CLUB INFORMATIQUE DES GRANDES ENTREPRISES FRANÇAISES
21, avenue de Messine. 75008 Paris, téléphone 40.42.24.94

Réf. 89 183

ARCHITECTURE DE SECURITE DANS LES RESEAUX INFORMATIQUES

ET

IMPACT DE LA SECURITE SUR L'ARCHITECTURE DES RESEAUX

- RAPPORT -

Mai 89

"Toute reproduction de ce rapport est interdite. En effet, sa version définitive sera publiée dans la collection AFNOR TECHNIQUE et sera disponible en juin 1989".

ARCHITECTURE DE SECURITE DANS LES RESEAUX INFORMATIQUES

ET

IMPACT DE LA SECURITE SUR L'ARCHITECTURE DES RESEAUX

C I G R E F

		pages
CHAPITRE I	- INTRODUCTION	2
CHAPITRE II	- LE CONTROLE D'ACCES	5
	II.1 L'AUTHENTIFICATION	6
	II.2 LA GESTION DES DROITS	22
CHAPITRE III	- LES MESURES COMPLEMENTAIRES AU CONTROLE D'ACCES	48
CHAPITRE IV	- LA GESTION DES SECRETS	51
CHAPITRE V	- L'APPORT DES ANTESERVEURS	61
CHAPITRE VI	- L'APPROCHE HORIZONTALE	76
CHAPITRE VII	- CONCLUSION	91

CHAPITRE I

INTRODUCTION

L'information est un élément stratégique du patrimoine des entreprises.

Les réseaux de télé-informatique internes ou externes se développent de plus en plus pour en assurer la diffusion et en faciliter le traitement.

Partie intégrante du système d'information, le réseau devient donc un organe vital au fonctionnement de l'entreprise. Toute atteinte, blocage ou parasitage de ce système peut aller jusqu'à la mise en cause de la survie de l'entreprise. Il importe donc que la sécurité soit prise en compte dès la conception au même titre que les autres critères de rentabilité, de marketing...

OBJECTIFS

L'objectif de ce document est de servir de référence en matière de sécurité des réseaux et de faciliter les échanges entre les membres du CIGREF afin :

- d'aider à faire progresser le niveau général de sécurité,
- d'assister les entreprises membres dans leurs études en particulier pour prendre en compte l'aspect sécurité dans l'architecture des réseaux,
- de constituer une référence pour les constructeurs et développeurs de logiciels exprimant les besoins communs des entreprises, tout en laissant ouverts les points encore mal connus ou qui doivent rester adaptables aux spécificités de chacun,
- d'être une contribution aux travaux des organismes de normalisation en même temps qu'une garantie sur la prise en compte de nos besoins dans les standards.

REMARQUES

Ce document est une première version appelée à vivre; il deviendra donc au fil du temps plus complet et plus précis. En particulier la liste des principes à respecter devrait s'enrichir progressivement.

LA SECURITE

Partant des travaux actuels au sein de l'ISO, de l'AFNOR et de la CEE, le C.F.O.N.B. a effectué un travail de préstandardisation. Il nous paraît utile de rappeler les principes de base pour introduire les chapitres de ce document.

En matière de sécurité, il est souhaitable de distinguer :

- les PROPRIETES que doivent offrir les systèmes de sécurité, propriétés dont le niveau d'exigence doit être fonction des conséquences qu'aurait un sinistre pour l'entreprise,

- les MESURES qui sont les moyens de se protéger pour éviter les sinistres et dont le niveau de solidité doit correspondre aux exigences fixées pour les propriétés,

- les OUTILS qui sont les réalisations pratiques éventuellement disponibles sur le marché.

Les propriétés ont été classées en cinq groupes :

- disponibilité
- intégrité
- confidentialité
- auditabilité
- existence de preuve (non-répudiation)

Les mesures peuvent être réparties en deux groupes :

- le contrôle d'accès qui recouvre l'authentification et la gestion des droits d'autorisation,

- les mesures complémentaires :

  . chiffrement
  . scellement
  . signature
  . notarisation
  . ...

Ce document consacré à la sécurité des réseaux concerne l'ensemble des propriétés et des mesures. Afin de produire rapidement un document concret, seuls quatre points ont été approfondis actuellement :

- l'authentification,
- la gestion des droits,
- la gestion des secrets liés aux algorithmes,
- l'apport de la notion d'antéserveur à la sécurité et son impact dans les choix sur l'architecture du réseau.

Un chapitre reprenant ces points, mais avec une approche par niveau au sein d'un réseau, vient compléter cette étude.

CHAPITRE II

LE CONTROLE D'ACCES

1 - L'AUTHENTIFICATION

1. INTRODUCTION

1.1 Définition
1.2 Importance dans le contrôle d'accès
1.3 Authentification / Identification
1.4 Authentification continue et mutuelle
1.5 Authentifications locale et à travers un réseau

2. PRINCIPES ET MECANISMES D'AUTHENTIFICATION

2.1 Moyens d'authentification d'une entité

2.1.1 Ce que connaît l'utilisateur
2.1.2 Ce que détient l'utilisateur
2.1.3 Ce que connaît et ce que détient l'utilisateur
2.1.4 Ce qu'est l'utilisateur
2.1.5 Ce qu'est et ce que détient l'entité
2.1.6 Ce qu'est, ce que détient et ce que connaît l'entité

2.2 Les techniques et les outils

2.2.1 Par ce que connaît l'utilisateur
. mot de passe simple
. mot de passe variable (dynamique)
. codes confidentiels

2.2.2 Par ce que détient l'utilisateur
. contrôle physique
. contrôle visuel
. contrôle automatisé

2.2.3 Par ce que connaît et détient l'utilisateur
. carte à piste magnétique
. carte à puce
. authentifieurs

2.2.4 Par ce qu'est l'utilisateur
. caractéristiques physiques utilisées
. reconnaissance

2.2.5 Par ce qu'est et détient l'utilisateur

2.2.6 Par ce qu'est, détient et connaît l'utilisateur

3. AUTHENTIFICATION A TRAVERS UN RESEAU

4. L'ACCES UNIVERSEL

1. INTRODUCTION

1.1 Définition

L'authentification consiste à vérifier l'identité d'une entité (logique, matérielle ou humaine), par une autre à partir d'une de ses caractéristiques physiques spécifiques ou d'un élément supposé détenu ou connu de cette seule entité.

1.2 Importance dans le contrôle d'accès

L'authentification est une des mesures les plus indispensables à l'ensemble de la sécurité. Il n'est pas possible d'assurer la confidentialité, l'intégrité, la non-répudiation ni même parfois la disponibilité sans s'appuyer sur un contrôle d'accès préalable.

Ce contrôle d'accès et par conséquent l'authentification, qui est l'un de ses éléments, peuvent être mis en place pour :

- l'accès physique aux locaux,
- l'accès physique aux éléments du réseau (terminaux, lignes ou ordinateurs centraux),
- l'accès logique à ces éléments.

1.3 Authentification et Identification

L'identification se borne à constater l'identité d'une entité dans une population préalablement recensée. Cette identité est généralement connue mais peut être facilement usurpée.

L'authentification va permettre d'avoir la garantie de l'identité d'une personne.

S'il est envisageable, à la limite, de concevoir un identifiant utilisé par un groupe de personnes, l'authentification, quant à elle, ne doit concerner qu'un et un seul individu.

1.4 Authentification continue et mutuelle

Outre les authentifications classiques décrites ci-après, deux notions doivent être prises en compte :

- authentification continue :

  L'authentification en début de session peut ne pas être suffisante, par exemple lorsque le terminaliste est amené à quitter son poste. Pour couvrir le risque que le terminaliste oublie dans ce cas de clore la session, il faut prévoir une déconnexion automatique après temporisation, détecter l'arrachage éventuel du support d'authentification et éventuellement réauthentifier périodiquement le support, voire l'utilisateur.

- authentification mutuelle :

  En utilisation réseau, il est nécessaire d'authentifier les deux interlocuteurs, même si l'un des deux est un serveur.

1.5 Authentifications locale et à travers un réseau

Dans la plupart des cas (par exemple lorsque le poste de travail est un micro-ordinateur, connecté ou non), il sera nécessaire d'authentifier localement la personne, le logiciel ou le matériel ayant accès ou faisant partie du réseau, et dans le cas de l'accès à des ressources distantes, cette authentification devra également être garantie de bout en bout à travers le réseau.

Dans le cas de l'utilisation d'un terminal informatique "classique", l'authentification locale n'est pas utile (car il n'y a pas localement de ressources à protéger), mais l'authentification à travers le réseau est alors indispensable.

2. PRINCIPES ET MECANISMES D'AUTHENTIFICATION

Les principes énoncés ci-après sont généraux et concernent l'authentification d'une entité, indépendamment du fait que celle-ci s'effectue à travers un réseau ou non. Les problèmes spécifiques induits par l'authentification à travers un réseau seront traités dans la section suivante.

2.1 Moyens d'authentification d'une entité

Elle peut se faire à partir de trois méthodes de base :

- ce que connaît l'entité (mot de passe, code confidentiel,...);

- ce que détient l'entité (carte à piste magnétique, carte à puce, authentifieur, clé physique,...);

- ce qu'est l'entité (caractéristiques biométriques ou anthropométriques de l'individu).

Ces trois méthodes, seules ou combinées, présentent chacune des avantages et des inconvénients :

2.1.1 Ce que connaît l'utilisateur

Il est difficile de prouver :

. que personne n'a pu découvrir le secret,

. que le détenteur ne l'a pas confié volontairement ou non à un autre.

Cette information est de plus facilement "interceptable" : plusieurs personnes peuvent la détenir et l'utiliser simultanément. L'authentification n'est pas certaine, excepté, peut-être, pour des conversations téléphoniques incorporant des indications très personnelles.

2.1.2 Ce que détient l'utilisateur

Deux faiblesses peuvent exister : le vol du matériel et la duplication.

L'authentification sera d'autant meilleure qu'il sera impossible de dupliquer l'élément physique.

2.1.3 Ce que connaît et ce que détient l'utilisateur

Il s'agit là d'augmenter le niveau de sécurité par rapport à une information connue seule ou possédée seule. Le fraudeur doit détenir un support et connaître une information secrète (mot de passe, code confidentiel).

Dans ce cas :

. le support d'authentification authentifie lui-même l'utilisateur,

. l'ordinateur authentifie le support.

Par exemple :

1. le terminal ou le central authentifie l'utilisateur grâce à un fichier de mots de passe.

2. le central authentifie le terminal grâce à une clé secrète dans une mémoire.

2.1.4 Ce qu'est l'utilisateur

L'authentification devient plus sûre dans la mesure où certaines caractéristiques physiques des individus sont très personnelles et généralement uniques. Par contre la faiblesse vient de ce que les appareils de reconnaissance ou de mesure ne sont pas encore très fiables. Il subsiste généralement des possibilités d'authentifier à tort un individu ou de refuser l'authentification à la bonne personne.

2.1.5 Ce qu'est et ce que détient l'entité

L'enregistrement des caractéristiques physiques de l'individu est présent sur le support (empreintes digitales, la signature,...).

2.1.6 Ce qu'est, ce que détient et ce que connaît l'entité

La combinaison des trois techniques est évidemment la solution la plus solide, mais sans doute pas la moins chère, ni la plus facile à accepter par l'utilisateur.

2.2 Les techniques et les outils

Ce paragraphe reprend les différents moyens d'authentification définis ci-dessus en énonçant quelques possibilités techniques de les réaliser.

Au préalable, il est nécessaire de bien rappeler la différence entre ce que connaît l'entité, c'est-à-dire l'utilisateur, et les informations secrètes placées dans un matériel afin d'authentifier le matériel. Ce type d'utilisation de secret n'est donc qu'une forme de l'authentification par ce que détient l'utilisateur.

2.2.1 Par ce que connaît l'utilisateur

Plusieurs appellations existent pour ce type de secret : code secret, mot de passe, code confidentiel, P.I.N. (numéro d'identification personnel),... Elles ne sont pas normalisées.

Dans ce texte, le code secret recouvre l'ensemble des possibilités, le mot de passe est retenu comme un secret utilisé seul, le code confidentiel ou P.I.N. sont souvent utilisés en association avec un support tel que les cartes.

Dans tous les cas, pour rester réellement confidentiel un code secret doit le plus possible :

. être individuel,

. avoir une durée de validité limitée et donc être modifié périodiquement.

a) Mot de passe simple

Avantage : facile à mettre en oeuvre car la majorité des outils de sécurité existants sont basés sur son utilisation.

Les risques :

. lecture de la table des mots de passe. Il est donc conseillé de la chiffrer et/ou de la stocker dans une boîte sécurisée,

. possible à trouver par déduction parce que souvent trivial par recherche exhaustive si le nombre de tentatives n'est pas contrôlé,

. subtilisé par des tiers :

- par lecture lors de la frappe,
- intercepté dans le système,
- par lecture sur un document s'il a été écrit par son propriétaire.

Les parades :

. utiliser des mots de passe mémorisables par l'individu mais aléatoires,

. surveiller les tentatives d'accès illicites par comptage,

. surveiller les accès illicites réussis en affichant à l'utilisateur sa dernière date et heure d'accès.

b) Mot de passe variable (dynamique)

Les mots de passe générés aléatoirement ou semi-aléatoirement par un algorithme sont considérés comme des codes confidentiels.

Une des possibilités manuelles est la génération préalable par un des interlocuteurs d'une liste de mots de passe dont il donne une copie à l'autre et dans laquelle les mots sont utilisés séquentiellement et une seule fois.

Risque :

. perte de confidentialité de la table pendant la diffusion ou le stockage,

. difficulté de conservation par l'utilisateur,

. lacune dans le processus de synchronisation suite à une erreur.

c) Codes confidentiels

Leur contrôle se fait par comparaison soit avec une information stockée dans ou sur le support, soit à une information calculée à partir d'autres informations détenues dans ou sur le support.

Ces supports peuvent être : carte à piste, carte à puce, authentifieurs, carte à laser,...

2.2.2 Par ce que détient l'utilisateur

Ce type d'authentification peut être classé en trois catégories en fonction de la manière d'effectuer le contrôle : physique, visuel ou automatisé.

a) Contrôle physique

Clé physique : clé de la porte du local ou de la serrure du terminal qui ne s'ouvrent que si la clé est bonne.

Risques :

. perte, avec utilisation par un intrus ou impossibilité de continuer à travailler,

. duplication,

. serrure facile à forcer parce qu'acceptant par exemple plusieurs clés.

Limite : si la clé est unique et non duplicable, une seule personne peut mettre le terminal en fonction, l'authentification est meilleure, mais l'ergonomie d'utilisation par plusieurs personnes est faible.

b) Contrôle visuel

Le contrôle est exercé par un "gardien". Le support peut être en papier (carte d'identité, passeport,...) ou en plastique (badge,...). Leur qualité d'authentification est d'autant meilleure qu'il est induplicable, non reproductible, inaltérable... et qu'il est possible de faire un lien visuel avec le porteur grâce à une photo, une signature,...

Différentes possibilités permettent d'améliorer ces caractéristiques : embossage, hologramme, fil incorporé, photo gravée, tampon sec,...

c) Contrôle automatisé

Dans ce paragraphe, seules sont traitées les utilisations sans code confidentiel :

- carte à code barre,
- carte à laser,
- carte à lecture distance,
- carte à piste magnétique,
- carte à micro-circuit,
- authentifieurs (Grenouille, Secur Id....),
- "bouchons ou clés électroniques" (matériels connectés sur une prise du terminal PC ou MINITEL).

Les risques sont communs à toutes ces formes mais éventuellement avec des niveaux différents :

- perte : risque identique,

- effacement des informations rendant le support inutilisable : risque identique,

- duplication ou contre-façon : quasiment impossible pour les cartes à micro-circuits, les authentifieurs, les cartes à lecture à distance et les clés électroniques.

2.2.3 <u>Par ce que connaît et détient l'utilisateur</u>

Les supports sont les cartes à piste magnétique ou à puce et les authentifieurs. Leur association avec un code confidentiel diminue les risques.

a) Carte à piste magnétique

Bien que duplicable, la nécessité de connaître le code confidentiel réduit nettement le risque de perte à condition que ce code ne soit pas facile à trouver : par étourderie du propriétaire, par facilité à deviner, par faiblesse de l'algorithme de calcul ou par lecture de la piste s'il est écrit en clair.

b) Carte à puce

Trois types de cartes doivent être distingués selon les techniques utilisées :

Cartes à mémoire

La puce est simplement une mémoire sans possibilité d'incorporer un programme et par conséquent des algorithmes.

