LISTE DES ABBREVIATIONS

ACL	Access Control List
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
CHAP	Challege Handshake Authentication Protocol
DES	Data Encryption Standard
DNS	Domain Name Server
DSRP	Document Stratégique pour la Réduction de la Pauvreté
EAP	Extensible Authentication Protocol
HIDS	Host-based Intrusion Detection System
IDEA	Internation Data Encryption Algorithm
IDS	Intrusion Detection System
TCP/ IP	Transport Control Protocol / Internet Protocol
IP AH	IP Authentication Header
IP ESP	IP Encapsulation Security Payload
MAC	Media Access Control
MD5	Message Digest 5
MEFB	Ministère de l'Economie, des Finances et du Budget
OSI	Open System Interconnection
OTP	One Time Password
PAP	Password Authentication Protocol
RPC	Remote Procedure Call
S/MIME	Secure / Multipurpose Internet Mail Extenstions
SA	Security Association
SASL	Simple Authentication and Security Layer
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
TTL	Time To Live
UDP	User Datagram Protocol

CONTENUS

INTRODUCTION

Dans le cadre d'une modernisation et de renforcement de la gestion des finances publiques, répondant au principe de la bonne gouvernance inscrit dans le DSRP, le MEFB a décidé de mettre en place un système intégré informatisé. Ce SI est spécialement conçu pour traiter les informations en temps réel afin de pouvoir y tirer des résultats statistiques nécessaires à la décision. Le SI répond aux besoins d'une entreprise étendue permettant ainsi la collaboration étroite des différentes branches de la MEFB, géographiquement éloignées, comme le site pilote du MEFB sis à Toamasina, qui est lui-même divisé en plusieurs domaines sous-jacents tels que la douane, le trésor, le CDE, le budget et les centres fiscaux. En conséquence, le SI répond à la gestion transparente des finances publiques, demandées aussi par le DSRP.

Ainsi, le SI doit assurer la disponibilité permanente des données stockées ou échangées, leur intégrité et leur confidentialité suivant la sensibilité de ces données. Pour atteindre ce but, il est impératif d'implémenter des procédures de sécurité en conformité avec les standards internationaux, garantissant ainsi l'aspect évolutif et l'interopérabilité du système.

En effet, la disposition et l'accès des données en temps réel sur le système intégré du MEFB posent des risques potentiels sur son bon fonctionnement, i.e. sur l'accomplissement des lourdes responsabilités que ce ministère a sur l'Etat. Vue l'importance du rôle que le SI joue au sein du MEFB, ainsi que les données qui s'y résident, il est fortement indispensable de protéger le SI des malveillants et des menaces qu'elles soient accidentelles ou intentionnelles.

Lors de mon stage au sein de ce Ministère, on m'a chargé de sécuriser l'échange des données entre le MEFB et son site pilote sis à Tamatave, ce qui a été étendu à la sécurisation des données en stockage dans le serveur de données. Ce qui m'a conduit aux quatre objectifs bien précis suivants:

- Sécurisation des systèmes d'information des administrations, i.e. assurer la protection des systèmes et des données y résidant. Cette partie englobe : la protection du réseau local et les postes de travail individuelles, la fiabilité des applications y installées pour assurer la performance et la disponibilité des services et données.
- Sécurisation des moyens de transmissions des données. Comme les deux sites du MEFB résident sur deux lieux très espacés l'un de l'autre, la transmission des données se fait par

satellite, i.e. exposition des données à l'espace libre. Le garanti de l'intégrité des données et leur confidentialité sont donc primordiales.

- Proposer une politique de sécurité répondant aux exigences des utilisateurs. La règle de sécurité est aussi indispensable car elle indique clairement les besoins en sécurité que l'on doit répondre.
- Mettre en place des capacités opérationnelles de réponse aux attaques informatiques, ce qui implique la mise en place d'un tableau de bord et un plan de mitigation et de contingence des risques.

La protection du système d'information doit répondre aux besoins d'une entreprise évolutive, c'est-à-dire l'utilisation des produits standardisés et génériques est recommandé. Ainsi, l'intégration de nouveaux modules n'affecte pas négativement le niveau de performance du système.

On remarque aussi que l'on a affaire à un système d'information déjà existant Il est donc impératif de suivre et d'obéir la logique métier que le MEFB a déjà implanté, entre autres l'architecture métier (qui documente le processus de l'entreprise), l'architecture fonctionnelle et les fonctions nécessaires aux utilisateurs pour mener à bien leurs activités, l'architecture applicative et l'architecture technique. Cependant, une architecture technique est proposée à la fin de ce rapport en guise d'amélioration du SI en matière de la sécurité.

Pour atteindre les objectifs sus citées, on a adopté le plan suivant. Premièrement, on entame la partie théorique de la sécurité des SI. Cette partie passe en revue les protocoles de sécurité appliquée à la sécurisation du SI du MEFB. La partie suivante montre d'une façon concise les concepts utilisés, tels que la façon de déployer l'architecture du réseau local et le VPN pour la confidentialité des données en stockage et lors de leur transmission. Cette partie nous montre aussi la gestion des ressources matérielles ou humaines prises en compte par le SI, pour améliorer et faciliter la modification et l'évolution du système.

PARTIE I : APPROCHE THÉORIQUE DE LA SECURITE DES SI

CHAPITRE I : INTRODUCTION A LA SECURITE

1.1. Notion de la sécurité

1.1.1. Introduction – pourquoi la sécurité est-elle primordiale ?

Les Systèmes d'Information (SI) reposent en partie sur des machines qui stockent, traitent et transmettent de l'information [1]. Ces machines peuvent être des ordinateurs mais aussi des périphériques informatiques, des imprimantes, des télécopieurs,... Elles sont souvent reliées par des réseaux locaux à l'intérieur de leur organisme d'appartenance, mais dans de nombreux cas, elles peuvent se communiquer avec l'extérieur. Ainsi de multiples informations et services offertes par le SI, sont accessibles de presque n'importe quel point du globe, facilitant les échanges entre les acteurs économiques et permettant de traiter des problèmes de façon plus efficace et plus sûre. Cependant, cette ouverture du SI a l'extérieur présente aussi bien des inconvénients qui fragilisent aussi bien les fournisseurs que leurs utilisateurs [2]. En effet, l'information est une ressource stratégique, une matière première, elle est un atout supplémentaire pour ceux qui la possèdent légitimement ou illégalement. La protection de ce patrimoine contre les malveillances doit par conséquent être un souci permanent.

1.1.2. Menaces existantes pour le SI

1.1.2.1. Introduction

Les SI gèrent des informations qui peuvent être convoitées intentionnellement ou accidentellement par des individus. En proposant de nouveaux services et en traitant toutes sortes d'informations les SI forment de nouvelles cibles qui ne sont pas toujours l'objet d'attentions particulières de la part de leurs propriétaires, qui vont parfois jusqu'à sous-estimer ou ignorer l'importance de leur capital.

La concentration des données et leur disponibilité sur un réseau permettent d'obtenir rapidement, dans la discrétion et parfois dans l'anonymat le plus complet, une grande quantité d'information qu'il était auparavant difficile de se procurer.

Origine de la menace

La connaissance de l'origine de la menace est l'un des éléments qui va permettre au défenseur d'évaluer la force et les moyens de son agresseur potentiel [3]. En comprenant les motivations de ce dernier, le défenseur pourra éventuellement adapter sa politique de sécurité et anticiper les actes

malveillants. Un SI sera d'autant plus menacé que les informations qu'il possède auront une valeur pour leur propriétaire et pour d'autres entités. Il ne faut pas pour autant conclure qu'un SI ne gérant pas d'information de valeur n'est sujet à aucune menace puisque son rôle peut être primordial pour assurer un autre service important.

1.1.2.3. Catégories de menace

1.1.2.3.1. Menaces accidentelles

Cette catégorie de menaces regroupe d'une part tous les événements naturels à caractère catastrophique comme les incendies, les inondations dues au cyclone, les tremblements de terre, et d'autre part, tous les types d'erreurs que l'on peut imaginer tels que les erreurs de saisie, de transmission, etc., qui sont le plus souvent provoquées par l'inattention ou le manque de formation des utilisateurs [4].

Notons que les conséquences des accidents seront le plus souvent les mêmes que celles dues aux malveillances intentionnées.

1.1.2.3.2. Menaces intentionnelles

Caractère stratégique :

Pour un Etat, la menace stratégique s'intéresse par essence à toutes les informations concernant le secret de Défense et la Sûreté de l'État, mais également à celles appartenant au patrimoine national, qu'il soit d'ordre scientifique, technique, industriel, économique ou diplomatique. La menace stratégique peut également attaquer la disponibilité de systèmes d'information, dont le fonctionnement continu est nécessaire au fonctionnement normal des institutions.

Pour une entreprise ou une société, la menace d'origine stratégique a pour but d'obtenir toute information sur les objectifs et le fonctionnement de celle-ci, pour récupérer des clients prospectés, des procédés de fabrication, des résultats de recherche ou de développement.

Caractère terroriste :

On définira la menace terroriste comme regroupant toutes les actions concourant à déstabiliser l'ordre établi ; les actions entrant dans cette catégorie peuvent avoir un caractère violent (destruction physique de systèmes) ou plus insidieux (intoxication et désinformation par détournement ou manipulation d'informations sensibles ou non, perturbations engendrées dans un système et susceptibles de déclencher des troubles sociaux présents à l'état latent....).

Caractère cupide :

Les attaques dans cette catégorie peuvent avoir plusieurs buts tels que :

• Gain pour l'attaquant ; ce gain peut être financier (détournement de fonds), ou lié à un savoir-faire (vol de brevet, concurrence déloyale...).

• Le second occasionne une perte pour la victime qui se traduira par un gain pour l'agresseur (parts de marché, accès au fichier des clients, à des propositions commerciales...) ; ce peut être la destruction de son système ou de ses informations, une perte de crédibilité ou de prestige (image de marque) vis-à-vis d'une tierce personne, etc.

Les victimes figurent en général parmi les organismes qui détiennent l'argent : banques, compagnies d'assurances, etc.

Caractère vengeur :

La vengeance peut être la motivation de l'employé qui se sent mal utilisé par rapport à ses capacités, ou qui vient d'être licencié ou qui sait qu'il va être. Il faut alors craindre des actes destructeurs et souvent non corrélés avec leur cause dans le temps.

1.1.2.4. Attaquants :

1.1.2.4.1. Pirates :

Nous proposons les deux profils de pirates les plus souvent identifiés :

Hacker :

Un hacker est un individu curieux, qui cherche à se faire plaisir. Pirate par jeu ou par défi, il ne nuit pas intentionnellement et possède souvent un code d'honneur et de conduite. Plutôt jeune, avec des compétences non négligeables, il est patient et tenace.

Cracker :

Un cracker est plus dangereux que le hacker, il cherche à nuire et montrer qu'il est le plus fort.

Souvent mal dans sa peau et dans son environnement, il peut causer de nombreux dégâts en cherchant à se venger d'une société - ou d'individus - qui l'a rejeté ou qu'il déteste. Il veut prouver sa supériorité et fait partie de clubs où il peut échanger des informations avec ses semblables.

Les crackers possèdent rarement des moyens importants : assez fréquemment il s'agira d'un micro-ordinateur associé à un modem. Leur population, tend à s'accroître car les compétences en informatique se répandent et les SI sont de plus en plus nombreux.

1.1.2.4.2. Fraudeurs :

Les fraudeurs se répartissent en deux catégories avec des compétences similaires :

Le fraudeur interne :

Possédant de bonnes compétences sur le plan technique, il est de préférence informaticien et sans antécédents judiciaires. Il pense que ses qualités ne sont pas reconnues, qu'il n'est pas apprécié à sa juste valeur. Il veut se venger de son employeur et chercher à lui nuire en lui faisant perdre de l'argent. Pour parvenir à ses fins il possède les moyens mis à sa disposition par son entreprise qu'il connaît parfaitement.

Le fraudeur externe :

Bénéficiant presque toujours d'une complicité, volontaire ou non, chez ses victimes, il cherche à gagner de l'argent par tous les moyens. Son profil est proche de celui du malfaiteur traditionnel. Parfois lié au grand banditisme, il peut attaquer une banque, falsifier des cartes de crédit ou se placer sur des réseaux de transfert de fonds, et si c'est un particulier il peut vouloir fausser sa facture d'électricité ou de téléphone.

1.1.2.4.3. Espions :

Ils travaillent pour un État ou pour un concurrent. Choisis pour leur sang-froid et leur haut niveau de qualification, ils sont difficiles à repérer.

L'espion d'État :

Professionnel ayant des connaissances techniques élevées, il dispose de nombreux moyens d'attaque et d'une importante puissance de calcul. Il peut aller jusqu'à acquérir, légalement ou non, une copie du système qu'il veut attaquer pour l'analyser et l'étudier sous toutes les angles. Il est patient et motivé. Il exploite les vulnérabilités les plus enfouies d'un SI car elles seront les plus difficiles à détecter et il pourra les utiliser longtemps. Il sait garder le secret de sa réussite pour ne pas éveiller les soupçons et continuer son travail dans l'ombre.

L'espion privé :

Souvent ancien espion d'État reconverti, il a moins de moyens mais une aussi bonne formation.

1.1.2.4.4. Terroristes :

Moins courant, les terroristes sont aidés dans sa tâche par l'interconnexion et l'ouverture des réseaux. Les terroristes sont très motivés, ils veulent faire peur et faire parler de lui. Ses actions se veulent spectaculaires.

1.1.3. Les méthodes d'attaques :

Nous présentons quelques types d'attaques génériques et par ailleurs très connus. Les attaques peuvent porter sur les communications, les machines, les traitements, les personnels et l'environnement. Nous les classons en deux catégories : attaques physiques, attaques logiques [2].

1.1.3.1. Attaques physiques :

Nous plaçons ici des attaques qui nécessitent un accès physique aux installations ou qui se servent de caractéristiques physiques particulières.

1.1.3.1.1. Interception :

L'attaquant va tenter de récupérer un signal électromagnétique, électrique, ou les trafics circulant dans le réseau informatique et de l'interpréter pour en déduire des informations compréhensibles. L'interception peut porter sur des signaux hyperfréquences ou hertziens, émis, rayonnés, ou conduits. Les techniques d'interception seront très variées pour les différents cas évoqués.

1.1.3.1.2. Brouillage :

Utilisée en télécommunication, cette technique rend le SI inopérant. C'est une attaque de haut niveau, car elle nécessite des moyens importants, qui se détectent facilement. Elle est surtout utilisée par les militaires en temps de crise ou de guerre.

1.1.3.1.3. Écoute :

L'écoute consiste à se placer sur un réseau informatique ou de télécommunication et à analyser et à sauvegarder les informations qui transitent. L'écoute est une attaque passive, i.e. elle ne cause directement aucune perturbation du fonctionnement du SI, mais peut en revanche conduire à d'autres attaques très sévères. De nombreux logiciels commerciaux ou libres, disponibles sur l'Internet, facilitent les analyses et permettent notamment d'interpréter en temps réel les trames qui circulent sur un réseau informatique.

1.1.3.1.4. Balayage (scanner) :

Le balayage consiste à envoyer au SI un ensemble d'informations de natures diverses afin de déterminer celles qui suscitent une réponse positive. L'attaquant pourra entre autre automatiser cette tâche et déduire par exemple les ports ouverts ou les numéros téléphoniques qui permettent d'accéder à un système. Cette technique est analogue à celle qui consiste à balayer une gamme de fréquences pour trouver un signal porteur.

1.1.3.1.5. Piégeage :

L'agresseur tentera d'introduire des fonctions cachées, en principe en phase de conception, de fabrication, de transport ou de maintenance des logiciels, dans le SI. Seule une évaluation de la sécurité du
SI donnera au défenseur une certaine assurance.

1.1.3.2. Attaques logiques :

1.1.3.2.1. Détournement de flux :

Les techniques de détournement de flux servent à rediriger le flux réseau vers un client, vers un serveur, ou vers une autre machine.

ARP-Poisoning :

Toute carte réseau possède une adresse physique MAC. C'est cette adresse qui lui permet de recevoir les paquets qui lui sont destinés sur le réseau local. Cette adresse physique est associée à l'adresse IP grâce au protocole ARP. La table de correspondance entre les adresses IP et les adresses physiques est contenue dans le cache ARP. Lorsqu'un échange doit s'établir entre 2 machines du réseau local, ces deux machines envoient des requêtes ARP avec l'adresse IP du récepteur, associée à un champ vide pour son adresse physique. Ce récepteur va renvoyer son adresse physique dans une réponse ARP.
Si un attaquant envoie un message de réponse ARP avec son adresse physique correspondant à l'adresse IP du récepteur, tout le flux IP dirigé vers le récepteur sera redirigé vers l'attaquant. On dit qu'il a empoisonné le cache ARP du récepteur.

Fouille :

La fouille informatique, par analogie avec la fouille physique, consiste à étudier méthodiquement l'ensemble des fichiers et des variables d'un SI pour un retirer des données de valeur.

Cette recherche systématique d'informations est en général grandement facilitée par la mauvaise gestion des protections classiques qu'il est possible d'attribuer à un fichier. Quand on se déplace dans les divers répertoires d'un système informatique, il est courant de constater que des fichiers et des répertoires ont des protections insuffisantes contre des agresseurs potentiels, uniquement par manque de connaissance, dû le plus souvent à l'insuffisance de formation de l'utilisateur. Ainsi, est-il bien utile de donner un droit de lecture à ses fichiers pour l'ensemble des utilisateurs du système ?

Si l'attaquant est quelque peu entraîné, il aura recours à une attaque plus subtile. Pour s'emparer de certaines informations il va lire la mémoire centrale ou secondaire, ou les supports de données libérés par les autres utilisateurs. Une parade efficace consiste à effacer physiquement toute portion de mémoire ou tout support libéré. En contrepartie, les performances du SI seront moindres.

Canal caché :

Ca type d'attaque est de très haut niveau et fait appel à l'intelligence de l'attaquant. Il permet de faire fuir des informations en violant la politique de sécurité. On propose de classer les canaux cachés en quatre catégories:

Les canaux de stockage qui permettent de transférer de l'information par le biais d'objets écrits en toute légalité par un processus et lus en toute légalité par un autre

Les canaux temporels qui permettent à un processus d'envoyer un message à un autre en modulant l'utilisation de ses ressources systèmes afin que les variations des temps de réponse puissent être observées ;

Les canaux de raisonnement qui permettent à un processus de déduire de l'information à laquelle il n'a pas normalement accès ;

Les canaux dits de "fabrication" qui permettent de créer de l'information en formant des agrégats qui ne peuvent être obtenus directement.

Ces attaques peuvent être réalisées dans le système ou les bases de données à plusieurs niveaux de confidentialité.

Déguisement (masquerading) :

Forme d'accès illégitime, il s'agit d'une attaque informatique qui consiste à se faire passer pour quelqu'un d'autre et obtenir les privilèges ou des droits de celui dont on usurpe l'identité.

Un utilisateur est caractérisé par ce qu'il est, (empreintes, digitales ou palmaires, rétiniennes, vocales, ou toute autre authentifiant biométrique), ce qu'il possède (un badge, une carte magnétique, à puce, un jeton, un bracelet...) et ce qu'il sait (un mot de passe, sa date de naissance, le prénom de ses parents...). Pour se faire passer pour lui, un agresseur doit donc s'emparer d'un ou plusieurs éléments propres à l'utilisateur. Si le contrôle d'accès au SI se fait par mot de passe, l'attaquant tentera de le lire quand l'utilisateur le rentrera au clavier ou quand il le transmettra par le réseau. Si le contrôle d'accès se fait avec une carte à puce, l'attaquant cherchera à en dérober ou en reproduire une. Si le contrôle d'accès est biométrique, la tâche de l'attaquant sera plus difficile mais pas impossible comme le montre ce cas où un dirigeant d'entreprise a été enlevé par des malfaiteurs qui lui ont sectionné un doigt afin de tromper un système de contrôle d'accès.
Sans arriver à des solutions lourdes et coûteuses, le défenseur pourra combiner des méthodes d'identification et d'authentification comme carte et mot de passe pour renforcer sa sécurité.

Mystification:

Dans ce cas, l'attaquant va simuler le comportement d'une machine pour tromper un utilisateur légitime et s'empare de son nom et de son mot de passe. Un exemple type est la simulation de terminal et le comportement d'une machine pour tromper un utilisateur légitime et s'emparer de son nom et de son mot de passe. Un exemple type est la simulation de terminal.

1.1.3.2.2. Man in The Middle attack:

Man-in-the-Middle signifie l'homme du milieu. Cette attaque fait intervenir trois protagonistes : le client, le serveur et l'attaquant. Le but de l'attaquant est de se faire passer pour le client auprès du serveur et se faire passer pour le serveur auprès du client. Il devient ainsi l'homme du milieu. Cela permet de surveiller tout le trafic réseau entre le client et le serveur, et de le modifier à sa guise pour l'obtention d'informations (mots de passe, accès système, etc.).

1.1.3.2.3. Rejeu (replay) :

Le rejeu et une variante du déguisement qui permet à un attaquant de pénétrer dans un SI en envoyant une séquence de connexion effectuée par un utilisateur légitime et préalablement enregistrée à son insu.

1.1.3.2.4. Substitution :

Ce type d'attaque est réalisable sur un réseau ou sur un SI comportant des terminaux distants.

L'agresseur écoute une ligne et intercepte la demande de déconnexion d'un utilisateur travaillant sur une machine distante. Il peut alors se substituer à ce dernier et continuer une session normale sans que le système note un changement d'utilisateur.
Un cas bien connu est celui des ordinateurs sur un réseau local qui ne sont déclarés que par leur adresse Internet. Un attaquant peut alors attendre qu'une machine soit arrêtée pour se faire passer pour elle en usurpant l'adresse de la machine éteinte.

1.1.3.2.5. Faufilement :

Par analogie avec le faufilement physique où une personne non autorisée franchit un contrôle d'accès en même temps qu'une personne autorisée, on dira qu'il y a faufilement électronique quand, dans le cas où des terminaux ou des ordinateurs ne peuvent être authentifiés par un SI, un attaquant se fait passer pour le propriétaire de l'ordinateur ou du terminal.

1.1.3.2.6. Saturation (Denial of Service DoS):

Cette attaque contre la disponibilité consiste à remplir une zone de stockage ou un canal de communication jusqu'à ce que l'on ne puisse plus l'utiliser. Il en résultera un déni de service.

1.1.3.2.7. Cheval de Troie (Trojan horse) :

En informatique un cheval de Troie est un programme qui comporte une fonctionnalité cachée connue de l'attaquant seul. Elle lui permet de contourner des contrôles de sécurité en vigueur. Cependant un cheval de Troie doit d'abord être installé et ceci n'est possible que si les mesures de sécurité sont incomplètes, inefficaces ou si l'agresseur bénéficie d'une complicité.
Un cheval de Troie doit être attirant (nom évocateur) pour être utilisé, posséder l'apparence d'un authentique programme (un utilitaire par exemple) pour inspirer confiance et enfin ne pas laisser de traces pour ne pas être détecté. La simulation de terminal, dont le but est de s'emparer du mot de passe d'un utilisateur, est un cheval de Troie.
En conséquence, identifier la présence d'un cheval de Troie n'est pas aisée et une bonne connaissance du système et des applications installées est nécessaire.

