N° d'ordre : 014/2005-M/IN

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie *Houari Boumédiene*

Faculté d'Electronique et d'Informatique
Département d'Informatique

Mémoire présenté
pour l'obtention du diplôme
de Magister

En : Informatique

Spécialité : Intelligence Artificielle et Bases de Données Avancées

Par : Naci Mohamed Djamel

Sujet :

Module Comportemental De l'EIDS* Pour Clients Mobiles

* Embedded Intrusion Detection System

Soutenu le : 12– 12 - 2005, Devant le jury composé de :

– Mr N. BADACHE	Professeur	USTHB	Président
– Mr A. BELKHIR	Maître de Conférence	USTHB	Directeur de thèse
– Mr A. NACER	Professeur	USTHB	Examinateur
– Mr A. AISSANI	Professeur	USTHB	Examinateur

REMERCIEMENTS

Mes remerciements s'adressent à Mr. A. BELKHIR pour m'avoir proposé le sujet, et pour son entière disponibilité durant toute la période de la thèse.

Je remercie Mr. N. BADACHE de l'honneur qu'il nous a fait en présidant le jury.

Je remercie aussi Mr. A. AISSANI et Mr. A. NACER d'avoir accepté de faire partie de ce jury.

Comme je tiens à remercier toute l'équipe du CERIST pour leur soutien durant la période de ma thèse, et en particulier aux responsables et aux éléments du laboratoire des Logiciels de Base (LLB).

Enfin je remercie tous les membres de ma famille, la famille Naci; à tous mes amis et collègues du CERIST et d'*iQualix* Algérie, de la RUB III .

Dédicaces

Je dédie ce mémoire :

A mes très chers parents qui m'ont beaucoup soutenu et encouragé durant toutes mes années d'études.

A ma grande mère *Hamida*.

A mon frère *Saad* et à ma sœur *Wassila*.

A mes tantes *Yamina, Amina, Atika, Souraya, Kenza*, *Malika*, *Habiba* et toutes leurs familles pour m'avoir soutenu durant tous mon cycle universitaire. Et à mes oncles *Mohamed, Mohamed, NourEddine* et leurs enfants.

A tous les membres de ma famille, grands et petits, proche et lointain.

A mes collègues de travail au sein d'*iQualix Algérie*

A tous les membres du Laboratoire LLB et DCTD du CERIST.

A tous mes voisins de la cité *S.N.V.I* (Mazzouni).

A mes amis: *Abdelah, Amine, Rachid, Kamel, Samir, Rezki, BenCherki, Khiter, Moukrane, Abdel Djébbar, Djamel, Mokhtar, Brahim, Ammari, Badni, Abddeka, Hamid, Ali, Amer,Chafik, Hadi, Nourine, Youssef, Mohamed, Salim, Arbi, Djaber, Ahmed, Adel, Houssine, Omar, Mechikel, Ezzaim, Omar, BenDeken, Sid Ahmed, Nassim, Sallah, Bertrand, Hadou, Issa, Mustapha, Amine, Reda, Abbas, fical, Abderrahmane,Haddad*, *Mizi, Kortebi, Geninech, Abdelaziz,Smail, Farouk, Messoud, Athmane Amine, Fateh, Mohamed,Baghdad, Hichem, Amine, Samir, Sofiane, Sofiane, Hichem (a_hic), Khaled, Seba, Lyes….*

Et surtout à : *Amine Taibi, Mohamed Boutouiga, Amer Bendriss, Amine Garici, Djamel Tahraoui, Medjahdi Fateh*

A tous mes professeurs et enseignants…

A mon directeur de thèse M. *A. Belkhir*…

Naci Djamel.

… … …

Résumé

Résumé-

Ce dernier siècle est marqué par le grand succès qu'a connu le monde des nouvelles technologies de l'information et de la télécommunication. Ce succès a encouragé deux phénomènes: l'évolution technologique des terminaux mobiles sans fil, et la dépendance des êtres humains de ces terminaux. Les terminaux mobiles sont devenus des ordinateurs à part entière, en offrant tout ce qu'offre les ordinateurs comme services tout en étant mobiles. Cette évolution a poussé beaucoup de gens à en être dépendant. Les terminaux mobiles sont devenu des outils de travail; en contenant les informations confidentielles, en permettant l'accès à distance aux environnements de travail, et en offrant les services d'Internet, de téléphonie et de vidéoconférence. Ce qui a permis aux attaquants d'élargir leurs champs d'action vers les réseaux mobiles sans fil et leurs terminaux.

Notre première étape dans ce travail a été d'étudier, de recenser et d'analyser les différents risques et menaces dans l'environnement des réseaux mobiles sans fil ainsi que leurs terminaux. Ces terminaux mobiles sont exposés à plusieurs vulnérabilités et attaques, allant des attaques virales au risque de vol physique. Ce qui nous a motivé à proposer une solution pour la protection de ces terminaux, en proposant la mise en œuvre d'un système de détection d'intrusion embarqué sur ces terminaux EIDS [BNR04].

Par la suite nous avons analysé notre solution EIDS. L'EIDS est un IDS hybride qui protège le terminal de plusieurs risques et attaques, mais reste néanmoins incomplet et inefficace face aux risques d'attaques récentes (non préalablement recensées), ainsi qu'aux risques d'usurpation d'identité ou de vol. Ces inconvénients ajoutés au fait que le terminal mobile est à utilisation personnel (un seul propriétaire), ont motivé notre présent travail pour le renforcement de l'EIDS, par la proposition et la mise en ouvre d'un module comportemental.

Le module comportemental trouve tout son intérêt du fait que le propriétaire est unique, et du fait que ce dernier coopère et interagit avec tous les autres modules de l'EIDS, afin d'établir le profil du propriétaire. Un module comportemental sert à profiter au mieux des informations collectées par les différents modules. L'analyse globale de toutes ces informations servira à déceler les nouvelles formes d'attaques.

Au début le module comportemental agit en constituant un profil de référence de du propriétaire du terminal mobile, et en ce basant sur ce dernier il audite le système et analyse les informations émanant des autres modules afin de déceler un changement de comportement. Ce changement anormal du comportement se traduit par une variation excédant un certain seuil, entre le profil de référence et le profil instantané.

Pour mettre en œuvre le module comportemental on a opté pour l'approche statistique; qui est connu pour sa robustesse et pour le fait d'aboutir à des implémentations de manière rapide. Dans cette approche il fallait trouver un modèle statistique pour modéliser notre système (*comportement* et *profil*). Dans ce cadre nous avons proposé d'utiliser les histogrammes et leurs fonctions de distances. Le profil est représenté par des histogrammes de fréquences d'événements, ces derniers collectés par les différents modules de l'EIDS. La variation du

comportement est calculée en utilisant des fonctions de distances d'histogrammes ; nous en avons choisi quatre : *forme L1*, *forme-L2*, *Quadratique*, et *Mahalanobis*. Nous avons implémenté ce module en utilisant ces quatre distances et nous les avons testé afin d'en choisir ceux qui étaient les plus adaptées à notre cas.

Afin de choisir et de valider notre choix du modèle nous avons effectué des tests sur un échantillon d'utilisateurs au sein d'une entreprise. Les scénarios des tests ont été classés en deux catégories. Une catégorie des tests pour valider la constitution du profil par les histogrammes, en étudiant pour les mêmes utilisateurs le comportement de leurs profils pendant une période et le niveau de stabilité de ces derniers. Et une seconde catégorie pour vérifier l'efficacité du module comportemental dans la détection d'intrus, en essayant de simuler plusieurs attaque par usurpation d'identité par le changement d'utilisateurs. Finalement nous avons aboutis à des résultats concluant que les deux premières distances donnaient de bons résultats contrairement aux deux dernières qui n'étaient pas adaptées au contexte choisi (ce qui représente en soit un résultat).

Par ce travail nous avons pu explorer le domaine des IDS comportementaux, et nous avons essayé de proposer un petit apport dans le domaine de la sécurité mobile. Dans un domaine ou le 100% n'existe guère ce modeste travail représente un apport pratique. Ce travail ne ce limite pas aux terminaux mobiles mais peut être appliqué à tout poste à usage personnel, notamment dans le cadre d'un réseau local d'entreprise.

Comme perspective à notre travail nous proposant d'approfondir l'étude et l'analyse des autres approches comportementales afin d'en développer une nouvelle, qui profite des avantages de tous les autres approches tout en comblant leurs défauts. Et tout en respectant les spécificités des environnements mobiles sans fil. Ainsi que l'élargissement du domaine d'application de notre approche pour les réseaux privés. Sans oublier de chercher une meilleure méthode pour gérer les faux positives et les faux négatives, qui représente l'un des problème majeur du domaine des IDS.

Sommaire

Sommaire

Chapitre II : *Les **S**ystèmes de **D**étection d'**I**ntrusion -**IDS***

Introduction

Introduction

Le domaine de la sécurité informatique peut être simulé à un champ de mines car il évolue avec d'énormes contraintes tout en préservant le principe que «l'infaillible n'existe pas», et que son but et d'essayer de limiter les dégâts, mais cela n'empêche pas de travailler à se rapprocher le plus possible de la solution idéale.

La difficulté existe du fait qu'il y'a une variété des problèmes (les programmes contiennent des bugs, les protocoles réseaux admettent beaucoup de failles, les gens sont malveillants, l'élaboration d'un système de sécurité puise beaucoup de ressources …) [COL05].

Ces dernières années, la sécurité informatique est devenue un problème majeur dans le domaine de la technologie de l'information, surtout avec l'avènement des réseaux informatiques, qui imposent l'idée de partage de données et de circulation de l'information à travers ces réseaux en offrant la possibilité d'accéder à l'information à distance [COL05]. Ce qui représente en soit un des maillons faibles des systèmes informatiques. Avec l'émergence du nombre d'attaques et d'attaquants, des tentatives de piratage, d'intrusion interne et externe (les attaques qui proviennent de l'extérieur représente moins de 20% des attaques commises et le reste sont dus à des utilisations internes du réseau) [ANO99], contre les différentes institutions économique, politique, ou commerciale, est née l'idée de la nécessité de protéger et de sécuriser ces systèmes.