Risque : ce type de carte est sans doute plus difficile à contrefaire qu'une carte à piste, mais la lecture du secret stocké en mémoire est relativement facile lors de sa lecture pour comparaison.

Cartes "bi-chips"

Une des puces est programmable, la seconde est une mémoire de stockage.

Risque : possibilité de lecture du code secret lors du transfert entre la mémoire et le programme.

Cartes à micro-processeur

Seules ces cartes sont actuellement réputées inviolables, tout au moins sans un matériel sophistiqué et très coûteux.

Ces cartes contiennent des données, des clés, des algorithmes de calcul.

Elle peuvent assurer leur propre sécurité et permettre à leurs propriétaires de s'authentifier localement par son code confidentiel et à distance par un système algorithmique.

Il existe plusieurs types d'algorithmes qui permettent d'offrir des authentifications ayant des qualités différentes : le problème de gestion des clés est traité dans le chapitre "Gestion des secrets". La non-répudiation est traitée dans le chapitre "Mesures complémentaires au contrôle d'accès".

Risque : subtilisation du code confidentiel : mêmes possibilités théoriques que pour la carte à piste mais la possibilité de l'inscription d'un secret dans la mémoire protégée rend la fraude plus compliquée.

c) Authentifieurs

Il s'agit de matériels dotés de micro-processeurs comme la carte à mémoire, mais non connectés. Ils peuvent également être considérés comme le moyen de générer des mots de passe "une fois".

Avantage : basés sur le même type d'échange que la carte à mémoire, ils permettent un niveau d'authentification équivalent sans nécessiter de lecteur de carte.

Inconvénients :

- ne permettent pas toujours l'utilisation conjuguée d'un code secret personnel, ce qui accroît le risque lié au vol ou à la perte;

- n'étant pas connectés, ils nécessitent des entrées de données supplémentaires sur le clavier du terminal, et par conséquent ils entraînent des risques d'erreurs de manipulation;

- ne permettent pas de gérer facilement des clés de session utilisables par les autres algorithmes.

2.2.4 Par ce qu'est l'utilisateur

Appelée identification biométrique ou anthropométrique, elle s'appuie sur la reconnaissance des caractéristiques physiques de l'utilisateur.

Avantages :

- unicité et stabilité de certaines caractéristiques physiques.

Inconvénients :

- nécessité d'un dispositif sophistiqué,
- pas toujours toléré par les utilisateurs,
- encore insuffisamment précis.

a) Caractéristiques physiques utilisées

- empreintes digitales (dermatoglyphes) - lecture difficile et longue à utiliser pour les applications très sensibles;

- surfaces externes des doigts - lecture par cellules photo électriques - mieux accepté que les empreintes digitales;

- forme de la main surtout utilisée en contrôle d'accès physique; référentiel sur carte magnétique;

- fond de l'oeil;

- reconnaissance de la voix :

  . nécessité d'un environnement peu bruyant (circuit téléphonique dédié),

  . la difficulté est d'acquérir un référentiel,

  . la voix est digitalisée.

b) Reconnaissance de la signature

<u>Principe</u> :

- transformation en impulsions électriques des mouvements produits lors de la signature;

- analyse statistique de la signature (pression, accélération, freinage, levée de plume...);

- ignorance du graphisme car trop facile à contrefaire.

<u>Qualité</u> :

- pas de perte, vol, prêt
- geste habituel pour l'utilisateur
- auditable
- stockage possible sur carte à micro-processeur

<u>Limites</u> :

- définir le seuil d'acceptabilité des variations par rapport au référentiel : (LA TOLERANCE). Un réglage fin du seuil d'acceptabilité permet d'éliminer tous les imposteurs mais par contre, multipliera les refus injustifiés et inversement avec un réglage de seuil bas.

  Ce problème est commun aux autres caractéristiques physiques.

2.2.5 <u>Par ce qu'est et détient l'utilisateur</u>

Voir 2.2.6

2.2.6 <u>Par ce qu'est, détient et connaît l'utilisateur</u>

Le cumul de ces possibilités diminue progressivement le risque d'acceptation à tort d'un utilisateur, mais par contre augmente le risque de refus à tort.

De plus, ce cumul complexifie tant la gestion que l'utilisation de l'authentification.

Dans ce type d'utilisation, les caractéristiques du porteur peuvent être soit enregistrées sur la carte elle-même, soit sur un fichier local au central. La protection de ces caractéristiques contre la modification doit évidemment être forte.

3. AUTHENTIFICATION A TRAVERS UN RESEAU

Dans les réseaux, il faut que lorsqu'une opération arrive à son destinataire, central ou terminal, celui-ci soit assuré de l'identité de l'émetteur.
Les risques sont :

- soit que quelqu'un intercepte des données d'identification et les réutilise,

- soit qu'il les modifie,

- soit que les données s'altèrent au cours de la transmission.

Il est nécessaire d'assurer la confidentialité et l'intégrité des informations d'authentification de bout en bout.

Deux entités qui veulent communiquer en se protégeant contre des tentatives de fraude doivent être capables de se reconnaître mutuellement. Cette authentification n'est possible que si elles ont préalablement échangé par un moyen inattaquable des informations de reconnaissance.

Il est nécessaire d'introduire un élément secret et aléatoire (procédure de Hand-shaking) variant à chaque session et permettant à chaque entité de s'assurer qu'un tiers ne cherche pas à se substituer à l'une ou l'autre des entités. Ceci par un double échange lors de l'établissement de la connexion (principe de l'accusé de réception).

L'authentification à distance comporte deux procédures, dont la première est obligatoire :

- l'authentification de l'entité (l'utilisateur) par le code confidentiel lié au support ou le mot de passe donné par l'utilisateur,

- l'authentification du matériel : terminal ou support individuel.

Pour garantir l'intégrité et la confidentialité des données d'authentification télétransmises, deux techniques sont possibles :

- l'utilisation d'un "canal sûr",

- l'échange de codes non réutilisables.

a) canal sûr

- Dans certains cas ce "canal sûr" est clairement identifiable : lorsque deux partenaires s'adressent des messages chiffrés par un algorithme du type DES après avoir échangé sur un support quelconque les clés secrètes de chiffrement et de déchiffrement, cet échange apparaît comme un canal sûr.

- Dans d'autres cas, comme l'authentification par un système basé sur RSA, l'existence de ce canal sûr existe aussi mais de façon moins évidente. L'acheminement de la clé publique doit être protégée contre toute altération (intégrité).

  Il est donc nécessaire d'assurer la confidentialité et l'intégrité de l'information télétransmise. En conséquence, le problème de l'authentification à distance se ramène à ces deux propriétés : c'est le problème de la gestion des secrets traité au chapitre 2.

b) échange de codes non réutilisables

Plusieurs techniques peuvent être utilisées :

- utilisation de tables de codes une fois par les deux interlocuteurs,

  Ces codes n'étant utilisés qu'une seule fois et dans une séquence figée, l'interception d'un code ne permet pas de le réutiliser ensuite. Le seul moyen de frauder est de se procurer tout ou partie de la liste détenue par les deux interlocuteurs.

- génération de codes une fois par chaque extrémité :

  Dans ce cas, chacun des interlocuteurs dispose d'un mécanisme leur permettant de générer simultanément le même code secret, par exemple à partir de la date et de l'heure. Deux conditions doivent être remplies :

  . le mécanisme ou la base de calcul doivent être confidentiels,

  . les bases de calcul (date et heure par exemple) doivent être parfaitement synchronisées.

- vérification d'un calcul sur un nombre aléatoire :

  L'un des interlocuteurs envoie un nombre aléatoire à l'autre. Le récepteur exécute alors un calcul à partir d'un algorithme et d'une clé spécifique pour un couple d'interlocuteurs. La vérification par l'émetteur du résultat du calcul lui permet de vérifier que le récepteur dispose bien de la clé secrète du couple.

Deux types d'outils sont utilisés :

. les authentifieurs qui sont des sortes de calculettes détenues par l'utilisateur alors que le central est doté de l'algorithme et des clés de chaque authentifieur;

. la carte à micro-circuit, chaque carte dispose d'une clé spécifique. Le micro-circuit du central ne dispose que d'une clé maître, mais est capable de recalculer les clés filles à partir de l'identifiant de la carte. C'est la technique de diversification de la clé.

<u>Schéma</u> :

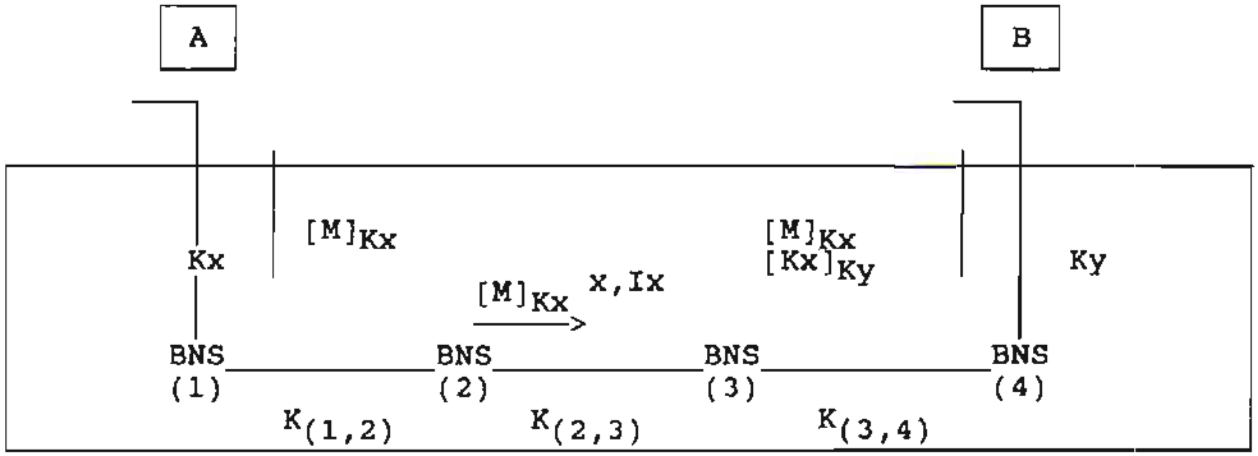
	Carte	Terminal	Central	Processeur de sécurité
Authentification de l'individu	Vérification du code			
Authentification de la carte par le central		Demande de Session ——>		
	<——			Nombre aléatoire A
	R=F(A,Sc,I) ——>			Sc=F(S,I)
				R'=F(A,Sc,I) R=R' ?
Génération de clés de session pour la sécurisation des messages	Ki=f o F(A,S'c,I)			S'c=F(S',I) Ki=f o F(A,S'c,I)

. chiffrement

. scellement

Le calcul mathématique (f) permet de générer des clés dont le format est adapté aux besoins des algorithmes de chiffrement et de scellement

Il est ici important de noter que, dans la mesure où la clé de base est unique, cette solution permet de transmettre un message d'un bout du réseau à l'autre sans nécessiter de déchiffrement-rechiffrement aux frontières des sous- réseaux. Le graphique suivant illustre cette possibilité.



BNS = Boîte Noire de Sécurité

L'avantage de la carte à mémoire sur les authentifieurs est qu'elle est connectée, les échanges d'informations sont donc automatiques.

Par contre les authentifieurs nécessitent souvent de saisir sur le terminal le résultat du calcul et de plus ils nécessitent rarement l'entrée d'un code secret personnel, ce qui les rend plus faibles face au vol.

4. L'ACCES UNIVERSEL

C'est la possibilité laissée à certains utilisateurs d'accéder à un réseau à partir de plusieurs (ou même de tous les) points d'accès du réseau. Cet objectif fonctionnel peut avoir des répercussions importantes sur le choix des outils et même sur l'architecture du système.

Dans beaucoup de systèmes existants jusqu'à présent l'authentification se fait par authentification du terminal + mot de passe.

Pour l'accès universel, trois solutions sont possibles :

- vérification du mot de passe en centralisé :

  Une bonne authentification nécessite d'avoir un canal sûr entre le terminal et le central et impose donc l'authentification du terminal.

De plus, cette vérification centralisée allonge le temps de réponse ce qui est surtout pénalisant lors des erreurs de saisie.

- vérification locale du mot de passe :

  Dans ce cas également, il est nécessaire d'avoir un canal sûr pour assurer la continuité de l'authentification.

  La difficulté complémentaire vient du besoin de détenir le mot de passe d'un individu sur plusieurs terminaux, avec les risques qu'entraîne cette multiplication.

- vérification du code confidentiel par le support lui-même :

  Dans ce cas l'authentification du terminal n'est plus nécessaire, l'authentification de l'individu est plus souple puisque celui-ci transporte avec lui tous les éléments nécessaires.

  Toutefois, si pour différentes raisons, il est souhaitable de limiter l'accès à certains terminaux, l'authentification du terminal pourra aisément venir en complément.

  Dans la pratique, il semble que l'authentification de la personne soit plus importante que celle du terminal en particulier lors d'une recherche après fraude.

2 - LA GESTION DES DROITS - L'AUTORISATION

INTRODUCTION

1) ETUDE DE L'EXISTANT

1.1 ACTEURS

1.1.1 Utilisateurs

a) Catégories d'utilisateurs

b) Nature des applications accédées

1.1.2 Propriétaires des ressources accédées

1.1.3 Administrateur de la sécurité

1.1.4 Gestionnaires de la sécurité

1.1.5 Responsable opérationnel de l'utilisateur

1.1.6 Prestataire de service

1.2 LES TYPES DE DROITS

1.2.1 Droit d'accès aux informations et droit d'accès aux transactions

Droit d'accès aux applications et/ou au système

1.2.2 Nature des accès et localisation

a) Site central

b) Processeurs de télécommunications

c) Réseaux publics

d) Boîtes noires de chiffrement

e) Micros-stations de travail intelligentes

1.2.3 Modalités

a) Les droits doivent-ils être individuels ou partagés et indépendants ou hiérarchisés ?

b) Les droits doivent-ils être attribués par individu ou par fonction ?

c) Les droits doivent-ils être tous définis ou existe-t-il des droits par défaut ?

d) Les droits sont-ils fonction de l'organisation administrative, géographique ou technique de l'entreprise ?

e) Les fichiers de droit doivent-ils être centralisés ou décentralisés ?

f) Existe-t-il un circuit de secours pour les contrôles des droits ?

2) MISE EN OEUVRE DU CONTROLE DES DROITS

2.1 GESTION ET UTILISATION DES DROITS EN FONCTION DE LEUR LOCALISATION

2.1.1 Droits sur la carte

2.1.2 Gestion des droits sur le terminal

2.1.2.a Mode micro

2.1.2.b Mode conversationnel

2.1.2.c Mode "batch" avec connexion différée

2.1.2.d Mode terminal multi-fonctions

2.1.3 Droits sur des processeurs intermédiaires

2.1.3.a Protection du noeud

2.1.3.b Protection des circuits, des transactions et informations

2.1.4 Droits sur les centraux

2.2 L'ADMINISTRATION DE LA SECURITE

2.2.1 La gestion des droits

2.2.2 La sécurité du contrôle des droits

2.3 L'IMPACT DES PRESTATAIRES DE TRANSPORT SUR LES DROITS

RECOMMANDATIONS

INTRODUCTION

L'essentiel de la protection de l'information est constitué de mesures visant à contrôler l'accès aux données, c'est-à-dire que seules les personnes habilitées doivent pouvoir accéder aux informations et ne réaliser que les natures d'accès autorisées.

Il apparaît alors qu'un des éléments principaux de la sécurité réside dans la gestion des droits ou autorisations d'accéder et/ou de manipuler les informations.

Pour réaliser cette gestion, plusieurs actions doivent être entreprises dans le respect de quelques principes qui apparaissent comme fondamentaux :

- un système de classification de référence doit être spécifié préalablement;

- la valeur et le contexte d'échange des informations déterminent le niveau de leur sensibilité face aux risques encourus;

- l'usager du système d'information doit connaître ces risques lors des opérations qu'il effectue afin de pouvoir :

  . définir ses objectifs de sécurité,
  . élaborer les mesures de protection,
  . apprécier les techniques qu'il doit mettre en oeuvre;

- chaque information doit avoir un propriétaire désigné;

- les responsabilités doivent être parfaitement définies;

- les fonctions de sécurité doivent être réparties entre plusieurs personnes afin de compliquer la tâche des fraudeurs éventuels (principe de séparation des fonctions);

- les fonctions, outils et procédures doivent pouvoir être contrôlés et audités.