1.1.3.2.8. Salami :

La technique du salami permet à un attaquant de retirer des informations parcellaires d'un SI afin de les rassembler progressivement et de les augmenter de façon imperceptible. Cette technique est utilisée par de nombreux fraudeurs pour détourner subrepticement des sommes d'argent soit en

s'appropriant de faibles sommes sur de nombreux comptes, soit en faisant transiter d'importantes valeurs sur des périodes courtes mais sur des comptes rémunérés leur appartenant.

1.1.3.2.9. Trappe (backdoor) :

Une trappe est un point d'entrée dans une application généralement placé par un développeur pour faciliter la mise au point des programmes. Les programmeurs peuvent ainsi interrompre le déroulement normal de l'application, effectuer des tests particuliers et modifier dynamiquement certains paramètres pour changer le comportement original. Il arrive quelquefois que ces points d'entrée n'en soient pas enlevés lors de la commercialisation des produits et qu'il soit possible de les utiliser pour contourner les mesures de sécurité.

1.1.3.2.10. Bombe :

Une bombe est un programme en attente d'un événement spécifique déterminé par le programmeur et qui se déclenche quand celui-ci se produit. Ce code malicieux attend généralement une date particulière pour entrer en action. Les conséquences peuvent être bénignes comme l'affichage d'un message, d'une image ou d'un logo mais aussi dommageables, comme la destruction de données et plus rarement la destruction du matériel.

1.1.3.2.11. Virus :

Nommé ainsi parce qu'il possède de nombreuses similitudes avec ceux qui attaquent le corps humain, un virus est un programme malicieux capable de se reproduire et qui comporte des fonctions nuisibles pour le SI : on parle d'infection. Le virus dispose de fonctions qui lui permettent de tester s'il a déjà contaminé un programme, de se propager en se recopiant sur un programme et de se déclencher comme une bombe logique quand un événement se produit.
Ses actions ont généralement comme conséquence la perte d'intégrité des informations d'un SI et/ou une dégradation ou une interruption du service fourni.

1.1.3.2.12. Ver (worm) :

Un ver est un programme malicieux qui a la faculté de se déplacer à travers un réseau qu'il cherche à perturber en le rendant indisponible. Cette technique de propagation peut aussi être utilisée pour acquérir des informations par sondage.

1.1.3.2.13. Cryptanalyse :

Le cryptanalyse ne peut se faire que lorsqu'on a accès aux cryptogrammes qui peuvent être interceptés lors d'une communication ou qui peuvent être pris sur un support quelconque .
Cette attaque nécessite en général d'excellentes connaissances en mathématiques et une forte puissance de calcul.

1.1.4. Les services de sécurité :

1.1.4.1. La politique de sécurité :

En général, la politique de sécurité est l'ensemble des lois, règlements et pratiques qui conditionnent (régissent) la gestion, la protection, la diffusion et les actions prises vis-à-vis des ressources et les informations du SI [20]. Ces règles sont recueillies à partir des besoins en matière de sécurité appelés aussi objectifs de sécurité de point de vue technologique ou relatifs aux personnels et organisationnels (administratifs) que l'entreprise a préalablement spécifiée [4].

1.1.4.2. Authentification :

L'authentification est la façon de définir précisément l'identification d'une entité avant d'accéder à un ou plusieurs services que le SI offre [1]. L'authentification est divisée en deux catégories :

1.1.4.2.1. Authentification d'entités: (*entity authentication*)

C'est un procédé permettant à une entité d'être sûre de l'identité d'une seconde entité à l'appui d'une évidence corroborante (ex.: présence physique, cryptographique, biométrique, etc.). Le terme *identification* est parfois utilisé pour désigner également ce service.

1.1.4.2.2. Authentification de l'origine de données: (*data origin authentication*)

C'est le procédé permettant à une entité d'être sûre qu'une deuxième entité est la source originale d'un ensemble de données. Par définition, ce service assure également l'intégrité de ces données.

1.1.4.3. Confidentialité :

C'est la protection de l'information de la divulgation non autorisée [1,3].

1.1.4.4. Non répudiation :

Elle offre la garantie qu'une entité ne pourra pas nier être impliquée dans une transaction ou une action [1,3].

1.1.4.5. Intégrité des données :

C'est la prévention d'une modification non autorisée de l'information [1,3].

1.1.4.6. Disponibilité des informations :

C'est la prévention d'un déni non autorisé d'accès à l'information ou à des ressources du SI. La disponibilité assure que les ressources sont accessibles aux utilisateurs légitimes [1,3].

1.1.4.7. Non duplication :

C'est la protection contre les copies illicites [1,3].

1.1.4.8. Anonymat (d'entité ou d'origine de données) :

Il permet de préserver l'identité d'une entité ou de la source d'une information ou d'une transaction [1,3].

1.1.5. Dangers et attaques menaçant les services de sécurité :

Les dangers contre un type de service sont résumés dans le tableau ci-dessous. Par exemple, le service de l'anonymat d'un utilisateur est mis en péril par l'identification de cet utilisateur. Cette identification peut être obtenue par l'analyse d'une transaction ou accès non autorises aux bases de données des utilisateurs.

Tableau 1 résumé des dangers et attaques pouvant nuire les services de sécurité

Services	Dangers	Attaques
Confidentialité	Faite d'informations	masquerade, écoutes illicites, analyse du trafic
Intégrité	modification de l'information	création, altération ou destruction illicite
Disponibilité	Denial of Service, usage illicite	Virus, accès répétés visant à inutiliser un système
Auth. de données	falsification d'informations	falsification de signature, faille dans le protocole d'auth.
Non-répudiation	nier la participation a une transaction	prétendre un vol de cle ou une faille dans le protocole de signature
Non-duplication	duplication	falsification, imitation
Anonymat	identification	analyse d'une transaction, accès non autorises permettant l'identif.

1.1.6. Mécanisme de sécurité

Le mécanisme de sécurité (security mechanism) est la logique ou algorithme qui implémente par matériel ou logiciel une fonction particulière dédiée à la sécurité ou contribuant à la sécurité. Nous entamons seulement les implémentations logiciels de ces mécanismes de sécurité dans cette paragraphe, puisque les implémentations matériels sont spécifiques aux différents constructeurs, même si le but est le même.

Tableau 2: résumé des méthodes digitales assurant les services de sécurité

Services	**Mécanismes classiques**	**Mécanismes digitaux**
Confidentialité	Scelles, coffre-fort, cadenas	cryptage, autorisation logique
Intégrité	encre speciale, hologrammes	fonctions à sens unique + cryptage
Disponibilité	contrôle d'accès physique, surveillange video	contrôle d'acces logque, audit, anti-virus
Auth. d'entities	presence, voix, piece d'indentite, reconnaissance biometrique	secret + protocole d'auth. adresse reseau+userid+carte a puce + PIN
Auth. de donnees	sceaux, signature, empreinte digitale	fonction a sens unique + cryptage + signature digitale
Non-duplication	encre speciale, hologrammes, tatouage	tatouage digital (watermarks), verrouillage cryptographique
Anonymat	brouilleur de voix, deguisement, argent liquide	mixers, remailers, argent electronique

1.1.6.1. Méthodes digitales de sécurité :

1.1.6.1.1. Principe de l'intégrité des données :

Les fonctions de hachage cryptographiques permettent d'assurer l'intégrité des données [9, 16].

Introduction :

Une fonction de hachage h est aussi appelée fonction de hachage à sens unique (ou 'one-way hash function). Ce type de fonction est très utilisé en cryptographie, principalement dans le but de réduire la taille des données à traiter par la fonction de cryptage. En effet, la caractéristique principale d'une fonction de hachage est de produire un haché Y= h(X) (ou condensé) différent pour chaque donnée différente X de longueur finie mais arbitraire. Le condensé Y résultant est de taille fixe, dont la valeur diffère suivant la fonction utilisée.

Le haché Y est caractéristique du texte ou de données X. Différentes données donneront toutes des condensés différents. Le condensé ne contient pas assez d'information en lui-même pour permettre la reconstitution du texte original. D'ailleurs, c'est pour cela même que l'on parle d'ailleurs de fonction à sens unique. L'opération de hachage est destructive dans le sens où elle conduit à une perte d'information.

Une fonction de hachage est dite “à clé” (**keyed hash function**) si une clé intervient dans le calcul du condensé ($h_k(X) = Y$); sinon on l’appelle fonction “sans clé” (**unkeyed hash function**).
Les hash functions ont des nombreuses applications informatiques dont l’archivage structuré facilitant la recherche. Coté sécurité nous allons étudier deux catégories :

- Les codes d’authentification de message (**message authentication codes ou MAC**) qui sont des keyed functions permettant d’authentifier la source du message et d’assurer son intégrité sans utiliser des mécanismes (cryptage) additionnels.
- Les codes détecteurs d’altérations (**manipulation detection codes (MDC)** or message integrity codes (MIC)): ce sont des unkeyed functions permettant de fournir un service d’intégrité sous certaines conditions. Le résultat d’une telle fonction est appelée MDC-value ou, simplement, digest.

On remarque que le but d’un condensé n’est pas de véhiculer ou de transporter de l’information. Il est juste représentatif d’une donnée particulière et bien définie. D’autant que les algorithmes de hachage les plus courants sont publics et ne représente pas en eux-mêmes un secret.

a. Propriétés des fonctions de hachage :

- ‘Preimage resistance’ : soit un haché Y, il est pratiquement impossible de trouver le texte original X tel que $h(X) = Y$
- ‘2^{nd}-preimage resistance’ : étant donné un texte X, et son image $Y / Y = h(X)$, il est pratiquement impossible de trouver un texte X’ tel que $h(X) = h(X')$. Le 2^{nd}-preimage resistance est aussi appelée ‘weak collision resistance’.
- ‘Collision resistance’ : il est calculatoirement impossible de trouver deux pré images X et X’ distinctes pour lesquelles $h(X) = h (X')$ (pas de restriction sur le choix des valeurs). La collision résistance est aussi appelée strong collision résistance.

b. Code d’authentification des messages MAC :

Un Message Authentication Code (MAC) est une famille de fonctions h_k paramétrées par une clé secrète k ayant les propriétés suivantes:

- **Prop1. compression**: comme pour les fonctions de hash génériques mais appliqué à h_k.
- **Prop2. facile à calculer**: à partir d’une fonction hk, et d’une clé connue k, on peut facilement calculer h_k (X). Le résultat est appelée un *MAC-value* ou, simplement, un *MAC*.

- **Prop3. résistance calculatoire** (*computation-resistance*): sans connaissance de la clé symétrique k, il est (calculatoirement) impossible de calculer des paires (X, $h_k(X)$) à partir de 0 ou plusieurs paires connus (X_i, h_k (X_i)) pour tout $X \neq X_i$

La prop3. implique que les paires (X_i, $h_k(X_i)$) ne peuvent non plus servir à calculer la clé k (*key non-recovery*). Cependant la propriété *key non-recovery* n'implique pas *computation-resistance* car des attaques *chosen/known -plaintext* pourraient mener à des paires (X, $h_k(X)$) falsifiées.
L'impossibilité de calculer des paires (X_i, $h_k(X_i)$) se traduit également en *preimage* et *collision resistance* pour toute entité ne possédant pas la clé k.

Principe de la cryptographie :

La cryptographie avait été développée dans le but de garantir la confidentialité des informations en échange. Il existe deux types de systèmes de la cryptographie : la cryptographie symétrique et la cryptographie asymétrique.

a. Chiffrement symétrique (utilisation de clefs privées) :

Aussi appelée cryptographie conventionnelle ou à clés secrètes ou privées, l'idée du chiffrement symétrique est de réaliser une transformation capable de rendre illisible (cryptage) et de restituer une pièce d'information (décryptage), basée sur l'utilisation d'une seule clef tenue secrète entre les deux intervenants (Alice et Bob dans le cas de la figure 1) i.e. seuls ces deux entités connaissent la clef. Afin de garantir donc que la clef est tenue secrète, son échange entre les deux intervenants doit se faire par un canal confidentiel alternatif (courrier postal, ...).

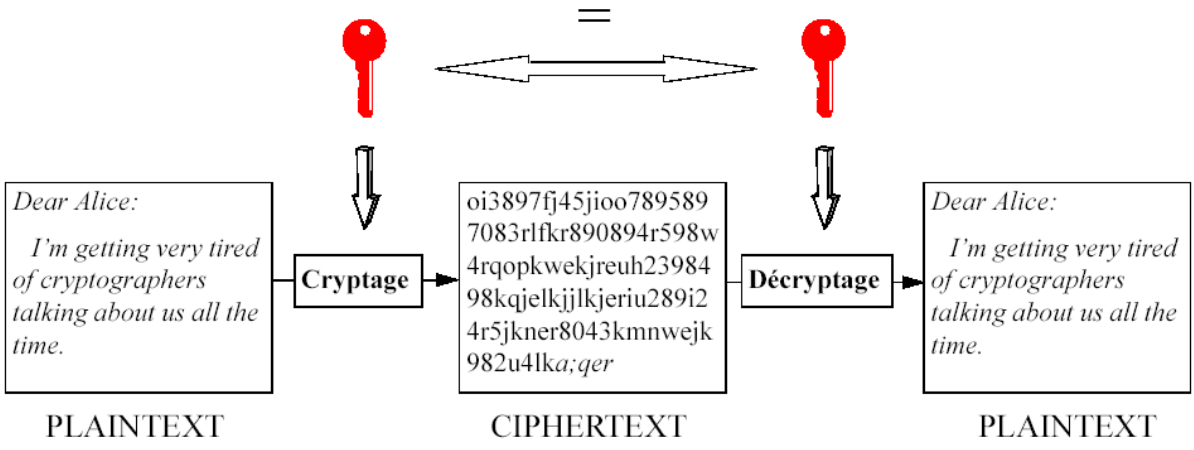


Figure 1: Chiffrement symétrique du dialogue entre Alice et Bob

Il existe des nombreux systèmes de cryptage symétriques (AES, DES, IDEA, RC4, RC5, etc.) [8, 9, 10, 11, 12,13] dont certains sont gratuits et de libre accès (open source) i.e. leur source code est disponible au grand public.

La cryptographie symétrique a pour objectifs la confidentialité, l'authentification et l'intégrité des données. Il est mieux adapté à la protection de documents personnels qu'à des transactions impliquant des grandes populations telles que le commerce électronique.

b. Chiffrement asymétrique :

Aussi appelée cryptographie publique ou à clés publiques (1976, W. Diffie & M. Hellman), le chiffrement asymétrique utilise deux clés différentes - une *secrète* et une *publique* - respectivement pour les opérations de cryptage et de décryptage. Chaque utilisateur dispose alors d'un *porte-clés* (*keyring*) contenant, au moins, sa clé publique et sa clé privée.

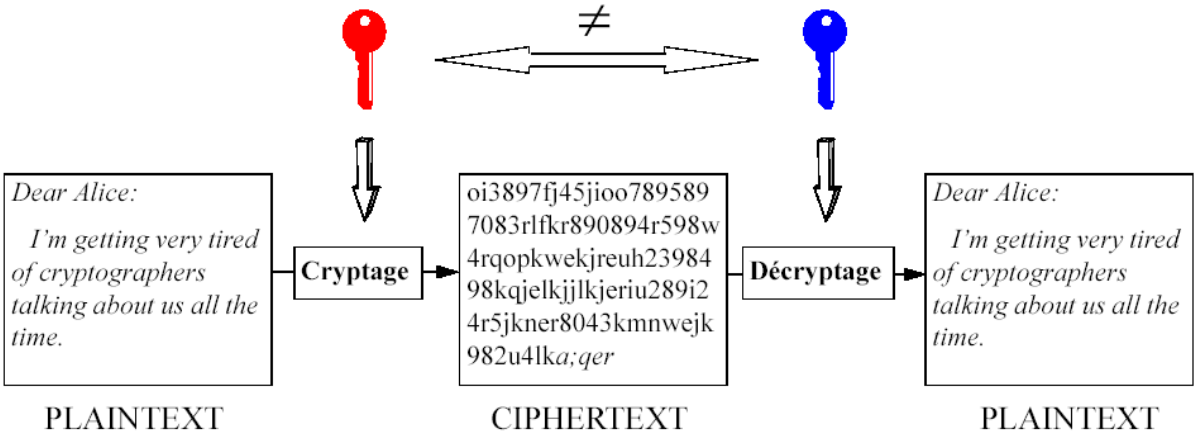


Figure 2: Chiffrement asymétrique du dialogue entre Alice et Bob

Principe de fonctionnement :

L'expéditeur dans notre cas Alice, crypte l'information avec la clé publique du destinataire (Bob) qui est globalement disponible. Le destinataire décrypte alors cette information cryptée avec sa clé privée i.e. connue de lui seul (cf. figure 3). Cette clef secrète n'est pas échangée alors entre les deux intervenants. Par conséquent, la nécessité d'une autre voie confidentielle n'est plus essentielle contrairement au chiffrement symétrique.

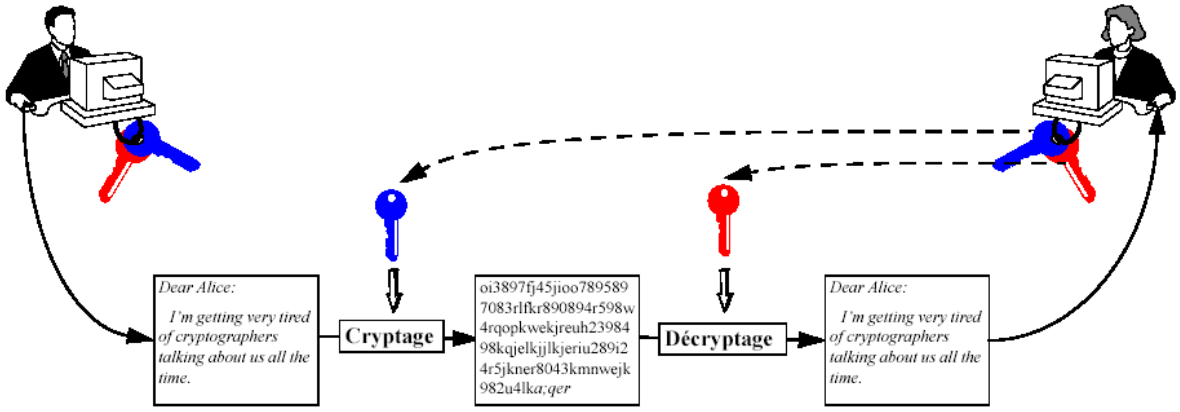


Figure 3: Principe de fonctionnement d'un chiffrement asymétrique. Seules les cles publique et prive du destinataire sont impliquees dans l'echange confidentielle des donnees.

Principe de la signature numérique :

La signature numérique ou digital signature est basée sur le chiffrement asymétrique [17].

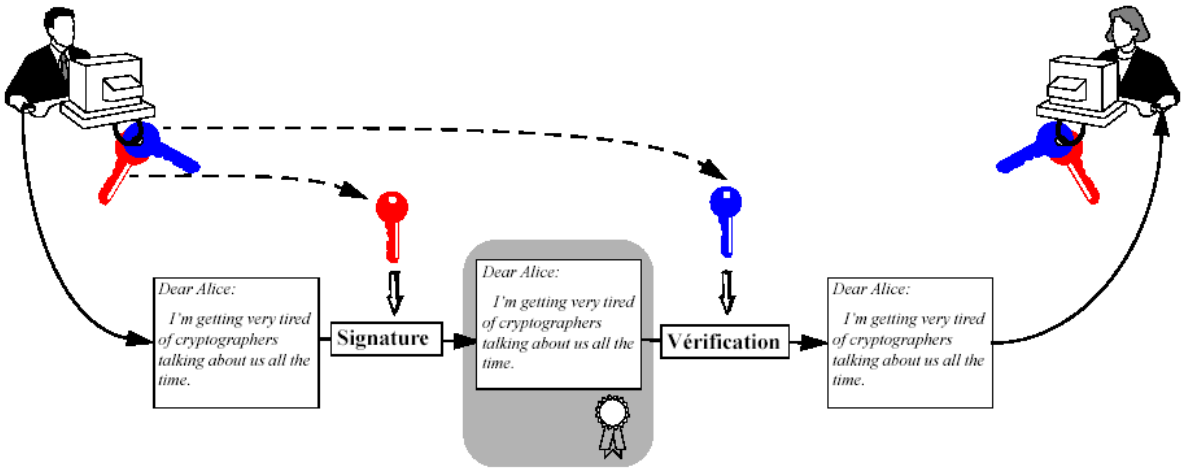
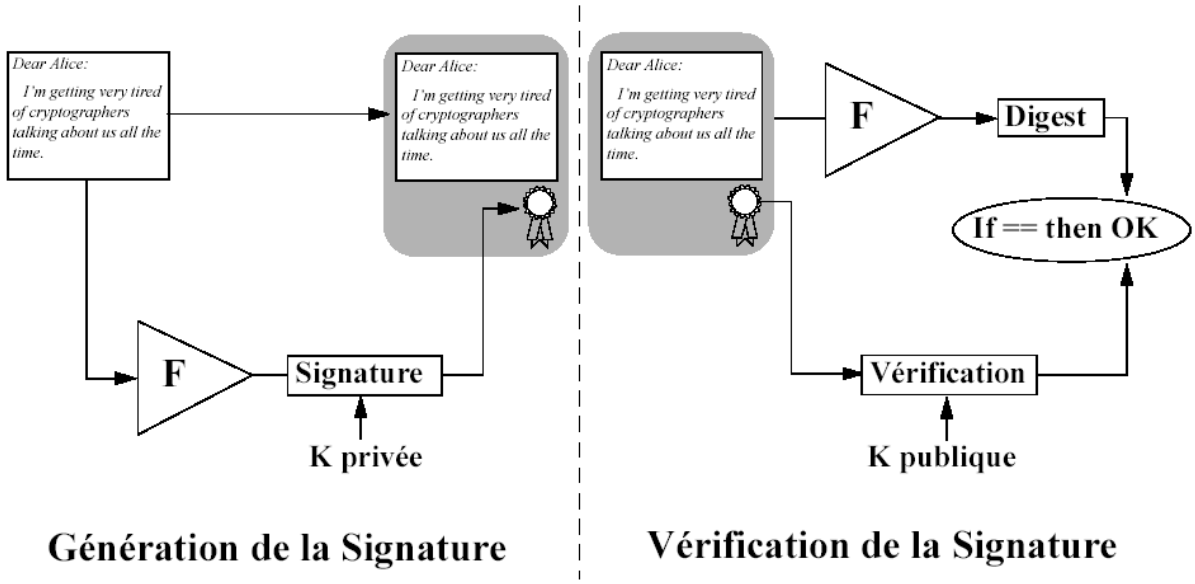


Figure 4: Principe de base de la signature numérique

L'expéditeur signe l'information avec sa clé privée (connue de lui seul) avant de la transmettre au destinataire. Quand le destinataire reçoit l'information, il vérifie sa signature avec la clé publique de l'expéditeur (globalement disponible).