Les clients mobiles qui participent aux réseaux de 2^{ieme} et 3^{ieme} génération connaissent une grande évolution technologique; ils sont devenus carrément des petits ordinateurs à part entière, en fournissant tout ce qu'un ordinateur peut offrir, tout en étant, mobile, moins encombrant et plus privé; chose qui les rend d'une autre part plus vulnérables [FAR03a][FAR03b][PEI02] [WRI03]. Ils sont d'une part soumis à toutes les attaques et faiblesses qui touchent les ordinateurs liées à un réseau (Internet); et d'autre part ils sont soumis aux contraintes et vulnérabilités spécifiques aux environnement mobiles sans fil; tel la nature physique du support sans fil et la difficulté matérielle à le protéger, les limitations des clients en matière d'autonomie d'énergie, de puissance de calcul, d'espace de stockage; en plus du risque de vol qui n'est pas négligeable [PEI02].

Tous ces risques, qui feront l'objet des premiers chapitres, représentent les problèmes à résoudre par une solution de sécurité mise en oeuvre sur une plateforme embarquée.

La problématique qui se pose pour nous est : « *Comment protéger les clients mobiles sans fils de ces différents risques ?* ».

L'étude s'est focalisée à travers le moniteur de comportement sur l'aspect comportemental de notre EIDS (*Embedded Intrusion Detection System*) [BNR04]; ce domaine peu exploré dans les IDS et qu'on veut à travers ce modeste travail franchir le premier pas dans ce volet des IDS. En vue de proposer des solutions aux problèmes de sécurité futurs qui peuvent se poser avec l'introduction de la norme UMTS [CCR98] (réseaux mobiles sans fils de la 3eme génération).

Cette approche s'intéresse au facteur humain de l'usager, en essayant de voir comment ce dernier se comporte afin de déceler des tentatives d'attaques non préalablement enregistrées, et afin de remédier aux problèmes d'usurpation d'identité et de vol. L'étude se focalisera sur les habitudes et les actions entrepris par le propriétaire du terminal mobile, afin d'établir un profil utilisateur. Ce dernier qui va être employé pour le suivi de l'utilisateur. Cependant le calcul du profil exige un choix d'approche et de modèle, et c'est dans ce contexte que notre apport intervient.

On commence l'étude par la présentation de notre architecture [BEL04], par la suite on présentera la conception du noyau de l'EIDS qui est le *Module Comportemental*. Ce module puise ces informations à partir de tous les autres modules pour essayer de tracer un profil au propriétaire du terminal; et qui au fur et à mesure contrôle l'authenticité de l'utilisateurs actuel.

Ce travail ne se limite pas aux terminaux mobiles mais peut être appliqué à tout poste à utilisation personnelle, notamment dans le cadre d'un réseau local d'entreprise.

Ce mémoire sera organisé en respectant le plan suivant :

- Chapitre I : «*Sécurité informatique dans l'environnement mobile sans fil – Etat de l'Art* »

  Étude et synthèse des diffèrent problèmes de sécurité et les techniques de défense dans un système informatique. Ainsi qu'une synthèse sur les environnements mobiles sans fils ; afin de cerner les problèmes de sécurité qui en découlent.

- Chapitre II : «*Les Systèmes de Détection d'Intrusion*»

  Etude détaillée des IDS (Système de détection d'intrusion), de leurs taxonomies, de leurs classifications ainsi que l'énumération de quelques IDS.

- Chapitre III : «*L'EIDS – un IDS hybride embarqué* »

  Dans cette partie nous décrivons notre architecture pour un IDS hybride sur une plateforme embarquée, qu'on a nommé « EIDS : *Embedded Intrusion Detection System* » [BEL04].

- Chapitre IV : «*Le Module Comportemental de l'EIDS – La Solution* »

  Dans cette section on présente la solution qui s'inscrit dans notre solution globale [BEL04]; on expose les motivations et les avantages de l'ajout d'un *Module Comportementale* à l'architecture de l'EIDS. On décrit la conception de ce module avec les méthodes utilisées pour sa mise en œuvre, et l'interaction qu'a ce dernier avec les autres modules de l'EIDS. Et on montre l'apport de cette solution à notre architecture globale.

- Chapitre V : «*Tests & Résultat*»

  Dans cette section on expliquera la logique d'élaboration des tests et leurs résultats, afin de valider l'approche proposée.

Chapitre I:

Sécurité Informatique dans l'environnement Mobile Sans Fil

–Etat de l'Art–

Sécurité Informatique dans l'Environnement Mobile Sans-Fil

– Etat de l'Art –

Sécurité VS Mobilité.

I. Introduction :

Aujourd'hui les deux domaines de la sécurité informatique et des environnements mobiles sans fil sont devenus très liés. On ne peut pas parler d'infrastructure mobile sans fil sans évoquer le niveau de sécurité assuré dans cet environnement. Afin d'assurer une bonne qualité de service (confidentialité, disponibilité) aux usagers, en dépit des attaquants quelque soit leurs natures. Un environnement mobile sans fil est bénéfique à l'homme, mais sans sécurité il demeura sans usagers. Les environnements mobiles sans fil apportent de nouvelles spécificités, ce qui rend la tache de la sécurisation plus difficile.

A travers ce chapitre on évoque les facettes de la sécurité informatique, et on explore les spécificités des environnements mobiles; afin d'énumérer les problèmes de sécurité dans ces environnements.

II. Sécurité :

Avant l'apparition des réseaux informatiques, lorsque les entreprises disposaient d'un centre de calcul d'une seule machine, assurer la sécurité était un problème simple. La seule chose à faire était de poster un garde en faction devant la porte d'accès au centre de calcul, qui pouvait vérifier qu'aucun dérouleur, aucun disque ou même aucune carte n'était déplacée sans une autorisation explicite [TAN90] tout en supposant bien sur la confiance de ce garde. Le problème était plus, un problème de *protection* que de sécurité [SIL94].

Avec l'avènement des réseaux, la définition de la sécurité a radicalement changé. Personne ne peut plus contrôler manuellement les millions des bits qui transitent quotidiennement entre les ordinateurs du réseau [TAN90]. A la mise en oeuvre de l'Internet, le critère de la sécurité était très loin d'être un critère important, le but principal était alors que toutes les machines des sites, sans exception, pouvaient accéder et être accessibles de l'Internet avec le meilleur débit possible. Maintenant l'Internet est devenu un outil de communication mondial utilisé par les bons et les mauvais citoyens, l'Internet n'est pas plus noir que le monde mais elle n'est pas plus blonde non plus.

On a pu voir rapidement que cette connectivité totale est une aubaine pour les personnes malintentionnées qui pouvaient ainsi essayer très facilement d'attaquer toutes les machines d'un site et d'en découvrir rapidement un maillon faible.

Le choix du « tout ouvert» (*Full connectivity*), au moment ou il a été fait n'était pas une erreur mais rester maintenant dans la même logique en est une [ARC00]. C'est là où intervient l'un des rôles de la sécurité informatique, en limitant les possibilités de communication entre l'intérieur et l'extérieur, et en ne laissant passer que ce qui est utile.

La sécurité informatique est un ensemble de moyens mis en oeuvre pour minimiser la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles, sans faire la confusion avec la protection, la protection est strictement un problème interne, en revanche la

sécurité requiert non seulement un système de protection adéquat, mais également la prise en compte de l'environnement externe du système.

La sécurité doit protéger l'information stockée dans le système (données et codes) ainsi que les ressources physiques contre les accès non autorisés; la destruction ou altération malveillante, et l'introduction accidentelle d'incohérences [SIL94].

II.1. Caractéristiques d'un Système Sécurisé

Un système sécurisé doit assurer les critères suivants [COL05]: l'*Authentification,* la *Confidentialité,* la *Disponibilité,* l'*Intégrité,* le *Contrôle d'accès*: Ce sont les cinq éléments clés de l'évaluation d'un système sécurisé.

a. Authentification :

La première étape afin de protéger les ressources d'un système informatique est de pouvoir vérifier l'identité des utilisateurs, cette vérification s'appelle Authentification. [CST96]

Le système de protection dépend de la capacité à identifier les programmes et les processus en cours d'exécution, cette capacité s'appuie sur la possibilité d'identifier chaque utilisateur du système.

Généralement l'authentification s'effectue sur trois ensembles : [SIL94]

- Possession utilisateurs (une clé ou une carte).
- Connaissance utilisateurs (identificateur d'utilisateur ou un mot de passe).
- Attribut utilisateurs (emprunte digitale, configuration de la rétine, signature,…).

En d'autre terme, elle se base sur quelque chose que l'on possède, quelque chose que l'on connaît et quelque chose que l'on est.

Parmi les mécanismes d'authentification :

- Mot de passe (code d'identification).
- Biométrie.
- Carte à puce.

b. Confidentialité :

C'est une protection contre les menaces qui peuvent causer la divulgation non autorisée d'information alors qu'il faut veiller au caractère privé de l'information. On devrait utiliser des mesures ou services de confidentialité, constituant en quelque sorte une protection de première ligne. Ces mesures peuvent comporter des mécanismes utilisés conjointement avec les mesures de contrôle des accès (utilisation de LCA liste de contrôle d'accès), mais elles peuvent aussi utiliser des techniques de chiffrement afin d'accroître d'avantage la confidentialité de l'information. Les mesures de confidentialité peuvent également comprendre l'utilisation d'une voie de communication secrète. [CST96]

c. Disponibilité :

C'est la protection contre les menaces qui peuvent causer la perturbation des fonctions du réseau, y compris la non-disponibilité des services, le vol ou la destruction de matériel (ou) de données, ainsi que la défection du matériel comme leur nom l'indique. Les services de disponibilité assurent à tous les utilisateurs l'accès aux ressources et aux données, comme prévu. Dans certaines applications, ces services visent expressément les attaques ou les événements pouvant mener à un déni de service. Dans les organisations où la perturbation des fonctions du réseau peut causer de graves préjudices, il ne sera probablement pas suffisant de faire

régulièrement des copies de sécurités des donnés. Les services de disponibilité vont au-delà de la simple copie de sécurité.

On peut diviser ces services en deux groupes principaux. Dans le premier, nous retrouvons des services de limitation c.à.d les services qui sont requis pour empêcher les personnes, que leurs intentions soient malicieuses ou non, de sur utiliser les ressources du réseau, comme l'espace disque, la mémoire, la largeur de bande… etc, de telle sorte que ces ressources ne soient plus disponibles pour les autres utilisateurs. Par ailleurs, un deuxième groupe de services de disponibilité assure le maintien des fonctions du réseau lorsqu'il y a une panne de matériel ou de logiciel ; ce groupe est désigné sous l'appellation « Tolérance aux pannes ».

d. Intégrité :

C'est la protection contre les menaces qui peuvent causer la modification non autorisée de la configuration du système ou des donnés.