1) ETUDE DE L'EXISTANT

Avant de traiter les avantages et inconvénients des différentes mesures en fonction du cadre dans lequel elles sont mises en oeuvre, ce chapitre recense les différents éléments ou critères qu'il apparaît souhaitable d'envisager lors d'une étude de sécurité :

- quels sont les acteurs de la sécurité ?
- quels types de droits peuvent être envisagés ?
- quelles sont les localisations des éléments de gestion de ces droits ?

1.1 ACTEURS

Sans prétendre à l'exhaustivité, les fonctions suivantes sont susceptibles de participer à la gestion des droits :

- utilisateurs,
- propriétaires des ressources,
- administrateurs de la sécurité,
- gestionnaires de la sécurité
- responsables opérationnels de l'utilisateur,
- prestataires de service

Les fonctions et critères décrits ci-après ne sont qu'indicatifs et devront être complétés et appréciés selon les besoins et les caractéristiques propres à l'entreprise.

1.1.1 Utilisateurs

Selon la taille et les fonctions de l'entreprise, il est possible de distinguer les utilisateurs par :

- leur catégorie,
- la nature des applications qu'ils accèdent.

Mais attention, il ne faut pas négliger, chez l'utilisateur, l'existence possible de compétences non implicitement déduites de sa catégorie d'appartenance.

a) Catégories d'utilisateurs

Les utilisateurs peuvent être regroupés en tant que :

- informaticiens,
- utilisateurs internes et externes,
- pseudo-utilisateurs.

*** Informaticiens**

Ils peuvent être caractérisés par leur "agilité d'évolution" au sein du système informatique.

Le principe est admis de les regrouper en deux sous-ensembles de population représentatifs de profils de besoins et de risques différents :

- développement,

- centre de production (atelier, assistance, réseaux, système, administration).

* **Utilisateurs internes**

Il s'agit du personnel de l'entreprise utilisateur de l'informatique sur son lieu de travail et qui ne peut accéder qu'aux seules données ou applications qui lui sont autorisées.

Il peut s'agir également de prestataires de service dont la présence est temporaire dans l'entreprise.

* **Utilisateurs externes**

Ce sont des acteurs appartenant ou non à la société mais accédant au réseau ou au système d'information à partir de terminaux spécifiques ou indéterminés :

- accès par réseau commuté, par réseau TRANSPAC,
- accès pour des besoins de télémaintenance,
- ...

* **Pseudo-utilisateurs**

- d'applications spécifiques (type transfert de fichiers),

- de processus d'interconnexion de réseaux.

Pour les trois premières catégories d'utilisateurs, le contrôle d'accès est basé sur :

- l'authentification sûre du terminaliste en plus du contrôle d'accès physique aux locaux;

- et sur l'authentification éventuelle du terminal (identifiable physiquement et logiquement).

Pour la dernière catégorie d'utilisateurs, le contrôle d'accès est fondé sur des dispositifs sûrs d'authentification et de gestion des droits.

b) Nature des applications accédées

Cette nature prend en compte :

- le type d'application accédée :infoservice, transaction TP, programme batch, tests, VIDEOTEX,

- le domaine de gestion de l'entreprise affecté : bancaire, autre.

Il est donc alors souhaitable de bien différencier les types de gestion des droits.

1.1.2 Propriétaires des ressources accédées

Fonctions envisageables :

- définition des biens dont il a la responsabilité,
- classification de ces biens,
- spécification des contrôles nécessaires,
- accord d'autorisation aux utilisateurs concernés,
- avoir l'assurance que les règles de protection sont bien respectées.

1.1.3 Administrateur de la sécurité

Fonctions envisageables, avoir l'assurance :

- que les acteurs, prestataires et utilisateurs connaissent les règles de gestion des droits,

- de l'adéquation du niveau de protection aux besoins de l'organisation,

- de la mise en oeuvre des contrôles.

1.1.4 Gestionnaires de la sécurité

Fonctions envisageables :

- attribution des droits,

- gestion des droits.

1.1.5 Responsable opérationnel de l'utilisateur

Fonctions envisageables :

- définition des autorisations d'accès selon les besoins du service,

- protection des équipements d'accès mis à disposition,

- application des règles de sécurité,

- information sur le départ des collaborateurs

1.1.6 Prestataire de service

Ils peuvent être regroupés selon les aspects suivants :

* prestataires de transport :

  Nous citerons par exemple TRANSPAC, les P.T.T., les prestataires de télémaintenance.

  Dans ce cadre, il apparaît nécessaire de bien maîtriser les conditions d'intervention de ces prestataires et les risques éventuels induits sur le système d'information de l'entreprise cliente.

* prestataire informatique du central :

  Fonctions envisageables :

  - connaissance, application des mesures de sécurité relative à la classe de sécurité choisie,

  - informations du propriétaire, du responsable et des utilisateurs de la ressource, des modifications exceptionnelles de la protection de cette dernière,

  - mise en oeuvre (et administration éventuelle) des moyens de contrôle de la gestion des droits.

1.2 LES TYPES DE DROITS

1.2.1 Droit d'accès aux informations et droit d'accès aux transactions.

La différence d'objectif de la gestion des droits entre informations et transactions est très importante car elle peut conduire à des choix d'outils très différents.

En effet lorsque les droits s'appliquent aux informations ils consistent à préciser : les fichiers accessibles par l'utilisateur, les opérations autorisées (lecture, écriture, destructions, ...).Le cadre est en fait relativement souple.

Pour ce type de gestion de droits il est nécessaire d'avoir au préalable classifié les informations selon leur degré de sensibilité. Pour ce faire, il faut apprécier pour chaque information quels sont les risques en cas de divulgation.

Par contre, lorsque les droits concernent les transactions, l'utilisateur est par principe plus limité. Les transactions correspondent en effet à des séries de commandes figées.

Par exemple : l'utilisateur ne peut pas choisir le fichier auquel il veut accéder, les fichiers accessibles ont été prédéterminés. Ceci n'empêche pas que certains droits soient liés à la valeur de l'information.

Le degré de liberté laissé aux mécanismes mis à disposition dans ces deux cas a toutefois une grande importance, car, à la limite, même si les philosophies et la manière de gérer les droits sont différentes le résultat peut être le même si le degré de liberté ou de souplesse est très grand.

Ces deux types de gestion de droits sont en général utilisés dans des domaines professionnels différents :

- la gestion des droits en fonction des informations est celle retenue par les militaires qui cherchent, en outre, essentiellement à protéger la confidentialité. Les normes émises par le DOD correspondent à cet objectif. Dans le domaine professionnel classique cette gestion correspond assez bien aux environnements de développement et d'infocentre,

- la gestion des droits par transaction correspond plus au domaine commercial, la propriété recherchée en priorité étant l'intégrité. Aucune norme n'existe dans ce domaine, ce qui entraîne les constructeurs à respecter les normes du DOD relativement inadéquates plutôt que des règles adaptées mais inexistantes.Un effort dans ce sens est nécessaire.

Ce type de gestion des droits basée sur les transactions est plutôt nécessaire pour les utilisateurs car hormis en infocentre ou en informatique personnalisée, ils ont besoin de disposer de bases de données ou de fichiers bien précis.

Les deux notions peuvent également être associées. Il est possible d'avoir des droits d'accès aux transactions dont certains nécessitent en outre des droits d'accès aux données et inversement.

De même, quand on a la gestion par information, on peut avoir des droits d'accès par utilisateur.

Droits d'accès aux applications et/ou au système

De la même manière, il est nécessaire de distinguer et généralement de séparer les droits d'accès aux applications de ceux qui donnent accès au système. En résumé, les droits d'accès aux applications devraient être réservés aux utilisateurs, alors que ceux liés au système concernent exclusivement l'exploitation informatique.

Cette séparation est cependant rarement totale car en cas d'incidents les exploitants sont parfois amenés à accéder aux applications, mais ceci doit alors donner lieu à un suivi et à un contrôle rigoureux. De plus, le cas le plus complexe est celui des développements qui impose généralement d'offrir aux développeurs des droits des deux types.

D'une manière générale, les droits système sont plutôt du type accès aux informations et aux fonctions systèmes, alors que les droits applications, dans le domaine des réseaux et donc du temps réel, font appel à des droits par transaction.

Cette partition entre les droits système et applicatifs peut s'avérer particulièrement intéressante, voire nécessaire, dans le cas des antéserveurs traités dans un chapitre ultérieur.

1.2.2 Nature des accès et localisation

En complément à la définition des droits d'accès, les aspects relatifs à la nature des accès autorisés et à leur localisation sont exposés ci-après.

La mise en oeuvre de ces autorisations implique :

- de connaître la nature des accès réalisables par ressource identifiée;
- la mise en oeuvre de dispositifs standard ou spécifiques;
- le choix des lieux d'implantation de ces dispositifs.

La réalisation du contrôle peut être effectuée :

- au site central,
- sur le processeur de télécommunications,
- au niveau des réseaux publics,
- dans les boîtes noires de chiffrement,
- dans les micros ou stations de travail intelligentes.

Une liste d'éléments d'appréciation associés aux ressources identifiées, natures des accès et dispositifs de mise en oeuvre, est proposée pour chacun des niveaux de localisation géographique précisés ci-dessus.

a) Site central

* Ressources identifiées :

- fichiers, base de données,
- volumes bandes-disques,
- logiciels utilisateurs de bases, moniteurs associés,
- transactions,
- ordinateurs,...

* Nature des accès :

- interdiction, autorisation complète,
- lecture,
- écriture,
- chargement,
- suppression,
- habilitation par mot de passe,...

* Dispositifs :

- logiciel de base standard du constructeur,
- progiciels de contrôle d'accès.

b) Processeurs de télécommunications

* Ressources identifiées :

- chemins d'accès,
- noeuds du réseau,
- liaisons,
- administration de réseau,
- logging du réseau,
- applications spécifiques.

* Nature des accès :

- masquage de liaisons d'applications,
- localisation par mot de passe,
- identification du chemin et du sens autorisés,
- restriction de connexion (automatique, semi-automatique),
- appartenance à un G.F.A.,
- autorisation d'établissement d'une session,
- lecture, écriture (outils de maintenance interactifs)...

* Dispositifs :

  - logiciels standard de gestion de réseau,
  - progiciels spécifiques de contrôle, d'exploitation du logging...

c) Réseaux publics

* Ressources identifiées :

  - abonnés (N° TRANSPAC),
  - circuits virtuels,
  - équipements terminaux...

* Nature des accès :

  - appel entrant,
  - appel sortant.

* Dispositifs :

  - groupe fermé d'abonnés,
  - taxation...

d) Boîtes noires de chiffrement

* Ressources identifiées :

  - algorithme,
  - clés,
  - équipements associés...

* Nature des accès :

  - lecture, écriture,
  - procédure d'échange des clés...

* Dispositifs-matériels et logiciels de :

  - personnalisation,
  - suivi des alarmes,
  - protection contre les tentatives de violation...

e) Micros-stations de travail intelligentes

Les éléments descriptifs sont à apprécier selon le mode d'utilisation de la station :

- en local : il s'agit d'une version réduite du site central,

- connecté au central : les modalités du contrôle sont réparties entre le central et la station locale,

- connecté en réseau local...

Il est nécessaire de tendre vers un seul mode de gestion des droits quel que soit le mode d'utilisation de la station (un mode opératoire commun).

1.2.3 Modalités

1.2.3.a Les droits doivent-ils être individuels ou partagés, et indépendants ou hiérarchisés ?

α) Droits individuels ou partagés ?

Faut-il donner la possibilité à un utilisateur d'effectuer seul une action ?

Il existe en effet différentes possibilités d'améliorer la sécurité en partageant les droits, chacun ayant une partie d'un droit et ne pouvant agir qu'avec l'intervention d'une ou plusieurs autres personnes.

Exemple :

- certains systèmes de génération de mots de passe imposent l'implication de deux ou n officiers de sécurité pour la création et la diffusion des mots de passe : chacun génère une partie du mot de passe et la remet à l'utilisateur qui reconstitue le secret par combinaison ou juxtaposition des différentes parties.

- Autre exemple : pour la gestion de fichiers de clés secrètes bilatérales entre plusieurs établissements, il est envisageable que la fonction de gestion ne puisse être activée que si plusieurs mots de passe sont introduits.

Avantages : Impose au fraudeur une complicité qui présente un risque certain avec une ou plusieurs personnes.

Inconvénients : Complexité des procédures qui nécessitent l'intervention simultanée ou quasi-simultanée de plusieurs personnes.

Conclusion :

Ce type de mécanisme doit être utilisé lorsque les risques fonctionnels sont élevés, ce peut en particulier être le cas des systèmes hiérarchisés dans lesquels une seule personne pourrait détenir ou s'attribuer l'ensemble des droits.

ß) Droits indépendants ou hiérarchisés

En préalable, à l'énoncé des avantages ou inconvénients de la hiérarchisation des droits, il est nécessaire de bien rappeler la différence entre structure hiérarchique des droits et structure hiérarchique de l'attribution des droits, c'est-à-dire entre l'utilisation et la gestion.

Dans le premier cas, tout supérieur hiérarchique dispose des mêmes droits que ceux qui dépendent de lui. Alors que dans le second, c'est lui qui attribue les droits, dont il ne dispose pas forcément lui-même. Il est même préférable qu'un individu ne puisse pas s'attribuer lui-même des droits.

Le système doit donc être conçu pour bien séparer le droit d'utilisation et celui de gestion des droits.

Hiérarchisation de la gestion des droits :

Dans ce cas, chaque responsable hiérarchique peut attribuer des droits à ses subordonnés. Le nombre de niveaux de délégation n'est pas limité.

Ce type de décentralisation de l'attribution des droits est indispensable dans les systèmes où les utilisateurs sont nombreux, la gestion centralisée par un officier sécurité serait en effet trop compliquée et lourde.

Ce type de hiérarchisation ne pose pas de problème dans la mesure où la séparation entre les droits et leur gestion est bien réalisée et qu'une personne ne peut pas directement ou indirectement s'attribuer elle-même des droits.

Un contrôle périodique des droits par une personne n'ayant éventuellement aucun droit elle-même est cependant indispensable: c'est la notion d'audit.

1.2.3.b Les droits doivent-ils être attribués par individu ou par fonction ?

Avantage de l'attribution par individu :

Plus grande souplesse fonctionnelle de gestion des droits.

Les responsabilités d'un individu sont souvent liées simultanément à la fonction qu'il exerce, à sa personnalité, à son ancienneté dans le poste,... Il est donc préférable de pouvoir adapter les droits à ces critères.

Inconvénient :

Gestion plus complexe tant pour l'attribution des droits que pour le suivi des attributions de droits et de leur utilisation.

Remarques :

Lorsque les droits sont attribués par individu, il devient quasiment nécessaire d'effectuer l'authentification de l'individu et non du terminal.

Une solution mixte combinant les avantages des deux solutions est de relier les droits d'un individu à un groupe de droits par fonction mais avec possibilité de rajouter ou d'enlever des droits à ce groupe. Dans ce cas, l'authentification doit aussi porter sur l'individu.

Le choix sera fait selon la plus ou moins grande rigidité des droits affectés à une fonction et selon les coûts, en n'oubliant pas d'anticiper sur la possibilité d'évolutions futures.

1.2.3.c Les droits doivent-ils être tous définis ou existe-t-il des droits par défaut ?

Deux solutions sont possibles :

Tout ce qui n'est pas défendu est permis et tout ce qui n'est pas permis est défendu.

Il est clair que la seconde proposition est plus limitative et qu'elle permet de mieux maîtriser la sécurité.

Cependant, cette solution n'est pas toujours retenue dans la mesure où l'important pour une entreprise est souvent plus de travailler que de faire de la sécurité. Il existe donc des cas où l'entreprise préfère limiter la gestion des droits à quelques points, tout le reste étant autorisé afin de limiter les impacts négatifs de la sécurité sur l'ergonomie du travail.

1.2.3.d Les droits sont-ils fonction de l'organisation administrative, géographique ou technique de l'entreprise ?

Ces organisations sont un fait dans une entreprise. Une étude du besoin fonctionnel est donc indispensable avant de choisir l'outil et de définir l'architecture des droits. L'adéquation des droits aux structures d'une entreprise doit permettre, d'une part, à l'entreprise de travailler, d'autre part, de limiter les risques en ne laissant pas une latitude inutile.

α) impact de l'organisation administrative

Dans une entreprise à succursales multiples, telle qu'une banque, les droits d'accès peuvent être hiérarchisés.

