent un partenaire, le quittent, de nouvelles organisations adhèrent à l'extranet, etc. Le déploiement satisfaisant d'une architecture multipartite de partage de ressources suppose qu'un nombre important d'utilisateurs puissent accéder à une ressource, y compris pour un court instant : seul un contrôle d'accès à base de capacités permet d'y répondre.
Dans notre modèle d'extranet adaptatif, nous séparons les rôles et les responsabilités de chacun des partenaires : l'opérateur de ressources contrôle les accès aux ressources et chaque partenaire gère l'identité et la base de ses employés autorisés. Chaque partenaire met à disposition des opérateurs de ressources un moyen de vérifier qu'un utilisateur fait toujours partie de son personnel autorisé, par exemple par le biais d'une liste de révocation. Chaque opérateur de ressources peut signaler à un partenaire un comportement malveillant d'un de ses employés.
En gérant lui-même l'identité de ses employés autorisés, un partenaire peut protéger ses données d'usage en dissimulant par exemple l'identité d'un utilisateur de l'extranet.
La notion de rôle [SaSa97] offre une solution et peut être intégrée dans des capacités. A cet égard, les certificats de groupe font de Simple Public Key Infrastructure (SPKI) la solution idéale pour gérer les droits d'accès accordés sur des ressources de l'extranet.
SPKI [EFL98a][EFL98b][EFL99] tend à répondre aux problèmes de contrôle d'accès sur des réseaux étendus et est standardisé par l'IETF : les capacités sont représentées sous la forme de certificats d'autorisation. Au contraire de X.509 [ITU88], SPKI n'est pas conçu pour nommer un tiers, mais pour formuler ses droits d'accès. SPKI dispose aussi d'un mécanisme essentiel pour un extranet adaptatif : la délégation. A partir d'un certificat de groupe, une entreprise est capable d'émettre des autorisations à ses employés pour accéder à des ressources de l'extranet.
Le Handle System se marie particulièrement bien avec SPKI pour définir des droits d'accès sur une ressource . Les handles, comme éléments de désignation de ressources, sont utilisés directement dans les certificats SPKI. D'autre part, les handles peuvent rendre les certificats plus compacts. En effet, un handle référence une ou des ressources mais aussi des méta-données associées. Ainsi, par exemple, il n'est pas nécessaire d'inclure des informations sur les mode d'accès à une ressource dans un certificat : elles peuvent être référencées par le handle. Enfin l'unicité d'un handle permet d'indexer les certificats, rendant plus facile la recherche de certificats.

3.3 Administration de l'Extranet

Ce module s'intercale entre les deux précédents et met en œuvre les opérations de contrôle d'accès sur la base des informations transmises par ces deux modules. En particulier, il gère le pare-feu et les enregistrements d'activité des utilisateurs.
Le module Administration vérifie aussi que les utilisateurs possèdent le droit d'accès à une ressource. Un extranet adaptatif s'adresse à des applications où les utilisateurs se connectant depuis leurs réseaux d'entreprises respectifs accèdent à des ressources dans un autre réseau d'entreprise et collaborent ensemble au travers d'Internet. Par conséquent, il est impératif de concevoir une architecture qui protège contre les attaques non seulement de pirates informatiques sur Internet, mais aussi d'utilisateurs malveillants quand bien même leur communications sont présumées venir d'un partenaire agréé. Les droits d'accès d'un utilisateur sont vérifiés avant de pénétrer dans le réseau d'entreprise de l'opérateur de ressources, de manière transparente, puis le comportement des utilisateurs autorisés est éventuellement enregistré par un système de détection d'intrusion. La détection d'un comportement suspect peut entraîner l'interdiction d'accès de l'utilisateur à l'intranet de l'opérateur.
Les services disponibles pour chacun des partenaires sont aussi définis dans un accord initial de partenariat constituant l'extranet. Cet accord est utilisé pour automatiser un grand nombre de processus : génération des droits d'accès des parties autorisées et configuration des pare-feux et des

postes d'administration. Il s'exprime en XML, en utilisant les définitions de CPPA [CPPA02]. Il peut être mis à jour chaque fois qu'un partenaire rejoint ou quitte l'extranet. De plus, les règles régissant l'extranet, telles que la définition des responsabilités ou les paramètres de sécurité, et les services offerts peuvent évoluer, requérant une mise à jour de l'accord.