Dans la pratique, la signature d'un document entier s'avère très lourde (chargement du CPU : temps de traitement). On recourt alors à la signature du digest du document résultant d'une fonction de hachage sur tout le document (cf. paragraphe précédente), comme le représente la figure suivante.



On applique la fonction de hachage h au document tout entier, et on obtient le digest F.

- On chiffre alors le digest obtenu F avec la clef privée de l'expéditeur pour obtenir sa signature.
- L'expéditeur envoie alors le document non chiffré conjointement avec la signature que l'on vient de calculer.

Quand le destinataire reçoit le document signé :

- D'une part, il vérifie la signature du document à l'aide de la clef publique du destinataire, i.e. il déchiffre la signature et doit obtenir le digest F du document entier.
- D'autre part, il calcule le digest du document entier avec la même fonction de hachage que l'expéditeur avait utilisé.
- Si ce document n'est pas alterné lors de la transmission, on trouvera le même digest F. Sinon, le document doit être changé ou la signature n'est pas celle de l'expéditeur. En effet, la signature change si le document change, la clé privée utilisée lors de la signature reste la même. Par conséquent, en cas de modification du document ou de la signature, la signature ne sera pas vérifiée (l'intégrité du document est alors garantie). En outre, il est virtuellement impossible (même pour le détenteur de la clé privée) de générer un deuxième document avec la même signature (la fonction à sens unique est sans collisions) et seul le détenteur de la clé privée peut générer une signature qui se vérifie avec la clé publique correspondante. Ces dernières caractéristiques de la signature digitale garantissent l'authentification et le service de non répudiation de l'expéditeur.

1.1.6.1.2. Principe d'authentification

Les types de secrets utilisés pour l'authentification sont ce que l'on a (carte à puce), ce que l'on sait (nom d'utilisateur et le mot de passe), et ce que l'on est (biométrie)

Authentification faible :

L'utilisateur présente un couple (*userid*, *password*) au système afin de s'identifier. Le *userid* étant l'identité prétendue et le *password* l'évidence corroborant. Les systèmes d'authentification faible sont divisés en deux catégories principales: l'authentification à mot de passe fixe et celle à mot de passe variable.

Authentification par mot de passe fixe :

Le mot de passe ne dépend pas du temps ni du nombre de fois que le protocole d'identification a été exécuté. Cette catégorie inclue les systèmes où le mot de passe est changé par décision de l'utilisateur ou par mesure de sécurité du système (ex : le nom d'utilisateur et mot de passe de l'utilisateur de Windows).

Pour être authentifié, l'utilisateur présente un couple (*userid*, *password*) au système afin de s'identifier. Le *userid* étant l'identité prétendue et le *password* l'évidence corroborant. Le système compare alors le couple (userid, password) avec ceux stockés dans la base de données, et en découle si l'identité est acceptée (authentifiée) ou refusée.

Ce stockage du password peut être *en clair ou encrypté.* Dans le cas où il est stocké en clair, le fichier est protégé par les mécanismes de contrôle d'accès propres au système d'exploitation. Ce type de stockage présente des problèmes tels que les failles dans le OS, privilèges du "super-user", *backups*, etc. Le stockage du password encrypté est le résultat d'une *one-way function* appliquée au password (éventuellement en rendant publique l'accès à ce fichier, cf. exemple UNIX). Mais ce système de stockage présente aussi des problèmes tels que les attaques *off-line,* ie. *guessing attacks, brute-force dictionary attacks, identification de collisions, etc.*

En outre, l'authentification faible à mot de passe fixe est vulnérable aux attaques par le rejeux. L'écoute des trafics du réseau non protégé présente alors une très haute menace pour la sécurité du système. Cette situation conduit alors au développement de plusieurs techniques de protection des systèmes de password fixe :

- Règles strictes de comportement concernant la création, le maintien et la mise à jour des passwords en tenant compte de la faible entropie des passwords choisis habituellement par les utilisateurs.

- Ralentir le processus d'identification ainsi que limiter le nombre d'essais infructueux afin de contrer les "*on-line brute force attacks*".
- Le technique de salting (UNIX).
- Restreindre ou même éviter la diffusion des fichiers de mots de passe, même encryptés.

Authentification par mot de passe variable :

Le système d'authentification par le password variable demande la modification du password en fonction du temps et/ou du nombre d'exécutions fait partie du protocole d'identification. Les deux techniques les plus connues d'identification par password variable sont les *one time passwords* et les *générateurs (hardware) de nombres aléatoires.*

a. One time password (OTP)

Définition:

Le protocole OTP est un mécanisme d'authentification basée sur le mot de passe. Il est conçu pour protéger contre les attaques de rejeux (password sniffing). Il utilise des fonctions de hachage (MD5) et un défi.

Fonctionnement :

L'utilisateur A, l'entité devant prouver son identité choisit un secret W qui contient au moins 10 caractères. Le système B, l'entité chargée de vérifier cette identité de A, envoie à A un nombre aléatoire appelé 'seed' S de longueur 1 à 16 caractères. Ces deux valeurs W et S sont utilisées par A pour générer la séquence de OTP qu'il doit utiliser pour s'identifier auprès de B. La figure 1 montre l'organigramme utiliser pour ce calcul.

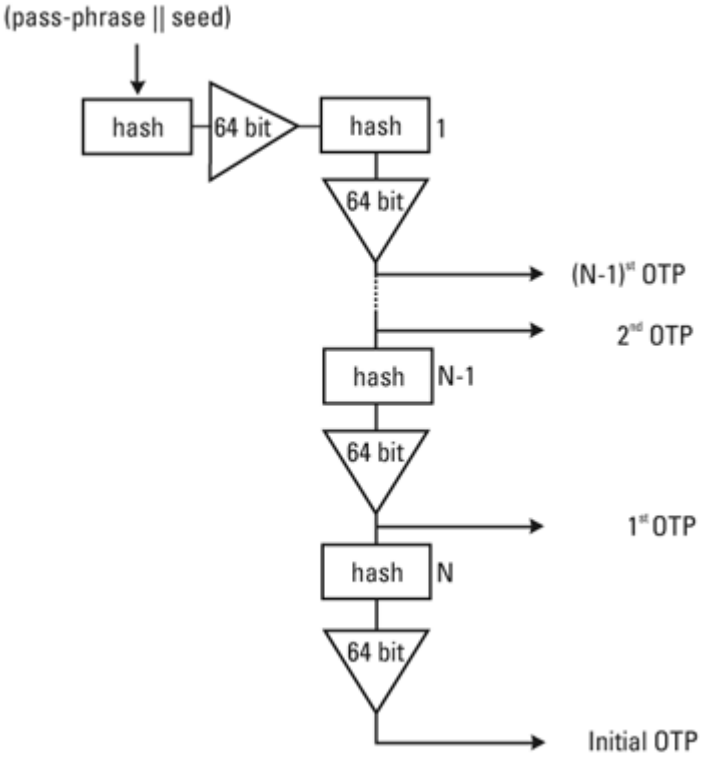


Figure 5: Génération de séquence d'OTP

La génération est initialisée par le hachage du secret w concatiné avec le seed t. Le résultat obtenu est de longueur 64bits. Ce résultat est re-haché N fois pour engendrer la séquence de N OTPs que A utilisera pour s'authentifier auprès de B où N est le nombre d'identifications que l'on choisira. La dernière OTP engendrée est l'OTP utilisé par A pour initialiser son authentification. Il est à noter que cet OTP initial doit être échangé sur un canal sûr afin que les attaquants ne puissent l'intercepter.

Afin d'authentifier A, B envoie un défi à A sous le format suivant :

otp-<identification de l'algorithme><numéro de l'itération courante><seed>

Par exemple, 'otp-md5 487 dog2'. Le seed et le numéro de l'itération courante sont les paramètres que l'utilisateur peut utiliser pour calculer le bon OTP et de l'envoyer au serveur d'authentification pour une vérification.

Le serveur B tient dans une base de données les derniers OTPs admis, ou les OTPs initiaux de tous les utilisateurs, leurs seeds ainsi que les itérations courantes correspondantes à ces derniers OTPs. Pour vérifier le OTP reçu d'un utilisateur, il le hache et compare le résultat obtenu avec le dernier OTP admis stocké dans la base de données correspondant à cet utilisateur. Par exemple, A envoie le premier OTP (1erOTP) à B. B hache alors ce OTP, i.e. h(1erOTP) = OTP initial. Il compare ensuite ce résultat calculé avec le OTP initial dans sa base de données. Si les valeurs calculées et

stockées sont égales, alors l'authentification de A est réussie et ce nouveau OTP est stocké dans la base de données de B, et le numéro d'itération est diminué de 1. Si ce numéro d'itération est réduit à 0 (i.e. tous les OTPs sont utilisés), A doit choisir un nouveau secret w, et la génération de OTPs est à refaire.

Attaques sur le OTP:

Si une machine C arrive à intercepter un OTP, elle ne peut pas générer l'OTP suivant car la fonction de hachage est à sens unique. Le mot secret w n'est jamais échangé durant toute l'opération d'authentification. Cependant, il existe une possibilité qu'un attaquant écoute la ligne de communication et réussi à récolter de nombreux OTPs, il peut alors deviner le numéro d'itération et générer tous les OTPs restants, puis les utiliser avant que l'utilisateur légitime aie la possibilité de les utiliser (pre-play attack). Cette attaque peut être prévenue en mettant en oeuvre un mécanisme qui assure qu'un procès d'authentification ne peut être initié qu'après la terminaison d'une autre. Le OTP n'assure pas la protection des données échangées après la réussite d'une authentification.

b. Générateur de nombres aléatoires:

Il s'agit des cartes à puces qui génèrent périodiquement (~ tous les 30 ou 60 secs) des nombres différents servant à identifier le détenteur de la carte. La génération se fait à partir d'une clé secrète présente sur la carte et connue du système.
Le générateur de nombres aléatoires le plus connu est *SecureId* fabriquée par *Security Dynamics*, qui génère un nombre à 6-digits valables pour 60 secondes. La carte a été adopté par des nombreuses banques (dont le *Crédit Suisse*) comme support d'authentification du *tele-banking* sur Internet.
Comme le OTP, le générateur de nombres aléatoires est également exposé au *pre-play attack* mais le délai pour rejouer le password se limite à la fréquence de changement (30 ou 60 sec).

Authentification forte

Contrairement à l'authentification faible, le secret permettant de corroborer l'identité n'est pas révélé explicitement mais, plutôt, l'utilisateur fournit au système d'authentification une preuve de possession de ce secret.
Le protocole d'authentification forte utilise les techniques de la cryptograhie.

Authentification à transfert nul de connaissance (zero-knowledge protocol) :

Ce sont des protocoles d'authentification forte qui ont en plus la caractéristique de prouver l'identité de l'utilisateur sans dévoiler aucune information (ni même une piste...) sur le secret lui même. En d'autres mots, il s'agit de donner une preuve d'une assertion sans en révéler le moindre détail.

1.1.6.1.3. Principe de contrôle d'accès

Le contrôle d'accès fournit un service de sécurité visant à vérifier la légitimité de l'accès d'une entité aux ressources du SI. L'autorisation d'accéder à un élément du SI dépend principalement de ce contrôle d'accès [32]. Par exemple, les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section. Le contrôle d'accès peut être implémenté sous plusieurs formes telles que le ACL ou liste de contrôle d'accès, listes de capacités, tables d'autorisation. Le contrôle d'accès peut être catégoriser en deux grandes familles : le contrôle d'accès basé sur l'identité de l'utilisateur et celui basé sur le rôle. Mais il existe des méthodes d'implémentation dérivées de la combinaison de ces modèles, comme le mur de chine, visant à affiner et adapter au mieux le contrôle d'accès logique suivant l'activité de l'organisation.

Présentation générale du contrôle d'accès logique

Le contrôle d'accès ou CA est réalisé par un 'moniteur de référence' ou 'arbitre de référence' qui accepte ou refuse chaque tentative d'accès aux éléments du SI par une entité i.e. utilisateur ou les programmes exécutés sur demande de l'utilisateur, afin que l'on puisse restreindre leurs actions vis-à-vis de leurs privilèges. L'arbitre de référence consulte une base de données de privilèges de chaque entité afin de vérifier la légitimité d'une tentative d'accès. Cette base de données a été conçue suivant les mécanismes de contrôle d'accès qui est dicté par la politique de sécurité de l'organisation. On note que le contrôle d'accès considère que l'identité de l'utilisateur a été préalablement vérifiée avant d'appliquer le contrôle d'accès via un moniteur de référence.

a. Matrice des contrôles d'accès :

La matrice des droits d'accès est une représentation conceptuelle des autorisations d'un système. Il s'agit d'un tableau représentant les droits et modes d'accès des entités aux ressources du système. On remarquera que la possession d'une ressource est considérée comme un droit.

Tableau 3: Exemple de matrice des droits d'accès

	Ressources			
Entités	Fichier1	Fichier2	Fichier3	Imprimante
Utilisateur1	Lire, écrire, executer	Lire	Lire, ecrire	Utiliser
Utilisateur2	Rien	rien	Lire	Pas utiliser
Utilisateur3	Rien	Lire, ecrire	Lire, ecrire, execter	Pas utiliser

b. Listes de contrôles d'accès :

Les listes de CA ou ACLs sont un moyen d'implémenter la matrice des droits d'accès. Chaque entité est associée à une liste de contrôle d'accès, contenant les autorisations d'accès pour chacun des ressources du système. Une ACL correspond donc à une colonne de la matrice des droits. A chaque accès, on vérifie que l'entité possède les droits conformes à l'opération demandée.
Les ACL offrent la possibilité de consulter rapidement les autorisations des entités pour une ressource. Il est ainsi très facile de révoquer toutes les autorisations sur une ressource en remplaçant son ACL par une ACL vide. En revanche, il est beaucoup plus difficile de déterminer tous les objets auxquels une entité a le droit d'accéder. Les ACLs sont largement utilisés dans les systèmes d'exploitation.

c. Listes des capacités (C-lists) :

Les listes de capacités ou listes d'habilitations sont une implémentation de la matrice des droits d'accès 'inverse' par rapport aux ACLs, en ce sens qu'une liste de capacités correspond à une ligne de la matrice d'accès. Ainsi, une liste de capacités est associée à chacun des entités du système, et définit les droits d'accès aux ressources du système pour l'entité associée.
Contrairement aux ACLs, les C-lists permettent une consultation et révocation rapide de tous les droits d'une entité sur les ressources du système, mais rendent difficile la vérification de toutes les autorisations associées à une entité donnée.

Relations d'autorisation

La relation d'autorisation est un tableau au sein duquel chaque ligne définit un mode d'accès pour une entité à une ressource.

Tableau 4: Relation d'autorisation extraite de la matrice des droits d'accès (cf. tableau1)

Entités	Droits d'accès	Ressources
Utilisateur1	Lire, ecrire, executer	Fichier 1
Utilisateur1	Lire, ecrire	Fichier 2
Utilisateur1	Utiliser	imprimante
Utilisateur2	Rien	Fichier 1
Utilisateur2	lire	Fichier 3
Utilisateur2	Pas utiliser	imprimante
Utilisateur3	Lire, ecrire, executer	Fichier 3
Utilisateur3	Pas utiliser	imprimante

Si l'on trie ce tableau par rapport à la colonne 'Entités', on obtient les C-lists. Si on trie le tableau par rapport à la colonne 'Ressources', on obtient les ACLs. Cette approche est principalement employée au sein des systèmes de gestion de bases de données relationnelles.

Les modèles de contrôle d'accès :

a. Contrôle d'accès basé sur l'identité :

Le contrôle d'accès discrétionnaire (DAC Discretionary access control) :

Le modèle de contrôle d'accès DAC a été défini en 1976 par Harrison, Ruzzo et Ullman, appelé aussi HRU. Le concept principal de DAC est que le propriétaire d'une ressource (la plupart des temps son créateur), a une autorité absolue sur l'accès à cette ressource. Autrement dit, le noyau de la politique DAC est une administration basée sur la propriété de l'information.

Dans la politique de DAC, le propriétaire peut accorder les droits d'accès à une autre entité. Certaines variantes de politiques de contrôle d'accès discrétionnaires offrent la possibilité de déléguer à une autre entité les droits d'accorder l'accès.

Lors d'une tentative d'accès, les autorisations sont vérifiées afin de déterminer si le type d'accès demandé est autorisé pour l'entité en question. Si aucune entrée correspondante n'est trouvée, alors l'accès est refusé dans le cas des politiques 'fermées' i.e. 'refuser tout sauf' ; en revanche, l'accès est accepté dans le cas des politiques 'ouvertes' si aucune entrée ne correspond i.e. 'accepter tout sauf'.

b. Le contrôle d'accès mandataire ou (MAC Mandatory Access Control)

Les politiques de contrôle d'accès mandataire reposent sur la classification des objets et des sujets d'un système. Chaque utilisateur et chaque objet sont associés à un niveau de sécurité.

Le niveau de sécurité d'un objet reflète la sensibilité des informations contenues dans cet objet, c'est-à-dire, les éventuels dommages engendrés par une diffusion ou une modification non autorisée de l'information.

Le niveau de sécurité attribué à un sujet (appelé « clearance » en anglais), traduit le degré de confiance placée dans le sujet à ne pas révéler des informations aux autres utilisateurs de niveau plus bas. Ce niveau de sécurité pourrait par exemple être établi suivant la position hiérarchique.

Dans le milieu militaire et gouvernemental, ces niveaux sont 'diffusion restreinte', 'confidentiel défense', 'secret défense', et 'très secret défense'. La 'diffusion restreinte' représente les informations non classifiées mais concernant le patrimoine scientifique, technique, industriel, économique ou diplomatique (on dit que ce niveau est « dominé » par tous les autres), et la mention « très secret défense » est réservée aux informations dont la divulgation est de nature à nuire à la Défense nationale et à la sûreté de l'État (ce niveau « domine » tous les autres).

L'accès à un objet par un sujet est accordé si les deux niveaux de sécurité associés sont compatibles. Les modèles de contrôle d'accès mandataires peuvent remplir des objectifs différents :

- assurer la confidentialité des informations,
- ou garantir l'intégrité des informations.

Il existe plusieurs modèles pour l'implémentation du MAC.

<u>Le modèle Bell-La Padula :</u>

Bell et La Padula développèrent en 1975 un modèle de contrôle d'accès mandataire appelé « Lattice-Based Access Control » (Contrôle d'accès basé sur les treillis) ou LBAC, pour la Défense américaine. Ce modèle traite les flux d'informations afin d'en assurer la confidentialité. Il repose sur deux grands principes :

« read down » : le niveau de sécurité d'un sujet doit dominer le niveau de sécurité d'un objet afin que la lecture soit autorisée,

« write up » (aussi appelé « propriété étoile », « *-property » en anglais) : le niveau de sécurité d'un sujet doit être dominé par le niveau de sécurité de l'objet dans lequel il souhaite écrire.

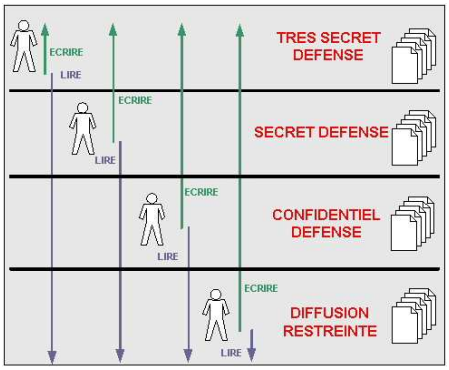


Figure 6: Modèle Bell-La Padula: contrôle du flux d'informations pour la confidentialité

Ce principe permet de régler le problème des chevaux de Troie : en effet, si le système met en oeuvre un contrôle d'accès de ce type, aucune information ne peut « fuir » vers un niveau de classification inférieur :

- d'une part, on ne peut lire des informations ayant un niveau de sécurité plus élevé que le « clearance » (« read down »), il est donc exclus d'accéder directement à une information « secret défense » si l'on est classé « confidentiel »,
- d'autre part, un sujet ne peut divulguer des informations vers un niveau de sécurité plus bas, il est donc impossible de consulter une information classée « secret défense » et de l'envoyer par mail à un sujet « confidentiel » par exemple.

Dans le cas d'un Cheval de Troie, les informations captées par ce programme ne pourront être diffusées vers un niveau de sécurité inférieur.

Cependant, un grand inconvénient de ce modèle est qu'un utilisateur ayant un niveau de sécurité « confidentiel » peut écrire et donc endommager un objet classé « très secret défense ». Pour pallier cette faille, « la propriété étoile » (« write up ») peut être modifiée afin de n'autoriser l'écriture que dans les objets ayant le même niveau de sécurité que le sujet.

Le modèle de Biba :

C'est un modèle complémentaire à celui de Bell et La Padula qui s'attache à protéger l'intégrité des informations.

Pour cela il se base sur les deux principes suivants :

- « read up » : le niveau de sécurité d'un objet doit dominer la « clearance » du sujet afin d'être accessible en lecture par ce dernier,
- « write down » (« *-property ») : un sujet doit être associé à un niveau de sécurité supérieur à celui de l'objet qu'il souhaite écrire.

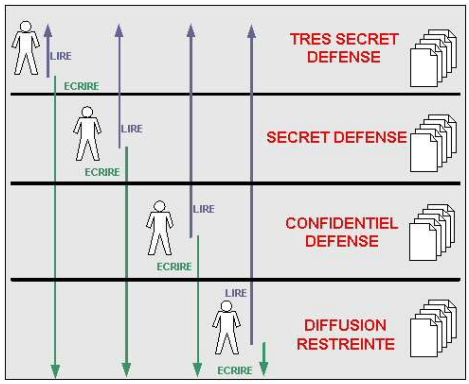


Figure 7: Modèle de Biba: contrôle de flux d'informations pour l'intégrité

Ce modèle prévient les modifications inattendues, ou non autorisées des informations sensibles par des sujets non qualifiés, ou n'ayant pas un niveau de confiance suffisant.
Inversement, ce modèle ne résout pas le problème du Cheval de Troie, c'est-à-dire la fuite d'informations vers le bas, qui peut être résolu, de la même manière que pour le modèle Bell-La Padula en modifiant « la propriété étoile » afin de n'autoriser l'écriture à un sujet que pour les objets de même niveau.

c. Contrôle d'accès basé sur les rôles (RBAC Rule-based Access Control)

Objectifs :

Les différentes techniques vues dans les chapitres précédents ont leurs avantages, mais présentent presque toutes un inconvénient au niveau de l'administration des autorisations (complexité de la révocation et de la revue des droits, lourdeur dans l'attribution des autorisations, …). De plus, l'utilisation de ces techniques ne permet pas forcément de se conformer à la politique de sécurité de l'organisation.
C'est donc dans l'optique de fournir un standard dans le domaine de la gestion du contrôle d'accès, de se calquer aux besoins des entreprises et de faciliter l'administration des autorisations que Ferraiolo et Kuhn ont introduit en 1992 le contrôle d'accès basé sur les rôles. Promu par le NIST (National Institute of Standards and Technology) et reconnu comme standard américain le 19 février 2004 (AINSI INCITS 359-2004), RBAC s'impose progressivement dans le domaine du contrôle d'accès.
Ses objectifs principaux sont les suivants :

- décrire une politique de contrôle d'accès complexe,
- réduire les erreurs d'administration,

- réduire les coûts de l'administration

Principes fondamentaux :

RBAC repose sur trois grands principes :

- Les utilisateurs se voient attribuer des rôles,
- Les rôles sont associés à des permissions/autorisations,
- Un utilisateur possède une autorisation s'il est autorisé à utiliser un rôle associé à cette autorisation.