Par exemple, la Direction Centrale a droit d'accéder à toutes les entités qui dépendent d'elles. La Direction Régionale a droit d'accéder aux informations du Groupe et des Sièges mais pas à celles de la Direction Centrale, et ainsi de suite...

Les droits ne sont pas obligatoirement aussi stricts. On peut aussi admettre que la structure hiérarchique ait le droit d'accès aux niveaux inférieurs en lecture mais pas en écriture.

ß) Impact de la structure géographique

* Lier les droits aux terminaux.

  Dans ce cas les droits d'accès sont attachés aux sites dans lesquels sont situés les terminaux ou ordinateurs.

  Par exemple, il est envisageable d'empêcher les employés de travailler à partir des terminaux d'entités dans lesquelles ils n'ont pas habituellement accès.

  L'analyse fonctionnelle des besoins doit donc déterminer si l'authentification du terminal ou de la liaison apporte un plus aux droits de la personne.

  Dans un réseau comme le SIT, il est intéressant d'avoir une structure des droits géographiques dans la mesure où un agent d'une Banque n'a aucune raison de se connecter à partir d'une autre Banque.

  Par contre, à l'intérieur du réseau d'une Banque, ce qui compte,c'est d'être sûr de l'identité du donneur d'ordre. Si un agent ou un client passe un ordre de son bureau ou de chez lui, ce n'est pas forcément gênant à condition que le procédé d'authentification soit totalement fiable. Si ce n'est pas le cas, l'authentification des terminaux autorisés peut compléter l'authentification du porteur.

  Il faut en outre conserver une trace de ces transactions. Elles devront faire l'objet d'un suivi tout particulier.

* Limiter les droits par une authentification géographique

  Dans le cas d'un réseau important, par exemple international, l'entreprise peut vouloir diviser les risques. Elle peut dans ce cas, utiliser pour ses algorithmes d'authentification des clés différentes par région. Un utilisateur aura accès à une ou plusieurs régions s'il dispose d'une ou plusieurs clés.

  Dans ce cas la gestion des droits se fait non pas en gérant directement des droits, mais en jouant sur les facilités d'authentification.

* Limiter les droits en fonction des régions d'origine ou traversées

  Le droit d'accès pourra être géré en liaison avec la structure géographique lorsque, bien que l'utilisateur soit authentifié à Tokyo, bien qu'il ait le droit de faire des transactions boursières, il pourra lui être interdit de les réaliser de Tokyo, mais par contre il pourra interroger.

  De même au niveau international, certains pays n'acceptant pas le chiffrement des messages, il est envisageable que certains messages ne puissent pas transiter par ces pays et que des messages autorisés généralement entre Bruxelles et Paris, en direct, soient refusés lorsque des problèmes de liaison les amènent à transiter par exemple par Londres.

Γ) Impact de la structure technique

Parallèlement à la gestion des droits géographiques, certains droits peuvent être liés à la structure technique, c'est à dire aux circuits.

Certains messages sensibles peuvent être acceptés à partir du terminal de Vesoul lorsque la connexion se fait par TRANSPAC en GFA, mais être refusés lorsque ce réseau est coupé et que le terminal est connecté en back-up par ligne louée considérée comme insuffisamment sécurisée.

1.2.3.e Les fichiers de droit doivent-ils être centralisés ou décentralisés?

Les besoins peuvent en fait être contradictoires pour la gestion et pour l'utilisation.

Sur un strict point de vue de sécurité, il est préférable que pour une même personne la gestion de ses droits soit centralisée afin qu'un contrôle de cohérence puisse être effectué.

En effet, un client de Banque pourrait par exemple être surpris d'avoir le droit d'effectuer des opérations de change jusqu'à 1 million et de ne pouvoir acheter en Bourse que jusqu'à 100.000 F.

Par contre, au niveau des performances, si les fonctions auxquelles un utilisateur peut faire appel, sont situées sur des ordinateurs différents, le temps de réponse sera plus court si les contrôles sont effectués sur l'ordinateur appelé que s'il faut passer par un intermédiaire détenant toutes les autorisations.

Plusieurs solutions sont possibles :

1) Gestion décentralisée des droits

   Chaque ordinateur gère les droits qui le concernent de manière indépendante.

   Avantages : performances.
   Inconvénients : absence de cohérence entre les droits.

2) Gestion centralisée et droits dupliqués

   La gestion des droits se fait en un point unique mais tout ou partie du fichier d'autorisation est dupliquée sur les ordinateurs respectifs.

   Avantages : cohérence assurée, performances améliorées.
   Inconvénients : mise à jour complexe des fichiers.

   Problème de la mise à jour en temps réel des fichiers dupliqués.

3) Gestion centralisée

   Avantages : cohérence des droits.

   Inconvénients :

   - diminution des performances pour les fonctions situées sur un autre matériel

   - Lourdeur de réaction

   - Rigidité plus grande vis-à-vis des besoins spécifiques des entités opérationnelles.

<u>1.2.3.f Existe-t-il un circuit de secours pour les contrôles des droits ?</u>

Le contrôle des droits ne doit pas être abandonné même en cas d'anomalies du système. Il faut donc prévoir que le niveau de contrôle des droits reste cohérent en cas d'utilisation de circuits de secours.

Ceci doit rester valable, que les secours soient administratifs ou techniques, internes ou externes, partiels ou globaux.

La cohérence des droits entre le secours et le fonctionnement normal peut impliquer de dégrader le niveau des fonctionnalités proposées (lorsque l'insuffisance de la sécurité oblige à interdire un certain type de fonction).

2) MISE EN OEUVRE DU CONTROLE DES DROITS

Objectif : donner les avantages et inconvénients pour l'utilisateur des droits, l'administration de la sécurité et l'impact sur les prestataires en fonction de la localisation des droits. Ces indications n'étant manifestement pas exhaustives, elles doivent être combinées et amendées en fonction de l'environnement.

Préliminaire :

Le choix de la localisation des droits doit se faire en prenant en compte plusieurs critères tels que : sécurité, coût, performances, ergonomie d'utilisation et de gestion. Ce choix est toujours un compromis entre une sécurité à 100 % et un coût et une utilisation acceptables.

Quatre types de localisations principaux peuvent être retenus, sur la carte du porteur, sur le terminal, sur un noeud intermédiaire de type antéserveur ou sur le central, sachant que la structure des ordinateurs centraux peut également offrir plusieurs possibilités.

2.1 GESTION ET UTILISATION DES DROITS EN FONCTION DE LEUR LOCALISATION

2.1.1 Droits sur la carte

Avantages :

- réduction des temps de réponse à l'utilisation,
- disponibilité en cas de coupure de ligne pour les fonctions off-line,
- utilisation possible sur des terminaux non connectés en permanence tels que les TPE, TPV.

Inconvénients :

- Manque de fiabilité temps réel. Ce problème est lié à la difficulté de gestion des droits en particulier pour leur mise à jour en temps réel. En effet deux modes d'utilisation sont possibles :

  . soit le terminal ne consulte que la carte pour vérifier les droits comme dans un TPV et une opération sera autorisée même si entre-temps la carte a été mise en opposition,

  . soit le terminal interroge un fichier des oppositions, il y a deux solutions :

    * le fichier est sur le terminal. Encore deux cas :

      . les oppositions sont diffusées en temps réel:

        la mécanique de gestion est alors très lourde,

      . les oppositions sont diffusées en différé ou périodiquement :

        la sécurité est d'autant moins bonne que le différé est long.

    * le fichier est au central

      Le temps d'interrogation du fichier d'opposition est similaire à l'interrogation d'un fichier des droits, seule la taille du fichier est plus petite.

  La sensibilité des opérations est un critère à prendre en compte pour faire le choix du niveau de temps réel nécessaire pour la mise à jour des droits directement ou à travers des oppositions.

- Gestion des droits difficiles.

  La mise à jour des droits sur la carte nécessite soit de récupérer la carte ce qui est lourd, soit de mettre à jour en temps réel lors d'une mise en session, ce qui revient au même que d'interroger les droits au central et rend la décentralisation inutile.

- Problème de capacité de la carte.

  La gestion des droits sur la carte, au moins avec les premiers types de carte dont la taille est restreinte, est limitée par la capacité mémoire de la carte. La place prise par les droits lorsqu'elle est suffisante, réduit simultanément la place disponible pour enregistrer des transactions.

2.1.2 Gestion des droits sur le terminal

Plusieurs cas peuvent être envisagés selon le mode de fonctionnement, en mode micro seul, en conversationnel, en batch avec connexion différée ou en terminal multi-fonction pouvant travailler indifféremment dans l'un des trois modes précédents.

2.1.2.a Mode micro

Les fonctions à réaliser étant locales, il est logique d'avoir les droits en local. Toutefois si les utilisateurs sont amenés à travailler sur n'importe quel micro, la gestion uniquement locale amène à gérer les droits autant de fois que de terminaux accessibles. Dans ce cas une gestion centralisée, avec objectif de ne réaliser les fonctions de gestion qu'une seule fois et de garantir une meilleure cohérence des droits est nécessaire. Cette solution apporte une diminution de la charge pour le gestionnaire des droits et une plus grande souplesse pour l'utilisateur.

2.1.2.b Mode conversationnel

1. Accès à un terminal fixe.

Si les droits sont sur le terminal, les temps de réponse sont réduits mais comme pour les droits sur la carte, le problème est celui de la fiabilité des droits en temps réel.

2. Accès universel.

La gestion des droits sur les terminaux est difficilement envisageable dès lors que le nombre de terminaux est élevé. La seule possibilité pourrait être la gestion en centralisée avec rapatriement des droits, soit lors de la mise en session, soit périodiquement sur les terminaux les plus souvent utilisés.

2.1.2.c Mode "batch" avec connexion différée.

Lorsque certains travaux sont réalisés en local, le résultat étant transmis au central par vacation comme pour la saisie par lots, il y a trois solutions :

- Les droits sont présents sur le terminal. Ils peuvent alors être gérés localement si le terminal d'accès est figé, ou en central avec diffusion périodique lorsque les terminaux autorisent l'accès universel.

- Les droits sont uniquement au central. Dans ce cas, il doit y avoir un contrôle des habilitations en central avant que les mouvements saisis ne soient traités. Les mouvements non autorisés doivent réapparaître sur des listes spéciales contrôlées par des responsables.

- Les droits sont présents sur le terminal et en central, les contrôles sont alors effectués deux fois : à la saisie et avant traitement.

2.1.2.d Mode terminal multi-fonctions.

Ce mode doit tenir compte de l'ensemble des avantages et inconvénients des trois modes précédents : nécessité des droits sur le terminal pour le travail off-line, intérêt des droits au central pour la validité en temps réel.

Une des solutions qui combine le mieux ces besoins, en particulier pour l'accès universel, semble être de gérer les droits en centralisé avec diffusion périodique des droits et diffusion ou vérification de validité à chaque mise en session.

L'un des objectifs complémentaires de la solution doit être d'offrir aux utilisateurs un mode opératoire unique d'utilisation et de gestion des droits.

2.1.3 Droits sur des processeurs intermédiaires

Afin de limiter la charge du central, et de protéger les centraux les droits peuvent être gérés sur des matériels situés entre les terminaux et les serveurs centraux eux-mêmes.

Plusieurs types de droits doivent être pris en compte pour lesquels l'intérêt d'une semi-décentralisation est variable :

- protection du noeud lui-même,
- protection des circuits,
- protection des transactions ou informations.

a) Protection du noeud.

Il appartient à chaque noeud contenant de l'applicatif ou des fonctions de service telles que le routage ou le contrôle d'accès, de protéger sa fonction et son logiciel.

Une gestion des droits spécifiques au noeud est alors nécessaire en distinguant les droits des personnes ayant accès au noeud pour la gestion ou l'utilisation des fonctions propres du noeud (facturation...), et ceux des opérations n'utilisant que des fonctions de service intermédiaire vis-à-vis d'un central (exemple : adaptation de protocoles...).

b) Protection des circuits, des transactions et informations.

Parmi les droits intermédiaires intéressants à mettre sur un noeud de type antéserveur, on peut recenser ceux ayant trait:

- à la juridiction géographique,

- à la juridiction sur les circuits,

- au contrôle d'accès à un central, dans la mesure où l'antéserveur apporterait une meilleure sécurité que le central lui-même .

Problème de back-up.

Lorsque les droits sont situés sur un antéserveur et que celui-ci est en panne mais qu'il existe un antéserveur de secours, il est nécessaire de mettre à jour en permanence les droits sur les deux antéserveurs. Cette gestion pouvant s'avérer complexe et coûteuse, la solution des droits sur le central est de ce point de vue préférable.

2.1.4. Droits sur les centraux

Les paragraphes précédents décrivent les avantages et inconvénients des autres solutions, pour le central, il suffit donc d'inverser les conclusions.

Cependant, plusieurs solutions sont possibles pour la gestion des droits en centralisé :

. gestion en un site unique,

. gestion décentralisée sur chacun des serveurs,

. gestion centralisée mais avec duplication de tout ou partie des droits sur les serveurs.

D'un point de vue de sécurité, il est préférable que la gestion des droits d'un utilisateur donné soit centralisée afin de garantir la cohérence de ces droits entre eux et d'éviter qu'une opposition générale doive être diffusée en différents sites. Par contre cette solution présente des inconvénients au niveau des performances lorsque les droits ne sont pas sur le serveur accédé puisqu'elle nécessite des échanges supplémentaires avec le serveur gérant les droits.

Dans ces conditions, il est possible de garder la gestion des droits sur un site centralisé, mais de diffuser sur chacun des serveurs pouvant être accédé l'ensemble ou la partie des droits correspondant à un serveur. La solution de gestion décentralisée est par contre déconseillée.

2.2 L'ADMINISTRATION DE LA SECURITE

2.2.1 La gestion des droits.

Elle dépend de la structure administrative de l'entreprise. Selon le cas l'entreprise pourra désigner un seul responsable de la gestion des droits pour toute l'entreprise, ou un par entité administrative, ou encore un pour un groupe d'entité...

Il peut y avoir également un responsable par catégorie d'utilisateurs ou par catégorie de ressources.

Par exemple : un responsable pour l'attribution des droits aux informaticiens, un pour les utilisateurs finals ...

Le responsable doit respecter les règles d'attribution définies par les propriétaires des données et il doit en vérifier la cohérence.

Par exemple : il doit s'assurer que par une suite d'interrogations autorisées et anodines on ne puisse pas retrouver une information définie confidentielle par le propriétaire.

Les compétences en matière d'attribution des droits ne doivent pas être uniques : si le responsable est absent on doit pouvoir supprimer, créer, modifier les droits d'un employé (la sécurité ne doit pas empêcher les gens de travailler).

Mais le nombre de responsables doit quand même être limité. Si ce n'est pas le cas, car par exemple on a décidé d'avoir un responsable par entité administrative alors ses pouvoirs devront être limités. Chaque responsable ne pourra attribuer ou modifier que les droits des agents de son entité.

Il est envisageable également si l'on ne souhaite pas avoir plusieurs responsables mais si l'on ne veut pas non plus bloquer l'activité, d'autoriser un ou deux employés à déléguer les droits qu'ils possèdent (le mécanisme de gestion des droits doit permettre de spécifier pour un employé quels sont les droits qu'il peut déléguer).

Dans certains cas, pour attribuer des droits stratégiques, il est possible d'imposer la validation de l'attribution par un deuxième responsable.

2.2.2 La sécurité du contrôle des droits

Ce sujet recouvre plusieurs idées :

- Le système doit être tel que le contrôle d'accès et en particulier le contrôle des droits soit incontournable,
- il doit également garantir que la gestion des droits est soumise à un contrôle d'accès très strict,
- il doit en outre permettre de suivre toutes les anomalies (tentatives d'accès illicites, erreurs...).

Pour atteindre ces objectifs, différentes mesures peuvent être mises en place :

- scellement des logiciels,
- encapsulage de tout ou partie des logiciels système et ou applicatifs,
- utilisation de boîtes noires (processeurs de sécurité),
- journalisation de toutes les actions sur les ressources et outils d'analyse de ces journaux,
- éventuellement à l'avenir, utilisation de systèmes experts d'analyse des anomalies et de déclenchement automatique de mesures conservatoires,
- comparaison, selon une périodicité variable, du fichier des droits des employés à un fichier des services du Personnel,
- affichage de la dernière date de connexion pour déceler d'éventuelles pénétrations illicites.

2.3 L'IMPACT DES PRESTATAIRES DE TRANSPORT SUR LES DROITS

- TRANSPAC,
- P.T.T.,
- PLUCE,
- RVA,
- Prestataires de télémaintenance...