4. Définition et Gestion du Contrôle d'Accès

Le contrôle d'accès a un rôle crucial, sinon central, dans l'architecture d'extranet adaptatif. Les droits d'accès doivent être distribués, stockés en lieu sûr mais ensuite ils doivent être gérés. La gestion des droits d'accès peut être déterminée au démarrage, par exemple avec la durée de vie d'un certificat d'autorisation, mais aussi par un événement soudain tel que la détection d'une intrusion.

4.1 Accréditation des utilisateurs

L'objectif de l'accréditation est de transcrire l'accord d'extranet dans l'organisation d'un partenaire : il s'agit de communiquer les services de l'extranet aux utilisateurs autorisés et de leur distribuer les droits d'accès correspondants. Les entreprises ont généralement une organisation hiérarchique. L'allocation des nouveaux services et des droits d'accès associés suit ce chemin hiérarchique.
Dans le projet SEVA, les postes d'administration s'appuient sur des agents pour générer automatiquement de nouveaux certificats SPKI à partir de ceux qui sont délivrés régulièrement par les administrateurs des autres partenaires (opérateurs de ressources). La délégation SPKI est utilisé dans ce processus. A n'importe quel niveau hiérarchique, des utilisateurs habilités peuvent déléguer ou restreindre les droits d'accès à leurs subordonnés.
Les certificats SPKI ont un atout supplémentaire, dans notre architecture, pour échapper à des problèmes de révocation : à la fin de leur période de validité, spécifiée par un administrateur, ils deviennent automatiquement inutilisables. Pour exploiter cette caractéristique, la meilleure façon est encore d'automatiser la génération des certificats. L'infrastructure envisagée pour une telle tâche est un ensemble d'agents intelligents représentant chaque utilisateur et générant les nouveaux certificats suivant un paramétrage défini par l'administrateur. Dans le projet SEVA, notre prototype a utilisé la plate-forme d'agents JADE [BPR00] à cette fin.

4.2 La carte à puce : un outil de gestion des droits d'accès

La carte à puce de l'utilisateur a un rôle essentiel lors du processus d'accréditation. La carte est un objet personnel et portable permettant d'accéder aux services de l'extranet. Elle peut être utilisée pour protéger des clés cryptographiques mais aussi pour stocker les références des services ou ressources. Les cartes à puce utilisées sont de type JavaCard et supportent plusieurs applications dans une carte. Dans notre cas, deux applications cohabitent : l'une est un « card applet » cryptographique et l'autre est un serveur sécurisé de type LDAP [Mac00], utilisé pour stocker les références sur les services ou les ressources ainsi que les droits d'accès. L'applet cryptographique est un composant du système d'authentification et de contrôle d'accès décrit dans le chapitre suivant.
La capacité de la mémoire des cartes à puce actuelles est encore limitée : seulement quelques dizaines de Kilo-octets pour enregistrer les programmes et les données. La carte est idéale pour stocker les clés cryptographiques secrètes et protéger les données personnelles du porteur de la carte. Ainsi, nous avons choisi de ne stocker seulement que la référence d'un certificat : le certificat complet, ou sa chaîne, est stocké dans un serveur LDAP se trouvant dans l'intranet de l'entreprise de l'utilisateur. Du point de vue de l'utilisateur, le processus est transparent : tout se passe comme si les certificats se trouvaient dans la carte.