Les services d'intégrité visent à assurer le bon fonctionnement des ressources et la transmission ou l'enregistrement sans problème des donnés, ces services assurent une protection contre la modification délibérée ou accidentelle et non autorisée des fonctions du système (intégrité du système) et de l'information (intégrité des données). [CST96]

e. Contrôle d'Accès :

C'est la protection des ressources contre les accès non autorisés (il faut posséder les bons droits et les privilèges pour utiliser la ressource), elle inclue aussi la protection physique des équipements.

Donc pour protéger un système il faut prendre des mesures de sécurité à deux niveaux ; un niveau bas qui inclus l'implantation des mécanismes de sécurité (SE et les logiciels de gestion de la sécurité); et un niveau haut qui lui-même peut inclure deux parties :

Physique : les sites contenant des systèmes doivent être physiquement protégés.

Humaine : les utilisateurs doivent être autorisés en prenant de grandes précautions, pour diminuer la possibilité qu'un utilisateur offre l'accès à un intrus.

Une faiblesse à un haut niveau de sécurité (physique ou humaine) permet de contourner les mesures strictes de sécurité de bas niveau (SE) [SIL94].

II.2. Problèmes de la Sécurité

La sécurité informatique à pour objectifs de minimiser les vulnérabilités, et de protéger les systèmes informatiques contre les différentes attaques. Ces vulnérabilités consistent en :

a. Les bugs :

Plusieurs logiciels et applications présentent des bugs qui sont exploités par les attaquants pour acquérir les droits administrateur de la machine vulnérable [ARC00].

Les bugs se situent aux niveaux applications serveur, applications client, système d'exploitation et des piles réseaux. Parmi ces bugs :

- ✓ *Buffeur Overflow*: (débordement de tampon) comme exemple une procédure de login avec un *Username* de 256 caractères max, si en envoi 300 caractères ceci risque de faire crasher le système. [LEG00]
- ✓ *Manipulation suspecte* : Les programmes interagissent avec le système d'exploitation en lui donnant des entrées (comme le langage Perl); comme exemples d'attaques on cite les injections SQL. [LEG00]
- ✓ *Entrée non traité*: Au cas où on accepte des entrées dont on n'a pas traité leurs cas, cela peut causer des crash; la réaction de la pile TCP/IP au configuration d'entêtes non traités. [LEG00]

b. Limite de la cryptographie :

La cryptographie a ses faiblesses (Cryptanalyse) et les clés peuvent être cassées, et il n'existe pas une organisation gérant l'ensemble des clés et autres éléments cryptographiques.

c. L'abus des droits légitimes :

Même un système fiable peut être attaqué par des personnes abusant de leur légitimité, car on estime que plus de 80% des attaques viennent de l'intérieur du réseau par des personnes abusant de leurs droits [SUN96].

d. Administration lourde :

Les machines utilisant ces systèmes sont livrées avec de nombreux services installés par défaut. Nous ne les utilisons pas tous, mais ils restent néanmoins actifs dans le système et augmentent inutilement sa vulnérabilité [ARC00].

e. L'Environnement Multi-tâches:

La plus part des systèmes offrent un environnement qui permet au processus de générer dynamiquement d'autre processus; cela peut conduire à une situation ou les ressources du système et les fichiers des utilisateurs sont mal utilisés [SIL94].

f. Vulnérabilités liées au réseau :

Ces vulnérabilités se classent sous cinq catégories qui sont [CST96]:

- Accès non autorisé au réseau.
- Divulgation non autorisée.
- Modification non autorisée.
- Perturbation des fonctions Réseaux.
- Actions trompeuses.

g. les Attaques :

Différents types d'attaques sont recensées et leur niveau de technicité et de sophistication n'a guère cessé d'accroître, comme le montrent la figure suivante : (*Center for Education and Research in Information Assurance and Security* (CERIAS) et *National Institute of Standards and Technology* (NIST))

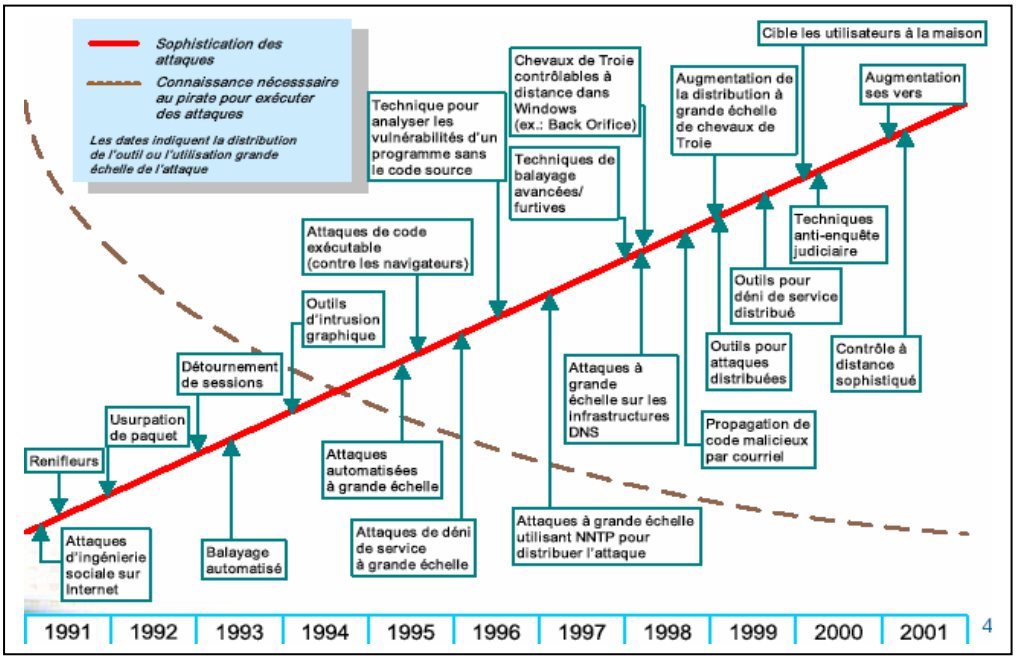


Figure I.1 : *Sophistication des attaques* [MER04]

Ces attaques peuvent être englobés en: *Virus* [LUD97][ANO99], *Vers* (worms), *Chevaux de Troie* [ANO00], *Sniffers* [KOA01], *Trappes* , *Crackers*[ANO99], *Spoofing, DoS & DDoS*[ISO89][KOR01], *Scanneurs* [ADG01][DEN01]…. .

II.3. Techniques et Méthodes de Sécurisation – Mécanismes de Sécurité

Devant cette grande variété d'attaques et de vulnérabilités; il existe plusieurs méthodes de protection. Ces mécanismes de sécurisation et de protection essaient de remédier aux attaques provenant des différentes catégories d'agresseurs (plaisantins, vandales, compétiteurs et espions) ou par des manipulations malintentionnées (accidentelles) [CHA97]. Nous citons [ANO02] [COL05] : les *Mots de Passes,* la *Cryptographie* [TAN90][SIL94][CST96], les *Firewalls* [CHA97], les *VPNs* [SHE00], les *Proxy* [SHE00], les *Antivirus* [TEC01][LUD97], et les IDS.

III. Mobilité :

III.1. Introduction

L'informatique mobile permet aux utilisateurs de se déplacer tout en restant connectés au réseau, il leur devient donc possible d'accéder à leur environnement de travail et de continuer à communiquer. Pour cela, les machines doivent disposer d'interfaces de communication sans fil utilisant des ondes radio fréquences ou lumineuses; et constituant de ce fait un réseau sans fil.

Les réseaux sans-fil se développent très rapidement et devraient représenter un marché énorme au XXI siècle. Le premier réseau commercial analogique sans fil a vu le jour en 1982 à Chicago. Puit à la fin des années 80s, les premiers réseaux GSM (numériques) sont apparus, remportant le grand succès que nous connaissons aujourd'hui.

Les réseaux mobiles sans fil sont classés en :

- Les WPAN (Wireless Personal Area Network): avec les deux normes Bluetooth, HomeRF.
- Les WLAN (Wireless Local Area Networks): IEEE 802.11 (US) et Hiperlan (Europe).
- Les technologies Cellulaires (GSM, GPRS, UMTS).
- Les technologies Satellite (VSat qui est bidirectionnel, mais aussi DVB pour la diffusion Vidéo).

Les réseaux sans fil représentent donc un enjeu important, surtout au niveau financier; ils permettent d'éviter d'investir dans un câblage coûteux, et qui peut s'avérer rapidement obsolète ou inutile en cas de déménagements de locaux.

III.2 Applications des réseaux sans fil :

Les réseaux sans fil peuvent s'interconnecter à d'autres réseaux filaires existant (Internet), tout en permettant la mobilité des utilisateurs. De plus, le câblage n'est plus nécessaire, ce qui représente un avantage certain dans le cas des réseaux momentanés de courte durée (chantiers, exposition,…)

Ils sont utilisés dans plusieurs domaines: dans les hôpitaux, ils sont déjà utilisées pour accéder aux informations enregistrées sur chaque patient pendant les visites. De même pour les aéroports et les chantiers de constructions. Ils servent à faire la liaison par voie hertzienne entre deux bâtiments ayant chacun leur réseau câblé.

Les WLAN peuvent également être utilisés pour la lecture des codes barres dans les supermarchés. Et selon les constructeurs, ces technologies devraient s'étendre dans les prochaines années pour équiper tous les objets de notre vie quotidienne. Les voitures ouvriront leurs portes à la seule approche de leur propriétaire ou communiqueront directement avec la pompe de la station-service, le réfrigérateur fera lui-même sa commande par Internet, les PDA se synchroniseront automatiquement avec les PC et s'échangeront fichiers et e-mails. En arrivant chez vous, la porte d'entrée se déverrouillera automatiquement, le système d'alarme se mettra en veille et les lumières s'allumeront.