Dans la mesure où un réseau, même pour les réseaux prévus en France, fait toujours appel à des prestataires extérieurs, il est important d'analyser l'impact de leur présence sur la sécurité.

En ce qui concerne la gestion des droits, leur impact apparait limité sauf peut-être pour les droits concernant les circuits et également pour tout ce qui concerne les services dits de valeur ajoutée.

Pour les circuits, il est possible soit d'imposer l'interdiction de certains circuits, soit lorsque le type de circuit utilisé n'est pas certain, le fournisseur de service garantissant un secours mais sans prévenir à chaque fois de son utilisation, le niveau de sécurité devra être aligné sur le type de liaison le moins sûr.

Pour les services de valeur ajoutée, certains concernent directement la sécurité, c'est par exemple le cas de PLUCE dont c'est le seul objectif. Certaines fonctions ayant trait au droit peuvent dans ce cas leur être confiées :

- interdire l'accès par certains types d'authentification par exemple :

  . uniquement la carte à mémoire,

  . uniquement la carte à mémoire de l'entreprise.

- limiter l'accès en fonction des transactions, de la géographie.

En fait les prestataires peuvent réaliser les mêmes fonctions que les antéserveurs (voir le paragraphe sur l'apport des antéserveurs).

RECOMMANDATIONS

1. Le choix d'une organisation et d'un système de gestion des droits d'accès à un réseau téléinformatique doit toujours être précédé d'une analyse fonctionnelle des risques aussi poussée que possible :

   - Quels sont les besoins fonctionnels de sécurité ?

     Il faut déterminer en fonction des conséquences prévisibles d'un sinistre :

     . les propriétés qui doivent être assurées;
     . le niveau de solidité des mesures couvrant ces propriétés.

   - Quelles sont les limites à la sécurité qui sont imposées par l'environnement ?

La sécurité est généralement la cause de dégradations des performances ou de l'ergonomie d'utilisation, jusqu'à quel point les utilisateurs et les gestionnaires peuvent-ils admettre ces dégradations, sachant que l'objectif principal est quand même de travailler ?

. limite de dégradation des temps de réponse;

. capacité à mémoriser des codes secrets et à conserver sa carte en sécurité;

. ...

- Quelles sont les contraintes fonctionnelles dont il faut tenir compte?

  . faut-il envisager de donner l'accès universel à certains utilisateurs ?

  . le système est-il amené à évoluer largement et rapidement ?

2. Il est conseillé de définir une cible fonctionnelle sans tenir compte des outils existants plutôt que de bâtir directement des solutions techniques.

   En effet, l'évolution technologique est telle en matière de sécurité que certains outils non disponibles aujourd'hui, le seront demain. Si la cible est bien décrite l'évolution sera plus facile.

3. Toute la sécurité repose sur le contrôle d'accès et en particulier sur l'authentification. En effet, il ne sert pratiquement à rien d'avoir un système de gestion des droits très perfectionné si l'authentification est faible.

4. La gestion des droits doit être souple pour s'adapter à l'ensemble des besoins, mais elle doit aussi être cohérente, et surtout elle doit permettre la séparation des fonctions d'habilitation, de contrôle, d'utilisation afin qu'une personne seule ne puisse pas perpétrer une fraude ou une malveillance.

CHAPITRE III

LES MESURES COMPLEMENTAIRES AU CONTROLE D'ACCES

Ces mesures sont :

- le chiffrement, le scellement, la signature électronique,
- la notarisation et la non-répudiation,
- l'acquittement.

1. Le chiffrement, le scellement et la signature électronique font tous les trois appel à des algorithmes. Ceux-ci peuvent être de différents types, chacun étant plus ou moins adapté aux différentes utilisations.

   Ces mécanismes nécessitent presque toujours un certain niveau de confidentialité qui peut porter soit sur l'algorithme lui-même, soit sur une clé ou sur les deux.

   Le problème de cette confidentialité est traité dans le chapitre sur la gestion des secrets.

2. L'acquittement

   C'est un mécanisme intervenant au niveau du protocole d'échange. La réception par l'émetteur d'un message d'acquittement peut lui permettre de prouver que le récepteur a bien reçu, vérifié et/ou pris en compte son opération, ceci en fonction des engagements contractuels définis.

   Ce message d'acquittement doit bien évidemment être sécurisé tel que décrit dans le paragraphe suivant pour avoir une valeur de preuve.

3. La non-répudiation

   Cette mesure est un moyen de prouver qu'un message a bien été envoyé ou reçu.

   Plusieurs schémas existent :

   - notarisation par un tiers de confiance des échanges effectués,

   - utilisation d'un système algorithmique symétrique auquel s'ajoute un élément de dissymétrie,

   - utilisation d'un système algorithmique asymétrique.

3.1 Tiers de confiance

Dans un échange entre deux entités, si cet échange se fait par l'intermédiaire d'un réseau géré par une tierce partie et dans la mesure où cette tierce partie a été reconnue contractuellement comme arbitre, la preuve d'un échange peut être apportée par ce dernier à partir du stockage qu'il effectue. C'est par exemple le cas de SWIFT pour les échanges entre Banques.

3.2 Système symétrique

Dans un système symétrique, la détention par l'un des interlocuteurs d'un message chiffré supposé émis par l'autre ne constitue pas une preuve de l'origine du message. En effet, cette possession garantie l'appartenance à l'un ou à l'autre des partenaires mais ne permet pas de distinguer lequel puisqu'ils disposent tous les deux du même algorithme et de la même clé secrète.

Pour pallier cet inconvénient, un mécanisme a été mis en place dans la carte à mémoire. Il consiste à permettre à la carte à mémoire du récepteur de calculer la signature, de la comparer à celle reçue et d'extérioriser le résultat de la comparaison, mais en lui interdisant d'extérioriser la signature elle-même.

Ceci nécessite, pour avoir une valeur technique (le problème de la valeur juridique n'étant pas à ce jour résolu) que le dispositif de vérification, c'est-à-dire la carte mère, ait été audité et reconnu conforme. Les cartes à base de DES ou de TELEPASS permettent cette utilisation.

3.3 Système asymétrique

Dans ce cas, bien que disposant des mêmes algorithmes, l'émetteur et le récepteur utilisent des clés différentes. Le récepteur est donc incapable de chiffrer un message à la place de l'émetteur, il peut seulement déchiffrer. La production en cas de litige d'un message chiffré avec la clé secrète de l'émetteur par le récepteur constitue donc une preuve technique de l'envoi du message par l'émetteur.

La validation de cette preuve devra être cependant faite a posteriori par un organisme indépendant reconnu par les deux parties.

Les algorithmes utilisés sont RSA ou FIAT-SHAMIR.

CHAPITRE IV

LA GESTION DES SECRETS

PLAN

INTRODUCTION

1. HIERARCHISATION DES CLES

   1.1 Généralités
   1.2 Typologie d'utilisation
   1.3 Clés de chiffrement des fichiers
   1.4 Clés de chiffrement des messages du réseau

2. ETAPES DE LA VIE D'UN SECRET

   2.1 Création
   2.2 Transport et stockage
   2.3 Utilisation
   2.4 Archivage
   2.5 Destruction

3. ASPECTS COMPLEMENTAIRES

   3.1 Relations entre les clés
   3.2 Recommandations attachées à l'architecture de sécurité de distribution des clés
   3.3 Recommandations attachées à l'utilisation des clés

INTRODUCTION

Au niveau de la sécurité dans un réseau téléinformatique, plusieurs types de secrets doivent être gérés :

- les secrets servant à l'authentification et qui peuvent être de deux types:

  . informations connues de l'utilisateur,

  . informations placées dans le support détenu par l'utilisateur;

- les clés des algorithmes utilisés pour les différentes mesures techniques : authentification, scellement, chiffrement, signature électronique.

Ce chapitre traite essentiellement de cette dernière catégorie selon les aspects :

- hiérarchisation des clés,
- étapes de la vie d'un secret,
- conséquences sur l'architecture de distribution des clés.

1) HIERARCHISATION DES CLES

Dans le domaine des algorithmes, deux catégories d'informations peuvent être confidentielles :

- les algorithmes eux-mêmes,
- les clés utilisées pour les algorithmes.

Les moyens d'assurer leur confidentialité étant similaires, seule la catégorie des clés sera traitée.

Les éléments suivants sont développés :

- généralités,
- typologie d'utilisation des clés,
- clés de chiffrement des fichiers,
- clés de chiffrement des messages sur réseau.

1.1 Généralités

Elles concernent :

- les systèmes de clé,
- les objectifs de sécurité.

* Systèmes de clés

D'une manière générale, les clés sont hiérarchisées en plusieurs niveaux et leur besoin de confidentialité croît en même temps que leur place dans la hiérarchie.

De même que, généralement dans un système de clés, il existe une clé maître qui doit être protégée physiquement dans une "maison inviolable" et des clés filles qui sont elles-mêmes chiffrées par la clé maître.

* Objectifs de sécurité

Cette hiérarchisation est guidée par la volonté de donner le moins d'éléments de décryptage (cassage de l'algorithme) possible au fraudeur potentiel.

En effet, si un système utilise une seule clé pour l'ensemble de ses utilisateurs, un agresseur disposera d'un nombre important de couples : messages chiffrés ou sceaux, correspondants en clair. Il pourra donc plus facilement essayer de deviner ou de retrouver cette clé.

Plus une clé est spécifique à une entité et son utilisation limitée dans le temps, meilleure est la sécurité.

1.2 Typologie d'utilisation des clés

Une autre notion doit être prise en compte selon le type d'utilisation :

- locale,
- sur un réseau.

. Pour une utilisation locale, par exemple pour le chiffrement, c'est-à-dire pour la confidentialité des fichiers, la clé doit rester fixée sur des périodes de temps relativement longues.

  Il est en effet nécessaire de conserver la même clé, lors de la création d'un fichier et lors de ses utilisations ou modifications successives, une modification périodique de cette clé reste cependant souhaitable.

. Pour une utilisation sur un réseau, il est par contre recommandé de changer continuellement de clé. Il est par exemple possible de la modifier à chaque session, voire en cours de session.

1.3 Clés de chiffrement des fichiers

Si l'on prend pour exemple le cas des fichiers sur un micro :

- une des solutions est de disposer d'une clé maître unique pour le micro et d'attribuer des clés de chiffrement à chaque utilisateur, voire à chaque fichier ou type de fichier

- la liaison entre la clé maître et les clés filles se fait par l'intermédiaire d'un algorithme utilisant des informations spécifiques à l'utilisateur ou au fichier, ou par une table : l'utilisateur choisissant lui-même sa (ou ses) clé(s).

- dans le cas où un utilisateur souhaite disposer du même fichier sur plusieurs micros ou pouvoir reprendre, sur un micro,le fichier créé par un autre, il faudra prendre en compte ce besoin afin que la gestion du secret ne soit pas trop compliquée ou qu'elle ne nuise pas à sa confidentialité.

Le cas des fichiers chiffrés sur un serveur central reste à considérer compte tenu des spécificités d'un centre de traitement informatique (partition des clés) :

- clés fixes,

- clés intermédiaires destinées à permettre la modification périodique des clés sans pour autant être obligé de rechiffrer les fichiers concernés.

1.4 Clés de chiffrement des messages sur un réseau

Dans un réseau, les liaisons entre deux noeuds peuvent être sécurisées (chiffrées ou scellées) en utilisant des clés de session évolutives. Dans ce cas, à chaque mise en session, ou même en cours de session, les clés sont différentes et plusieurs moyens sont utilisables :

- en début de session, échange des clés de session sous couvert de la clé maître,

- échange des clés de session sous couvert de la clé de session précédente,

- pas d'échange de clé de session :

  calcul de la clé par les deux interlocuteurs à partir d'une information évoluant parallèlement dans les deux noeuds, par exemple la date et l'heure :

  . utilisation de table de clé une fois,

  . calcul de la clé par les deux interlocuteurs à partir d'un élément aléatoire généré par l'un des interlocuteurs.

  Ce type d'accès impose une parfaite synchronisation.

2) ETAPES DE LA VIE D'UN SECRET

La sécurité du processus de chiffrement repose sur la sécurité et la confidentialité des clés utilisées.

Il est souhaitable que le système de gestion des clés :

- génère et distribue les clés de façon aléatoire,
- restreigne la diffusion des clés pour en limiter l'accès illicite,
- stocke, détruise ou archive les clés de façon sûre, contrôlable et traçable,
- puisse être testé pendant son fonctionnement.

Le cycle de vie d'une clé peut se décomposer en cinq étapes :

- création,
- transport et stockage,
- utilisation,
- archivage,
- destruction.

2.1 Création

Elle consiste à choisir, d'une manière aléatoire, un ou plusieurs nombres de longueur donnée.

Les conditions d'acceptation des clés dépendent de la qualité de l'algorithme (certaines catégories de clés peuvent être déclarées faibles par le concepteur de l'algorithme).

La création des clés est à entourer de précautions de nature à :

- restreindre leur accès aux utilisateurs habilités :
  - . dans la mesure du possible, les gestionnaires ne devraient pas connaître le contenu de la clé,
  - . l'utilisateur lui-même peut ne pas connaître la clé si elle est mise automatiquement dans la mémoire protégée de son dispositif de sécurité,
- produire des clés réellement aléatoires,
- éviter leur analyse à distance par rayonnement.

2.2 Transport et stockage

Après leur production, les clés ne doivent être transportées, lorsque c'est indispensable, sur le lieu de leur utilisation qu'après s'être assuré que les éventuelles entités en communication aient pu se reconnaître de façon sûre (authentification mutuelle).

La distribution peut être effectuée de manière manuelle ou automatique :

- sur support papier ou assimilé,
- par module électronique, par carte à micro-processeur,
- en télétransmission.

Les mesures de protection et prévention suivantes peuvent être envisagées :

- transfert à effectuer sous double contrôle avec :

  . comptabilisation du nombre de clés reçues,

  . contrôle par le récepteur de la séquence de numérotation des clés,

  . réduction de la durée de stockage intermédiaire et effacement de la mémoire de stockage après le transfert,

  . protection des clés par chiffrement.

La distribution automatique des clés peut être effectuée selon trois aspects :

- en point à point : dans ce cas, l'un des correspondants au moins doit pouvoir générer des clés,

- par centre de distribution de clés,

- par centre de traduction des clés.

2.3 Utilisation

Les précautions, exposées ci-après, sont envisageables :

- introduction manuelle de clés avec affichage, de telle sorte que seules les personnes habilitées aient à en connaître,

- introduction automatique de clés sans affichage pendant l'opération,

- limitation d'accès physique et ou logique au dispositif d'introduction des clés au seul personnel habilité,

- absence de toute réutilisation de clé que l'un des partenaires aurait cessé d'employer,

- possibilité, laissée à un partenaire, d'invalider la clé (mise en oeuvre d'un dispositif spécifique d'opposition).

2.4 Archivage

Il est une réponse aux risques suivants :

- mauvais respect de la date d'obsolescence de la clé et utilisation illicite de cette dernière,

- modification de la clé par un opérateur mal intentionné.

Il est donc souhaitable que l'archivage soit sûr et qu'il permette la recherche de clés inactives mais antérieurement utilisées pour le transport de messages chiffrés (preuve disponible pour un éventuel contentieux).

Il est recommandé également que cet archivage ne soit disponible qu'à une tierce partie reconnue par les intervenants.

2.5 Destruction

Les clés devenues définitivement inutiles sont à détruire si possible physiquement car elles peuvent présenter un certain danger.

Il est important de comptabiliser toute destruction de manière à pouvoir effectuer des opérations de recherche ultérieure.

3) ASPECTS COMPLEMENTAIRES

Les risques à couvrir au niveau de la gestion des clés amènent à prendre en compte les aspects suivants :

- relations entre les clés,

- recommandations attachées à l'utilisation des clés.

3.1 Relations entre les clés

Les contraintes de hiérarchisation des clés dans les réseaux amènent à disposer d'une architecture de distribution à deux ou trois niveaux :

* Architecture à deux niveaux de clés

- Niveau 1 : - 1 clé de base (N1) :
  . distribuée manuellement;

- Niveau 2 : - 1 clé de session (N2) :
  . distribuée automatiquement,
  . chiffrée à partir de la clé N1;

* Architecture à trois niveaux de clés secrètes

- Niveau 1 : - 1 clé de base (N1) :
  . distribuée manuellement;

- Niveau 2 : - 1 clé de chiffrement des clés de session (N2):
  . distribuée automatiquement,
  . chiffrée à partir de la clé N1;

- Niveau 3 : - 1 clé de session (N3) :
  . distribuée automatiquement,
  . chiffrée à partir de la clé de N2.