4.3 Détection d'intrusion et gestion des droits d'accès

L'authentification d'un utilisateur n'écarte pas le risque d'une attaque de sa part. Le partenaire, opérateur de ressources, peut, dans ce cas, souhaiter révoquer les droits de l'utilisateur effectuant de manière répétée des opérations illicites ou suspectes.
Les utilisateurs mobiles présentent encore un autre risque : ils peuvent accéder à des services hors du périmètre sécurisé de l'intranet de leur entreprise. Ils sont alors plus susceptibles de subir des attaques, telles que le détournement de leur machine par un cheval de Troie, créant des dommages dans l'intranet d'un partenaire de l'extranet.
Dans les deux cas, un système de détection d'intrusion devient un composant important de l'infrastructure de sécurité et doit s'interconnecter avec l'infrastructure de gestion du contrôle d'accès. Le système de détection d'intrusion Snort [Roe] a été intégré dans notre prototype d'extranet adaptatif en utilisant le langage standardisé d'échanges IDMEF [CuDe01]. Si une intrusion est détectée, la responsabilité de l'utilisateur peut être établie, avec l'aide de l'entreprise qui détient son identité et gère ses droits.

5. Mise en Œuvre de l'Authentification dans l'extranet

Lorsque les droits d'accès ont été distribués, sous la forme de certificats, les communications peuvent être établies avec l'intranet du partenaire. Les échanges sont contrôlés sur la base des droits attribués précédemment. Un extranet adaptatif doit effectuer une authentification forte des communications échangées et en rapport avec les ressources accédées.

5.1 Un pare-feu authentifiant

Les pare-feux [ChBe94] sont la technique la plus répandue pour mettre en œuvre un contrôle d'accès et protéger un intranet : le contrôle est réalisé sur les communications en filtrant les paquets et les connexions. Ce modèle de sécurité par filtrage est attrayant car il est effectué sur des composants intermédiaires du réseau et par conséquent, n'affecte pas les serveurs applicatifs. Grâce à une gestion centralisée des opérations de filtrage, il reste aussi relativement facile à utiliser.
Cependant, le plus couramment, le filtrage utilise des listes de contrôle d'accès détaillant les opérations autorisées pour chaque utilisateur. Comme expliquée précédemment dans le chapitre 3, l'architecture d'un extranet adaptatif nécessite un filtrage des accès basé sur des capacités.

5.1 Contrôle d'accès et authentification utilisant des certificats

Garantir de bonnes performances est une des lignes directrices de notre conception. C'est la raison pour laquelle le contrôle d'accès est effectué en deux étapes : les droits applicatifs d'un utilisateur sont établis par l'envoi d'un jeu de certificats SPKI ; tout le trafic en provenance de cet utilisateur est par la suite authentifiée en utilisant des mécanismes d'authentification plus simples.
La figure ci-après décrit le processus. Lorsqu'un handle (1) doit être résolu en une ressource applicative (une URL par exemple), l'authentification initiale et la résolution du contrôle d'accès (message (3)) sont effectuées simultanément.