III.3. Caractéristiques et Spécificités des Environnements Mobiles sans fil

Afin d'assurer tous ces avantages, les réseaux mobiles sans fil introduisent de nouvelles spécificités, liées à leurs natures. Ces nouvelles spécificités résultent en de nouvelles contraintes en matière de sécurité; qu'il faudra contrer.

a. Le Support Physique des réseaux sans fil

La nature physique du support est fréquentielle ou lumineuse; cette nature a ses propres spécificités en matière d'affaiblissement du signal, la méthode d'accès au support ainsi qu'aux méthodes de modulation. Par la nature hertzienne, l'étendu du réseau devient grand et immaîtrisable; en plus que les tentatives d'écoute clandestine deviennent plus faciles moyennant les bonnes antennes (fréquences).

Plusieurs solutions sont envisagées, la première étant d'avoir une seule borne qui effectue le relais entre les différentes stations par voie hertzienne, la deuxième étant d'avoir des microcellules (typiquement, chaque pièce) qui utilisent l'infrarouge. Les bornes sont dans ce cas interconnectées soit par voie hertzienne, soit par un réseau filaire classique. [LEG00]

b. Héterogénités des réseaux.

En informatique mobile, l'environnement n'est pas fixe. Il existe une multitude de types de sites mobiles mais également un grand nombre de réseaux avec ou sans fil. Les environnements mobiles sont donc fortement hétérogènes [PEI02].

Contrairement aux ordinateurs fixes, les ordinateurs mobiles se déplacent de réseau en réseau. Lorsqu'ils quittent une station de base, ils sont contraints d'en chercher une autre. Dans différentes cellules, les mobiles risquent d'être confrontés à différentes qualités de service. En effet, un mobile peut même voir sa communication s'interrompre s'il tente d'entrer dans une cellule surchargée. De plus, la qualité des équipements sans fil n'est pas constante sur tous les réseaux.

Parmi les problèmes d'hétérogénéité et de qualité de service des réseaux sans fil on peut citer : [LEG00]

- Les accès sans fils.
- Sélections de fréquences.
- Charge des cellules.
- Taux d'interférence et d'erreurs.
- L'utilisation conjointe par les mobiles de connexion sans fil et filaire de qualité variable.
- Changement des interfaces de communication sans fil entre l'intérieur et l'extérieur

c. Nommage et Routage des Sites Mobiles

En se déplaçant, un mobile utilise différents points d'accès au réseau, et différentes adresses. Or, les adresses tendent à désigner des machines précises, et pas seulement une interface de connexion. Pour gérer la mobilité, il faut donc disposer de deux adresses : une adresse fixe pour identifier le mobile de manière unique et une adresse temporaire qui varie à chaque changement de point d'accès.

Les procédures de nommage doivent être effectuées de façon automatique, Mais la génération de noms locaux peut poser des problèmes de conflit :

- L'adresse temporaire peut être identique à une adresse existante sur le réseau visité. Il est donc parfois préférable d'utiliser les noms permanents avec certaines applications sous peine de ne plus pouvoir joindre l'utilisateur si celui-ci s'est déplacé.

- Tout comme l'adressage, le routage doit être dynamique. Il est essentiel que lorsqu'un mobile se déplace, les paquets qui lui sont destinés ne soit plus dirigés vers l'ancienne localisation du mobile, mais vers la nouvelle. Il arrive que les protocoles de

routage limitent le nombre de sites mobiles qu'ils peuvent supporter dans un sous-réseau donné. Malheureusement, avec une telle méthode, le nombre de mobiles dans un sous réseau est alors borné par le nombre d'adresses disponibles et non par la largeur de bande passante utilisable.

d. Localisation des Ressources (& des Sites Mobiles)

En se déplaçant, le mobile doit connaître les emplacements des différentes ressources, pour cela il faut réaliser des protocoles de localisation des ressources qui fonctionnent de manière transparente.

Lorsqu'une information est destinée à un mobile, il est important de pouvoir la délivrer à la localisation courante du mobile, et non à son réseau d'attachement. Il faut donc prévoir des mécanismes capables de délivrer l'information directement au mobile.

e. Sécurité et Authentification.

Des mécanismes de sécurité et d'authentification dans les réseaux sans fil sont indispensables car ils sont beaucoup plus vulnérables que les réseaux filaires. Ces mécanismes sont souvent relativement complexes car les utilisateurs se déplacent et traversent des domaines de sécurité différents. Les problèmes rencontrés concernent donc l'usurpation d'identité, le piratage de données émises et le vol des droits d'accès à un service ou à un réseau. De plus, lorsqu'un mobile traverse les frontières d'un domaine, sa crédibilité doit être vérifiée.

IV. Sécurité VS Mobilité – Vulnérabilités Des Réseaux Mobiles sans Fils.

Les réseaux sans fil offrent de nouvelles failles aux pirates. De part la nature immatérielle du support physique (le support sans fil), l'écoute clandestine sur un réseau sans fil est facile. Il faut donc protéger l'accès aux ressources sans fil et aux informations qui circulent dans les trames.

Les systèmes mobiles sont généralement équipés de processeurs moins puissants que les machines fixes, et ne peuvent se permettre d'effectuer de longs calculs demandés par les systèmes de cryptographie. L'énergie de la batterie est une ressource rare et pose également des problèmes de sécurité.

La mobilité en elle même est une vulnérabilité, du fait que la gestion s'alourdit et les protocoles se compliquent et donc ouvre la porte à plusieurs vulnérabilités. On peut résumer les vulnérabilités dans les grands points suivants [FAR03a] [KRU04] [PEI02]:

- Problèmes liée aux connections sans fils (Ondes hertziens)
- Problèmes de sécurité physique (vol,..)
- Vulnérabilités du réseau mobiles

Faiblesse du WEP : [KRU04] [PEI02]

Les réseaux sans fil sont sujets à une variété de menaces. La méthode standard du chiffrage 802.11, **WEP** (Wired Encryption Protocol) est faible. En effet, selon [FLU01], la clef WEP d'une transmission sans fil peut être acquise par l'intermédiaire d'une attaque BruteForce. Ainsi même si le chiffrage WEP est utilisé sur un LAN sans fil, un attaquant peut potentiellement intercepter et déchiffrer des données sensibles.

La plupart des produits de WEP mettent en application une clef partagée 64-bit, en utilisant 40 bits de ceci pour le principal secret et 24 bits pour le Vecteur d'*i*nitialisation (IV :

Initialization Vector). La clef est installée dans le point d'accès du réseau filaire et doit être aussi dans chaque client.

Le WEP n'a pas été conçu pour résister à une attaque cryptographique dirigée. WEP a des failles connues dans les algorithmes de chiffrage employés pour sécuriser les transmissions sans fil. Deux programmes capables d'exploiter la vulnérabilité RC4: *AirSnort*, et le *WEPCrack*, tous les deux fonctionnent sous Linux, et tous les deux exigent un peu de données capturées.

Un certain nombre de chercheurs ont étudié des attaques sur WEP [KRU04].

Faille avec le Service Set Identifier (SSID): [KRU04] [PEI02]

Le *Service Set IDentifier* (SSID) est une valeur d'identification programmée dans le point d'accès ou le groupe de points d'accès pour identifier le sous réseau local sans fil. Cette segmentation du réseau sans fil en de multiples réseaux est une forme de contrôle d'authentification. Si une station sans fil ne connait pas la valeur du SSID, l'accès est nié sur ce point d'accès. Quand un ordinateur de client est relié au point d'accès, le SSID agit en tant que mot de passe simple, qui fournit une mesure de sécurité. Le point d'accès sans fil est configuré pour diffuser son SSID. Une fois activé, n'importe quel client sans SSID peut le recevoir et avoir accès au point d'accès. Les utilisateurs peuvent également configurer leurs propres systèmes client avec le SSID approprié parce qu'ils sont largement connus et facilement partagés. Un problème est provoqué par le fait que la plupart des points d'accès qui diffusent leurs SSIDs dans leurs signaux utilisent les SSIDs fournis par défaut par les fabricants, et où une liste de ces SSIDs par défaut est disponible pour le téléchargement sur l'Internet. Ceci signifie qu'il est très facile pour un intrus de déterminer le SSID d'un réseau et d'y accéder par l'intermédiaire des outils logiciels.

Balayage (scannage) sans fil et écoute clandestine : [KRU04] [PEI02]

La technologie sans fil est également vulnérable à l'écoute clandestine, particulièrement parce que les intrus ne doivent pas se brancher physiquement sur un réseau. Soit à travers une salle, ou de l'extérieur du bâtiment, un intrus peut passivement "sniffer" votre trafic réseau sans un accès physique moyennant une carte réseau sans fil qui admet le mode «promiscuous». La surveillance secrète d'un réseau sans fil est simple. À moins que spécifiquement configuré pour empêcher un autre dispositif WLAN de joindre le réseau, un réseau sans fil acceptera des communications de n'importe quel dispositif dans son champs.

En plus, le protocole 802.11 laisse l'en-tête de la couche physique non crypté, fournissant des informations critiques à l'attaquant. Par conséquent, le chiffrage de données est une couche critique de défense, mais souvent des données sont transmises en claire. En utilisant les sniffeurs (renifleurs) de paquet sans fil, un attaquant peut passivement capturer le trafic sans fil du réseau et, par l'analyse de paquet, déterminer des IDs de sessions et des mots de passe, ainsi que d'autres données sensibles.

War Driving : [KRU04] [PEI02]

War Driving (ou *War Walking*) est un terme employé pour décrire un intrus qui, armé d'un ordinateur portable et d'une carte sans fil, se déplace par l'intermédiaire d'une voiture, d'un autobus, d'un métro, ou toute autre forme de transport, afin de renifler un réseau sans fil.

Le concept de *War Driving* est simple. Utilisant un dispositif capable de recevoir un signal 802.11b, un dispositif capable de se localiser sur une carte, et d'un logiciel qui trace des données à la seconde prés où un réseau est détecté par le premier dispositif; l'intrus se déplace d'un endroit à l'autre, laissant ces dispositifs agir. Avec le temps, l'intrus accumule une base de données

comportant le nom du réseau, la puissance du signal, l'endroit, et les IPs/namespace en service. Par l'intermédiaire du SNMP, l'intrus peut même noter des échantillons de paquet et sonder le point d'accès pour des données disponibles. L'intrus peut également marquer l'endroit du réseau sans fil vulnérable avec la craie sur le trottoir ou sur le bâtiment. Ceci s'appelle *warchalking*, et alerte d'autres intrus qu'un WLAN exposé est voisin.