* Architecture à trois niveaux de clés publiques

- Niveau 1 : Utilisateur - Clé secrète (N1), clé publique (N2.N3)

- Niveau 2 : Serveur - Clé secrète (N2), clé publique (N1.N3)

- Niveau 3 : Autorité garantissant la validité des clés publiques - Clé secrète (N3), clé publique (N1.N2)

3.2 Recommandations attachées à l'architecture de sécurité de distribution des clés

Dans le cadre d'échanges entre deux partenaires, il est souhaitable que l'architecture permette :

- l'utilisation d'au moins une clé de session,

- l'échange automatique des clés ou leur non échange selon les algorithmes utilisés,

- la communication avec des interlocuteurs ne disposant pas de générateurs de clés.

Par ailleurs, il apparaît intéressant que les équipements cryptographiques disposent de dispositifs et de procédures destinés à assurer leur intégrité selon les aspects :

- vérification du bon fonctionnement de l'équipement (tests, alarmes),

- documentation et enregistrement des erreurs et du mauvais fonctionnement,

- invalidation des clés en cas de capture.

3.3 Recommandations attachées à l'utilisation des clés

Les mesures devraient pouvoir concourir :

- à l'absence de compromission d'une tierce personne si une clé échangée entre deux personnes est divulguée,
- à garantir la confidentialité et l'intégrité des clés.

* Recommandations liées aux clés de session

- utilisation spécifique pour le chiffrement ou pour l'authentification,
- protection contre une utilisation abusive par une tierce personne,
- distribution possible pour un usage immédiat ou futur.

CHAPITRE V

L'APPORT DES ANTESERVEURS

PLAN

1 - OBJECTIFS

2 - DEFINITION

3 - IMPLEMENTATION DES FONCTIONS DE SECURITE
DANS LES COUCHES DE COMMUNICATION

4 - ELEMENTS D'APPRECIATION D'UNE ARCHITECTURE DE RESEAU
AVEC ANTESERVEURS

4.1 AU PLAN DE LA SECURITE

4.2 AU PLAN DE L'ADMINISTRATION

5 - ARCHITECTURE DE RESEAU SANS ANTESERVEUR

6 - CONCLUSION

1 - OBJECTIFS

. obtenir des éléments de réponse à la question : faut-il ajouter dans une architecture de réseau des dispositifs physiques supplémentaires appelés antéserveurs pour en accroître la sécurité ?

. avoir des éléments d'appréciation de la solution la plus adaptée à son entreprise à partir de la discussion sur les problèmes à résoudre (section 4) et les cas d'architecture envisageables sans antéserveurs (section 5).

2 - DEFINITION

La notion d'antéserveur existe depuis quelque temps sans avoir été précisée de façon claire. Parmi les fonctions évoquées pour un antéserveur, on peut noter :

- le support de fonctions applicatives
- la sécurité
- des services tels que la conversion de protocole, le routage...
- l'allégement de la charge des systèmes centraux ou du réseau
- l'amélioration de la qualité de service des terminaux.

A partir de ces fonctions, la définition d'un antéserveur pourrait être la suivante :

Un antéserveur est un dispositif physique pouvant notamment assurer certaines fonctions de sécurité et placé en un point tel du réseau qu'il contribue à résoudre les problèmes techniques (performance, charge...), organisationnels (mise à jour des droits d'accès...) et humains (convivialité...) de manière optimale.

3 - IMPLEMENTATION DES FONCTIONS DE SECURITE DANS LES COUCHES DE COMMUNICATION

L'analyse des recommandations de l'ISO (tableaux joints en annexe) fait ressortir que la quasi-totalité des services de sécurité peut être placée au niveau de la couche 6 (présentation) du modèle d'architecture de réseau. Ainsi, les processeurs de communication, qui ne gèrent que les couches 1 à 4, peuvent supporter certaines fonctions d'antéserveur, mais ne peuvent pas jouer le rôle d'antéserveurs à part entière, au sens support des services de sécurité tel que le préconise le modèle ISO.

De plus, ces services sont relativement mal assurés par les systèmes d'exploitation actuels. Il convient donc de se demander quels pourraient être les apports d'un antéserveur dans l'architecture de sécurité d'un réseau.

4 - ELEMENTS D'APPRECIATION D'UNE ARCHITECTURE DE RESEAU AVEC ANTESERVEURS

L'insertion d'un antéserveur dans un réseau suppose l'examen des points suivants :

4.1 - Au plan de la sécurité

1) Contrôle d'accès
   a) localisation du contrôle d'accès
   b) Implantation des fichiers de droits et des mots de passe
2) Chiffrement et scellement
3) Secours (back-up)
4) Audit

4.2 - Au plan de l'administration

1) Nombre et implantation des antéserveurs dans le réseau (incidence sur la gestion des droits et la charge du réseau)
2) Délestage des systèmes centraux et routage
3) Stockage local de données et support d'applications à bas niveau de sécurité (facturation,...)
4) Conversion de protocoles et gestion de l'hétérogénéité des systèmes centraux
5) Convivialité
6) Notion d'accès universel limité

Principes

. le système d'information constitue un patrimoine de l'entreprise, les informations qu'il contient doivent donc être sécurisées

. les données de référence sont des informations indispensables au fonctionnement, elles doivent donc être particulièrement protégées

. pour toutes les informations qui sont dupliquées, il est impératif de préciser lesquelles sont des données de référence et quelle est leur localisation, ce qui pose le problème de la protection des données de contrôle si elles sont situées sur l'antéserveur (ou le système de contrôle d'accès est parfait et alors il pourrait se situer aussi bien directement sur les centraux, ou il ne l'est pas et alors la mauvaise protection des fichiers de droits constitue une faiblesse).

Discussion sur les éléments d'appréciation

N.B. La discussion est abordée thème par thème, mais il est évident qu'il est impossible de les traiter tous séparément. De temps en temps, il sera par conséquent fait référence à des thèmes déjà évoqués, ou encore à traiter.

4.1 - Au plan de la sécurité

1) Contrôle d'accès

Le contrôle d'accès recouvre l'authentification et le contrôle des droits des utilisateurs, il constitue avec le chiffrement et le scellement l'un des mécanismes qui permet d'assurer l'intégrité et la confidentialité.

La question qui se pose est celle de la localisation du traitement de contrôle lui-même et celle des fichiers dont il se sert, c'est-à-dire des fichiers de mots de passe et de droits.

Le contrôle d'accès devrait s'effectuer le plus près possible du point d'accès utilisateur pour limiter les possibilités d'un intrus.

a) Localisation du contrôle d'accès

Si le contrôle d'accès était infaillible, le fait qu'il soit situé sur l'antéserveur n'apporterait rien de plus.

Dans le cas où les commandes système sont interdites ou non exécutées, l'utilisateur est alors confiné à l'antéserveur et ne pourra accéder aux données de référence sauf si celles-ci sont stockées temporairement sur l'antéserveur ou si les fichiers de droits s'y trouvent.

Même dans le cas où l'exécution de commandes-système sur le central à partir de l'antéserveur est possible, sa présence complique la tâche d'un intrus éventuel et ralentit sa tentative de pénétration, surtout si la conversion de protocole entre l'antéserveur et le central est mise en oeuvre (cf paragraphe 4.2.4).

Puisque la fonction d'un antéserveur est de renforcer la protection des applications et des données de référence, son apport est négligeable pour ce qui est de la sécurité de la fonction de contrôle d'accès elle-même.

Il serait possible d'exécuter cette fonction sous le contrôle d' un système d'exploitation hautement sécurisé, qui pourrait réaliser l'accueil des utilisateurs et leur routage, et fonctionner sans utilitaires dangereux comme les sous-systèmes de temps partagé. Aujourd'hui ce type de système d'exploitation n'est pas capable de supporter la charge d'un central mais pourrait fonctionner sur un antéserveur.

b) Implantation des fichiers de droits et des mots de passe

A priori, on pourrait mettre les fichiers de droits et des mots de passe soit sur les antéserveurs, soit sur les systèmes centraux.

La présence sur l'antéserveur de ces fichiers permet d'améliorer les temps de réponse. En effet, si ces données ne sont pas stockées sur l'antéserveur, il faudra, lors de la connexion et en cours de travail, chercher les informations sur un site distant.

Cependant, si le contrôle d'accès n'est pas infaillible, le stockage de ces fichiers sur l'antéserveur constitue une faiblesse à laquelle on pourrait remédier par le chiffrement.

2) Chiffrement et scellement

Ces deux techniques peuvent être utilisées d'une part pour les échanges de messages sur le réseau, d'autre part pour protéger les fichiers de droits et de mots de passe.

Si ces données sont stockées sur l'antéserveur, leur chiffrement peut constituer un remède contre l'imperfection du système de contrôle d'accès.

Pour assurer la protection de la liaison avec les terminaux, il faut chiffrer les messages envoyés. L'antéserveur peut assurer le chiffrement si celui-ci n'est pas mis en oeuvre au niveau des couches 1 et 2 du réseau.

La protection des clés nécessaires à ces algorithmes est traitée dans le chapitre consacré à la gestion des secrets.

3) Secours

L'ajout d'un antéserveur dans un réseau peut apporter des avantages en matière de secours.

Si un central devient indisponible, l'antéserveur peut assurer, de façon transparente pour l'utilisateur, hormis peut-être le délai de basculement,la liaison avec le site de secours sans que le dialogue de connexion ne soit modifié.

Dans certains cas, l'antéserveur peut prendre le relais d'un central devenu indisponible et assurer quelques fonctions vitales.

Mais l'antéserveur doit lui-même être doublé ou redondant pour éviter le blocage de l'accès au système d'information en cas de panne ou d'indisponibilité temporaire, ce qui suppose que les fichiers de l'antéserveur de secours soient à jour en permanence.

4) Fonction d'audit

En dehors des trois propriétés de sécurité de base que sont la disponibilité, l'intégrité et la confidentialité, il est important que l'on puisse disposer de contrôles comme, par exemple, l'établissement de la preuve ; il faut donc qu'un système soit auditable.

L'antéserveur peut supporter commodément cette fonction d'audit, à condition que le logiciel et les données correspondantes soient bien protégées. Sinon, un intrus parvenant à outrepasser ses droits pourrait, en manipulant les données enregistrées, effacer les traces de son passage.

4.2 - Au plan de l'administration

Lorsque l'on étudie l'impact de l'introduction d'un antéserveur dans un réseau, des aspects autres que ceux concernant la sécurité sont à prendre en compte.

1) Nombre et implantation des antéserveurs dans le réseau

L'introduction d'antéserveurs peut provoquer:

- une augmentation du trafic général,
- une augmentation du temps de réponse,
- une diminution de la charge du réseau vue par les terminaux.

Leur nombre dépend évidemment de l'architecture du réseau et de sa taille.

Leur implantation (choix de l'emplacement optimal par rapport aux centraux d'une part, aux stations de travail d'autre part), est liée aux aspects suivants:

- le contrôle d'accès devrait idéalement s'effectuer le plus près possible des utilisateurs (par exemple, si l'antéserveur est situé entre le processeur de communications et le central, la zone amont n'est pas protégée, et un intrus peut s'attaquer au réseau).

- plus le contrôle d'accès est proche des stations de travail, plus la charge du réseau diminue lors de la connexion (si rejet il y a, celui-ci se fait à la source, sans traversée du réseau), mais plus elle augmente lors de la mise à jour des droits qui devient plus complexe et qui doit alors être peu fréquente (quotidienne au pire) si les droits sont attribués de manière centralisée.

- plus le contrôle d'accès est proche des systèmes centraux, plus la charge du réseau augmente lors de la connexion (la demande traverse tout le réseau avant de se faire éventuellement refuser), mais plus elle diminue lors de la mise à jour des droits, qui s'en trouve simplifiée.

Il découle de ces remarques que pour une application sur un central accédée par un nombre limité d'utilisateurs, il est préférable que le fichier des droits soit proche des stations de travail. On évite ainsi de surcharger inutilement le réseau avec des demandes qui n'aboutiraient pas.

Cependant, s'il s'agit d'une application grand public, le réseau sera de toute façon chargé par le nombre important de connexions et il est alors préférable que le fichier des droits soit proche du central car sa mise à jour s'en trouvera simplifiée.

Ce raisonnement, qui est simple dans le cas d'un central et d'une application uniques, est compliqué dans le cas plus réaliste des grands réseaux d'entreprise avec plusieurs centraux et des applications multiples. L'implantation des antéserveurs et leur nombre doivent alors réaliser le meilleur compromis entre ces différentes exigences.

Il faut également que la mise en place d'antéserveurs dans le réseau ne vienne pas restreindre les voies d'accès en lignes de communication qui existaient auparavant vers les systèmes centraux afin de disposer de chemins de secours en cas d'indisponibilité d'une ligne.

2) Délestage des systèmes centraux et routage

Selon le nombre et le contenu des fonctions réalisées par l'antéserveur, sa présence devrait permettre de délester les centraux. Cependant il ne faut pas surestimer cet allégement. Ainsi pour les messages n'impliquant aucun traitement dans l'antéserveur, le temps de réponse et éventuellement la charge pourront être légèrement supérieurs.

Un antéserveur ajouté dans un réseau apporte une puissance de traitement supplémentaire et déleste les centraux dans la mesure où il peut prendre en charge certaines de leurs applications et effectuer le contrôle d'accès à leur place.

Dans un contexte de bases de données réparties ou distribuées avec une partie d'une base de données située sur l'antéserveur ou sur un autre central moins chargé, le délestage des systèmes centraux devient alors possible, soit par la fonction de routage vers un autre ordinateur, soit parce que l'antéserveur prend le relais du central saturé.

3) Stockage local de données et support d'applications

On peut utiliser les possibilités locales de stockage de l'antéserveur pour y mettre des informations non confidentielles.

En dehors des fonctions de contrôle d'accès, l'antéserveur peut délester le système central en exécutant des applications qui ne requièrent qu'un bas niveau de sécurité, par exemple la consultation d'informations de type grand public.

L'antéserveur, dans la mesure où il est le point de passage obligé de toutes les connexions et déconnexions, est bien adapté pour supporter la facturation des utilisateurs. Il est alors nécessaire que les données correspondantes soient efficacement protégées afin d'éviter les manipulations abusives.

4) Conversion de protocoles et gestion de l'hétérogénéité des systèmes centraux

L'introduction d'un antéserveur dans une architecture de réseau permet de différencier d'une part le dialogue avec l'utilisateur, d'autre part le protocole d'échange d'informations avec le système central qui n'est alors pas connu de l'utilisateur. Si celui-ci a pu outrepasser ses droits vis à vis de l'antéserveur, sa capacité de nuisance sur le central restera limitée du fait de son ignorance du protocole à employer.

L'antéserveur peut devenir l'interlocuteur unique de l'utilisateur et permettre ainsi l'uniformisation de son dialogue avec les applications en rendant transparente l'hétérogénéité de l'accès aux différents centraux.

La conversion de protocoles augmentera inévitablement les temps de réponse.

5) Convivialité

L'apport d'un antéserveur en matière d'ergonomie du dialogue avec l'utilisateur (qui est affranchi de la connaissance de l'architecture du réseau, de l'ordinateur qui héberge son application et du dialogue de connexion à mettre en oeuvre pour l'atteindre et qui peut différer selon le mode de raccordement au réseau de la station de travail qu'il utilise) est considérable, surtout dans le cas de réseaux hétérogènes, et cette propriété (qui n'est pas une fonction de sécurité) peut justifier à elle seule la mise en place d'un antéserveur dans une architecture de réseau complexe.

L'utilisateur est pris en charge dès la connexion par un menu d'accueil, pouvant être personnalisé, qui effectue les contrôles d'identification et d'authentification et affiche ensuite dans la langue de l'utilisateur la liste des applications autorisées en fonction de ses droits. Celui-ci choisit l'application souhaitée et l'établissement de la connexion avec le central approprié est transparent pour lui.

La mise en place d'un antéserveur peut ainsi permettre de résoudre rapidement et efficacement l'introduction de la sécurité logique dans un grand réseau, car cet interface permet à tous les utilisateurs de n'avoir qu'une identification unique vis à vis du système d'information quelle que soit l'application à laquelle ils souhaitent se connecter, ce qui est en général loin d'être le cas aujourd'hui. Elle apporte également une aide à l'administration du réseau dans la mesure où elle permet un dialogue entre les gestionnaires des ressources et les utilisateurs.