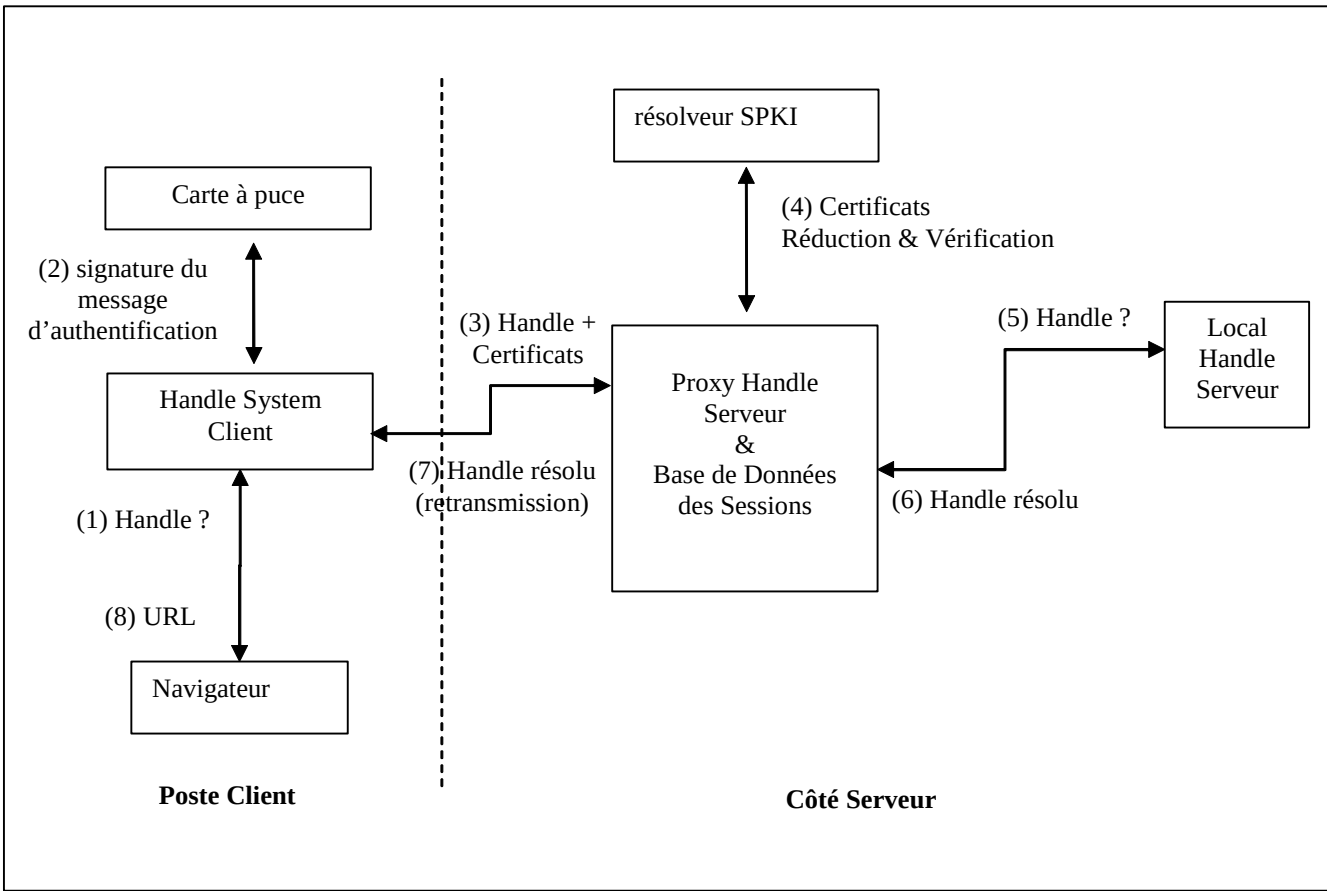

Figure 1. Vérification des droits d'accès

Dans notre prototype, le Handle Server proxy a été ajouté aux proxys disponibles avec le pare-feu TIS [TIS]. Il réalise la résolution des certificats SPKI associés au handle (4), prouvant les droits d'accès de l'utilisateur. Ensuite, afin d'authentifier l'utilisateur, ce proxy vérifie la signature effectuée par la carte à puce de l'utilisateur (2) du message contenant le handle.
Si l'utilisateur est authentifié, le proxy Handle Serveur effectue la résolution du handle (5), confiée au serveur LHS modifié, qui nous évite de contacter le serveur racine du Handle System hébergé par le CNRI. Après cette authentification, l'utilisateur est enregistré temporairement dans une base de données des sessions, permettant par la suite de reconnaître un utilisateur grâce à une clé de session transmise dans le message d'authentification (cf. chapitre 5.3).

5.3 Marquage du trafic

Le marquage du trafic a pour objet de garantir que les paquets transmis proviennent de l'utilisateur, le détenteur exclusif de la clé secrète, sans pour autant effectuer l'opération coûteuse de signer chacun des paquets transmis. Deux conséquences importantes en découlent : le trafic est fortement authentifié ; un utilisateur peut être enregistré et identifié par sa clé publique, mais son nom n'est pas révélé au pare-feu enregistrant ses accès. La clé publique est comme un pseudonyme de l'utilisateur, attribué par son employeur.
Le marquage peut être réalisé par l'incorporation d'une couche de communication spécifique (voir Figure 2) dans le poste client. Les données transmises sont encapsulées et marquées avec un ticket cryptographique (3). Basé sur la clé de session, unique pour chaque utilisateur, le ticket établit l'identité de l'utilisateur et garantit en même temps l'intégrité des données transmises : il consiste simplement en un code d'authentification de message (MAC) utilisant la clé de session générée préalablement par la carte à puce. Le chiffrement n'a pas été mis en œuvre, mais il aurait pu être envisagé en utilisant cette même clé de session. Nous avons volontairement limité les mécanismes de sécurité de l'extranet à l'authentification afin d'impacter les performances le moins possible.