L'ouverture d'une session permet à l'utilisateur d'activer ces rôles (les implémentations de RBAC diffèrent sur ce point, dans certains cas, l'utilisateur aura le choix des rôles à exercer, dans d'autres, le ou les rôles associés lui seront imposés).

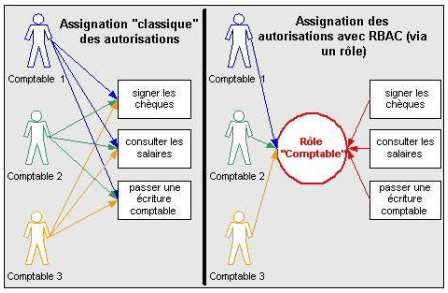


Figure 8: Assignation des autorisations, avec et sans RBAC (ampiana role hafa ankoatran ny comptable)

On peut aisément déduire de la Figure 3 le gain de temps conséquent à l'utilisation d'un modèle RBAC :

Soit U l'ensemble des utilisateurs ayant les mêmes tâches à accomplir et A les autorisations requises par ces utilisateurs pour effectuer leurs tâches, alors on a :

- Sans RBAC : (UxA) associations autorisations / utilisateurs
- Avec RBAC : (U+A)

  Le gain représenté par RBAC peut s'exprimer ainsi : (U+A) < (UxA), avec U et A > 2
- Sur l'ensemble des postes dans une entreprise :

  La somme des affectations de l'entreprise avec RBAC(S(Ui+Ai)) est inférieure à la somme des affectations sans RBAC (S(UixAi))

RBAC introduit également le concept de hiérarchie et d'héritage des rôles : « comptable » hérite d' « employé » par exemple, ainsi qu'un certain nombre de contraintes permettant d'affiner la politique de contrôle d'accès logique :

Séparation des tâches : il s'agit d'interdire une même personne d'effectuer deux tâches normalement séparées; par exemple un même employé ne doit pas être à la fois guichetier (encaissement des chèques) et comptable, afin de rendre la fraude plus difficile, il faudrait alors que deux employés soit corrompus. RBAC présente deux types de séparation de tâches :

Séparation statique des tâches : un utilisateur ne peut pas à la fois **affecter** le rôle de guichetier et contrôleur de caisse.

Séparation dynamique des tâches : un utilisateur ne peut pas **exercer** simultanément le rôle de guichetier et comptable.

Cardinalité des rôles : limite le nombre d'utilisateurs ayant le même rôle (exemple : il ne peut y avoir qu'un seul comptable, cinq guichetiers maximum …).

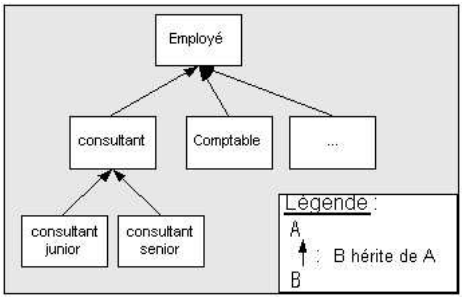


Figure 9: Héritage des rôles

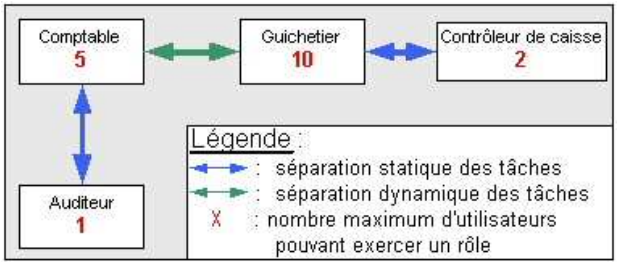


Figure 10: Contraintes de cardinalité et de séparation des tâches

En général, RBAC est implémenté dans les systèmes de gestion de bases de données ou au niveau d'applications spécifiques. Il peut en outre être simulé à l'aide des groupes d'utilisateurs.

Détecteur d'intrusion (IDS)

IDS signifie Système de Détection d'Intrusion (Intrusion Detection System) [31, 33, 34]. Dans la littérature, IDS est défini en tant que système combinant un système logiciel et/ou matériel capable de détecter en temps réel les tentatives d'intrusion sur un réseau interne ou sur un seul ordinateur hôte, de neutraliser ces attaques et d'assurer ainsi la sécurité du réseau d'entreprise. Il essaie de découvrir si la sécurité d'un hôte ou d'un réseau est menacée (s'il est "attaqué") afin de prendre les mesures de protection qui s'imposent. Puisque dans la plupart des cas, des fichiers de log sont créés, l'essentiel consiste à les analyser et à réagir à une intrusion ou à une tentative illégale d'un utilisateur d'augmenter ses droits.

Deux méthodes sont principalement utilisées par les IDS : la reconnaissance de signatures (knowledge-based) et la détection d'anomalies (behavior-based). La reconnaissance de signature est une approche consistant à rechercher dans l'activité de l'élément surveillé les signatures (ou empreintes) d'attaques connues. Le IDS fait appel à une bibliothèque de signatures (base de données) et ne peut alors détecter que les attaques dont il possède la signature. De son côté, la détection d'anomalies utilise l'analyse du statistiques du système : changement de mémoire, utilisation excessive de CPU,.... Le IDS signalera les divergences par rapport au fonctionnement normal (ou de référence) des éléments surveillés.

Contrairement au firewall, qui traite des requêtes et les interdits, un IDS les analyse de façon continue et ne réagit qu'en cas d'anomalie.

Puisqu'il existe une multitude de possibilités d'attaques contre le SI, on a développé différents types d'IDS qui assurent l'écoute et l'analyse des différentes branches selon l'endroit qu'ils surveillent et ce qu'ils contrôlent (les Sources d'Information). Ainsi, on inventorie le système d'intrusion basé sur le hôte (HIDS), le système d'intrusion basé sur le réseau (NIDS), le système d'intrusion basé sur le nœud réseau (NNIDS), le système d'intrusion basé sur l'application.

a. Le système d'intrusion basé sur l'hôte HIDS (Host-based IDS) :

Les systèmes de détection d'intrusion basés sur l'hôte analysent exclusivement l'information concernant une hôte. Il détecte les outrepassements de droits (obtention du compte root d'une manière suspecte) et d'autres types d'attaques, il contient une base de données sur différentes vulnérabilités.

Comme ils n'ont pas à contrôler le trafic du réseau mais "seulement" les activités d'une hôte ils se montrent habituellement plus précis. De plus, on remarque immédiatement l'impact sur la machine

concernée comme par exemple si une attaque avait été conduite avec succès. Les HIDS utilisent deux types de sources pour fournir une information sur l'activité : les journaux (log files) et les traces d'audit (auditing trails) du système d'exploitation. Les traces d'audit sont plus précises et détaillées et fournissent une meilleure information alors que les logs qui ne fournissent que l'information essentielle sont de taille plus petites. Les logs peuvent être alors mieux contrôlés et analysés en raison de leur taille.

Avantages de HIDS

- Avec le HIDS, on peut détecter des attaques impossibles à détecter avec des IDS réseau puisque le trafic y est souvent crypté.
- On peut observer les activités sur l'hôte avec précision

Inconvénients de HIDS

- L'analyse des traces d'audit du système est très contraignante en raison de la taille de ces dernières
- L'analyse des logs et auditing trails consomment beaucoup de ressources CPU.

b. Système de détecteur d'intrusion basé sur le réseau NIDS :

Le rôle essentiel d'un IDS réseau est l'analyse et l'interprétation des paquets circulant dans le réseau. Afin d'examiner les paquets au contenu suspect, comme par exemple /etc/passwd, des signatures sont créées. Principalement, des capteurs (souvent de simples hôtes) sont utilisés qui ne font rien d'autre que d'analyser le trafic et si nécessaire d'envoyer une alerte. Puisqu'il s'agit de leur unique tâche il est facile de mieux les sécuriser. Dans ce contexte, le "stealth mode" (mode furtif) est souvent choisi, c'est-à-dire que les capteurs agissent de manière invisible et il devient ainsi plus difficile pour un attaquant de les localiser et de les atteindre.
Le NIDS contient une base de données des codes malicieux et peut détecter leurs envois sur une des machines. Le NIDS travaille comme un *sniffer* sauf qu'il analyse automatiquement les flux de données pour détecter une attaque.

1.1. Sécurité de la communication

1.2.1 Le modèle de référence OSI (Open system interconnect)

1.2.1.1 Pourquoi un modèle de référence :

Pour résoudre le problème de l'incompatibilité des réseaux et leur incapacité à communiquer entre eux, l'*Organisation internationale de normalisation* (***ISO***) a mis au point un modèle de réseau pour aider les fournisseurs à créer des réseaux compatibles avec d'autres réseaux [18, 19, 20].

Le *modèle de référence* ***OSI*** (Open System Interconnexion - interconnexion de systèmes ouverts) , publié en 1984, a ainsi été créé comme une architecture descriptive. Ce modèle a offert aux fournisseurs un ensemble de normes assurant une compatibilité et une interopérabilité accrues entre les divers types de technologies réseau produites par de nombreuses entreprises.

Le modèle de référence OSI est le principal modèle des communications réseau. Bien qu'il en existe d'autres, la majorité des fournisseurs de solutions réseau relient aujourd'hui leurs produits à ce modèle de référence, en particulier lorsqu'ils souhaitent former les utilisateurs à l'exploitation de leurs produits. Ils le considèrent comme le meilleur outil offert pour décrire l'envoi et la réception de données sur un réseau.

Le modèle de référence OSI permet de voir les fonctions réseau exécutées au niveau de chaque couche. Plus important encore, ce modèle de référence constitue un cadre qu'on peut utiliser pour comprendre comment les informations circulent dans un réseau. On peut en outre se servir du modèle de référence OSI pour visualiser comment les informations, ou paquets de données, circulent à partir des programmes d'application (ex. : tableurs, documents, etc.), en passant par un média réseau (ex. : fils, etc.), jusqu'à un autre programme d'application se trouvant sur un autre ordinateur en réseau, même si l'expéditeur et le destinataire utilisent des types de médias réseau différents.

1.2.1.2. Avantages du modèle OSI

Le modèle de référence OSI comporte sept couches numérotées, chacune illustrant une fonction réseau bien précise. Cette répartition des fonctions réseau est appelée *organisation en couches*. Le découpage du réseau en sept couches présente les avantages suivants :

- Il permet de diviser les communications sur le réseau en éléments plus petits et plus simples.

- Il uniformise les éléments du réseau afin de permettre le développement et le soutien multi constructeur.
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux.
- Il empêche les changements apportés à une couche d'affecter les autres couches, ce qui assure un développement plus rapide.
- Il divise les communications sur le réseau en éléments plus petits, ce qui permet de les comprendre plus facilement.

1.2.1.3. Les sept couches du modèle OSI

Dans le modèle de référence OSI, le problème consistant à déplacer des informations entre des ordinateurs est divisé en sept problèmes plus petits et plus faciles à gérer. Chacun des sept petits problèmes est représenté par une couche particulière du modèle. Voici les sept couches du modèle de référence OSI :

Couche 7 : la couche application
Couche 6 : la couche présentation
Couche 5 : la couche session
Couche 4 : la couche transport
Couche 3 : la couche réseau
Couche 2 : la couche liaison de données
Couche 1 : la couche physique

1.2.1.4. Les fonctions de chaque couche

Chaque couche du modèle OSI doit exécuter une série de fonctions pour que les paquets de données puissent circuler d'un ordinateur source vers un ordinateur de destination sur un réseau.

Couche 7 : La couche application

La couche application est la couche OSI la plus proche de l'utilisateur. Elle fournit des services réseau aux applications de l'utilisateur. Elle se distingue des autres couches en ce sens qu'elle ne fournit pas de services aux autres couches OSI, mais seulement aux applications à l'extérieur du modèle OSI. Voici quelques exemples de ce type d'application : tableurs, traitements de texte et logiciels de terminaux bancaires. La couche application détermine la disponibilité des partenaires

de communication voulus, assure la synchronisation et établit une entente sur les procédures de correction d'erreur et de contrôle d'intégrité des données.

Couche 6 : La couche présentation
La couche présentation s'assure que les informations envoyées par la couche application d'un système sont lisibles par la couche application d'un autre système. Au besoin, la couche présentation traduit différents formats de représentation des données en utilisant un format commun.

Couche 5 : La couche session
Comme son nom l'indique, la couche session ouvre, gère et ferme les sessions entre deux systèmes hôtes en communication. Cette couche fournit des services à la couche présentation. Elle synchronise également le dialogue entre les couches de présentation des deux hôtes et gère l'échange des données. Outre la régulation de la session, la couche session assure un transfert efficace des données, classe de service, ainsi que la signalisation des écarts de la couche session, de la couche présentation et de la couche application.

Couche 4 : La couche transport
La couche transport segmente les données envoyées par le système de l'hôte émetteur et les rassemble en flux de données sur le système de l'hôte récepteur. La frontière entre la couche transport et la couche session peut être vue comme la frontière entre les protocoles d'application et les protocoles de flux de données. Alors que les couches application, de présentation et session se rapportent aux applications, les quatre couches dites inférieures se rapportent au transport des données.

La couche transport tente de fournir un service de transport des données qui protège les couches supérieures des détails d'implémentation du transport. Pour être précis, les questions comme la façon d'assurer la fiabilité du transport entre deux systèmes hôtes relèvent de la couche transport. En fournissant un service de communication, la couche transport établit et raccorde les circuits virtuels, en plus d'en assurer la maintenance. La fourniture d'un service fiable lui permet d'assurer la détection et la correction des erreurs, ainsi que le contrôle du flux d'informations.

Couche 3 : La couche réseau

La couche réseau est une couche complexe qui assure la connectivité et la sélection du chemin entre deux systèmes hôtes pouvant être situés sur des réseaux géographiquement éloignés.

Couche 2 : La couche liaison de données

La couche liaison de données assure un transit fiable des données sur une liaison physique. Ainsi, la couche liaison de données s'occupe de l'adressage physique (plutôt que logique), de la topologie du réseau, de l'accès au réseau, de la notification des erreurs, de la livraison ordonnée des trames et du contrôle de flux.

Couche 1 : La couche physique

La couche physique définit les spécifications électriques, mécaniques, procédurales et fonctionnelles permettant d'activer, de maintenir et de désactiver la liaison physique entre les systèmes d'extrémité. Les caractéristiques telles que les niveaux de tension, la synchronisation des changements de tension, les débits physiques, les distances maximales de transmission, les connecteurs physiques et d'autres attributs semblables sont définies par la couche physique.

Sécurité des différentes couches

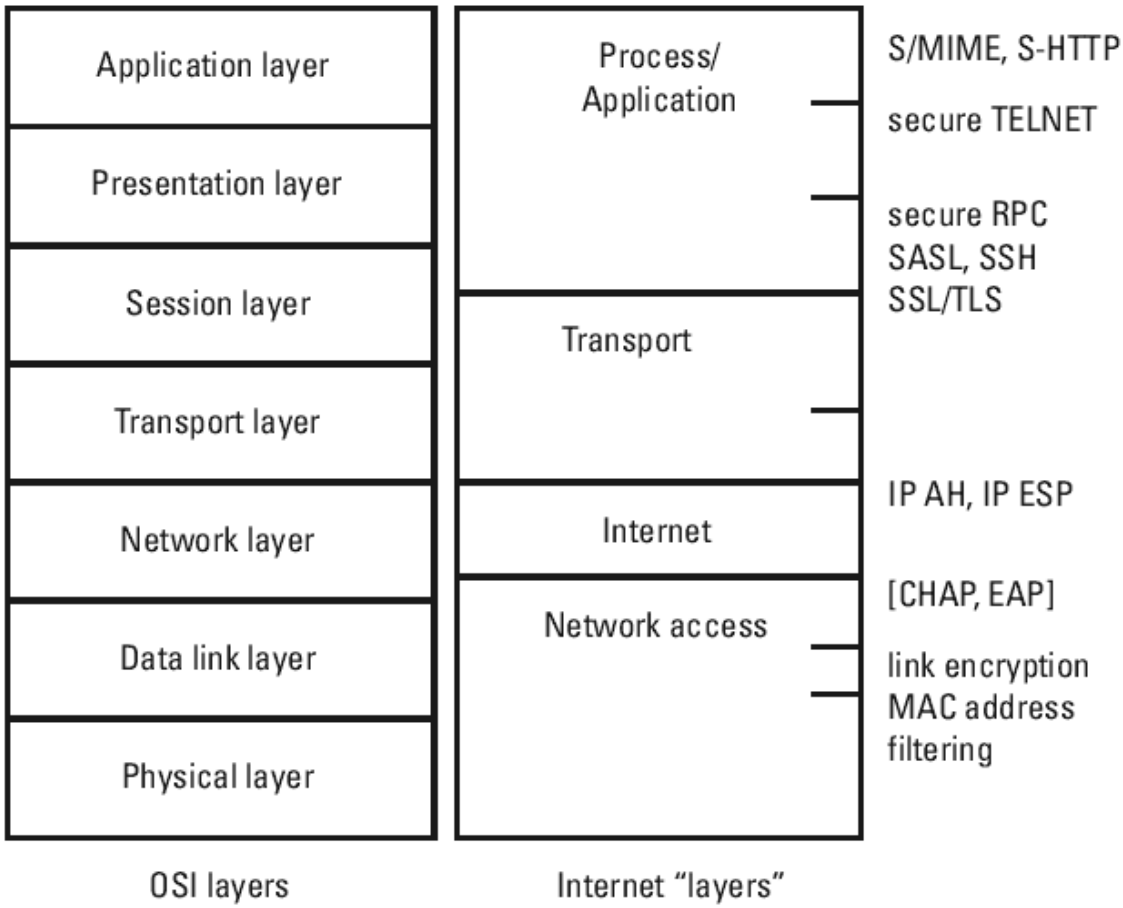


Figure 11 Les mécanismes de sécurité dans les différentes couches [20]

La figure 11 montre les différents mécanismes de sécurité habituels que l'on peut implémenter dans différentes couches du modèle TCP/IP. On peut voir quel protocole peut être sécurisé par quel mécanisme de sécurité. Par exemple, S/MIME peut être utilisé pour protéger les messages e-mail, et S-HTTP pour protéger les messages HTTP. Il est aussi possible pour les mécanismes de sécurité de basse couche de protéger les messages des protocoles de plus haute couche. Par exemple, IPSec AH et IPSec ESP peut protéger les segments TCP ou les datagrammes UDP encapsulés.

1.2.2.1. La couche d'accès au réseau :

Cette couche correspondant aux couches physique et liaison de données du modèle OSI. Elle offre seulement une communication point à point. La sécurité dans cette couche ne peut pas étendre la protection à travers des réseaux hétérogènes. Si le cryptage au niveau de la liaison est utilisé, les

deux bouts de chaque liaison doivent être équipée de dispositif de cryptage. De plus, le message doit être déchiffré à chacune des nœuds intermédiaires pour que les protocoles de plus haut niveau puissent traiter les informations de contrôle (adresse de la couche d'accès réseau et les informations de routage), puis ces nœuds les re-chiffrent. Cela nécessite que chaque paire de dispositif de cryptage partage la même clef, qui rend la gestion des clefs extrêmement difficile. En outre, puisque les messages sont décryptés à chaque nœud intermédiaire, elles sont exposées à des attaques emmenées sur ces nœuds, ce qui constitue un grand inconvénient de la sécurité au niveau de la couche d'accès au réseau.

1.2.2.2. Sécurité au niveau de la couche Internet :

Le principal avantage de placer le mécanisme de sécurité au niveau de la couche Internet est qu'il est transparent pour les utilisateurs et les applications [28, 40]. Cependant, la sécurité de cette couche nécessite le changement du système d'exploitation qui l'intègre. En outre, il est nécessaire que chaque hôte en communication emploie la même version du logiciel de sécurité utilisé au niveau de cette couche Internet. La mise à jour est alors très coûteuse et demande beaucoup de temps. De plus, si ces logiciels usités ne sont pas bien configurés, ils peuvent dégrader énormément le QoS du SI. Par exemple, si le cryptage est utilisé par défaut alors que l'application n'en a pas besoin, alors le temps de traitement est alourdi inutilement. Par addition, les mêmes paramètres de sécurité sont utilisés pour chaque connexion (i.e. les clefs de chiffrement basées sur l'hôte), qui offre une sécurité plus faible que celle offerte lorsque les paramètres de sécurité sont négociés de bout en bout (i.e. entre utilisateurs ou applications).

1.2.2.3. Sécurité de la couche application :

La sécurité de la couche application n'implique pas le changement du système d'exploitation qui l'intègre. Les mécanismes de sécurité offrent alors une meilleure protection de bout en bout car la configuration et le chiffrement ne dépendent pas du système d'exploitation. La gestion des clefs se fait au niveau de la couche d'application. Dans ce cas, les données ne sont pas exposées aux attaques liées aux faiblesses du système d'exploitation. De plus, le fonctionnement de la sécurité peut être configuré pour répondre exactement aux besoins de chaque application. Ainsi, les fonctionnements inutiles sont évités (par exemple le chiffrement de tout le trafic). Cependant, la négociation et la configuration entre les procédures communicantes peuvent être très complexes. Un autre inconvénient est que les applications sécurisées sont installées par des utilisateurs non

expérimentés, ce qui rend les risques de présence des codes malicieuses assez potentielles. Par exemple, le vol de mots de passe ou d'autres informations sensibles par la présentation d'un page de type formulaire simulé semblant être la page originelle (spoofing).

1.2.2.4. La sécurité de la couche transport :

La sécurité au niveau de la couche de transport [27] se place entre la couche application et la couche Internet (ex TLS). On peut la percevoir comme étant une interface sécurisée pour la couche de transport. D'une part, toutes les applications doivent utiliser les fonctions de sécurité correspondantes, d'autre part, la bibliothèque de sécurité de la couche de transport peut être installée et maintenue par le sysadmin alors toutes les applications installées sur les machines hôtes peuvent l'utiliser. Dans les réseaux virtuels privés (VPN), l'approche de tunnelage peut être utilisée. Les applications tournant au sein de la machine hôte ne sont pas conscientes de la présence de la sécurité implémentée par le VPN. Cependant, quand ces applications essaient d'établir une connexion vers une autre hôte au dehors de l'intranet mais appartenant au VPN, la passerelle de sécurité emploie le tunnel du VPN pour l'envoie des données de ces applications par le moyen du protocole de sécurité de la couche de transport.