6) Notion d'accès universel limité

L'accès universel est la propriété qui permet aux utilisateurs d'accéder à leurs applications à partir de n'importe quelle station de travail du réseau. Dans la pratique d'une grande entreprise (plusieurs dizaines de milliers de personnes), cette propriété a une répercussion directe sur le nombre d'antéserveurs à mettre en place et leur implantation dans le réseau pour réaliser un compromis acceptable entre les performances et la mise à jour des droits.

Pour réaliser au mieux ce compromis, il est possible d'introduire la notion d'accès universel limité, qui consiste à scinder la population de l'entreprise en 2 catégories :

- celle qui n'est pas mobile, ou qui au cours de ses occasionnels déplacements professionnels n'a a priori pas à accéder au système d'information (dans la plupart des entreprises, cette catégorie constitue la grande majorité du personnel). Il suffit dans ce cas que les droits de ces personnes soient gérés uniquement dans l'antéserveur le plus proche de leur lieu géographique de travail

- celle qui est mobile et qui doit avoir l'accès universel. Dans ce cas, les droits de ces personnes seront présents dans la totalité des antéserveurs du réseau, mais les mises à jour peuvent se faire par diffusion à partir d'un point central.

Cette solution ayant l'inconvénient de compliquer le système de gestion des droits, une étude au cas par cas devra bien en prendre en compte les avantages et les inconvénients.

5 - ARCHITECTURE DE RESEAU SANS ANTESERVEUR

Ce chapitre consiste à décrire comment les problèmes mentionnés au chapitre précédent sont traités dans des architectures de réseau sans antéserveur.

Dans le cas d'une grande entreprise, le réseau est composé d'éléments multiples et souvent hétérogènes : les systèmes centraux, les processeurs de communication (frontaux, concentrateurs de terminaux et commutateurs de circuits ou de paquets), les ordinateurs départementaux, les stations de travail et terminaux.

Les utilisateurs sont susceptibles de se connecter à de multiples applications situées sur différents ordinateurs et pas forcément toujours à partir de la même station de travail.

Si l'on veut gérer efficacement la sécurité logique, ce qui n'est pas possible actuellement par la simple utilisation des logiciels de base système et réseau offerts par les principaux constructeurs, il faut rajouter une structure de données qui comporte au minimum par utilisateur une dizaine d'octets pour l'identification et l'authentification et une centaine d'octets pour leurs droits, et du logiciel pour gérer cette structure et effectuer les liaisons avec les ordinateurs et les applications cibles.

Dans l'état actuel des matériels, il en découle que les volumes dont il faut disposer pour contrôler plusieurs dizaines de milliers d'utilisateurs sont incompatibles avec les ressources des processeurs de communication qui ne disposent souvent pas de possibilités locales de stockage et leur localisation sur les systèmes centraux ne permet pas de protéger la zone amont.Par ailleurs, il est presque impossible dans ce contexte, d'affranchir les utilisateurs de la connaissance du dialogue de connexion, de la localisation de l'ordinateur qui héberge leur application, et des spécificités des différents systèmes d'exploitation.

Si l'on veut se passer d'antéserveurs, tant que la sécurité logique ne sera pas parfaitement intégrée aux logiciels des constructeurs, tant que les applications n'auront pas été adaptées à cette situation, et tant que les logiciels réseau ne se comporteront pas vis à vis de l'utilisateur comme un système d'exploitation homogène uniformisant le dialogue de commande, un certain nombre de problèmes évoqués au chapitre précédent seront mal résolus ou impossibles à traiter.

Cependant, il est possible de mettre à profit les puissances réparties de traitement et de stockage (machines départementales, serveurs,...) pour assurer certaines fonctions d'antéserveur :

- <u>contrôle d'accès</u> : la présence de possibilités de stockage locales permet de mettre en place un mécanisme d'identification individuelle des utilisateurs et une gestion des droits. Mais, en raison de la dispersion des fonctions d'administration, il existe un risque important d'incohérence entre les différents sites.

- <u>données de référence</u> : les informations manipulées sur le site local peuvent être issues des serveurs centraux qui gèrent alors seuls les données de référence. Dans ce cas, lors du transfert vers un système central, les informations sont vérifiées à nouveau avant mise à jour des données de référence.

- <u>conversion de protocole</u> : lors des consultations de bases de données centrales à partir des sites locaux, le protocole de communication mis en oeuvre peut ne pas être directement accessible à l'utilisateur et diffère alors du dialogue homme-machine. Dans ce cas, une personne non habilitée ne pourrait se faire passer pour quelqu'un d'autre vis à vis du central à partir du site local.

- <u>secours</u> : en cas de consultation d'une base de données centrale, le module de connexion effectue de façon transparente pour l'utilisateur (hormis le délai de réponse) le routage vers le central de secours en cas d'indisponibilité. En cas de rupture totale et prolongée des liaisons vers les sites centraux, le site décentralisé peut fonctionner de façon autonome pendant plusieurs jours grâce au stockage local des informations indispensables à son fonctionnement.

6 - CONCLUSION

L'antéserveur offre des possibilités de sécurité et d'administration lorsqu'il est introduit dans l'architecture du réseau d'une grande entreprise, ce qui permet, dans l'état actuel des techniques disponibles en standard, de résoudre plus efficacement un certain nombre de problèmes.

Le nombre d'antéserveurs à mettre en place et leur implantation dépend de la taille du réseau, de sa typologie (ex : réseau international ou non), du nombre d'utilisateurs et de leur profil, ainsi que de la nature des applications et de la sensibilité des informations qui sont accédées.

L'antéserveur contribue partiellement, en liaison avec les autres éléments du système d'information, à assurer les fonctions de sécurité que sont la disponibilité, l'intégrité, la confidentialité et le contrôle. Il est inefficace pour la protection de la zone amont (critère à prendre en compte lors de l'étude de l'implantation) et notamment contre le brouillage actif d'une ligne de télécommunication, problème pour lequel un remède possible peut être la multiplication des chemins d'accès.

Sa présence dans un réseau peut être mise à profit pour lui faire exécuter d'autres fonctions que la sécurité et dont l'apport peut être considérable (convivialité du dialogue-utilisateur, gestion de l'hétérogénéité des ordinateurs et des systèmes d'exploitation, support d'applications à bas niveau de sécurité, délestage des centraux et routage automatique vers des systèmes de secours...).

1 - SERVICES ET MECANISMES DE SECURITE

Mécanisme / Service	Chiffrement	Signature	Contrôle d'accès	Intégrité des données	Echange d'authentification	Bourrage	Contrôle du routage	Notarisation
Authentification de l'entité homologue	S	S	.	.	S	.	.	S
Contrôle d'accès	.	.	S	S	S	.	.	.
Confidentialité d'une séquence	Y	.	.	.	.	.	S	.
Confidentialité d'une connexion	Y	.	.	.	.	.	S	.
Confidentialité d'un champ	Y	.	.	.	.	.	.	.
Secret du flux	Y	.	.	.	.	S	S	.
Intégrité sans connexion	S	S	.	Y	.	.	.	.
Intégrité d'un champ (sans récupération)	S	.	.	Y	.	.	.	.
Intégrité d'une séquence (sans répération)	S	.	.	Y	.	.	.	.
Intégrité d'une séquence (avec récupération)	S	.	.	Y	.	.	.	.
Authentification de l'origine	S	S	.	S	.	.	.	S
Non-répudiation (de l'origine)	.	S	.	S	.	.	.	S
Non-répudiation	.	S	.	S	.	.	.	S

Légende : Y : toujours
S : selon la configuration ou les autres mécanismes utilisés
. : jamais

2 - PLACE DES SERVICES DE SECURITE DANS LES COUCHES DU MODELE OSI

Service \ Couche	1	2	3	4	5	6	7
Authentification de l'entité homologue			Y	Y		Y	
Contrôle d'accès			Y	Y		Y	Y
Confidentialité d'une séquence	Y		Y	Y		Y	
Confidentialité sans connexion			Y	Y		Y	
Confidentialité d'un champ						Y	
Secret du flux	Y		Y				Y
Intégrité d'un champ (sans récupération)						Y	
Intégrité d'une séquence (avec récupération)			Y				
Authentification de l'origine			Y	Y		Y	
Non-répudiation (de l'origine)						Y	
Non-répudiation (de la délivrance)						Y	

Légende : Y : en option
blanc : jamais

CHAPITRE VI

L'APPROCHE HORIZONTALE

PLAN

INTRODUCTION

1. FACTEURS GENERAUX STRUCTURANTS

1.1. FACTEURS STRUCTURANTS INTERNES A L'ENTREPRISE

1.1.1. Au niveau du poste de travail
1.1.2. Au niveau des communications
1.1.3. Au niveau du système de production
1.1.4. Au niveau des applications

2. NIVEAU DE MISE EN OEUVRE DES MECANISMES

2.1. AUTHENTIFICATION

2.2. CONFIDENTIALITE

2.3. INTEGRITE

INTRODUCTION

L'architecture de la sécurité doit être définie globalement et préalablement à la mise en oeuvre des mesures qui la composent. En son absence, les mécanismes de sécurité (assurer les services d'identification, d'authentification, de contrôle d'habilitation, intégrité, de confidentialité, de certification, de notarisation) risquent d'être incohérents, inefficaces, voire inutiles.

Le choix des mécanismes de sécurité et leur degré d'application dépendent des risques encourus et constituent l'étape ultime de la sécurisation des ressources informatiques.

Pour aboutir à un modèle d'architecture pertinent, deux approches sont nécessaires :

- la première est une approche par les moyens ; elle a pour but de dégager d'une part les limites et possibilités offertes par les systèmes existants au sein de l'entreprise, et d'autre part, leur compatibilité avec les produits offerts sur le marché.

  Elle répond donc aux questions: où sont et quelles sont nos insuffisances et nos potentialités ?

  Un audit de l'existant associé à une analyse du marché fournit les réponses.

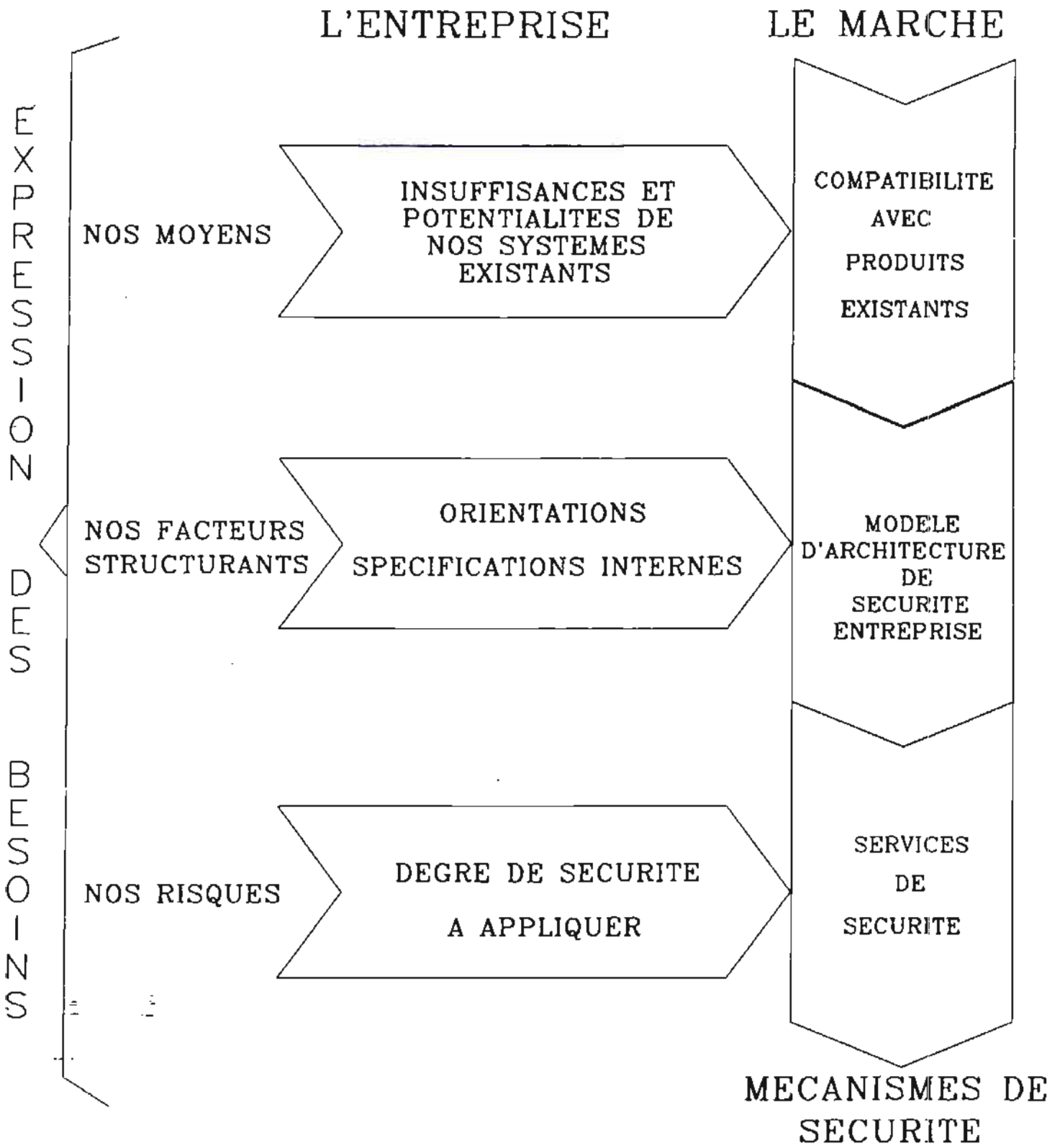
- la seconde est une approche par les facteurs généraux structurants qui conditionnent et orientent la modélisation de l'architecture de sécurité.

  Leur analyse participe donc à l'expression des contraintes et des besoins et permet d'établir les spécifications fondamentales sur lesquelles doit reposer le système de sécurité.

Ce chapitre a pour but d'expliciter ces aspects.

Le schéma de la page suivante illustre ces approches.

DEMARCHE POUR LA DEFINITION D'UN MODELE D'ARCHITECTURE DE LA SECURITE



1) FACTEURS GENERAUX STRUCTURANTS

L'architecture de sécurité est spécifique à chaque entreprise. Elle dépend aussi de facteurs généraux que nous allons passer en revue. Il s'agit :

- des facteurs structurants internes à l'entreprise,
- des normes et de la législation,
- des limites imposées par les produits sur le marché.

1.1 Les facteurs structurants internes à l'entreprise

Ils se définissent comme les choix d'organisation, déjà effectués ou à venir, susceptibles d'orienter ou de remettre en cause l'architecture de sécurité. Des variantes d'application de ces choix existent. Elles seront signalées comme étant des options possibles au niveau des solutions.

1.1.1 Au niveau du poste de travail

La classification des droits des intervenants :

Un profil est affecté à chaque opérateur en fonction du poste de travail qu'il occupe. Il combine les critères suivants :

- la position du poste dans l'organisation (agent du service X, chef du service...),
- son pouvoir d'engager l'entreprise,
- son domaine d'activité (informatique, comptabilité...) et les opérations qui y sont attachées,
- ses relations avec l'organisation (client direct, agent...),
- son implantation géographique (exemple: succursale à l'étranger)
- ses contraintes horaires...

Des classes de droits sont affectées aux profils en fonction des besoins des postes de travail. Ils définissent ainsi un système de référence unique, dans la mesure où un poste est unique dans une organisation, pour tous les systèmes de contrôle des habilitations (manuels ou automatiques) de l'entreprise.

Nous verrons, par la suite, qu'un des problèmes essentiels de la sécurité consiste à confronter les droits des intervenants (les besoins) avec les ressources utilisées (les moyens) en fonction les voies d'accès empruntées pour y parvenir (les réseaux...).

Les classes de droits affectés aux intervenants représentent les données de référence pour la sécurité informatique.

Option possible :

- classification par site isolé ou sous-ensemble de l'organisation,

- notion de représentant de groupe et de poste asservi (exemple : superviseurs des machines...).

L'accès universel :

C'est la possibilité offerte à chaque intervenant d'exercer ses droits à partir de tous les points d'accès aux ressources.

La banalisation de l'usage des terminaux et des voies d'accès procèdent de ce concept et en sont le corollaire.