En une première étape, une bibliothèque socket modifiée a été développée, et expérimentée, pour l'environnement Microsoft Windows : elle interceptait toutes les communications à destination d'un autre intranet SEVA (elle offre la même fonctionnalité que [eBorder]). Le paquet TCP était encapsulé avec un format spécifique, comprenant les données, le ticket cryptographique d'authentification, et des informations supplémentaires telles que l'adresse de la destination et le port. Avec cette approche au niveau réseau, il est possible de régler finement la granularité de l'authentification et ainsi la « bufferisation » des paquets.
Nous avons expérimenté aussi une autre technique : nous nous sommes concentrés sur le trafic HTTP, et nous avons finalement implémenté le marquage en utilisant un simple proxy HTTP, pour la facilité de déploiement sur différentes plates-formes (il fonctionne actuellement sous Linux ou Windows). Cette solution présente aussi l'avantage de pouvoir utiliser des informations au niveau applicatif. Par exemple, au lieu d'accéder à des ressources via des handles, l'utilisateur saisit, comme d'habitude, une URL dans son navigateur, et notre couche de communication reconnaît cette URL et la convertit en un des handles accessibles à l'utilisateur. L'intégration avec les applications devient alors complètement transparente.
La vérification du ticket est effectuée au niveau du pare-feu par le proxy correspondant (4), relativement à une résolution de handle authentifiée précédemment. Le proxy vérifie le ticket mais décapsule aussi le trafic initial avant de le retransmettre (5).