Des techniques commune de War Driving conduisant à la découverte des réseaux sans fil avec le service WEP désactivé et utilisant seulement le SSID pour le contrôle d'accès. Et, comme noté précédemment, le SSID pour un réseau sans fil peut rapidement être trouvé. Cette vulnérabilité rend ces réseaux vulnérables de ce qui s'appelle *l'attaque du parc de stationnement*, où à une distance sûre du périmètre du bâtiment, un attaquant accède au réseau cible.

Wireless Packet Sniffers et Scanners: [KRU04] [PEI02]

Les analyseurs sans fil de paquet, ou les renifleurs (sniffeurs), fonctionnent fondamentalement de la même manière que les analyseurs de paquet des réseaux filaires. Ils capturent des paquets du flux de données et permettent à l'utilisateur de les ouvrir et de les regarder, ou de les décoder. Quelques Scanners sans fil n'utilisent pas des outils de décodage mais montrent seulement les WLANs et SSIDs existants.

Parmi les Sniffers sans fil disponibles on cite :

AirMagnet : *AirMagnet* est un outil sans fil à l'origine développé pour l'inventaire et la gestion des réseaux sans fil.

NetStumbler : *NetStumbler* est un programme shareware pour localiser les SSIDs des WLANs. Il essaye d'identifier le fournisseur du WLAN, et une fois couplé à un GPS, *NetStumbler* peut fournir des informations directionnelles.

AiroPeek : *AiroPeek* de *WildPackets* est un analyseur de paquet pour les réseaux sans fil IEEE 802.11b, supportant tous les protocoles réseau de plus haut niveau tels que TCP/IP, Appletalk, NetBEUI, et IPX. *AiroPeek* est employé pour isoler des problèmes de sécurité en décodant les protocoles de 802.11b et en analysant les performances des réseaux sans fil avec l'identification des puissances des signaux, des canaux, et des débits.

Sniffer Wireless : *McAfee Sniffer Wireless* est également un analyseur de paquet pour gérer des applications réseaux et des déploiements sur les réseaux sans fil 802.11a et 802.11b. Il a la capacité de déchiffrer le trafic WEP.

Rogue WAP: [KRU04] [PEI02]

Les intrus peuvent également attaquer un réseau sans fil et recueillir des données sensibles en introduisant un Rogue WAP (Wireless Access Point) dans le champ de couverture du réseau sans fil. Le Rogue WAP peut être configuré pour ressembler à un WAP légitime et, puisque beaucoup de clients sans fil se relient simplement au WAP avec le meilleur signal, ils peuvent être «dupés». Une fois qu'un utilisateur est associé, toutes les communications peuvent être surveillées par l'intrus à travers le Rogue WAP.

En plus des intrus, les Rogues WAPs peuvent également être introduites par des utilisateurs légitimes; Car le prix réduit, l'exploitation facile couplés à la flexibilité des communications sans fil rendent les réseaux sans fil fortement souhaitables aux utilisateurs. En installant un WAP sur un LAN établi, un utilisateur peut créer une porte dérobée dans le réseau, renversant toutes les solutions de sécurité et laissant le réseau ouvert aux intrus. Il est très possible que les utilisateurs puissent installer un Rogue WAP, exposant même une organisation exclusivement câblée aux risques des réseaux sans fil.

Les réseaux employant 802.11 sont sujets également à un certain nombre d'attaques DoS qui peuvent rendre un réseau sans fil inopérable. Les communications sans fil sont en soi vulnérables aux dégradations du signal à la rencontre d'obstacles physiques (arbres, bâtiments, pluie, collines). En plus des obstacles physiques, beaucoup de dispositifs communs tels que des fours à micro-ondes, téléphones sans fil, et moniteurs de bébé peuvent interférer avec les réseaux 802.11.

Les intrus peuvent également causer des attaques DoS en submergeant les WAPs avec des requêtes d'associations jusqu'à les forcer à rebooter. En plus, ils peuvent employer les Rogue WAP pour envoyer de manière répétitive des requêtes de desassociation et desauthentification pour refuser le service à un client sans fil. [FAR03a].

Les réseaux sans fil sont vulnérables aux attaques DoS dues à la nature du milieu sans fil de transmission. Si un attaquant se sert d'un émetteur récepteur assez puissant, une interférence peut être produite pour empêcher les dispositifs sans fil de communiquer entre eux. Les dispositifs d'attaque DoS n'exigent pas être à côté des dispositifs étant attaqués, ils doivent seulement être dans le champs des transmissions sans fil.

Les exemples des techniques DoS employées contre un dispositif sans fil sont :

- Requêtes d'authentification sur les mêmes fréquences perturbant le trafic légitime.

- Requêtes de desauthentication des utilisateurs légitimes. Ces demandes ne peuvent être refusées selon la norme 802.11 courante.

- Imiter le comportement d'un point d'accès et convaincre les clients de communiquer avec lui.

- Transmettre à plusieurs reprises des trames RTS/CTS pour amortir le réseau.

La gamme de fréquence 2.4-GHz, dans laquelle 802.11b fonctionne, est partagée avec d'autres dispositifs sans fil tels que les téléphones sans fil, alarmes bébé surveille (bébé surveille), et les dispositifs basés Bluetooth. Tous ces dispositifs peuvent contribuer à la dégradation et à l'interruption des signaux sans fil. En outre, un attaquant déterminé et inventif avec l'équipement approprié peut inonder la fréquence avec du bruit artificiel et complètement perturber le fonctionnement du réseau sans fil.

Un point d'accès a une ou plusieurs méthodes disponibles pour gérer l'accès à un LAN sans fil, typiquement comprenant l'utilisation d'un SSID commun, ou de permettre l'accès en se basant sur l'adresse MAC, et le WEP. Puisque l'authentification par défaut dans 802.11 est une authentification ouverte, la plupart des systèmes authentifieront n'importe quel utilisateur qui demande le raccordement.

Une autre issue commune avec les réseaux 802.11b est que les points d'accès ont été conçus pour l'installation facile. Ainsi, bien que les dispositifs de sécurité sont présents, dans la plupart des cas les configurations par défaut sont désactivés. Les administrateurs réseau qui laissent leur équipement avec les configurations d'origines intact sont particulièrement vulnérables, car les intrus sont susceptibles d'essayer des mots de passe et des configurations connus en essayant de pénétrer les réseaux sans fil.

Même lorsque l'authentification par mot de passe est mise en application sur les points d'accès sans fil, l'accès non autorisé est encore possible par l'utilisation des attaques par dictionnaire en BruteForce. Les applications crackers de mot de passe peuvent méthodiquement examiner la puissance des mots de passe.

Le schéma suivant résume tous les cas d'intrusions à un réseau sans fil tel évoqué précédemment:

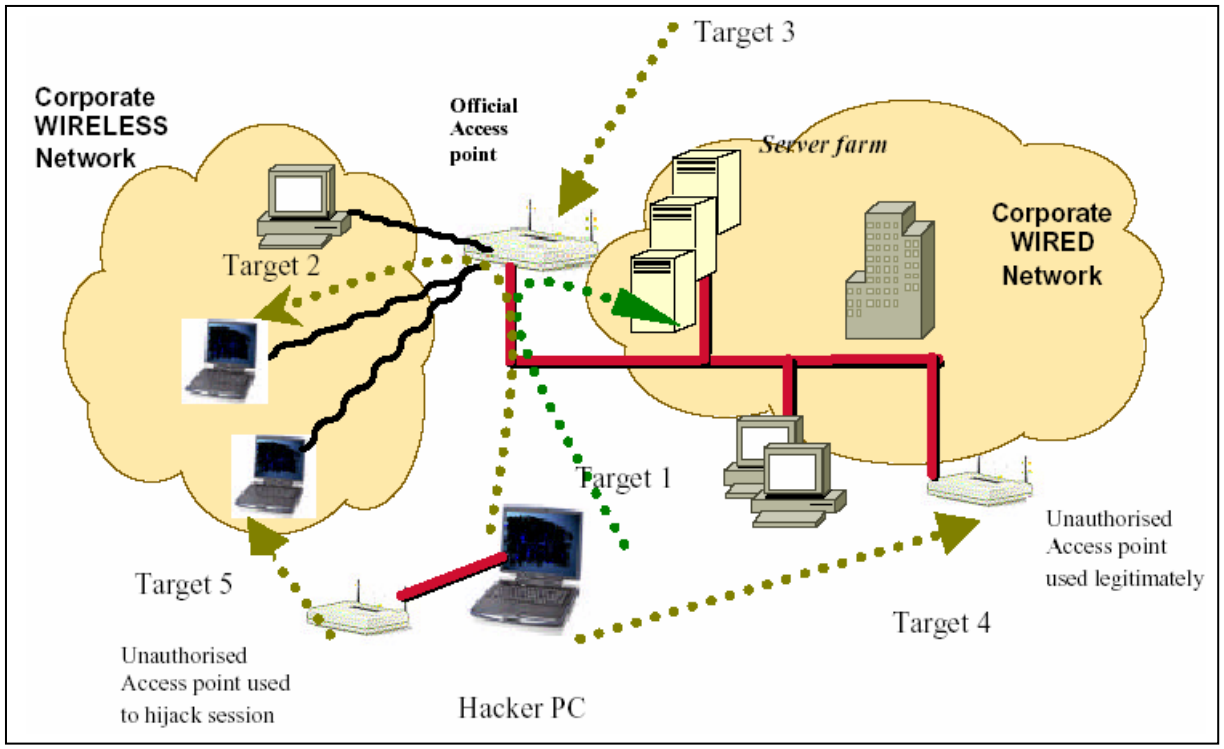


Figure I.2: *Intrusion sans fil* [WID03]

Les systèmes sans fil sont sensibles à deux attaques principales supplémentaires par rapport aux réseaux classiques. Ces attaques porte atteinte à la disponibilité du réseau et des nœuds :

- *Le blocage radio* : pour rendre le réseau inutilisable, le pirate peut bloquer les fréquences radio utilisées par le système.

- *Epuisement de la batterie* : l'attaquant peut interagir avec le nœud dans le seul but de lui faire consommer de la batterie. Les applications doivent donc restreindre leur accès pour éviter ce genre d'attaque.

Aussi, il ne faut pas oublier le risque de perte (***VOL***) des équipements PDA, du fait qu'il son petits et facile à perdre; et donc le risque de divulgation d'informations confidentielles qui étaient stockées dans les disques durs de ces PDA.