1.2.2.5. L'architecture de sécurité pour IP : l'IPSec

IPSec est l'extension du protocole IP. Il est spécialement conçu pour offrir une architecture de sécurité basée sur la cryptographie, de haute qualité et compatible avec IPv4 et IPv6. Il offre un ensemble de services de sécurité tels que :

- Le contrôle d'accès
- Connectionless integrity
- Authentification de l'origine des données
- Protection contre les rejeux (replaying)
- Confidentialité

Ces services de sécurité sont offerts au niveau de la couche 3 (couche Internet), pour protéger le protocole IP et les protocoles de plus haut niveau.

a. Architecture d'IPSec :

Les parties fondamentales de l'IPSec sont :

Les protocoles de sécurités AH, ESP

Algorithmes d'authentification et de chiffrement

Le gestionnaire de clef (IKE)

Les associations de sécurité (SA associations security)

Les protocoles de sécurité AH (Authentication Header) et ESP (Encapsulating Security Payload) sont conçus pour protéger les contenus des paquets IP. Quand ces protocoles de sécurité sont correctement implémentés et déployés, ils deviennent transparents pour les utilisateurs, les machines hôtes ou d'autres composants de l'Internet qui ne les utilisent pas pour la protection de leur trafic de communication.

En outre, ces protocoles de sécurité sont conçus pour être indépendants des algorithmes de cryptographie et d'authentification qu'ils utiliseront. Cette modularité permet la sélection de différents algorithmes sans affectée leur implémentation. Cependant, un ensemble de configurations standardisées par défaut de ces algorithmes a été spécifié pour une raison d'interopérabilité.

De même, différents systèmes de gestion de clefs peuvent être utilisés comme Kerberos, mais le gestionnaire de clefs automatique utilisé par défaut est l'IKE (Internet Key Exchange). Le principal rôle de IKE est l'établissement et la maintenance des associations de sécurité (Security association SA).

Une association de sécurité SA est une connexion réseau unidirectionnelle qui applique certains services de sécurité sur le trafic qu'elle circule. Il définit l'échange des clés et des paramètres de sécurité. Il rassemble ainsi l'ensemble des informations sur le traitement à appliquer aux paquets IP(les protocoles AH et/ou ESP, mode tunnel ou transport, les algorithmes de sécurité utilisés par les protocoles, les clés utilisées,...). L'ossature habituelle pour négocier, modifier ou supprimer une SA est le ISAKMP (Internet Security Association and Key Management Protocol). On remarque que l'échange des clefs peut se faire manuellement, ou avec le protocole d'échange IKE, qui permet aux deux parties (peers) de s'entendre sur les SA à utiliser.

Dans le SA, seul un protocole de sécurité (AH ou ESP) est appliqué au trafic. Si les deux protocoles sont nécessaires, on créerait deux SA pour chacun des protocoles. De même, pour une connexion bidirectionnelle, deux SAs différentes sont utiles. Ainsi, on peut choisir librement les attributs de sécurité (algorithmes de chiffrement,...) que l'on désire implémenter afin de pouvoir offrir différents services de sécurité, différente direction de la connexion.

b. Mécanismes de sécurité d'IPSec :

Authentification de l'entête (Authentication Header AH) :

Ce protocole offre l'intégrité, l'authentification de l'origine des données, et le service d'anti-rejeux qui est optionnel.

L'intégrité et l'authentification sont généralement offerts pour tout le paquet i.e. l'en-tête IP et le message (payload i.e. le protocole de plus haut niveau comme le segment TCP) [22, 23, 24, 26, 36, 42]. Les en-têtes IP peuvent être cependant changées lorsqu'elles sont en transit (ex. le champ TTL du paquet IP est réduit), dans ce cas, le AH ne peut pas les protéger. Les valeurs de ces champs sont alors réduites à zéro si on a besoin de l'authentification.

La non-répudiation peut être offerte si un algorithme à clef publique, pour la production de signature électronique, est utilisé pour l'authentification des données.

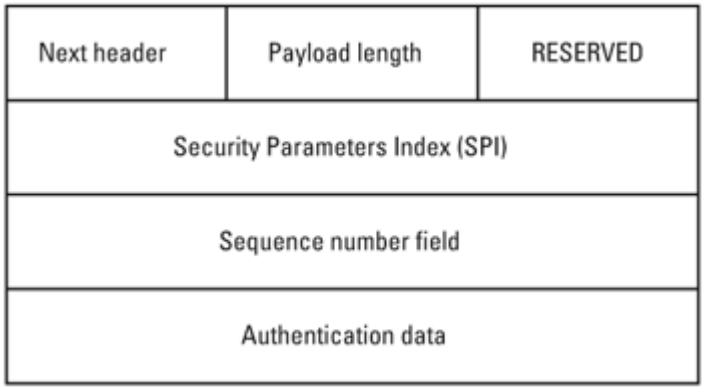


Figure 12: Structure de l'IP Authentication Header

Figure 12 montre la structure de AH. Tous les champs sont obligatoires. Le champ 'Next header' de 1bit indique le type de données (payload) après le AH (TCP ou UDP). Le 'Payload length) dénote la longueur du AH, qui est généralement de 30bits. Le champ 'RESERVED' de longueur 1bit est réservé pour une utilisation ultérieure de cette structure, elle assure l'évolutivité du protocole. Le SPI qui a une longueur de 32bits, peut être utilisé en collaboration avec l'adresse IP de destination pour déterminer le SA et les configurations des attributs de sécurité spécifiées (algorithmes et clefs) pour tous les paquets IP valides. Les champs nombre de séquence, qui lui aussi est de 32bits contient une valeur de compteur séquentielle incrémentale. Les compteurs du destinataire et expéditeur sont égalisés à 0 lorsqu'une SA est établie.

Si la protection des rejeux est nécessaire, les conditions suivantes sont requises :

- Le récepteur doit vérifier le nombre de séquence de tous les paquets IP entrants
- Le nombre séquentiel ne présente pas un cycle.

La deuxième condition signifie qu'une nouvelle SA doit être établie après la transmission de (232-1) paquets, car la suivante valeur possible est 0 (les valeurs possibles du nombre de séquence est de 0 à 231). En d'autres termes, le nombre de paquets que l'on peut transmettre à travers une SA est inférieure à 232.

Le champ 'Authentication Data' est de longueur variable. Il contient le ICV (Integrity Check Value i.e. valeur pour la vérification de l'intégrité) pour le paquet IP. Il contient aussi le 'padding' (rembourrage) pour assurer que le AH est un multiple de 32bits (pour IPv4) ou de 64bits (pour IPv6).

AH peut être utilisé dans le mode transport ou mode tunnel. Il peut être utilisé pour une connexion entre des machines hôtes, entre une hôte et une passerelle de sécurité (security gateway), ou encore entre deux passerelles de sécurité. Le Ah en mode transport est seulement appliqué à un paquet IP total (pas un fragment). Mais en mode tunnel, il peut être utilisé sur un paquet IP où le payload peut être fragmenté.

ESP Encapsulating Security Payload :

ESP définit le chiffrement des paquets. Il fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejeu.

c. Les deux modes de fonctionnement d'IPSec :

AH, ESP et IPcomp fonctionnent dans le mode transport ou le mode tunnel. Le mode "transport" encrypte directement les échanges entre deux machines. Le mode "tunnel" encapsule les paquets encryptés dans de nouveaux en-têtes IPv4/IPv6. Il est conçu pour les passerelles VPN.

1.2.3. Sécurité des DNS

Le protocole DNS assure la correspondance entre le nom d'une machine et son adresse IP. Un serveur DNS est en écoute par défaut sur l'UDP port 53. Pour se communiquer à une hôte A dont seul le nom est connu (ex : www.mamachine.com), une machine B lance une requête (DNS look up) au serveur DNS pour obtenir l'adresse IP correspondante (ex : 123.23.2.1). Cependant, le serveur DNS peut ne pas être crédible, i.e. les adresses IP stockées dans sa base de données sont corrompues (ex : la table de correspondance est changée par un pirate). Par conséquent, l'adresse IP obtenu de celui-ci peut être incorrecte ou peut rediriger l'hôte demandant vers la machine du pirate. Ils existent plusieurs attaques exploitant faiblesses du protocole DNS.

1.2.3.1. Le DNS ID spoofing

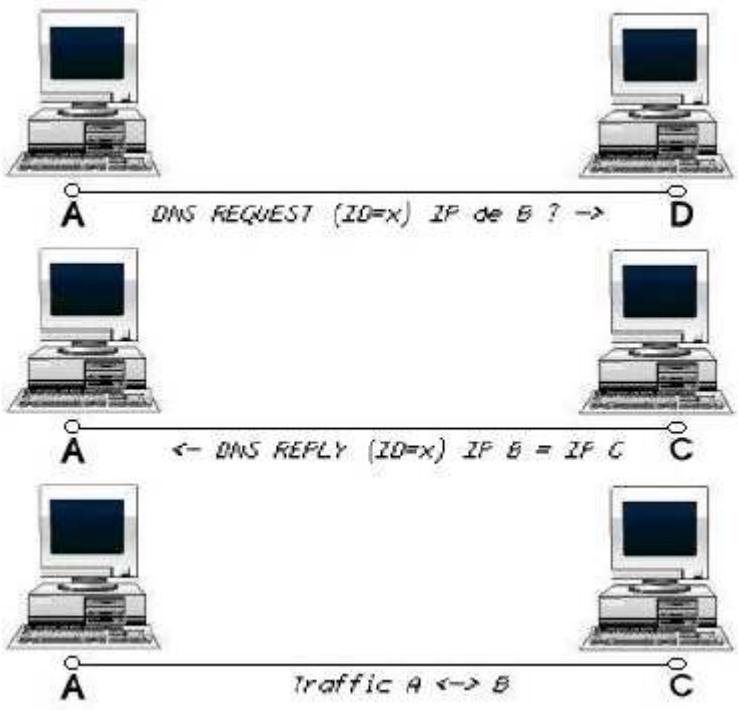
C'est la première attaque que nous allons décrire. Elle aboutit à un détournement de flux entre deux machines à l'avantage du pirate.

Imaginons qu'un client A veuille établir une connexion avec une machine B. La machine A connaît le nom de la machine B mais pas son adresse IP, ce qui lui empêche pouvoir communiquer avec. La machine A va donc envoyer une requête au serveur DNS du réseau de B pour connaître l'adresse IP de B, cette requête sera identifiée par un numéro d'identification (ID). Le serveur répond à cette requête en fournissant l'adresse IP de B et en utilisant le même numéro d'ID.

Ce numéro a une valeur comprise entre 0 et 65535.

Le DNS ID spoofing a pour but de d'envoyer une fausse réponse à une requête DNS avant le serveur DNS. De cette façon, le pirate peut rediriger vers lui le trafic à destination d'une machine qu'il l'intéresse.

Dans notre exemple, un pirate C doit répondre à A avant le serveur DNS (D) du réseau de B. Ainsi, il envoie à A son adresse IP associée au nom de la machine B. A communiquera alors avec le pirate C au lieu de la machine B.



Néanmoins, pour implémenter cette attaque, le pirate doit connaître l'ID de requête DNS. Pour cela, il peut utiliser un sniffer s'il est sur le même réseau, soit prédire les numéros d'ID par l'envoi de plusieurs requêtes et l'analyse des réponses.

1.2.3.2. Le DNS cache poisoning

Le principe de cette attaque est très similaire à celui de l'ARP-Poisoining. Pour gagner du temps dans la gestion des requêtes, le serveur DNS possède un cache temporaire contenant les correspondances adresses IP - noms de machine. En effet, un serveur DNS n'a que la table de correspondance des machines du réseau sur lequel il a autorité.

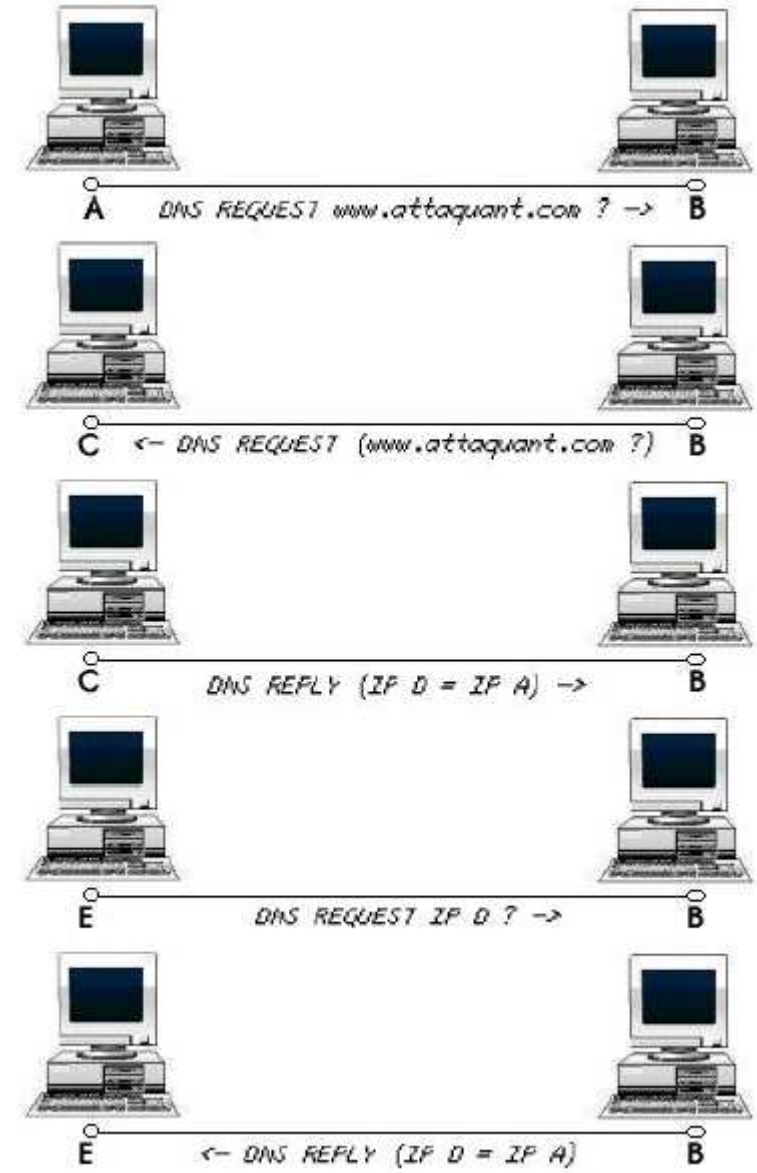
Pour des machines distantes, il doit interroger d'autres serveurs DNS. Pour éviter de les interroger à chaque requête, il garde en mémoire (dans un cache), le résultat des précédentes requêtes.

L'objectif du pirate est d'empoisonner ce cache avec de fausses informations. Pour cela, il doit avoir un nom de domaine sous contrôle et son serveur DNS.

Imaginons qu'un pirate (A) possède le nom de domaine attaquant.com, et son serveur DNS (C) et qu'il veuille empoisonner le cache du serveur DNS (B) du réseau cible.net.

Le pirate envoie une requête au serveur DNS (B) du réseau cible.net demandant la résolution du nom de domaine attaquant.com.

Le serveur DNS (B) de cible.net va donc envoyer une requête sur le serveur DNS (C) de l'attaquant (c'est lui qui a autorité sur le domaine attaquant.com). Celui-ci répondra et joindra des informations additionnelles falsifiées par le pirate (un nom de machine (D) associé à l'adresse IP (A) du pirate). Ces informations seront mises en cache sur le serveur DNS (B) de cible.net. Si un client quelconque (E) demande l'adresse IP pour le nom de la machine (D), il recevra l'adresse du pirate (A) en retour.


A
DNS REQUEST www.attaquant.com ? ->
B
C
<- DNS REQUEST (www.attaquant.com ?)
B
C
DNS REPLY (IP D = IP A) ->
B
E
DNS REQUEST IP D ? ->
B
E
<- DNS REPLY (IP D = IP A)
B


E
TRAFFIC D <-> E
A

Pour se protéger contre ce type d'attaque, il est recommandé de :

- Configurer le serveur DNS pour qu'il ne résolve directement que les noms de machine du réseau sur lequel il a autorité.
- Autoriser seulement des machines internes à demander la résolution de noms de domaines distants.
- Mettre à jour ou changer les logiciels assurant le service DNS pour qu'ils vous protégent des attaques décrites précédemment.

1.2.4. Contrôle d'accès et d'autorisation

Le contrôle d'accès fournit un niveau de sécurité d'accès réseau de base [31, 33, 34]. L'autorisation d'accéder à un élément du SI dépend principalement de ce contrôle d'accès. Par exemple, les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section. Il existe deux types de contrôle d'accès : le contrôle d'accès basé sur l'identité de l'utilisateur et celui basé sur son rôle.

1.2.5. Sécurité des systèmes d'exploitation

1.2.5.1. Failles applicatives

Ce sont les failles liées aux applications utilisées. Ces failles peuvent être de natures diverses : problèmes de configuration, problèmes au niveau du code du logiciel, problèmes liés à de mauvaises interprétations de commandes ou de mauvaises exécutions de scripts.

1.2.5.1.1. Les installations par défaut

Lors d'une installation, beaucoup de services inutiles peuvent être installés par défaut (un serveur Web, FTP ...). Ces services peuvent être exploités par les malveillants pour atteindre leur but.

1.2.5.1.2. Les mauvaises configurations

Lorsqu'une application est mal paramétrée, elle peut laisser l'accès libre à certaines bases de données sensibles (fichiers de mots de passe, d'utilisateurs) ou de permettre d'exécuter des commandes ou des scripts malveillants.
Il est important de bien lire le manuel avant d'activer un service et de bien définir «qui fait quoi».
Ce principe est simple : il suffit de bien définir les utilisateurs et les groupes et de limiter leurs droits sur certains types de fichiers et certaines opérations d'exécution de commandes système.

Le plus important est de restreindre au maximum les accès à certains fichiers sensibles et aux commandes systèmes.

1.2.5.1.3. Les bogues

Les bogues sont dus à des erreurs de programmation. Les bogues font apparaître différents types de problèmes de sécurité :

Des dénis de services applicatifs

Ce type de faille empêche le logiciel de fonctionner et ainsi de répondre aux requêtes demandées (d'où l'appellation déni de service). La technique est simple, il suffit d'utiliser un bogue connu qui va faire planter le logiciel assurant un service.

Outrepassement de droits

Les bogues de type dépassement de buffer (buffer over flow) ou d'exploitation de bogues de format posent de gros problèmes de sécurité. Ils visent majoritairement des applications fonctionnant avec les accès administrateur (*setuid root*) pour permettre à un attaquant d'obtenir un interpréteur de commande au niveau administrateur (*uid root*) sans aucune authentification.

Les scripts

Malheureusement, une mauvaise programmation de scripts ou l'utilisation de fonctions boguées peut être source de failles de sécurité. Il convient d'être très attentif au niveau du développement d'un script.

Les exploits

Pour exploiter ces bogues, le pirate fait appel à des «exploits». Ces «exploits» sont en fait de petits programmes permettant d'exploiter une faille dans un but précis (obtenir un interpréteur de commandes, accéder à certains fichiers, augmenter ses droits...).

Les exploits peuvent aussi fonctionner à distance, pour l'obtention d'un shell (parfois avec les droits administrateur) sans mot de passe, ni nom d'utilisateur.

PARTIE II : SECURISATION DU SYSTEME INTEGRE DE LA GESTION DES FINANCES PUBLIQUES : CAS DU MEFB

CHAPITRE I : METHODOLOGIE

Une perspective de la méthode utilisée pour sécuriser le si du MEFB est présentée ci-après. Elle comporte différentes étapes à suivre afin de pouvoir bien formuler les fiches de besoins en matière de la sécurité, ainsi que les plans de mitigations et de contingence des risques identifiées lors de l'étude des menaces et de ces impacts.

1.1 Expression des Besoins et Identification des Objectifs de Sécurité

Cette première étape permet de déterminer des objectifs et des exigences de sécurité adaptés [4]. La méthode prend en compte toutes les entités techniques (logiciels, matériels, réseaux) et non techniques (organisation, aspects humains, sécurité physique). Elle permet d'impliquer l'ensemble des acteurs du SI dans la problématique de sécurité et propose par ailleurs une démarche dynamique qui favorise les interactions entre les différents métiers et fonctions de l'organisation en étudiant l'ensemble du cycle de vie du système (conception, réalisation, mise en œuvre, maintenance…).

1.1.1. Élaboration de politiques de sécurité des systèmes d'information

La Politique de Sécurité des Systèmes d'Information reflète la vision stratégique de la direction DSI (du MEFB) en matière de sécurité des systèmes d'information (SSI) et de gestion de risques SSI.

Elle décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme.

L'élaboration d'une politique de sécurité des SI requiert une approche globale, considérant non seulement les domaines techniques tels que la sécurité logique, la sécurité des matériels informatiques et la sécurité des réseaux, mais aussi les domaines non techniques tels que la sécurité physique, la sécurité liée aux aspects humains et la sécurité organisationnelle.

Les règles de sécurité seront alors réalistes et cohérentes pour un périmètre généralement large et un champ d'application étendu.

CHAPITRE II : ANALYSES ET RESULTATS

2.1. Analyse des besoins et identifications des objectifs de sécurité :

2.1.1. Etudes du contexte

2.1.1.1. Etudes de l'organisme

Le MEFB est responsable de l'implémentation des lois de finance de notre pays, d'établissement des politiques financières et de la gestion des finances publiques. Pour plus de détail sur le fonctionnement de ce ministère, son organigramme, ainsi que les circuits de dépenses publiques sont expliqués en annexe. On peut tirer de ces fonctionnements le transfert de fichier abondant et la nécessité du traitement informatique de certaines tâches afin de gagner du temps.

PathFinance, un organisme privé engagé par ce ministère, qui a pour rôle l'informatisation des flux financiers des Etats. Il réponde aux problématiques de gestion des pays qui sollicitent des outils informatiques pour le suivi et la maîtrise des dépenses publiques dans le cadre de la bonne gouvernance. Cette entreprise a alors développé un système intégré de gestion des finances publiques de Madagascar. Donné ci-dessous est l'esquisse de l'architecture de ce système informatisé que l'on désire sécuriser tous les processus afin de garantir la protection des données stockées ou échangées entre les réseaux.

2.1.1.2. Etude du système cible

2.1.1.2.1. Détermination de la cible de l'étude de sécurité

Etude des menaces et gestion des risques

Le risque représente un sinistre possible. C'est le fait qu'un élément menaçant puisse affecter des éléments essentiels en exploitant les vulnérabilités des entités sur lesquelles ils reposent avec une méthode d'attaque particulière. On appelle vulnérabilité la faiblesse de la sécurité d'une cible d'évaluation (due par exemple à des défauts dans l'analyse, la conception, la réalisation ou l'exploitation). Afin de pouvoir formuler la politique de sécurité, il est nécessaire de gérer les risques que l'on identifiera préalablement.

La gestion des risques SSI constitue un *processus continu* dont il convient de définir précisément le cadre (ressources, moyens, responsabilités…) pour chacun de ses aspects :

- Appréciation du risque : cette tâche consiste à analyser et évaluer le risque SSI en comparant le niveau de risque à des critères de risques définis au préalable ;
- Traitement du risque : cette tâche consiste à réduire, transférer ou prendre le risque apprécié lors de la tâche précédente ;

- Acceptation du risque : cette tâche consiste à accepter le risque traité, et le cas échéant à accepter le risque résiduel ;
- Communication relative au risque : cette tâche consiste à échanger ou partager des informations concernant le risque.