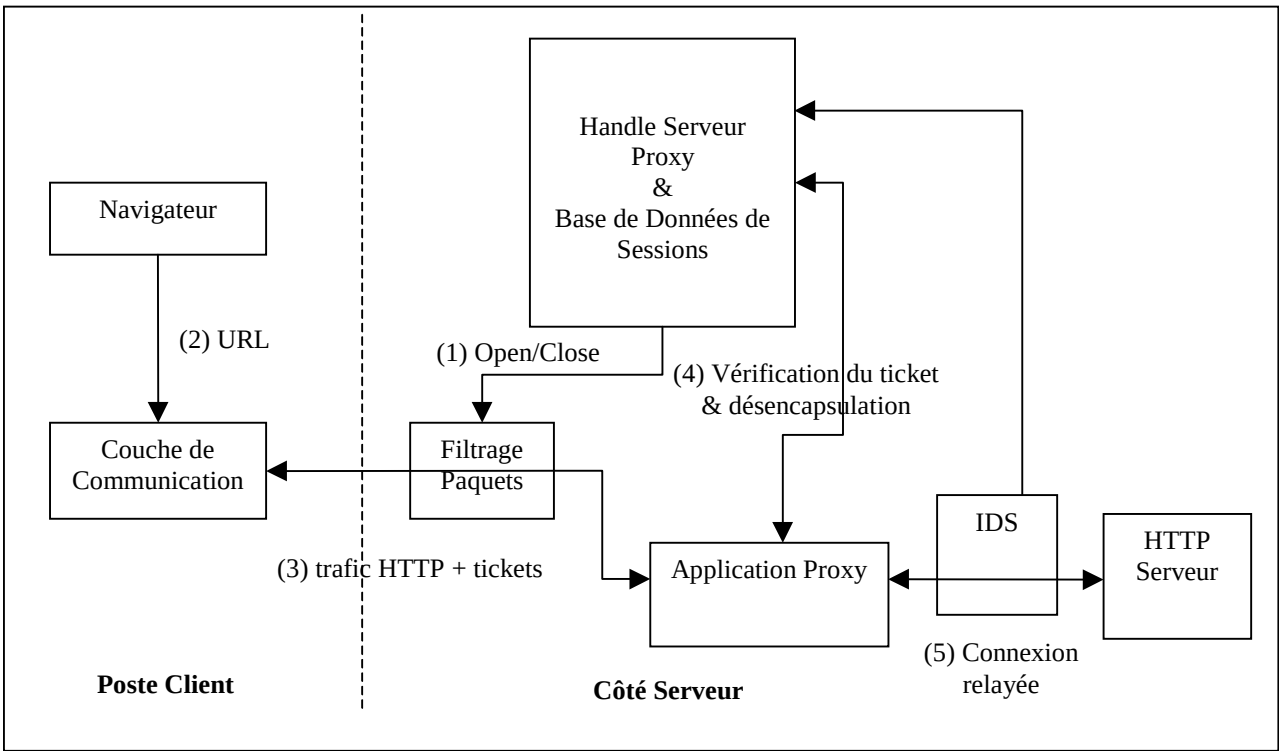

Figure 2. Marquage du trafic

La carte à puce est utilisée ici comme le sésame pour accéder à l'extranet adaptatif : elle protège la clé privée de l'utilisateur, évitant de la stocker sur son poste, et est un élément essentiel dans un protocole d'authentification de type défi-réponse. Aucun échange ne peut avoir lieu avec un partenaire de l'extranet sans la carte : l'étiquetage, et par conséquent l'authentification, n'est possible qu'avec une clé de session valide que seule la carte peut générer. En insérant sa carte à puce dans un lecteur connecté à son poste et après avoir saisi son code PIN l'authentifiant auprès de la carte, l'utilisateur peut accéder à l'extranet : une session, avec une durée de vie limitée, est alors établie. Lors de l'expiration de la session, une nouvelle clé de session est calculée par la carte et est échangée avec le handle serveur proxy. Toutefois, pour des raisons de performances, l'étiquetage n'est pas effectué par la carte mais par le poste client.

6. Conclusion

L'essor des services interentreprises, en particulier sous la forme de Web Services, passe par une remise en cause du modèle traditionnel de sécurité d'entreprise, basé sur un contrôle au niveau réseau. Le partage des ressources, les données aussi bien que les serveurs, requiert un contrôle beaucoup plus fin, au niveau d'une ressource, en utilisant la notion d'autorisation. Par ailleurs, une ressource peut être constituée par l'agrégation de services fournies par des tierces parties, nécessitant la propagation de l'autorisation jusqu'à celles-ci. Il s'agit de repenser le modèle de sécurité en le basant sur un contrôle au niveau ressource, et non plus au niveau réseau. La difficulté du problème réside, d'une part dans la complexité de référencer les services et les ressources partagées, et d'autre part, dans le fait que les droits de l'utilisateur final et son identité sont définis et gérés par son entreprise. Par ailleurs, la fréquence de mise à jour des équipements de sécurité requise nécessite d'automatiser les opérations correspondantes. Les équipements de sécurité utilisés actuellement ne satisfont pas à ces exigences.
Notre article propose de faire collaborer des équipements traditionnels de sécurité de manière à étendre les fonctionnalités du pare-feu de l'entreprise pour mettre en œuvre ce que nous appelons un extranet adaptatif. Les utilisateurs et leurs droits d'accès sont centraux dans l'architecture d'extranet adaptatif, et chacun est administré par une entité distincte : tous les deux peuvent être gérés en utilisant une infrastructure à clé publique SPKI et la notion d'identifiant générique de ressource, appelé handle. Les communications entre le poste utilisateur et le pare-feu de l'intranet visité sont authentifiés sans dégrader les performances. La forte intégration de l'authentification SPKI avec le procédé d'étiquetage du trafic, rend possible l'automatisation de la configuration du pare-feu. La carte à puce joue un rôle important dans l'authentification et remplace avantageusement un ou plusieurs mots de passe. La carte est un dispositif personnel de sécurité participant idéalement à l'automatisation de la configuration des équipements de sécurité de l'extranet : elle permet à un utilisateur de prouver son identité ou aux administrateurs d'émettre des certificats d'autorisation SPKI. Enfin, tout en offrant une authentification forte de l'utilisateur, le système protège sa vie privée en ne révélant pas son identité réelle.
Le projet SEVA a développé et déployé un prototype d'extranet adaptatif qui implémente toutes les fonctionnalités du contrôle d'accès et la distribution automatique des certificats. Les résultats obtenus sont encourageants : le contrôle d'accès à un serveur Web peut être complètement réalisé, sans modification aucune du serveur lors du déploiement du système. Le prototype a aussi montré qu'une authentification forte pouvait être ajoutée à des applications clientes sans les modifier. Un contrôle d'accès sur le trafic UDP a été aussi expérimenté, et il serait intéressant de le supporter plus complètement dans le futur.