Du fait que les PDA assurent des services Internet; cela implique l'existence d'un point d'accès et donc l'ouverture d'une grande porte de feu; car d'après le principe de sécurité qui dit: «la meilleur protection contre les attaques Internet est de ne pas avoir de connexion Internet» cela pose problème, c'est le problème d'ouverture vers l'extérieur avec tout ce qu'il peut entraîner.

Une autre chose nous semble intéressante à évoquer; c'est le fait que la notion d'***environnement privé*** pour les réseaux n'existe plus car les limites physiques n'existent plus et n'importe qui peut pénétrer dans le domaine (cellule, champs d'action) du réseau (Problématique des firewalls qui gardaient jadis, un seul point d'accès, et qu'aujourd'hui on n'arrive même pas déterminer le point d'accès du réseau).

On peut ajouter, les failles des mécanismes de sécurisations existant actuellement dans les réseaux existant; et leurs grandes vulnérabilités; en citant comme exemple, les systèmes des GSM qui provoquent aujourd'hui beaucoup de vacarme et de mécontents au sein des clients qui évoquent les lourdes factures à payer du à l'usurpation d'identité par des pirates.

WAP GAP : [KRU04] [PEI02]

Une attaque spécifique au protocole WAP est liée au "WAP GAP". Un ESPACE de WAP "WAP GAP" résulte au moment du passage par la passerelle WAP ou il faudrait changer les protocoles de sécurité du WTLS vers SSL. Dans la passerelle WAP, la transmission, qui est protégée par WTLS, est déchiffrée et puis re-chiffrée en utilisant SSL. Et la, les données sont temporairement en claire et peuvent être compromises.

Afin d'aborder cette question, le forum sur le WAP a mis en avant les caractéristiques qui réduiront cette vulnérabilité et soutiendront ainsi des applications d'e-commerce. Ces caractéristiques sont définies dans le WAP.1.2 (*WMLScript Crypto Library; WAP Identity Module* (WIM)). La bibliothèque *WMLScript Crypto Library* supporte la sécurité bout à bout en prévoyant des fonctions cryptographiques à lancer sur le client WAP à partir du serveur de contenu d'Internet. Ces fonctions incluent les signatures numériques avec le client WAP et le cryptage et le décryptage des données. Le WIM est un dispositif résistant, tel qu'une smartcard, qui coopère avec WTLS et fournit des opérations cryptographiques pendant la phase handshake.

Vulnérabilités des PDA : [KRU04] [PEI02]

Sans oublier d'évoquer les vulnérabilités liées aux PDAs qui représentent des PCs à part entière. Les virus ont infecté des modèles PDA ainsi que des mobiles GSM. Par exemple, le virus *Phage* qui infecte quelques uns des dossiers exécutables de Apple et les vers GSM : *SymOS.Skulls*(2005), *SymbOS.MGDropper*(2005), *SymbOS.Lasco*(2005), *SymbOS.Cabir*(2004),….

Les PDAs bénéficient d'une connexion Internet, donc ils sont vulnérables aux documents téléchargés du net comme les ordinateurs de bureau. Aussi ils peuvent être porteurs de virus qui infectent non pas les PDAs mais au contraire les PCs de bureau lors de la synchronisation.

Les PDAs n'ont pas été conçus aux mêmes normes et n'ont pas été exposés aux mêmes examens rigoureux que les systèmes d'exploitation de bureau, tels que les conditions fonctionnelles définies dans la norme ISO 15408. En faisant une comparaison avec les systèmes d'exploitation, sur les exigences de sécurité telles décrites dans cette norme ainsi que d'autre, la plupart des PDAs reçoivent une estimation très faible :

-Les logiciels d'exploitation des PDAs n'ont pas des dispositifs pour séparer les données d'un utilisateur des autres, chose exigée pour supporter le contrôle d'accès discrétionnaire (DAC : Discretionary Access Control).

-Il manque les possibilités d'audit.

-Ils n'ont aucun support de contrôle de réutilisation d'objet à travers l'identification et l'authentification (I&A).

-Ils n'assurent pas la protection de intégrité des données.

-Même lorsque l'OS est verrouillé par mot de passe, des applications peuvent être installées sur le PalmOS sans connaissance du propriétaire.

Perte De Confidentialité

Même si un PDA est protégé par mot de passe-, un utilisateur malveillant peut rechercher le mot de passe de ce dernier en utilisant le mode Palm Debug. Le mot de passe peut alors être décodé en utilisant des outils simples tels que l'outil de *PalmCrypt*.

Une fois que le mot de passe a été dévié, toute l'information sur le PDA est entièrement lisible par l'utilisateur malveillant. Actuellement, les administrateurs de sécurité n'ont pas la capacité de déterminer si ce type d'attaque s'est produit, et qui en était le responsable.

Perte Physique

La menace la plus commune pour un PDA est provoquée probablement par la perte physique du dispositif (le vol). Bien que quelques solutions techniques soient disponibles pour se protéger contre certaines des insuffisances de sécurité du système d'exploitation, aucun ne fournit des contre-mesures aux problèmes de sécurité physique. Ces dispositifs sont si petits et portatifs que la perte du dispositif et des informations contenus dedans est très fréquente. Leur mode d'utilisation les met dans un plus grand risque parce qu'ils sont généralement employés dans les environnements non contrôlés.

V. Conclusion.

La sécurité joue un rôle très particulier, parce que la moindre défaillance peut compromettre le bon fonctionnement du système. Si l'algorithme marche dans 95 % des cas, mais n'est pas équitable dans 5% des cas, le système continue à fonctionner. Si le système de sécurité n'opère que dans 95% des cas, les 5% restants peuvent être exploités par un adversaire et compromettre toute la sécurité du système.

La solution "risque 0" n'existe pas dans le domaine de la sécurité informatique, donc, comme solution générale pour les problèmes de sécurité qui peuvent se poser dans un système informatique, est une combinaison, des différentes méthodes de sécurité à différent niveaux qui peut paraître comme étant la solution idéale.

Une variété d'autres menaces contre les réseaux sans fils existe et des vulnérabilités additionnelles sont identifiées à un rythme toujours croissant. Le point est que les menaces sont réelles, elles peuvent causer de grands dommages, et elles se développent au fur et à mesure que la technologie 802.11 gagne en popularité. Sans un mécanisme de détection, il peut être difficile d'identifier les menaces d'un WLAN [FAR03a].

A travers cette étude, nous avons exploré le problème de la sécurité dans les environnements mobiles sans fil. Nous avons constaté que l'enjeu est plus important, du fait que les spécificités de ces environnements compliquent d'avantage la tache de sécurisation.

Chapitre II:

Les Systèmes de Détection d'Intrusion

- IDS -

*Les **S**ystèmes de **D**étection d'**I**ntrusion*

-IDS

I-INTRODUCTION

La détection d'intrusion est une technologie de sécurité complémentaire des autres mécanismes mis en œuvre dans le cadre d'une sécurité globale (contrôle d'accès physique et logique, authentification, chiffrement, outils de test de vulnérabilités, Firewalls) [KOR01]. Elle a pour objectif de détecter et d'isoler les «intrusions» contre les systèmes informatiques en contrôlant dynamiquement les actions des utilisateurs (externes et internes) du réseau.

Les IDS sont l'un des mécanismes de sécurisation; ils utilisent différentes ressources (trace d'audits système et réseau, fichiers logs, événement système). L'IDS joue le rôle d'un surveillant du système informatique et de ses utilisateurs. Il détecte des évènements ou des comportements susceptibles d'être une forme d'intrusions. Il peut réagir automatiquement (IDS actif) ou simplement informe l'administrateur de sécurité (IDS passif). Ce dernier qui doit être [NAC02] :

- ✓ En alerte.
- ✓ Un Administrateur système compétent.
- ✓ Familier à la machine hôte.
- ✓ Familier à la connexion réseau des utilisateurs.
- ✓ Familier aux habitudes des utilisateurs.
- ✓ Informé sur tout logiciel installé.

Les systèmes de détection d'intrusion sont une couche qui devrait être ajouté aux autres techniques de sécurité et qui visent à renforcer le périmètre entourant le système informatique; (ils forment les alarmes anti-cambrioleur [AXE00]). Le but est de défendre un système en employant: une combinaison d'*alarmes* qui se déclenchent toutes les fois que la sécurité du système a été compromise; et une entité - le plus souvent un officier de sécurité (SSO) agent humain ou logiciel- qui peut *répondre* à l'alarme et prendre de ce fait les mesures appropriées.

II-LES SYSTEMES DE DETECTION D'INTRUSION : [LON87] [CUF03] [KOR01]

II.1 Définition de l'Intrusion :

Par le terme «intrusion», [SIE01] on entend la pénétration par violence ou par ruse de processus ou de personnes non autorisées dans une zone délimitée, avec intention de vol, de dommage ou d'abus, avec tous les phénomènes annexes comme la contrainte, le chantage et les conséquences. Au sens le plus large, tous les actes criminels tombent sous le coup de cette définition.

Une ancienne étude effectuée par le pionnier des IDS, J.P. Anderson [AND80] a utilisé le terme de «*menace*» (threat) pour indiquer le même sens, et la définie comme : « *Une possibilité potentielle d'une tentative délibérée et non-autorisée de :*

- *Accéder à l'information.*
- *Manipuler l'information.*
- *Rendre le système instable et inutilisable.* »

Une intrusion peut être définie comme [HEA90][ZAM98] «*Toute Action* (ou groupe d'actions) *visant à compromettre l'intégrité, la confidentialité ou la disponibilité des ressources d'un système informatique* ».

Ou selon [ME 99] comme «*Actions pouvant être entreprises par un utilisateur (légitime ou non) ou par un programme malveillants (virus, vers, bombe, cheval de Troie) et portant atteinte à la confidentialité, à l'intégrité ou à la disponibilité des services et des données :*

-Furetage, vol de données (lecture, copie, prise), exploitation d'un canal caché.

-Modification illégitime de données, destruction de données.

-Déni de service (réduction illégitime ou abusive des droits des usagers légitimes) »

Toute intrusion est définie relativement à un référentiel constitué à partir d'une politique de sécurité. Cette politique permet de savoir ce qui est autorisé ou non sur un système d'information. Une intrusion devient de ce fait une violation de la politique de sécurité du système [KUM95b].