Leur application engendre deux séries de conséquences :

- le système de référence des droits d'accès (indépendamment de son organisation répartie ou centralisée) doit être accessible de tous les points d'accès où doivent s'effectuer les contrôles d'habilitation (réseaux, ordinateurs...),

- l'équipement terminal est dissocié du poste de travail, ce qui reporte au niveau de l'intervenant son identification et son authentification.

Option possible :

- restriction sur des groupes de terminaux, ou sur des opérateurs (exemple : équipement d'entrée-sortie sur réseaux spécialisés).

La décentralisation de la capacité de traitement et de stockage des informations :

L'implantation de micro-ordinateurs a pour effet de décentraliser une partie des ressources de l'entreprise sur des moyens puissants autonomes et vulnérables.

S'ils disposent de possibilités de transferts des informations de l'intérieur vers l'extérieur ou l'inverse (exemple : connexion aux réseaux internes ou externes, sortie de disquettes...), ils constituent des moyens de fraude par excellence. Ils doivent donc dans ce cas être protégés au même titre que les ordinateurs.

La décentralisation des ressources nécessite donc le contrôle de l'usage des micro-ordinateurs. Ce concept doit être intégré dans l'architecture de sécurité.

Option possible :

- absence de contrôle sur les terminaux non reliés aux sites centraux,

- contrôle des locaux et du personnel.

Notion de terminal multi-fonctions :

La volonté de pouvoir offrir n'importe quelle fonctionnalité disponible sur le réseau sur tout terminal lorsque c'est nécessaire impose de pouvoir disposer sur tous les points d'accès du niveau de sécurité de la fonction la plus sensible. Elle conduit à mettre à disposition sur tous les terminaux les mêmes mesures de sécurité.

Importance du nombre de terminaux :

L'importance du nombre de terminaux rend problématique l'utilisation des techniques d'authentification des terminaux eux-mêmes en raison de la difficulté à gérer de nombreux couples de clés (central-terminal) dans des mémoires protégées.

Ergonomie :

Elle impose de simplifier la tâche des utilisateurs et peut dans certains cas, comme en ce qui concerne les temps de réponse, amener à faire des choix moins sécuritaires :

- mécanismes d'authentification sans mots de passe,

- limitation du nombre d'authentifications,

- ...

1.1.2 Au niveau des communications

Multiplicité et hétérogénéité des réseaux :

La multiplicité des réseaux internes (locaux ou non) :

- multiplie les centres de gestion,

- exige un partage précis des responsabilités entre réseaux, et entre réseaux et ordinateurs,

- nécessite un niveau de sécurité identique pour chacun d'entre eux faute de quoi l'ensemble serait équivalent au maillon le plus faible,

- demande une continuité des procédures pour éviter des "trous" de sécurité.

L'hétérogénéité, qui va de pair avec la multiplicité, conduit généralement une entreprise, pour constituer ses réseaux privés internes, à choisir les possibilités offertes par les réseaux publics (Transpac et le protocole X25), associé à l'architecture du constructeur d'ordinateur dominant (SNA pour IBM, DSA pour BULL, DNA pour DEC) car les autres s'adaptent à leurs spécifications.

Le modèle de l'architecture de sécurité doit donc s'articuler autour de ces choix de telle sorte que la coordination inter-réseaux soit facilitée au niveau de la gestion et de l'organisation.

A cet effet, il doit avoir pour objectif :

- d'utiliser le même système de référence quelque soit le produit,

- d'unifier les langages de commande des sessions et de contrôle des habilitations propre à chaque système ou sous-système,

- utiliser les matériels de sécurité les plus standard possibles

- etc...

<u>Option possible</u> :

- par famille de réseau (exemple : références spécifiques du réseau local).

Taille du réseau :

- devrait en bonne sécurité conduire à partitionner les risques des différentes parties du réseau, mais la nécessité de ne pas dégrader les performances en-deçà d'un niveau acceptable par l'utilisateur conduit à éviter les déchiffrements-rechiffrements par différents algorithmes et/ou de clés et par conséquent à utiliser un mécanisme quasi-unique;

- également pour améliorer les temps de réponse les fichiers de droits peuvent être dupliqués (plutôt que décentralisés);

- toujours en raison des temps de réponse, l'authentification par mot de passe à partir d'un fichier centralisé est déconseillée. Cependant si les utilisateurs n'ont accès qu'à un terminal ou une partie du réseau limitée, cette technique peut être envisagée.

Ouverture des réseaux sur l'extérieur :

L'interconnexion des réseaux internes avec des réseaux externes ou publics a pour effet d'une part de méconnaître la population qui peut utiliser nos ressources avec des terminaux non identifiés, et d'autre part de rendre indénombrables les chemins d'accès.

Des barrières technologiques existent et restreignent l'espace des possibilités mais elles peuvent être contournées par erreur (exemple : erreur de définition de réseau à l'occasion d'une modification) ou malveillance et ne garantissent pas suffisamment contre les détournements d'usage des équipements.

Il est possible techniquement par exemple en partant d'un réseau local, de sortir sur le réseau commuté et de réentrer via Transpac dans un ordinateur de l'entreprise et ainsi de s'affranchir par cascade de l'usage normal des points d'accès.

Le choix de l'ouverture des réseaux sur l'extérieur oblige donc à mettre en oeuvre :

- une fonction "contrôle de l'usage" des réseaux à partir des droits exhibés par chaque intervenant et des chemins empruntés par les informations puisque tous les chemins ne présentent pas le même degré de sécurité,

- une classification des chemins possibles au travers des réseaux et de leur usage.

En d'autres termes, la topologie des flux autorisés, les règles de gestion et les mécanismes de contrôles qui sont associés à chaque noeud ou passerelle inter-réseaux, constituent des composantes essentielles de la sécurité des réseaux.

<u>Option possible</u> :

- partition des voies d'accès en fonction de leur degré de sûreté et de leur usage.

Multi-nationalité et lois nationales :

La répartition d'un réseau sur plusieurs pays peut amener à utiliser des mesures de sécurité différentes selon les pays, les lois et réglementations étant souvent différentes.

Il est à noter que, dans ce contexte, des mesures de protection doivent être prises pour éviter que les dégradations de niveau de sécurité imposées dans certains pays ne mettent en cause les bases de la sécurité de l'ensemble du réseau.

L'utilisation des algorithmes de cryptographie, y compris dans les cartes à mémoire, n'est pas libre dans certains pays (dont la France).

Le secours du réseau :

En cas d'incident, les réseaux sont redéfinis, les schémas de connexion modifiés provisoirement.

Il est donc évident que l'architecture de la sécurité doit être flexible et comporter un niveau de paramétrage suffisant pour intégrer des évolutions on line, rapides et temporaires.

Option possible :

- pas de distinction entre réseau de secours et normal.

Optionnalité :

La volonté d'optionnalité qui permet une meilleure administration en temps réel de la sécurité empêche l'utilisation de nombreuses boîtes noires placées en coupure sur les lignes, en particulier si la standardisation de ces boîtes est recherchée, ce qui tend à imposer l'absence d'applicatif au moins tant que la sécurité n'est pas normalisée par l'ISO.

Unicité de fonctionnalité :

Les réseaux spécifiques permettent souvent de mettre en place des mesures plus simples, car le besoin de mécanismes complexes lié à de multiples possibilités n'existe pas.

1.1.3 Au niveau de l'exploitation des ordinateurs

Multiplicité et hétérogénéité des équipements de sécurité :

Comme pour les réseaux, et pour les mêmes motifs, une coordination inter-ordinateurs est nécessaire.

Les logiciels de contrôle des ressources constituent ici les éléments de base. C'est donc à partir d'eux que doit s'élaborer le modèle d'architecture de la sécurité.

Back-up des ordinateurs :

Dans la mesure où l'on se situe déjà dans un environnement hétérogène, le secours des centres d'exploitation ne fait que l'accroître un peu plus, sachant que des sécurités équivalentes doivent leur être appliquées.

Le problème se situe au niveau des réseaux et du transfert des mécanismes de sécurité d'un site sur un autre et relève donc principalement du domaine de la portabilité des logiciels.

Besoin de performances :

Le besoin de performances, en tant que concept structurant, a des répercussions sur le choix d'une architecture de sécurité :

- authentification et vérification des droits proches de l'utilisateur,

- limitation du nombre des opérations de cryptographie.

Sécurisation d'un ordinateur : niveau des techniques disponibles :

La sécurité élevée d'un ordinateur est encore difficile à réaliser. Il en découle que certains matériels peuvent être spécialisés pour faire de la sécurité. Ces types de matériels peuvent entraîner l'utilisation des antéserveurs pour faire écran devant des centraux plus difficiles à protéger.

Fonction d'antéserveur :

Les systèmes antéserveurs peuvent satisfaire plusieurs objectifs (cf partie 4 du rapport).

La fonction antéserveur étant un mécanisme de protection du centre serveur contre l'intrusion, elle ne constitue pas un facteur structurant pour la sécurité.

<u>Option possible</u> :

- délégation partielle de services de sécurité à l'antéserveur.

1.1.4 Au niveau des applications

Nature de l'information :

Le choix des mécanismes de sécurité à appliquer, nous l'avons déjà indiqué, dépend des risques attachés à l'activité.

Dans le cadre du service d'identification et d'authentification, le risque se traduit par un niveau d'engagement personnel plus ou moins grand de l'intervenant en fonction des informations manipulées.

L'initiative du déclenchement du contrôle revient aux applications et à un moment de leur choix, car elles seules connaissent la valeur des objets informationnels en cours de traitement.

Il est donc essentiel de disposer d'une classification commune aux différents centres qui décrive les divers degrés d'engagements possibles (exemple : aucun engagement, confirmation, certification, contre-certification) des intervenants d'une part, et d'autre part en cas de besoin de répertorier dans chaque application les informations qui déclencheront le processus de contrôle.

Il est évident, dans ces conditions, que le mécanisme de rappel d'un service d'authentification en cours de session doit être envisagé.

Option possible :

- séparation des données et traitements en fonction de l'engagement des intervenants (exemple : transactions TP différentes en fonction des données nécessitant un engagement ou non).

Répartition des informations et des applications et accumulation des sécurités :

Dans la mesure où la répartition par site des applications et des informations n'est pas effectuée par domaine d'activité, il peut exister des redondances d'informations sur des machines différentes, et l'usage des équipements (notamment réseaux) est plus difficile à classifier.

En conséquence, l'architecture du système de sécurité devra prévoir et permettre de gérer la redondance des droits des intervenants sur plusieurs machines.

De même, à l'intérieur d'une même application un système spécifique (exemple : contrôle d'accès) peut se superposer au logiciel de sécurité du niveau système exploitation et conduire à une multiplicité d'une part des systèmes de contrôle et de référence, et d'autre part des interventions des opérateurs. Dans ce cas l'accumulation des sécurités sur une même application sera évitée. Un seul service d'authentification et d'habilitation sera retenu sur la même machine pour limiter les interfaces avec les logiciels de sécurité de base, source de risques. Il devra utiliser un système de référence unique.

Besoin de mise à jour des droits en temps réel :

Un système d'opposition étant tout aussi compliqué à gérer et à utiliser (exemple droits dans une carte à mémoire), les fichiers sont souvent centralisés avec d'éventuelles duplications.

Mise à jour des droits déléguée aux utilisateurs :

Ce critère implique un compromis entre l'installation de la gestion des droits proche de l'utilisateur et une gestion centralisée de ces mêmes droits; en effet, la possibilité laissée aux utilisateurs de se connecter sur différents noeuds du réseau en cas de problème sur la liaison ou sur le noeud de rattachement principal incline au choix d'une solution simplifiée pour le système de mise à jour des droits sur des noeuds répartis.

Type d'application :

Les modalités d'utilisation des mécanismes de sécurité diffèrent selon les types d'applications :

- batch ou interactif,
- transfert de fichiers internes ou externes,
- messagerie grand public ou professionnelle,
- échange de programme à programme...
- etc...

Cette distinction doit donc apparaître dans l'architecture de la sécurité car elle est notamment représentative de la population concernée (grand public, professionnels...) et des procédures à utiliser.

2) QUELQUES PROBLEMES POSES PAR LA MISE EN OEUVRE DES MECANISMES DE SECURITE

Selon l'approche effectuée, les mécanismes couvrent plus ou moins bien les risques. Nous allons les passer en revue au travers de trois notions principales : authentification, confidentialité et intégrité.

2.1 Authentification

Dans le cas d'une approche par site, l'authentification couvre tous les usagers (logiques ou physiques) d'un ordinateur. Les mécanismes de contrôle sont à implanter dans un point central de telle sorte que toutes les transactions entre les équipements terminaux et centraux soient filtrées d'une part, et que d'autre part une continuité soit assurée avec les systèmes de contrôle d'accès.

Ainsi, un "périmètre" de sécurité est constitué autour de chaque ordinateur, ce qui en limite l'usage aux seules personnes habilitées.

Cette approche est particulièrement recommandée pour prévenir les risques d'intrusion des personnes, nés de l'interconnexion des ordinateurs avec des réseaux.

Une approche de l'authentification par application ou par réseau revient à sécuriser un sous-ensemble qui peut être attaqué à partir du sous-ensemble non sécurisé. En outre, la coexistence de systèmes différents risque d'aboutir à des incohérences et à des difficultés pour la gestion des droits. Donc, seule l'approche par site convient.

2.2 Confidentialité

Elle concerne des informations spécifiques. Donc, une approche par site ou par réseau est inadaptée sauf à tout rendre confidentiel, ce qui équivaudrait à rendre stratégique toute information.

C'est une approche par application qui convient. Il faut donc effectuer une analyse de risque et, en fonction du résultat appliquer les mécanismes de confidentialité aux activités concernées.

Si un système d'authentification de niveau site existe déjà, il participe à la confidentialité et les transactions ne pourront être initiées que par les personnes habilitées.

Il restera à mettre en oeuvre des mécanismes sur les parties non transactionnelles par exemple Batch.

2.3 Intégrité

Comme pour la confidentialité, l'intégrité concerne quelques informations. C'est donc une approche par activité qui convient. Les mécanismes sont à implanter au niveau des applications et doivent couvrir tous les maillons de la chaîne de traitement (terminaux, réseaux, sites). L'intégrité s'applique notamment au système de gestion de la sécurité mais les mécanismes sont différents de ceux de l'authentification. De même, les mécanismes d'intégrité peuvent être, sans difficulté majeure, différer d'une application à l'autre.

En revanche, les mécanismes de confidentialité et d'intégrité peuvent être communs, par exemple le chiffrement.

En définitive, certaines approches conviennent mieux que d'autres pour appliquer certains mécanismes, mais il faut remarquer qu'elles sont complémentaires. De même, ces mécanismes ne sont pas toujours indépendants les uns des autres.

Il est à noter qu'une approche par les réseaux ne permet pas de conclure dans une entreprise qui privilégie les risques (les besoins) comme critère de choix. En revanche, si les moyens constituent le critère déterminant (c'est le cas des fournisseurs de réseaux) l'élaboration de l'architecture de sécurité doit être effectuée à partir d'une approche réseau.

Donc, dans le cas général, l'approche globale doit être effectuée. Le modèle d'architecture peut se résumer ainsi :

Niveau 1 : Mécanismes à appliquer = authentification + contrôle d'accès

Niveau 2 : Approche par applications en fonction de leur degré de risque

Propriétés à couvrir = confidentialité + intégrité.

CHAPITRE VII

CONCLUSION

Le présent document représente deux années de réflexion du groupe "Sécurité des réseaux" du CIGREF.

Il comporte un certain nombre de recommandations quant à l'approche utilisée, aux techniques et organisations souhaitées par les grands utilisateurs; nous ne reprendrons pas ici ces éléments qui sont rappelés dans la synthèse accompagnant le rapport. Cependant il nous apparaît utile d'insister sur l'importance d'un **Plan Sécurité** de l'entreprise; c'est dans ce cadre que sera trouvée la définition optimale de l'architecture de sécurité dans le réseau.

Conscients de l'évolution des risques et des techniques utilisées pour y parer, les membres du groupe ne souhaitent pas conclure cet important travail de manière définitive. Au contraire, ils se préparent, sur la base de leurs dicussions internes et de leurs contacts avec leurs partenaires - Administrations, fournisseurs, organismes de normalisation -, à faire vivre ce document de façon à ce qu'il reste un ouvrage de référence pour les entreprises membres du CIGREF et une contribution aux débats nationaux et internationaux en matière de sécurité des systèmes d'information.

Enfin, il est probable qu'à très court terme les problèmes posés par l'intégration des outils de sécurité, l'administration de celle-ci et son insertion dans l'administration des réseaux retiendront toute l'attention des grandes entreprises.