Identification des risques

i. Indisponibilité du SI (tampering, DoS)

Tout le système est en panne qui s'étend d'une panne électrique aux équipements endommagés. Dans ce cas, les services ne sont pas disponibles.

i. Description

L'indisponibilité du SI correspond au non fonctionnement du SI car ses services et ressources ne sont plus disponibles pour l'utilisation.

ii. Impacts

L'un des exigences du MEFB avant l'implémentation et l'utilisation du SI est la disponibilité des informations et applications y résidant. L'indisponibilité du SI est donc considérée comme étant une erreur fatale

iii. Causes

L'indisponibilité du SI a plusieurs causes :

- L'attaque du système par le déni de service (DoS) qui abuse les ressources du SI jusqu'à ce que celles-ci ne soient plus capables de soutenir tous les services demandés. Beaucoup de logiciels sont disponibles sur Internet pour mener à bien ce type d'attaque.
- Les anti-virus, anti-spyware, anti-vers n'est pas mis à jour, rendant le SI vulnérable.

ii. Gain d'accès non autorisé

i. Description

Le gain d'accès non autorisé est le contournement du contrôle d'accès mis en place afin de pouvoir entrer dans le SI et d'utiliser les ressources de ce SI avec les privilèges d'un utilisateur existant, mais sans avoir son autorisation.

ii. Impacts

Le gain d'accès non autorisé n'est pas une fin en soi-même. En effet, ce gain peut être utilisé pour des fins malveillantes, comme la lecture non autorisées, altération ou même destruction des données, l'utilisation abusive des ressources du SI.

iii. Causes

Le gain d'accès peut être dû par plusieurs causes :

- Contrôle d'accès non rigoureux
- La sécurité du système d'authentification des utilisateurs est faible ou non existante.
- La gestion des mots de passe n'est pas très stricte
- L'utilisation des logiciels comme les sniffers pour cueillir des couples d'usagers/mots de passes, alors que la sécurisation du SI n'est pas encore implémentée.
- Mal configuration des OS. Les services non utilisés tels que Telnet, serveur ftp, … i.e. les services disponibles par défaut lors de l'installation de l'OS ne sont pas bloqués.

iii. Altération, destruction et effacement des données

i. Description

L'ouverture du SI et la disponibilité permanente de ses informations aux opérateurs externes exposent le SI à un risque d'altération non autorisée de ces données, soit par les utilisateurs à l'extérieur du LAN ou par des utilisateurs locaux dans la zone de confiance.

ii. Impacts

Suivant la sensibilité des informations alternées, l'impact de ce risque s'étend de moindre niveau jusqu'au niveau sévère car le fonctionnement des branches du MEFB en est directement lié. En effet, le traitement des données falsifiées peut engendrer des statistiques fausses conduisant à des décisions erronées qui paralysent à leur tour tout l'Etat.

iii. Causes

La manipulation non contrôlée des données peut entraîner à l'altération non autorisée des données. Cette manipulation peut être le fait que le contrôle d'accès aux données (droits des utilisateurs à accéder à des différentes ressources du SI y compris les données suivant ses privilèges) est absent ou celui ci est endommagé.

La disposition des logiciels libres sur l'Internet permet d'exploiter cette faille de contrôle d'accès et entraîne éventuellement à l'altération, voire l'effacement des données sensibles.

iv. Vols de disques durs

i. Description

L'intrusion physique dans le centre de données facilite le vol des supports de données tels que les disques durs, les cassettes de back up, etc.… Ainsi, la disponibilité et la confidentialité des données ne sont plus respectées, et le flux de données est dérangé, d'où la dégradation du QoS du SI.

ii. Impacts

La violation du QoS du SI tels que la disponibilité, la confidentialité peut entraîner à l'arrêt total ou partiel travail de plusieurs branches du MEFB, qui dépendent du flux de données gérer par le SI. L'impact des vols des équipements est alors rangé de élevé car il paralyse tout le fonctionnement du SI. En plus, le recouvrement des équipements et des données perdus peut être très coûteux.

iii. Causes

L'absence de contrôle d'accès physique peut entraîner la facilité d'intrusion physique non autorisée au sein du centre de données, rendant ainsi la facilité du vol. De plus, l'absence de code d'ouverture des ordinateurs (cadenas et clefs) rend le vol moins périlleux.

v. Architecture de sécurité des applications non développée.

i. Description

Même si les développeurs d'application n'ont pas à se soucier de la sécurisation des applications développées avec les nouveaux Framework tels que .NET et J2EE, car ces deux plateformes proposent déjà une architecture de sécurité prête à l'emploi. Beaucoup de développeurs ne sont pas encore bien expérimentés pour utiliser les procédures fournies pour la sécurisation des applications, qui peuvent alors présenter des failles que les hackers peuvent exploiter pour gagner d'accès illicite au SI, et ainsi d'abuser les ressources du système.

ii. Impacts

Même difficile à exploiter, il est possible d'exploiter ces codes mal conçus. Néanmoins, la possibilité que ce risque arrive est classée de faible niveau, mais l'impact auquel il a sur le fonctionnement du système quand elle est survenue est grave.

iii. Causes

- Mal conception des applications développées (par exemple le SQL Injection pour les applications Web)
- L'architecture de sécurité des applications n'est pas bien suivie.

vi. Dégradation de la performance des serveurs (d'applications et de données), et des postes de travail

i. Description et impacts

La dégradation de la performance peut être classée comme un risque pour la sécurité du système car elle rompt la disponibilité des informations sur celui-ci. En effet, si les informations sont voulues en temps réel, comme l'est l'exigence du MEFB, faute de la vitesse de transmission des données par exemple, les informations ne sont plus utilisables en temps voulu. La dégradation de la performance ou QoS se résume alors en tant que la vitesse de transmission, de traitement ou d'accès aux ressources

ii. Causes :

La dégradation de la performance du SI peut être due aux attaques de type DoS qui entraine a la longue a l'indisponibilité totale du SI, ou par l'infection des virus qui paralyse petit a petit tout le SI.

vii. Incendie et cataclysme naturel

i. Description

Dès fois, l'incendie est la solution rapide des individus malveillants pour contourner la disponibilité des données qui servent de repère statistique pour la prise de décision importante. L'incendie est alors contre la disponibilité des informations sur le SI. Mais contrairement au vol, les malveillants n'auront pas une copie des données en main donc la confidentialité des données n'est pas violée.

ii. Impacts

L'incendie entraîne la perte totale du centre de données, i.e. les serveurs de données, les données elles-mêmes ainsi que les applications y résidant. Le flux et échange de données ne sont plus assurés et le bouleversement au niveau fonctionnel des différentes branches du MEFB est inévitable. L'impact de l'incendie sir le SI est alors classé de haut niveau même si sa probabilité

d’existence est moindre. On note que l’impact de l’incendie qu’elle soit intentionnelle ou accidentelle reste égal.

iii. Causes

La cause de l’incendie peut être intentionnelle ou accidentelle. Elle est intentionnelle lorsque le malveillant a un lien direct avec la décision que l’Etat peut prendre suite au résultat statistique que les données peuvent fournir. L’agresseur souhaite alors détruire les données en optant à l’incendie.

2.1.1.2.2. Expressions des besoins

La liste suivante représente la spécification des besoins (ou conditions) que le SI du MEFB a exigé.

- Les données sont chiffrées
- Les machines usitées sont linux
- Les bases de données utilisées sont oracle
- Les postes de travail sont connectées à l’Internet
- utilisation d’une liaison satellitaire pour connecter Tana et Tama
- assurer l’accès aux serveurs par des postes de travail autorisées
- mettre à jour les anti-virus
- La vitesse de connexion et de transmission des données acceptables
- La connexion aux serveurs disponible durant l’heure de travail.
- Le système peut s’évoluer (possibilité d’utilisation d’autre technologie), la maintenance facilitée

2.1.1.2.2. Synthèse de besoins de sécurité

- Besoin n°1 : le chiffrement de toutes les données peut dégrader énormément la performance du SI car les traitements des données consomment du temps et de la ressource du CPU. La classification des données peut contourner ce problème comme nous l’avons indiqué auparavant.
- Besoin n°2 : l’utilisation de Linux comme serveurs nécessite une connaissance approfondie du système d’exploitation pour bien configurer le serveur. La maintenance du système, et les patchs disponibles sur l’Internet sont à appliquer dès qu’ils sont disponibles

afin de garantir la sécurité (contourner les failles de l'OS) du serveur et éventuellement pour éviter la perte des données.

- Besoin n°3 : la gestion des ACLs et des utilisateurs, réplication, reprise après panne, gestion d'accès (multiple accès et manipulation des données simultanément) est primordiale pour le MEFB. Oracle datawarehouse répond toutes ces éventualités.
- Besoin n°4 : comme les postes de travail peuvent être la source des attaques d'autant plus qu'elles sont connectées. La configuration de ces postes de travail est utile, que nous entamerons plus en détail dans le paragraphe ci-après.
- Besoin n°5 : la liaison entre le site de Tananarivo et celui de Toamasina est assurée par une liaison satellitaire VSAT (Very Small Aperture T) Paradise Datacom P300 Series. La fiche technique détaillée peut être trouvée dans [réf.]. Pour assurer la protection des données en transmission, la mise en place d'un réseau privé virtuel VPN (Virtual Private Network) est nécessaire que nous discuterons plus tard.
- Besoin n°6 : la gestion des utilisateurs vis-à-vis des serveurs est nécessaire. On remarque que ces utilisateurs se situent à travers le LAN, le MAN et le WAN. Il s'avère donc utile de gérer ces utilisateurs, les authentifier lors de l'accès et pendant toutes les transactions. Une solution est de gérer centralement tous les utilisateurs qui veulent accéder aux ressources (serveurs de données) et de leur appliquer la règle d'ACLs. Cette solution nécessite un annuaire électronique qui gère les utilisateurs, les ressources du SI. Cet annuaire peut être conçu pour authentifier tous les utilisateurs qui demandent accès aux ressources, dans notre cas le serveur de données. La gestion des ressources (humaines et matérielles) est alors rendue facile : la mise à jour de l'annuaire est plus facile que d'ajouter ou de supprimer un par un tous les utilisateurs qui veulent accéder aux ressources.
- Besoin n°7 : même si un niveau de sécurité élevé est exigé, la performance du SI n'est pas à négliger. La vitesse de traitement et la transmission de données sont importantes vis-à-vis du fonctionnement du SI, ce qui est contradictoire avec le besoin n°1. Cependant, si les machines surtout des serveurs sont performants, et la bande passante de l'interconnexion est acceptable, le chiffrement des données n'impacte pas trop la performance du SI. En outre, la classification des données permet de catégoriser les types de données nécessitant entièrement un chiffrement, comme les données classées top secret.

- Besoin n°8 : les solutions technologiques choisies en matière de sécurité devront être standardisées pour assurer l'évolutivité et l'interopérabilité du SI.

2.1.1.3. Elaboration de la politique de sécurité

2.1.1.3.1. Définition de la politique de sécurité

La politique de sécurité est définie comme étant l'ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme, dans notre cas, le ministère de l'économie, des finances et du budget. Elle définit clairement ce qui est permis, prohibitif, ou la façon dont une activité peut être réalisée.

2.1.1.3.2. Recueil des règles

Règles générales

- Définir les règles de protection des mots de passe pour les différents systèmes
- Mettre à jour les anti-virus et les systèmes de détection d'intrusions.
- Mettre en place un suivi régulier des activités de contrôle de traces et des incidents détectés sous la forme de bilans diffusés aux responsables de l'audit.
- Pour la protection des informations, élaboration de l'ACL (Acces Control List) logique et physique :
    - Définir une classification des informations (serveurs de données et d'applications, les fichiers, ...), les règles de stockage et de diffusion associées (secret, très confidentiel, confidentiel,...).
    - Définir les privilèges des utilisateurs vis-à-vis de leurs rôles au sein du ministère.
    - Définir la stratégie d'accès aux informations classifiées vis-à-vis des privilèges des utilisateurs.
- Elaborer les règles et une procédure complète de gestion et de protection des supports d'information (papier ou magnétique) :
    - définir les procédures d'accès physique à la salle d'archivage et aux centres de données.
- Pour la sécurité des postes de travail et du réseau local :
    - Formaliser les procédures de gestion des comptes utilisateurs.

- Formaliser les règles d'utilisation des postes de travail et de l'environnement bureautique. Sensibiliser les utilisateurs au respect des ces règles.
- Inventorier les postes de travail nécessitant l'accès à l'Internet et les configurer à utiliser les différentes composantes conçues pour la sécurité (DHCP, firewall, ...)
- Définir et mettre en œuvre des règles sur le firewall régissant tout accès au réseau depuis l'extérieur et restreindre les connexions depuis le réseau local par les commutateurs en fonction des besoins de l'utilisateur principal du poste de travail.
- Appliquer une procédure de contrôle et d'audit régulier de la configuration du firewall : définir les règles et les moyens de journal et d'analyse des traces sur le firewall.
- Configurer les systèmes d'exploitation et les applications à utiliser afin de minimiser les trous de sécurité. Seules les applications et services nécessaires sont à installer (serveur FTP, TELNET,...)
- Vérifier que l'utilisation des privilèges root est nécessaire pour réaliser les tâches d'administration courantes et attribuer un compte personnel à chaque administrateur

2.2. Synthèses et solutions proposées

Afin d'affiner la performance du système intégré du MEFB pour la gestion des finances publiques, les solutions en sécurité suivantes sont proposées.

2.2.1. La sécurité physique

Cette section décrit les meilleures pratiques que l'on peut utiliser pour protéger physiquement les informations et les ressources du système intégré.

2.2.1.1. L'environnement de travail:

La préparation des sites pour les centres de données, ainsi que les serveurs d'application s'avère critique vu l'importance des ressources qui y sont entreposées. Quelques mesures sont alors à prendre pour assurer le bon fonctionnement du SI vis-à-vis de ces sites.

- L'électrification : l'utilisation des onduleurs est recommandée due à la nature de fournisseur d'énergie à Madagascar (JIRAMA)
- Ventilation et l'aération : comme tous les appareils électroniques, le système de ventilation des équipements (router, switch, terminaux et serveurs...) doivent être installée.

- Détection et protection contre les feux : ce n'est plus surprenant de constater que les lieux contenant des données importantes constituent des cibles d'incendie (Rova en 1996, Lapan'ny Tanana (1972))
- Le contrôle d'accès physique au centre de données. Quel que fois ce contrôle d'accès élimine des risques auxquelles les données sont exposées, comme le vol des disques dures ou la destruction des serveurs. Ainsi, une liste des personnes autorisées à s'introduire dans le centre de données est à maintenir.
- Le nettoyage périodique du site élimine les poussières qui peuvent nuire les circuits électroniques.

2.2.2. Le contrôle d'accès logique

Les départements devraient assurer que le droit d'accès aux données et aux applications ne soit pas accordé à moins que ce soit autorisé par les propriétaires de l'information, et que ces autorisations sont clairement documentées. La documentation de la liste des contrôles d'accès est une des méthodes que l'on peut utiliser pour assurer la cohérence entre les accès physiques aux centres de données, les données elles-mêmes, et les applicatifs.

Un système d'identification et d'authentification est nécessaire, que ce soit pour l'accès physique ou accès aux données et applications à travers le réseau. Il est d'autant plus que nécessaire quand on a affaire aux accès à distance des réseaux par des entités (utilisateurs, applications) de confiance ou non.

Du point de vue technique, les solutions prises dépendront de la sensibilité de la ressource (information, ressource matérielle ou logiciel) à laquelle une entité veut accéder et du contexte d'utilisation (sur un portable, à distance, d'une partie du LAN, ...). Les techniques suivantes sont globalement utilisées pour l'identification et l'autorisation :

- Code usager/mot de passe : cette solution permet d'authentifier l'utilisateur en acceptant le code d'usager (unique pour chaque utilisateur) et le mot de passe, ceci en comparant ce dernier du mot de passe correspondant dans une base de données ou dans un répertoire. Cette solution d'identification/authentification très répandue assure un niveau de sécurité un peu élevé, en particulier lorsqu'un faible contrôle de l'indentification est réalisé.
- Certificat électronique : le certificat électronique permet d'obtenir un niveau de sécurité plus élevé qu'avec le couple login/password, car il permet d'authentifier

l’utilisateur et de fournir un service de non-répudiation comme nous l’avons indiqué auparavant.

2.2.2.1. La gestion des mots de passe

2.2.2.1.1. Encryptage du fichier pour Linux

Les mots de passe utilisés sur un système d'information sont encryptés pour garantir leur confidentialité. Ces mots de passe encryptés sont stockés dans des listes de mots de passe sur des fichiers systèmes prédéfinis. Sous UNIX, la liste des mots de passe des utilisateurs système est divisée en deux fichiers /etc/shadow et /etc/passwd ou réunis seulement dans le fichier /etc/passwd. Le type d'encryptage peut être du MD5, DES.

Un pirate peut fort bien récupérer ces listes et tester la fiabilité des mots de passe. Il peut utiliser pour cela l'outil adéquat : un perceur de mot de passe.

La plupart des algorithmes d'encryptage repose sur l'utilisation de fonctions à sens unique. Ceci veut simplement dire qu'il est impossible de décrypter le mot de passe à partir sa forme encryptée. L'attaque consiste alors à encrypter différentes combinaisons de caractères et de comparer cette forme encryptée à celle du mot de passe voulu. Si les deux chaînes correspondent, alors la suite de caractères est celle du mot de passe.

Les administrateurs du SI sont invités à utiliser les mêmes outils que les pirates utilisent afin de tester la robustesse des mots de passes des utilisateurs du SI dont il est responsable. Il y a deux types d'attaques pour le craquage de mots de passe : l’attaque par dictionnaire et le brute forcing. On retrouvera aux annexes les définitions de ces mots techniques.

2.2.2.1.2. Sélection des mots de passe

Il est important de définir des règles pour la sélection des mots de passe, et de distribuer ces règles aux utilisateurs. Une directive est offerte ci-après pour la sélection des mots de passe :

A ne pas faire:

Ne pas utiliser les logins comme mots de passe

Ne pas utiliser le nom de famille, le surnom ou le prénom

Ne pas utiliser le nom de mari /ou femme, ou les enfants, ou les bêtes domestiques, ...

Ne pas utiliser des informations faciles à deviner

Ne pas utiliser des lettres ou des chiffres consécutifs ex : ‘abcdef’ ou ‘56789’ ou les touches adjacentes du clavier ex : ‘azertyuiop’

2.2.3. Sécurité des réseaux et de la communication

2.2.3.1. Architecture proposée

Il y a une infinité de possibilités d'organiser un réseau mais pour assurer une sécurisation qui évolue avec le temps et les nouvelles technologies disponibles répondant aux besoins spécifiques [29, 30, 35], il est indispensable de concevoir une architecture qui facilite l'intégration des nouvelles technologies en matière de maintenance, d'évolutivité et d'interopérabilité en tenant compte de la sécurisation.

2.2.3.1.1. Schéma global

La figure fig.13 ci après montre le concept que l'on a utilisé afin de sécuriser le réseau. Le choix de la technique utilisée sera expliqué.

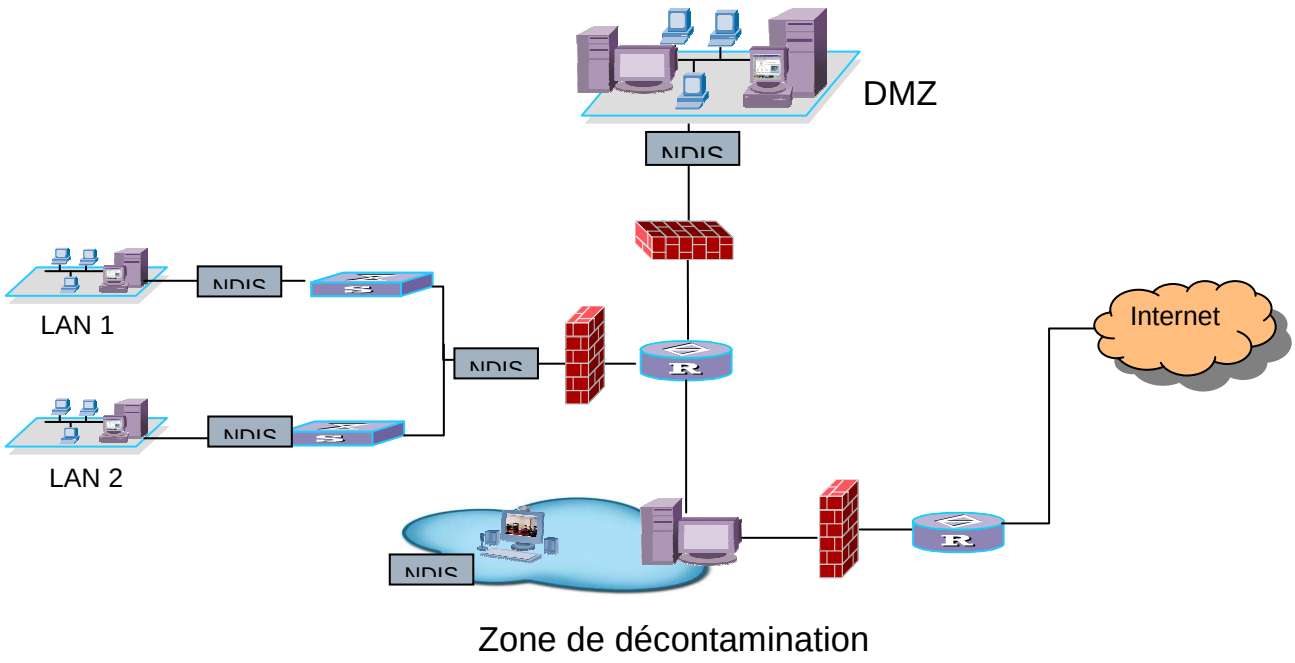


Figure 13: Architecture sécurisée du réseau lié à l'Internet

Les serveurs web et de messagerie que l'on peut accéder directement via l'Internet par les utilisateurs autorisés sont confinés dans une zone démilitarisée DMZ, i.e. dans une zone extérieure à celle du réseau local. Cependant, ces serveurs sont placés derrière un détecteur d'intrusion afin de pouvoir tracer et de prendre les mesures nécessaires pour contrer les attaques malveillantes. Le

firewall gère les ACLs i.e. il est configuré d'une sorte que seules les entités ayant les privilèges et les autorisations à accéder à ces serveurs peuvent accéder à cette DMZ.
De plus, le réseau local est subdivisé en sous réseaux à l'aide d'un switch afin de faciliter sa gestion. Un switch est préféré d'un hub car il diminue le domaine de collision et limite la zone de broadcast car seule la machine de destination reçoit l'information qui lui est destinée, donnant ainsi un niveau supérieur de sécurité face aux hubs. Chaque sous-réseau est connecté à un détecteur d'intrusion NIDS. Le firewall situé entre le réseau local et le routeur peut être configuré afin de ne laisser aucune connexion de l'extérieur vers le réseau local. De plus, le réseau local est subdivise en VLAN. Les membres des réseaux sont physiquement repartis mais ils sont confines dans le VLAN afin qu'ils puissent se connecter. La division du groupe est faite d'une façon que les membres partagent les mêmes taches et les mêmes données.

a. Configuration des serveurs de données et d'applications :

i. Le transfert des données :

Les fichiers classés en tant que très confidentiel, et confidentiel sont chiffrés lors de la transmission. Nous entamerons le détail de la configuration de ce chiffrement dans le paragraphe concernant la configuration du VPN.

ii. Les services nécessaires

Afin de garantir une sécurité maximale, il est nécessaire de n'installer ou d'arrêter les services que l'on n'a pas besoin. Par exemple, le service de SNMP, IMAP et POP ne sont pas utiles pour nos serveurs. Le serveur de partage de fichier FTP est nécessaire mais il faut bien le configurer tel que seul les utilisateurs autorisés peuvent y accéder, et de lire les fichiers ou les dossiers. Le privilège d'écriture à distance n'est pas autorisé sauf au cas de nécessité absolue.

iii. Configuration des postes de travail :

Selon le type d'utilisateurs et ses privilèges correspondants, sa poste de travail peut avoir un accès total aux serveurs d'applications et de données [46]. Afin de limiter la vulnérabilité que ces postes de travail peuvent introduire vis-à-vis du serveur, il est nécessaire de bien configurer et de contrôler les accès à ces postes de travail. La plupart des temps, le couple de mot de passe et de login constitue le premier signe de sécurité d'une poste de travail car la connaissance de ce couple peut offrir à l'utilisateur tous ses privilèges à effectuer des actions malveillantes ou non.