L'intrusion peut être de différents types. Par exemple, un utilisateur pourrait voler un mot de passe et par conséquent il aura le moyen pour prouver son identité à l'ordinateur. Nous appelons un tel utilisateur "déguisé"*;* et la détection de tels intrus est un problème important.

II.2 Définition de la Détection d'Intrusion :

La détection d'intrusion est définie par [ZAM98] comme «*la capacité à identifier les individus utilisant un système informatique sans autorisation et identifier ceux qui ont un accès légitime au système mais qui abusent de leurs privilèges* ». Comme on pourrait ajouter à cette définition l'identification des *tentatives* d'utilisation d'un système informatique sans autorisation et des *abus* de privilèges.

II.3 Définition d'un Système de Détection d'Intrusion -IDS : [COL05]

Pour de nombreuses organisations qui viennent de déployer une technologie à barrière de protection au premier lieu de leur réseau, les systèmes de détection d'intrusion (IDS) constitue la prochaine étape logique.

Les IDS sont des systèmes qui collectent des informations de différentes manières, soit à partir du système et/ou du réseau, sur les différentes activités se rapportant à ce même système pour les analyser à la recherche de signes d'une intrusion (attaques suspectes) et alerter dans le cas positif [BAC00].

Un IDS est en mesure d'assurer la protection requise contre les attaques internes (le trafic ne traverse absolument pas la barrière de protection) mais aussi il peut sécuriser le réseau contre les attaques externes.

La détection d'intrusions consiste, dans une approche curative, à mettre en œuvre des mécanismes d'analyse afin de démasquer les auteurs d'une intrusion. Ceci est réalisé par « l'*audit de sécurité* ».

Un système de détection d'intrusion se compose d'un *agent de collecte de données d'audit* qui rassemble des informations sur le système étant observé. Ces données sont alors *stockées* ou *traitées* directement par le *détecteur* proprement dit, dont le rendement est présenté au SSO (Administrateur de sécurité), pour qu'il prenne des des mesures.

Les systèmes de détection d'intrusion (IDSs) sont affirmés sur la prétention qu'un intrus peut être détecté par un examen de divers paramètres tels que le trafic réseau, l'utilisation de la CPU, les entrées/sorties, l'endroit de l'utilisateur, et les diverses activités sur les fichiers [LUN93]. Les moniteurs ou les démons du système convertissent les paramètres observés chronologiquement sur disque sous forme de "traces d'audit". Ces traces d'audit sont analysées à la recherche de comportement peu commun ou suspect.

La détection d'intrusion peut être divisée en deux catégories : *détection d'anomalies* et *détection d'abus*. La première concerne les intrusions qui peuvent être détectées en se basant sur un comportement suspect et une utilisation anormale des ressources.

La détection d'anomalie essaye de mesurer le comportement habituel ou acceptable et marque un autre comportement irrégulier comme étant potentiellement intrusif. Un des premiers rapports de recherche qui décrit comment des intrusions peuvent être détectées en identifiant le comportement anormal est le travail réalisé par Anderson [AND80]. Dans ce travail, Anderson a présenté un modèle de menace qui classifie les menaces comme : *pénétration externe*, *pénétration interne*, et *abus malintentionné* ; et a utilisé cette classification pour développer un gestionnaire de surveillance basé sur la détection d'anomalies dans le comportement de l'utilisateur. Une pénétration externe est définie comme une intrusion effectuée par un ordinateur non autorisé ; une pénétration interne est celle effectuée par un utilisateur authentifié mais n'ayant pas droit d'exploitation de certaines données ; les abus malintentionnés sont définies comme des abus commis par des utilisateurs authentifiés mais de manière involontaire.

La détection d'abus se rapporte aux intrusions qui suivent des modèles bien définis d'attaques qui exploitent des faiblesses dans les systèmes et applications. De tels modèles sont écrits à l'avance. Cette technique représente la connaissance au sujet du mauvais comportement et cherche à le détecter directement, par opposition à la détection d'anomalie, qui cherche à détecter le complément du comportement normal.

II.4 Les Composants général d'un IDS :

Les fonctionnalités d'un IDS peuvent être de manière simple distribuées en trois composants logiques: les *sondes*, les *analyseurs*, l'*interface utilisateur*. Ces composants sont communs à tous les modèles qui existent. [ALL00]

a) **Les sondes (Sensors) :** Ce module s'occupe de la collecte d'informations. L'entrée de la sonde peut être n'importe quelle partie du système qui peut contenir des informations pouvant nous permettre de détecter une intrusion. Les exemples de types d'entrée sont : les paquets du réseau, les fichiers logs et les traces des appels système. Les sondes rassemblent et envoient les informations collectées vers un autre module qui est l'analyseur.

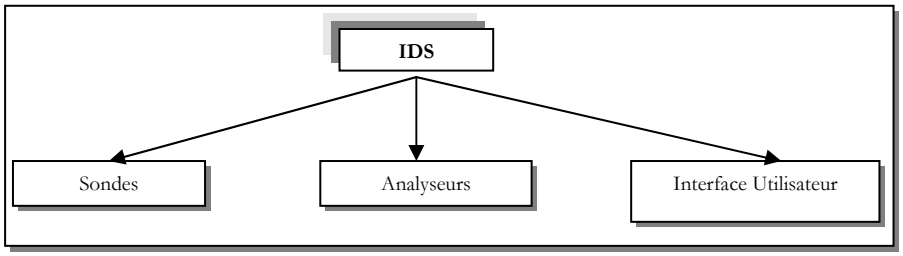


Figure II.1*: les composants d'un IDS*

b) **Les analyseurs :** Les analyseurs reçoivent comme entrée les données qui proviennent d'un ou plusieurs collecteurs ou à partir d'autres analyseurs qui auraient au préalables procédé à un premier traitement des données en vue de les raffiner et faciliter la tache à l'analyseur final. L'analyseur peut être considéré comme le noyau de l'IDS, il est responsable de déterminer si une intrusion s'est produite. Comme sortie l'analyseur doit en plus d'un indicateur indiquant une éventuelle attaque, retourner des informations sur l'état du système, et guider l'administrateur en proposant des solutions aux problèmes rencontrés.

c) **Interface utilisateur :** Ce module permet à l'IDS d'interagir avec l'utilisateur, pour pouvoir visualiser les sorties du système, configurer et fixer les paramètres en relation avec la politique de sécurité.

Et de manière plus détaillée on peut avoir le schéma de déploiement et d'interaction d'un IDS avec les autres solutions de sécurité dans un réseau d'entreprise comme suite :

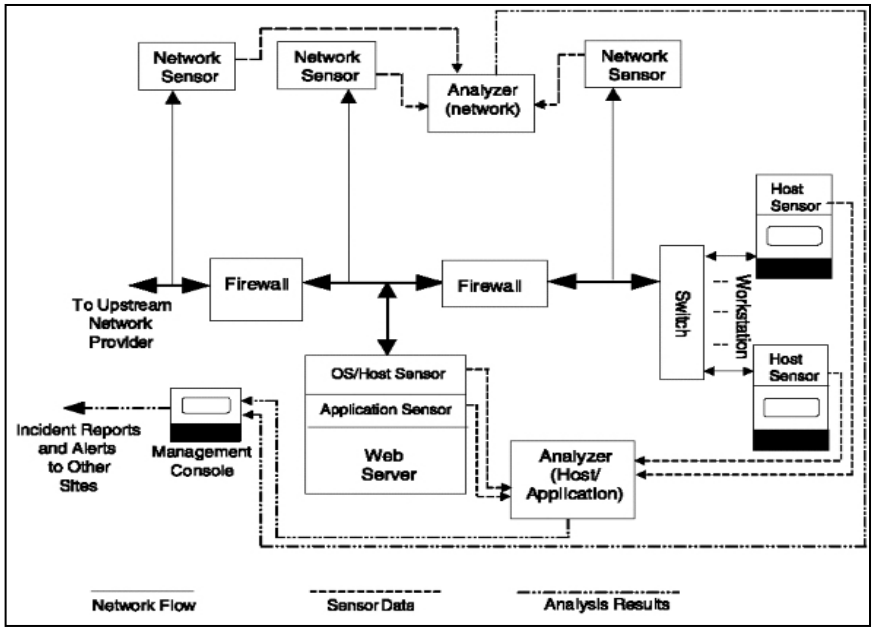


Figure II.2 : *Structure d'un Système IDS* [ALL01]

II.6 Exemple de placement d'IDS dans un sous réseau :

La figure II.3 montre une petite entreprise configurée avec des par-feu pour isoler son serveur web. Les ordinateurs configurés comme sondes réseau extraient les paquets soupçonneux à partir des trois principaux segments du réseau et les font suivre aux stations d'analyse réseau

appropriées. Le serveur web et les postes de travail sont équipés de logiciel pour surveiller les interactions soupçonneuses avec le système d'exploitation et les reporte à une station d'analyse. En plus, le serveur web recherche des abus tels que les exploits sur la passerelle qui sont spécifiques aux serveurs HTTP. Les analyseurs font rapport à une console de gestion qui sert d'interface utilisateur à l'IDS. La console de gestion alerte l'administrateur de l'entreprise qui peut, alternativement, rapporter des intrusions aux organismes de réponse d'incident.