Remerciements

Seva est un projet en partenariat entre ATOS, Electricité de France, l'institut Eurécom et Gemplus, et soutenu par le Ministère Français de l'Economie, des Finances et de l'Industrie, et le Réseau National de Recherche en Télécommunications (RNRT).

Références

[BPR00] F. Bellifemine, A. Poggi, G. Rimassa, and P. Turci. *An Object Oriented Framework to Realize Agent Systems*. in Proc. of WOA 2000 Workshop, Parma, May 2000, pp. 52-57.
[ChBe94] B. Cheswick and S. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison Wesley, 1994, ISBN 0-201-63357-4
[ClLy98] Clifford Lynch. *A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources*. Coalition for Networked Information (CNI). http://www.cni.org/projects/authentication/authentication-wp.html

[CPPA02] OASIS. Collaboration Protocol Profile and Agreement (CPPA) v2.0. September 2002. http://www.oasis-open.org/committees/ebxml-cppa/documents/ebcpp-2.0.pdf
[CuDe01] David Curry, Hervé Debar. *Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition* - draft-ietf-idwg-idmef-xml-06.txt. December 2001
[eBorder] http://www.permeotechnologies.com/technology/wpapers.htm. Permeo Technologies. *e-Border white papers.*
[EFL98a] C. M. Ellison, B. Frantz, B. Lampson, R. Rivest, B. M. Thomas, and T. Ylönen. *Simple Public Key Certificate*, Internet draft <draft-ietf-spki-cert-structure-05.txt>, March 1998.
[EFL98b] C. M. Ellison, B. Frantz, B. Lampson, R. Rivest, B. M. Thomas, and T. Ylönen. *SPKI Examples*, Internet draft <draft-ietf-spki-cert-examples-01.txt>, March 1998.
[EFL99] C. M. Ellison, B. Frantz, B. Lampson, R. Rivest, B. M. Thomas, and T. Ylönen. *SPKI Certificate Theory*, RFC 2693, September 1999.
[ENX] European Network Exchange web site. http://www.enx.com
[ITU88] ITU-T. *Recommendation X.509: The Directory - Authentication Framework*, 1988.
[KeAt98a] S. Kent, R. Atkinson. *IP Authentication Header (RFC 2402).* November 1998.
[KeAt98b] S. Kent, R. Atkinson. *IP Encapsulating Security Payload (ESP) (RFC 2406).* November 1998.
[LGL96] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones. *RFC 1928. SOCKS Protocol Version 5.* March 1996
[Mac00] A. Macaire. *An Open Terminal Infrastructure for Personal Services.* TOOLS Europe 2000, 5-8 June 2000, Le Mont-St-Michel, France
[Roe] Martin Roesch. *Snort - Lightweight Intrusion Detection for Networks* - http://www.snort.org/docs/lisapaper.txt
[SaSa97] R. S. Sandhu, P. Samarati. *Authentication, Access Controls, and Intrusion Detection*, in The Computer Science and Engineering Handbook, pp 1929-1948, 1997.
[SEVA] SEVA project home page - http://www.eurecom.fr/~nsteam/SEVA/
[S-Peer] Texar. *S-Peer*. http://www.s-peer.com/
[SRL] S.X. Sun, S. Reilly, L. Lannom. *Handle System Namespace and Service Definition.* IETF Draft. May 2001.
[SUN] SUN Microsystems. SunScreen Secure Net 3.1, Technical Whitepaper
[TIS] FWTK.ORG *unofficial page on TIS firewall toolkit* - http://www.fwtk.org/main.html
[W3C00] World Wide Web Consortium. *Extensible Markup Language (XML) 1.0. W3C Recommandation.* http://www.w3.org/TR/2000/REC-xml-20001006