La configuration du browser web

Etant donné que toutes les postes de travail du LAN sont connectées à l'Internet via une passerelle, il est d'autant plus important de bien configurer le browser web que l'utilisateur utilise pour surfer le net [47, 49]. Par exemple, l'acceptation des cookies, des certificats électroniques non signées ou des plugins.

2.2.3.1.2. Configuration d'accès réseau

Toutes les postes de travail doivent obtenir leur configuration attribuée automatiquement par un serveur DHCP. Ainsi, toutes connections vers l'extérieur i.e. à l'Internet sont contrôlées.

2.2.3.2. Configuration du réseau privé virtuel VPN :

Un réseau VPN ou réseau virtuel privé est utilisé pour interconnecter d'une façon sécurisée deux entreprises géographiquement très éloignées via un réseau public non contrôlé, comme l'Internet. Dans le cas du MEFB, le réseau non contrôlé est l'air, car les données sont émises et reçues d'une liaison satellitaire.

Afin d'abaisser le prix de connexion, et d'assurer l'évolutivité du produit fini, une solution ouverte (Open Source) a été choisi. On utilise pour ce fin le package FreeS/WAN.

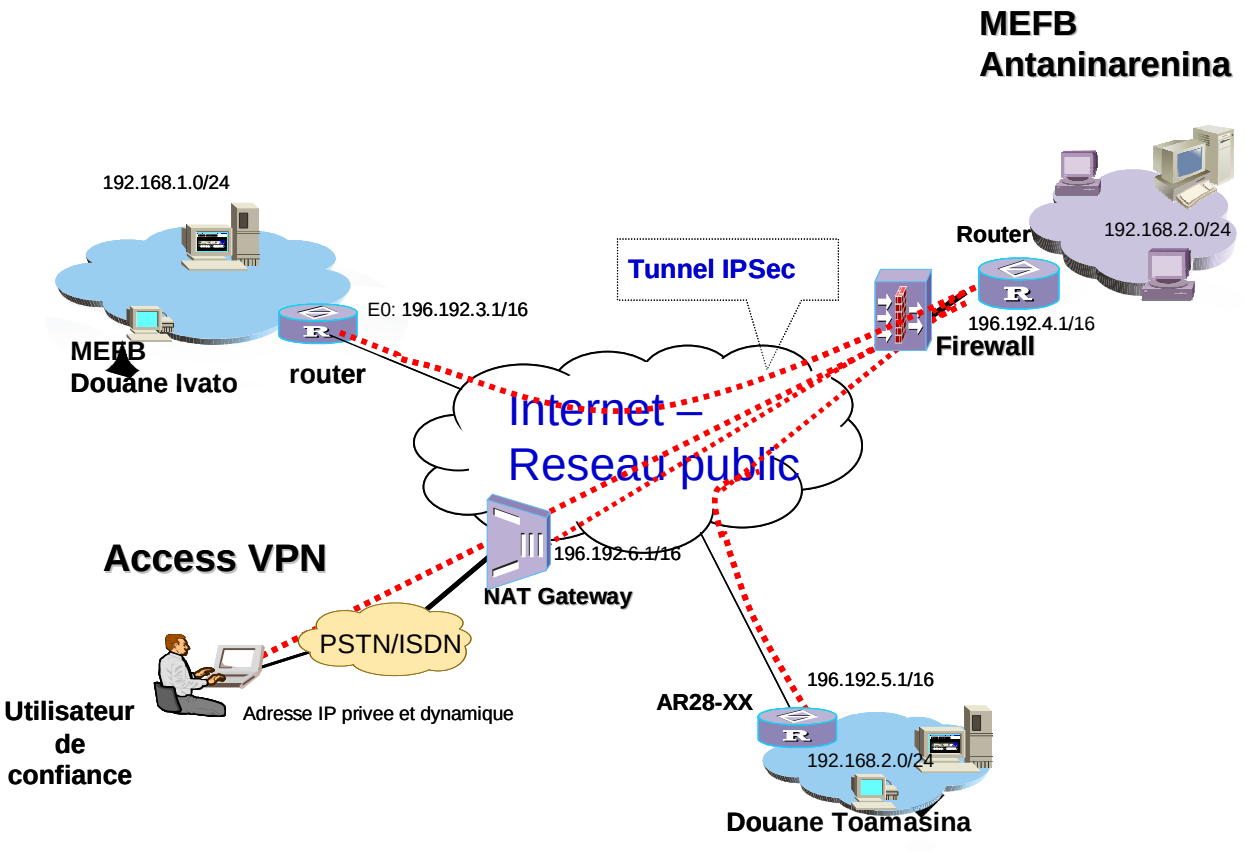


Figure 14: schéma synoptique du réseau VPN

La figure 14 nous montre le concept du VPN que l'on désire installer. Les postes de travail membres des LANs du site d'Antananarivo (site de la droite) peuvent se connecter aux postes de travail membre du site du gauche de Toamasina à travers un tunnel. Ce tunnel est établi lorsque les deux homologues veulent se communiquer suivant leur privilège.

2.2.3.2.1. Configuration de FreeS/WAN [50]

Le fichier de configuration de FreeS/WAN est .conf. Il suffit de changer les paramètres écrits dans ce fichier afin de configurer ce logiciel.

On remarque que FreeS/WAN utilise le certificat électronique pour l'authentification des données échangées entre les peers. Pour assurer que les peers sont vraiment ce qu'ils prétendent être, l'utilisation de clef asymétrique pour l'authentification est recommandée (RSA). Ces certificats électroniques peuvent être stockes dans un serveur DNS, pour faciliter leur emploi et leur mise à jour.

Un exemple de fichier de configuration de FreeS/WAN est illustré ci-dessous. Ce fichier de configuration se situe sous */etc/ipsec.conf.* On note que les adresses IP et d'autres valeurs ne sont pas celles utilisées au MEFB afin de ne pas divulguer les informations sur ce ministère.

Pour le site d'Antananarivo (site de la droite)

```
conn net-to-net
    left=196.192.4.1
    leftsubnet=192.168.2.0/24
    leftid=router_tana
    leftrsasigkey=0s1LgR7/oUM...
    leftnexthop=%defaultroute
    right=196.192.5.1
    rightsubnet=192.168.2.0/24
    rightid=@ab.example.com
    rightrsasigkey=0sAQOqH55O...
    rightnexthop=%defaultroute
    auto=add
```

Pour le site de Toamasina (site du gauche)

```
conn net-to-net
    left=196.192.5.1
    leftsubnet=192.168.2.0/24
    leftrsasigkey=0s1LgR7/oUM...
    leftnexthop=%defaultroute
    right=196.192.4.1
    rightsubnet=192.168.2.0/24
    rightrsasigkey=0sAQOqH55O...
    rightnexthop=%defaultroute
    auto=add
```

On remarque que les clefs RSA sont crées a partir de la commande sur les deux routeurs :

```
ipsec showhostkey –right
ipsec showhostkey –left
```

Pour démarrer le service VPN, on utilise la commande : `ipsec auto --up net-to-net.` On note que les noms de la connexion du site du droite et celle du gauche sont les mêmes (net-to-net).

2.2.4. Gestion des contrôles d'accès

2.2.4.1. Développement de l'annuaire électronique pour la gestion centralisée des ressources du MEFB

2.2.4.1.1. Cadrage et cas d'utilisation :

Le but de l'annuaire électronique est de faciliter la gestion des employeurs à accéder les différents serveurs et imprimantes en possession du MEFB (serveur de données, serveurs d'accès aux

réseaux, …). Ces employeurs peuvent être dans différentes branches du MEFB telles que le budget, ou la douane, …. Ils peuvent aussi être éloignes géographiquement. Ainsi, la gestion est rendue centralisée. L'annuaire est basé à Antaninarenina.

Les employeurs, selon leurs privilèges, ont accès aux serveurs de données pour lire, écrire, exécuter des fichiers, ou imprimer ces fichiers. On note que le système de gestion des bases de données utilisées par ces serveurs est Oracle. Ainsi, l'accès aux différentes tables et vues sont déjà gérer par ce SGBD. Notre rôle est donc limité à gérer globalement l'accès aux ordinateurs serveurs mais pas aux différentes données y résidant qui sont déjà gérées par Oracle.

2.2.4.1.2. Les données dans l'annuaire :

Les informations sur les employeurs, tels que le nom, numéro matricule, numéro de téléphone, l'adresse e-mail, département et nom de son activité sont obtenues automatiquement de la base de données des personnels du MEFB. Dans notre exemple que l'on peut trouver ultérieurement, les données utilisées sont tous fictifs afin de respecter les informations privées des personnels. Cependant, les informations sur les imprimantes et les serveurs sont entrées manuellement (le nom de l'ordinateur, son adresse IP, son groupe de travail, et nom de domaine, identification unique qui n'est rien d'autre que le numéro de série la machine).

2.2.4.1.3. Elaboration du schéma :

La description du schéma de l'annuaire se trouve dans le fichier slapd.conf contenu dans le répertoire */etc/openldap*

Modèle de nommage

Cette étape consiste à définir comment les entrées de l'annuaire vont être organisées, nommées et accédées. L'objectif est de faciliter leur consultation et leur mise à jour mais aussi de prévoir leur duplication, leur répartition entre plusieurs serveurs ou leur gestion par plusieurs personnes [51].

Personne : - inetOrgPerson

- Nom : cn
- Prénom : givenName
- Département : ou
- E-mail : mail
- Numéro de téléphone : telephoneNumber
- Numéro matricule : uid (identifiant unique de l'objet)

- Adresse : registeredAddress : pour l'envoi de lettres ou colis
- Activité professionnelle : businessCategory

Serveur : device

- Identifiant unique : oid (object identifier) qui n'est rien d'autre que le numéro de la machine
- Description : description du serveur
- Numéro de série : serialNumber
- Localité géographique de l'objet : l (étage, numéro de la porte, numéro de la table où l'objet est placé) ---- localisation
- Nom de l'ordinateur
- Adresse IP
- Groupe de travail
- Nom de domaine

Division ou site : - organizationalUnit

- Faritany
- Nom du site : cn (nom de l'endroit où le département est sis) par exemple : Ivato, Antaninarenina, …
- Nom du département : ou (ex : douanes, central, budget, …)

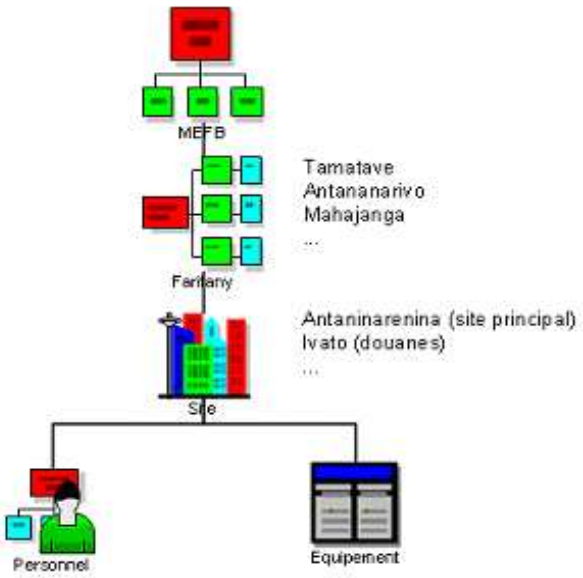


Figure 15: structure de l'annuaire LDAP pour le MEFB

A. MEFB (o)

A.1. central (ou)

A.1.1 Département informatique (department)

A.1.1.1 Personnel1 (inetOrgPerson)

…

A.1.1.n Personnel n

A.1.2 Soldes

…..

A.1.n Département

A.2. douanes

A.3. budget

….

A.n. unité organisationnelle

2.2.4.1.4. Exemples d'entrée :

Les entrées doivent être incluses dans le fichier /etc/openldap/organization/ldap-mefb.ldif. Ces entrées sont incluses avec la commande suivante:

ldapadd -D "cn=root,o= mefb.gov.mg" -f /etc/openldap/organization/ldap-mefb.ldif -w secret -x

Pour le pays (c)

```
BNC Syntax: 2.5.6.2 NAME 'country'
SUP top
STRUCTURAL
MAY (description
 $ searchGuid)
MUST ( c )
```

```
dn: c=MG
c: MG
objectClass : top
objectClass : country
description: Confoederatio Helvetica
description:Madagascar
description:Madagasikara
description: Mada
description: Gasikara
```

Pour l’organisation

```
BNC Syntax: 2.5.6.4 NAME 'organization'
SUP top
STRUCTURAL
MAY (businessCategory $ description $ destinationIndicator $
facsimileTelephoneNumber $ internationaliSDNNumber $ l $
physicalDeliveryOfficeName $ postOfficeBox $ postalAddress $ postalCode $
preferredDeliveryMethod $ registeredAddress $ searchGuide $ seeAlso $ st $
street $ telephoneNumber $ teletexTerminalIdentifier $ telexNumber $
userPassword $ x121Address)
```

MUST (o)

```
dn: o=MEFB, c=Madagascar
objectClass:top
objectClass:organization
objectClass:dcOrganizationNameForm
Description : Ministère de l’économie des finances et du budget
o : Ministère de l’économie des finances et du budget
o: MEFB
o: ministeran’ny toekarena sy ny tetibola
l:Antananarivo
l:Tananarivo
l:Tananarive
l: Antaninarenina
l: Taninarenina
postalAddress: MEFB Antaninareina BP. 1025 (valeur noforonina)
postalCode:101
telephoneNumber: +261 22 547 23
facsimileTelephoneNumber: +261 22 547 24
dc:mefb.gov.mg
```

Pour l’unité organisationnelle (organizationalUnit)

```
BNC Syntax: 2.5.6.5 NAME 'organizationalUnit'
SUP top
STRUCTURAL
MAY (businessCategory $ description $ destinationIndicator $
facsimileTelephoneNumber $ internationaliSDNNumber $ l $
physicalDeliveryOfficeName $ postOfficeBox $ postalAddress $ postalCode $
preferredDeliveryMethod $ registeredAddress $ searchGuide $ seeAlso $ st $
street $ telephoneNumber $ teletexTerminalIdentifier $ telexNumber $
userPassword $ x121Address)
MUST (ou)
```

```
dn: OU=central mefb, O=mefb, C=madagascar
objectClass: top
objectClass: organizationalUnit
description: mefb central sis à Antaninarenina
ou: central mefb
l: Antaninarenina
l: Taninarenina
postalAddress: MEFB Antaninareina BP. 1025 (valeur noforonina)
postalCode:101
telephoneNumber: +261 22 547 23
facsimileTelephoneNumber: +261 22 547 24
```

Pour les départements ministériels (department)

```
BNC Syntax: 2.5.6.6 NAME 'department'
SUP organization
STRUCTURAL
MAY (description $ l $ o $ ou)
MUST (cn)
dn: cn=Département des Systèmes d’Information , ou=central mefb, o= mefb,
c=Madagascar
objectClass: top
cn: Data Server
cn: data server
cn : serveur de données
description : serveur de données centralisé.
l : Antaninarenina
o : central mefb
ou : département de système d’informations
owner: Jean Baptiste Raly
serialNumber: Ant512
```

Le syntaxe du personnel est comme suit :

```
BNC Syntax: 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson'
SUP organizationalPerson
STRUCTURAL
MAY (audio $ businessCategory $ carLicense $ departmentNumber $ displayName $
employeeNumber $ employeeType $ givenName $ homePhone $ homePostalAddress $
initials $ jpegPhoto $ labeledURI $ mail $ manager $ mobile $ o $ pager $ photo
$ preferredLanguage $ roomNumber $ secretary $ uid $ userCertificate $
userPKCS12 $ userSMIMECertificate $ x500uniqueIdentifier)

dn: cn=Rakoto William , ou=département de système informatique, o=douane mefb,
c=Madagascar
```

objectClass: top

objectClass: person

objectClass: organizationalPerson

objectClass: inetOrgPerson

cn: Rakoto William

cn: Willy Rakoto

sn: Rakoto

givenName: William

initials: RW

title: manager, department de système informatique

uid: wrakoto

mail: wrakoto@mefb.gov.mg

telephoneNumber: +261 22 621 42

facsimileTelephoneNumber: +261 22 621 43

mobile: +033 11 257 95

roomNumber: 0209

departmentNumber: 6

employeeNumber: 423B

employeeType: full time

preferredLanguage: fr, en-gb;q=0.8, en;q=0.7

labeledURI: http://www.mefb.gov.mg/users/wrakoto My Home Page

Pour le serveur, qui n’est autre que device

BNC Syntax: 2.5.6.14 NAME 'device'
SUP top
STRUCTURAL
MAY (description $ l $ o $ ou $ owner $ seeAlso $ serialNumber)
MUST (cn)

dn :

dn: cn=Data Server , ou=département de système d’ informations, o=central mefb, c=Madagascar

objectClass: top

cn : Data Server

cn : data server

cn : serveur de données

description : serveur de données centralisé.

l : Antaninarenina

o : central mefb

ou : département de système d’informations

owner : Jean Baptiste Raly

```
serialNumber : Ant512
```

2.2.4.1.5. Slapd.conf

Données ci-après est l'extrait du contenu du fichier de configuration de slapd.conf

```
# $OpenLDAP: pkg/ldap/servers/slapd/slapd.conf,v 1.8.8.6 2001/04/20 23:32:43
kurt Exp $

include /usr/share/openldap/schema/core.schema
include /usr/share/openldap/schema/cosine.schema
include /usr/share/openldap/schema/corba.schema
include /usr/share/openldap/schema/inetorgperson.schema
include /usr/share/openldap/schema/java.schema
include /usr/share/openldap/schema/krb5-kdc.schema
include /usr/share/openldap/schema/kerberosobject.schema
include /usr/share/openldap/schema/misc.schema
include /usr/share/openldap/schema/nis.schema
include /usr/share/openldap/schema/openldap.schema

#include /usr/share/openldap/schema/rfc822-MailMember.schema
#include /usr/share/openldap/schema/pilot.schema
#include /usr/share/openldap/schema/autofs.schema
#include /usr/share/openldap/schema/samba.schema
#include /usr/share/openldap/schema/qmail.schema
#include /usr/share/openldap/schema/mull.schema
#include /usr/share/openldap/schema/netscape-profile.schema
#include /usr/share/openldap/schema/trust.schema
#include /usr/share/openldap/schema/dns.schema
#include /usr/share/openldap/schema/cron.schema

include /etc/openldap/schema/local.schema


# Define global ACLs to disable default read access.
include         /etc/openldap/slapd.access.conf


# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral       ldap://root.openldap.org

pidfile         /var/run/ldap/slapd.pid
argsfile        /var/run/ldap/slapd.args

modulepath      /usr/lib/openldap

#moduleload      back_dnssrv.la
#moduleload      back_ldap.la
#moduleload      back_passwd.la
#moduleload      back_sql.la

# SASL config
#sasl-host ldap.MyDomain.com

# To allow TLS-enabled connections, create /usr/share/ssl/certs/slapd.pem
# and uncomment the following lines.
#TLSRandFile            /dev/random
```

```
#TLSCipherSuite         HIGH:MEDIUM:+SSLv2
#TLSCertificateFile      /etc/ssl/openldap/ldap.pem
#TLSCertificateKeyFile   /etc/ssl/openldap/ldap.pem
#TLSCACertificatePath   /etc/ssl/openldap/
#TLSCACertificateFile    /etc/ssl/openldap/ldap.pem
#TLSVerifyClient 0


#######################################################################
# ldbm database definitions
#######################################################################

database        ldbm
suffix          "o=mefb.gov.mg"
#suffix         "o= mefb,c=MG"
rootdn          "cn=root, o=mefb.gov.mg"
#rootdn         "cn=administrator,o=My Organization Name,c=US"

# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw          secret
# rootpw                {crypt}ijFYNcSNctBYg

# The database directory MUST exist prior to running slapd AND
# should only be accessable by the slapd/tools. Mode 700 recommended.
directory       /var/lib/ldap
rootpw          secret

# Indices to maintain
#index  objectClass                             eq
index   objectClass,uid,uidNumber,gidNumber    eq
index   cn,surname,givenname            eq,subinitial
index   mail eq

# logging
loglevel 1

# Basic ACL
access to attr=userPassword
        by self write
        by anonymous auth
        by dn="uid=root,ou=users,o=mefb.gov.mg" write
        by * none

access to *
        by dn="uid=root,ou=users,o=mefb.gov.mg" write
        by * read
```

2.2.4.1.6. Configuration de access.conf (annexe)

Les règles pour le contrôle d'accès peuvent être incluses dans slapd.conf. Elles peuvent être aussi écrites dans un autre fichier tel qu'access.conf. Les syntaxes suivantes sont utilisées pour notre cas. On note que notre fichier de contrôle d'accès se trouve sous /etc/openldap/slapd.access.conf. Son contenu est comme suit:

```
access to dn=".*,dc=testdc" attr=userPassword
        by dn="cn=root,dc=testdc" write
        by self write
        by * auth

access to dn=".*,ou=People,dc=testdc"
        by * read

access to dn=".*,dc=testdc"
        by self write
        by * read
```

CONCLUSION

L'ouverture du système intégré de la gestion des finances publiques permet au MEFB de traiter des informations et de se communiquer entre ses branches d'une façon plus précise et plus rapide. Mais cette ouverture vers l'extérieur expose aussi le SI aux différentes attaques. La sécurisation du système intégré de la gestion des finances publiques est primordiale pour assurer son bon fonctionnement. La sécurité du SI est équivalente à celui de son maillon le plus faible. C'est-à-dire, pour assurer la confidentialité, l'intégrité et l'authentification des données, il faut garantir toutes ces services pour les données en circulation et les données en stockage, ainsi que tous les supports qui abritent ou transmettent ces données. Le contrôle physique des personnels du ME FB est fortement recommandé. Pour le contrôle d'accès logique, des solutions standardisées ont été choisi, ceci afin de pouvoir déployer, et d'évoluer le système dans le temps, et suivant les technologies disponibles.

La gestion des ressources et le control d'accès à ces ressources ont été déployées avec le protocole LDAP. Ceci dans le but de faciliter la modification comme l'ajout ou la suppression des ressources matérielles ou humaines. La maintenance du système intégré de la gestion des finances publiques est alors grandement améliorée.

ANNEXE A – ORGANIGRAMME DU MEFB

C’est le rôle du ministère des finances et de l’économie d’élaborer et de mettre en œuvre la politique financière et monétaire du gouvernement ainsi que sa politique économique. Toutes sortes des informations sont ainsi transférées d’une entité a une autre au sein du MEFB. La figure ci-dessous montre la circulation des informations entre les différentes entités de ce ministère.

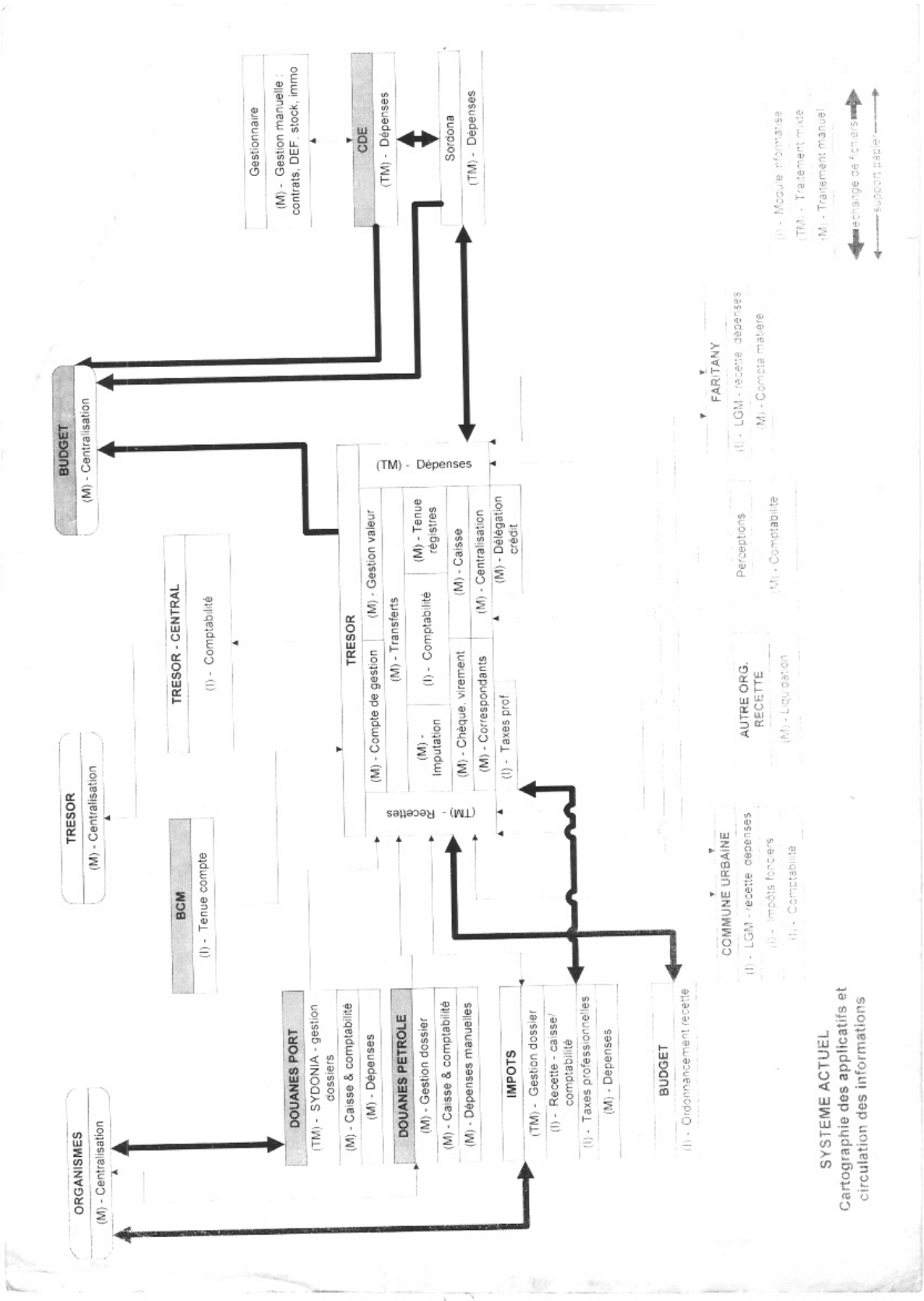


Figure 16: Cartographie des applicatifs et circulation des informations

ANNEXE B – PROCEDURE D'EXECUTION DES DEPENSES AU NIVEAU DE L'ORDONNATEUR

Les divers bureaux compris dans l'exécution des dépenses sont les CDE () et le Sordonna

La procédure de l'exécution des dépenses au niveau de l'ordonnateur est divisée en 4 phases :

- engagement
- liquidation
- ordonnancement
- paiement

a. Engagement

Exemples d'engament inclus la commande de fournitures, un contrat de travaux passé avec un entrepreneur, nomination d'un fonctionnaire, ... Dans cette phase, il y a l'engagement juridique et l'engagement financier ou comptable.

Processus général :

- Le gestionnaire rempli toutes les formalités d'usage de demande et comparaison de prix, d'appel d'offres, dévaluation du coût des travaux à réaliser
- Le gestionnaire formule une demande d'engagement où est indiqué les informations nécessaires à la détermination exacte de l'engagement et de l'autorité qui y a souscrit
- Le gestionnaire établit les liasses de titres d'engagement (3 feuillets) destinés au titulaire, au comptable et au gestionnaire
- A la réception de la demande d'engagement, le CDE vérifie la demande d'engagement et l'accomplissement des formalités (appels d'offre, comparaison des prix), confronte la situation de crédit portée à la demande avec ce qu'il détient en fonction des crédits ouverts.
- Le CDE vise, date et enregistre les formulaires établis par le gestionnaire
- Le CDE retourne l'ensemble de la liasse au gestionnaire
- Le gestionnaire signe les TEF (Titres d'Engagement Financier)
- Le gestionnaire engage la dépense auprès du titulaire.

On note que la fiche de comptabilisation des engagements et la comptabilisation se tient à la fois auprès du CDE et du gestionnaire.

b. Liquidation (rendre liquide la dette de l'Etat)

La liquidation comporte deux opérations :

- vérification que la dette de l'Etat qui résulte implicitement de l'engagement est bien née
- Détermination (par calcul) le montant de cette dette et vérification qu'elle est bien exigible

Modalités de la liquidation :

- Le gestionnaire rassemble le dossier de mandatement constitué par les pièces justificatives, le projet de mandat (qui est établit au nom du fournisseur, avis de crédit)
- Le gestionnaire procède aux vérifications du bon de commande, de la facture ou autres pièces des dépenses
- Le gestionnaire appose son nom, son cacher, sa signature à la formule de liquidation portée sur le bordereau des pièces
- Chaque dépense liquidée est enregistrée sur la FCL (Fiche de Comptabilité des Liquidations)
- Après enregistrement de l'écriture sur la FCL, le gestionnaire transmet pour ordonnancement à l'ordonnateur.

c. Ordonnancement

L'ordonnancement est la décision de payer i.e. l'ordre donné par l'ordonnateur qui porte précisément son nom, dans lequel il accepte de se dessaisir de ses fonds et de les remettre au créancier.

Modalités d'ordonnancement :

- L'ordonnateur reçoit du gestionnaire le dossier par l'ordonnancement.
- L'ordonnateur vérifie les factures et autres pièces, des certifications du gestionnaire, de la conformité de l'opération par rapport à l'autorisation consignée dans le titre d'engagement, des titres de paiement et des titres de règlement.
- L'ordonnateur signe les mandants, bons de caisse ou avis de crédit
- L'ordonnateur transmet le dossier au bureau d'émission
- Le bureau d'émission établit le bordereau d'émission des titres de paiement qui est adressé ensuite au comptable pour paiement.
- On note que l'ordonnancement est la phase finale de la démarche administrative de la procédure de dépenses.

d. Paiement

- L’ordonnateur transmet au comptable les documents établis ou recueillis par l’ordonnateur
- Le comptable est chargé de paiement

Le paiement va permettre au créancier de l’Etat d’entrer en possession des sommes qui lui sont dues au trésor publics.

ANNEXE C - EXECUTION DES DEPENSES AU NIVEAU DES COMPTABLES PUBLICS

Toutes les dépenses publiques sont payées par le trésor public dont il est assignataire (responsable) ou dont il est mandataire (pour le compte d'un autre comptable public)

Le trésor public est un département du ministère des finances qui a pour rôle d'assurer à l'Etat les disponibilités financières dont il a besoin pour faire face à ses obligations. La trésorerie principale est un lieu où l'on garde et où l'on gère les fonds publics.

Lors de la phase de paiement, le service de trésor public intervient dans l'exécution des dépenses publiques. Elle consiste à remettre de fonds au créancier, et ne peut être effectuée que par le comptable.

ANNEXE D – EXEMPLE D'ALGORITHME UTILISE POUR LA SIGNATURE ELECTRONIQUE

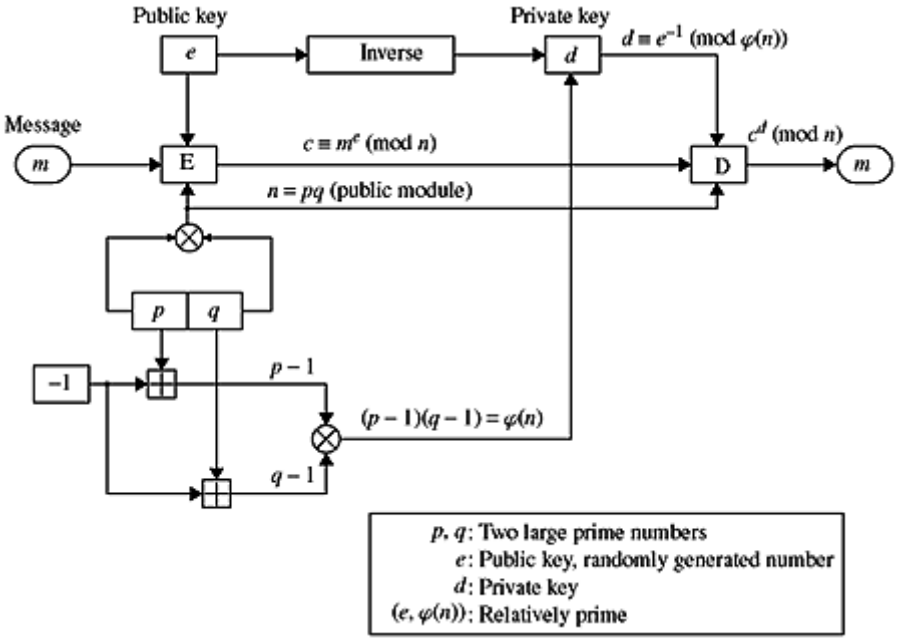


Figure 18: Le système RSA pour cryptage / décryptage

e : clef publique

n = produit de deux nombres premiers p et q qui sont tenus secrets

m = le message a encrypter

En utilisant le langage de programmation Java, voici un petit programme pour créer une classe de fonction RSA :

```
import java.math.BigInteger;
import java.security.SecureRandom;

class Rsa
{
  private BigInteger n, d, e;

  public Rsa(int bitlen)
  {
    SecureRandom r = new SecureRandom();
    BigInteger p = new BigInteger(bitlen / 2, 100, r);
    BigInteger q = new BigInteger(bitlen / 2, 100, r);
    n = p.multiply(q);
    BigInteger m = (p.subtract(BigInteger.ONE))
                   .multiply(q.subtract(BigInteger.ONE));
    e = new BigInteger("3");
```

```
    while(m.gcd(e).intValue() > 1) e = e.add(new BigInteger("2"));
    d = e.modInverse(m);
  }
  public BigInteger encrypt(BigInteger message)
  {
    return message.modPow(e, n);
  }
  public BigInteger decrypt(BigInteger message)
  {
    return message.modPow(d, n);
  }
}
```

BIBLIOGRAPHIE:

[1] F. Cuppens, M. Rusinowitch, "Sécurité informatique," *Technique et science informatiques*, RSTI série TSI Vol. 23 n° 3, 2004

[2] Z. Trabelsi, H. Ly , "La sécurité sur Internet ," *Coll. Management et informatique*, 2005

[3] Muftic′, S., *Security Mechanisms for Computer Networks*, Chichester: Ellis Horwood Ltd., 1989.

[4] Ekenberg, L., and M. Danielson, "Handling Imprecise Information in Risk Management," *In Information Security – the Next Decade*, Eloff, J. H. P., and S. H. von Solms (eds.), London: Chapman & Hall, 1995.

[5] International Organization for Standardization, *Information Technology – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*, ISO IS 7498-2, 1989.

[6] Hassler, V., *Aspects of Group Communications Security*, Ph.D. dissertation, Graz University of Technology, Graz, Austria, 1995.

[7] Schneier, B., and P. Mudge, "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)," *Proc. of the 5th ACM Conference on Communications and Computer Security*, San Francisco, CA, Nov. 2–5, 1998, pp. 132–141, http://www.counterpane.com/pptp.html.

[8] Rivest, R.L., "The MD5 Message-Digest Algorithm," The Internet Engineering Task Force, RFC 1321, April 1992.

[9] The National Institute of Standards and Technology, "Secure Hash Standard," FIPS PUB 180-1, April 17, 1995.

[10] Bellare, M., R., Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," In *Advances in Cryptology – Proc. CRYPTO '96*, pp. 1–15, N. Koblitz (ed.), LNCS 1109, Berlin: Springer-Verlag, 1996.

[11] Krawczyk, H., M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," The Internet Engineering Task Force, RFC 2104, Feb. 1997.

[12] Schneier, B., *Applied Cryptography*, 2nd edition, New York, NY: John Wiley & Sons, Inc., 1996.

[13] The American National Standards Institute, *American National Standard for Data Encryption Algorithm (DEA)*, ANSI X3.92, 1981.

[14] Hassler, Vesna.; Moore, Pedrick , "Security Fundamentals for E-commerce, " *Artech House Computer Security Series. New Series*. Boston, MA Artech House, Inc., 2001.

[15] Ingemarsson, I., D. T. Tang, and C. K. Wong, "A Conference Key Distribution System," *IEEE Trans. on Inf. Theory*, Vol. IT-28, No. 5, 1982, pp. 714–720.

[16] Koblitz, N., *A Course in Number Theory and Cryptography*, New York, NY: Springer-Verlag, 1994.

[17] European Commission, "Proposal for a European Parliament and Council Directive on a common framework for electronic signatures," May 1998, http://europa.eu.int/comm/dg15/en/media/infso/com297en.pdf.

[18] International Organization for Standardization, *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, ISO/IEC 9594-8, Sept. 1995.

[19] International Organization for Standardization, *Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types, Amendment 2: Certificate Extensions*, ISO/IEC 9594-6 DAM2, Nov. 1995.

[20] International Organization for Standardization, *Information Technology – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*, ISO IS 7498-2, 1989.

[21] Stallings, W., *Data and Computer Communications*, Englewood Cliffs, NJ: Prentice Hall, 1991.

[22] *Internetworking Terms and Acronyms*, Cisco Systems, Inc., Sept. 1995.

[23] Socolofsky, T., and C. Kale, "A TCP/IP Tutorial," The Internet Engineering Task Force, RFC 1180, Jan. 1991.

[24] Comer, D. E., *Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture*, London: Prentice-Hall International, Inc., 1995.

[25] Hauben, M., and R. Hauben, *Netizens: On the History and Impact of Usenet and the Internet*, Los Alamitos, CA: IEEE Computer Society Press, 1997.

[26] Postel, J., "Internet Protocol," The Internet Engineering Task Force, STD 5, RFC 791, Sept. 1981.

[27] Postel, J., "Transmission Control Protocol," The Internet Engineering Task Force, STD 7, RFC 793, Sept. 1981.

[28] Lambert, P.A., "Layer Wars: Protect the Internet with Network Layer Security," *Proc. Workshop on Network and Distributed System Security*, San Diego, CA, Feb. 11–12, 1993, pp. 31–37.

[29] Berson, T. A. (ed.), "Local area network security," *Proc. Workshop LANSEC '89*, Karlsruhe, Germany, April 3–6, 1989, LNCS 396, Berlin: Springer-Verlag, 1989.

[30] The Institute of Electrical and Electronics Engineers, Inc., "IEEE Standard for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS)," IEEE 802.10, 1998, http://standards.ieee.org/catalog/IEEE802.10.html.

[31] Schimmel, J., "A Historical Look at Firewall Technologies," Vol. 22, No. 1, 1997, pp. 21–23.

[32] Chapman, D. B., "Network (In)Security Through IP Packet Filtering," *Proc. 3rd USENIX UNIX Security Symposium*, Baltimore, MD, Sept. 1992, ftp://ftp.greatcircle.com/pub/firewalls/pkt_filtering.ps.Z.

[33] Cheswick, W. R., and S. M. Bellowin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Reading, MA: Addison-Wesley Professional Computing, 1994.

[34] Sun Microsystems, *Solstice™ FireWall-1™ Architecture and Administration. Version 3.0*, Revision A, April 1997.

[35] Hein, M., *TCP/IP: Internet-Protokolle in professionellem Einsatz*, Bonn: International Thomson Publishing, 1996.

[36] Bellowin, S. M., "Security Problems in the TCP/IP Protocol Suite," *Computer Communication Review*, Vol. 19, No. 2, 1989, pp. 32–38.

[37] Matus, J., "Setting up a Linux Firewall," ;*login:*, Special Issue on Security, November 1999, pp. 30–34.

[38] Egevang, K., and P. Francis, "The IP Network Address Translator (NAT)," The Internet Engineering Task Force, RFC 1631, May 1994.

[39] Srisuresh, P., and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," The Internet Engineering Task Force, RFC 2663, August 1999.

[40] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol," The Internet Engineering Task Force, RFC 2401, Nov. 1998.

[41] Postel, J., "Internet Protocol," The Internet Engineering Task Force, STD 5, RFC 791, Sept. 1981.

[42] Deering, S., and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," The Internet Engineering Task Force, RFC 2460, Dec. 1998.

[43] National Institute of Standards and Technology, "NIST Cerberus: An IPsec Reference Implementation for Linux," http://is2.antd.nist.gov/cerberus/.

[44] Rigney, C., et al., "Remote Authentication Dial In User Service (RADIUS)," The Internet Engineering Task Force, RFC 2058, April 1997.

[45] Finseth, C., "An Access Control Protocol, Sometimes Called TACACS," The Internet Engineering Task Force, RFC 1492, July 1993.

[46] Vaughn, R. B., Jr., and J. E. Bogess III, "Integration of computer security into the software engineering and computer science programs," *The Journal of Systems and Software*, Vol. 49, No. 2–3, 1999, pp. 149–153.

[47] Berners-Lee, T., R. Fielding, and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax and Semantics," The Internet Engineering Task Force, RFC 2396, Aug. 1998.

[49] Raggett, D., A. Le Hors, and I. Jacobs, "HTML 4.01 Specification," W3C Recommendation, Dec. 24, 1999, http://www.w3.org/TR/html4/.

[50] Gilmore J., et al., www.freeswan.org/

[51] Greg, L., "YoLinux LDAP Tutorial: Deploying OpenLDAP – Directory Installation and Configuration", http://www.yolinux.com/TUTORIALS/LinuxTutorialLDAP.html

RENSEIGNEMENTS :

Nom: RANDRIANARIVONY

Prénoms: Miarisoa Fenomanana

Adresse: Lot 2 j 60 HAC Ivandry, Antananarivo 101

Titre du mémoire: Sécurisation du Système d'Information Intégré de la Gestion des Finances Publiques du MEFB

Nombres de pages : 91 pages

Nombres de tableaux : 4 tableaux

Nombres de figures : 17 figures

Mots clés : Sécurité, système d'information, finance publique, MEFB, politique de sécurité, disponibilité, intégrité, authentification, signature électronique, réseau virtuel privé, tunnel, IPSec, L2TP, gestion de clefs, IKE, encryptage et décryptage, gestion de ressources, LDAP

Directeur de mémoire : Monsieur Lucien Elino RANDRIARIJAONA

RESUME :

Afin de répondre aux exigences du DSRP, le Ministère de l'Economie, des Finances et du Budget (MEFB) a mis en place un système d'information informatise pour gérer efficacement les finances publiques : la rapidité des travaux administratifs, l'exactitude des résultats obtenus, et aussi la transparence de la gestion. Puisque MEFB est constitué de plusieurs branches, l'utilisation de la technologie nouvelle de l'information au niveau de ce système d'information est cruciale.

Cependant, l'ouverture de ce SI au monde externe, notamment l'Internet menace le bon fonctionnement de ce SI. Une mesure de sécurité est donc nécessaire pour assurer les services que le SI fournisse. Cette mesure englobe la disponibilité des données en temps voulu, l'exactitude des données en stockage ou en transmission, ainsi que l'authentification des opérateurs du MEFB. C'est la mise en place de ce système de sécurisation qui est le but fondamental de ce mémoire. Subséquemment, une méthode de l'implémentation de la sécurité est tout d'abord entamée, suivie des meilleures pratiques visant les opérateurs et leurs outils de travail, et enfin les approches techniques pour installer un environnement informatique sécurisé pour le MEFB. Ce dernier point encadre les réseaux VPN, les différents outils pour répondre aux attaques informatiques, et la gestion des ressources matérielles ou humaines utilisant LDAP.

SUMMARY:

In order to adhere to the requirements of the DSRP, the Ministry of the economy, Finances and Budget (MEFB) installs a computerized information system to manage efficiently the public finances: the rapidity of the administrative works, the exactness of the obtained results, and also the transparency of the management. Since MEFB is constituted of several branches, the usage of the new information technology is crucial. Nevertheless, the opening of this IS to the external world, notably the internet threatens its good functioning. A measure of security is therefore necessary to assure the services that the IS offers. This measure includes the availability of the data in desired time, the exactness of the data in storage or in transmission, as well as the authentication of the operators of the MEFB. It is the goal of this book to offer a method and technical operation on how to implement the security system for MEFB information system. To achieve this goal, a method of the security strategy is given, followed by the best practices for operators and their working tools, and at last a technical approach on how to install a secure computerized environment for the MEFB. This latter includes the installation of VPN networks, the introduction of different tools against computer attacks as well as the implementation of a management system of the human and material resources using LDAP.