De manière simple le schéma de placement d'un IDS est le suivant :

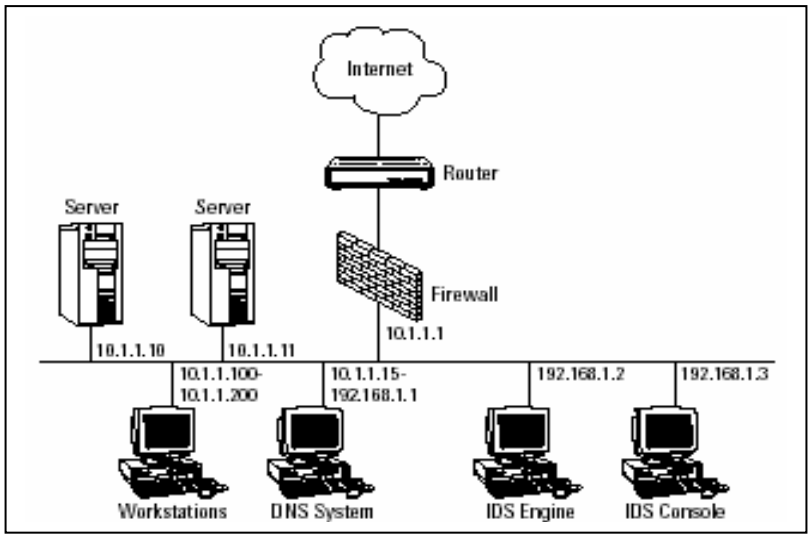


Figure II.3 : *L'IDS dans le sous réseau* [KRU04]

Le placement d'un IDS dans un réseau peut ce faire sur trois régions ou zones :

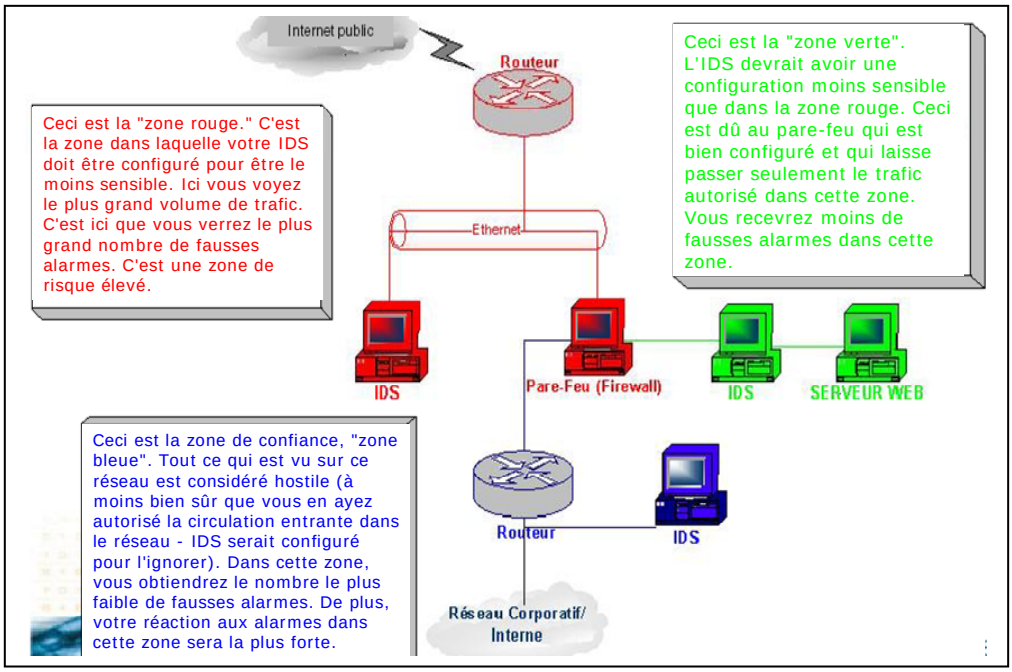


Figure II.4 : *Les trois Zones* [MER04]

- Une "***zone rouge***" : C'est la zone dans laquelle votre IDS doit être configuré pour être le moins sensible. Le volume du trafic est très dense dans cette zone. C'est ici que vous verrez le plus grand nombre de fausses alarmes. C'est une zone de risque élevé.

- Une "***zone verte***" : L'IDS devrait avoir une configuration moins sensible que dans la zone rouge. Ceci est dû au pare-feu qui est bien configuré et qui laisse passer seulement le trafic autorisé dans cette zone. Vous recevrez moins de fausses alarmes dans cette zone.
- Une "***zone bleue***" : Tout ce qui est vu sur ce réseau est considéré hostile (à moins bien sûr que vous en ayez autorisé la circulation entrante dans le réseau l' IDS serait configuré pour l'ignorer). Dans cette zone, vous obtiendrez le nombre le plus faible de fausses alarmes. De plus, votre réaction aux alarmes dans cette zone sera la plus forte.

III- CLASSIFICATION & TAXONOMIE DES IDS :

La classification des systèmes de détection d'intrusion est un sujet difficile à cerner. La raison principale est que la plupart des IDS sont basés sur plus d'une approche et peuvent implémenter un grand nombre de méthodes.

Nous présentons dans cette section l'une des typologies -Taxonomies- la plus connu [DEB98] des méthodes proposées à ce jour. A cet effet, nous reprenons en annexe les résultats du laboratoire d'IBM à Zurich [DEB98] et ceux des travaux de Stefan Axelsson [AXE00] ainsi que celles de Smaha [SMA88].

III.1 Classification selon [DEB98] :

Selon [DEB98] pour la classification des IDS on doit considérer les cinq caractéristiques suivantes:

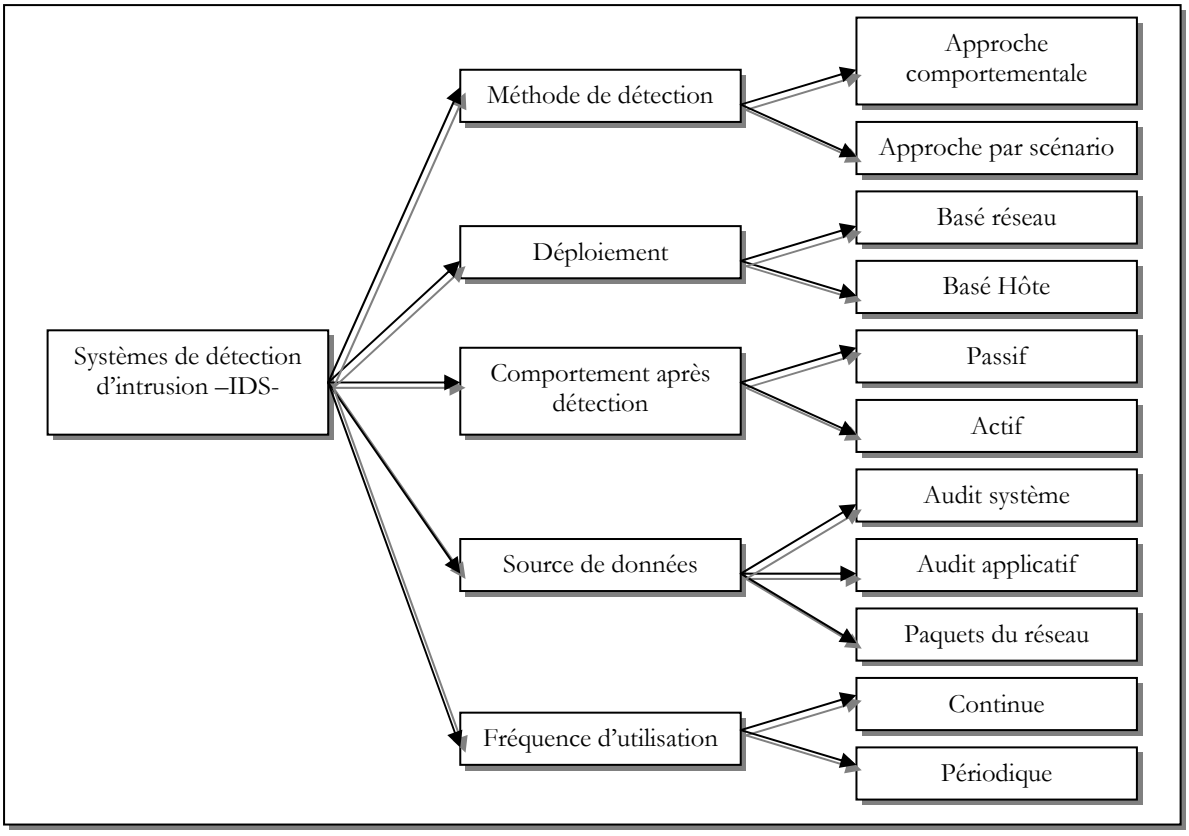


Figure II.5 : *Classification de base des IDS.*

- Le principe de détection utilise.
- Le déploiement.
- Le comportement en cas d'attaque détectée.
- La source des données à analyser.
- La fréquence d'utilisation.

III.1.1 Méthode De Détection :

Les deux approches qui ont été proposées à ce jour sont l'approche comportementale et l'approche par scénarios.

III.1.1.1 Approche Comportementale :

Le comportement normal d'un utilisateur ou d'une application (profil) peut être construit de différentes manières. Le système de détection d'intrusions compare l'activité courante au profil. Tout comportement déviant est considéré intrusif. Parmi les méthodes proposées pour construire les profils on cite :

a) Méthodes Statistiques :

Le profil est calculé à partir de variables considérées comme aléatoires et échantillonnées à intervalles réguliers. Dans un environnement informatique classique (Réseau des machines UNIX et NT), ces variables peuvent être le temps CPU utilisé, la durée et l'heure des connexions, etc. Un modèle statistique (ex : covariance) est alors utilisé pour construire la distribution de chaque variable et pour mesurer, au travers d'une grandeur synthétique, le taux de déviation entre un comportement courant et le comportement passé. L'outil NIDES (Next Generation Intrusion Detection Expert Système) utilise, entre autres, cette méthode.

b) Systèmes Experts :

Ici, c'est une base de règles qui décrit statistiquement le profil de l'utilisateur au vu de ces précédentes activités. Son comportement courant est comparé aux règles, à la recherche d'une anomalie. La base de règles est rafraîchie régulièrement. L'outil Wisdom & Sense [VAC 89] utilise cette méthode.

c) Graphes :

Certaines approches comportementales utilisent des modèles à base de graphes pour mettre en évidence des propriétés et des relations entre ces propriétés. L'intérêt de cette approche est qu'elle permet de traiter plus facilement des événements rares. L'outil GrIDS [STA96] utilise cette méthode.

d) Réseaux de Neurones :

La technique consiste à apprendre à un réseau de neurones le comportement normal d'un utilisateur. Par la suite, lorsqu'on lui fournira les actions courantes, il devra décider de leur normalité. L'outil Hyperview [DEB 92] comporte un module de ce type et plusieurs travaux de recherche vont dans le même sens. Cette méthode reste prometteuse, mais n'est pas encore industrialisée.

e) Immunologie :

Cette analogie informatique de l'immunologie biologique a été proposée par Forrest [WAR99]. Il s'agit de construire un modèle de comportement normal des services réseaux (et non un comportement normal d'utilisateurs) au travers de courtes séquences d'appels système qui sont considérées comme représentatives de l'exécution normale des services considérés. La phase d'apprentissage consiste à observer un service pendant un certain temps afin de construire une base de séquences d'appels normales. En phase de détection, toute séquence étrangère à cet ensemble est considérée comme une potentielle exploitation d'une faille de sécurité du service.

L'approche comportementale permet de détecter des attaques inconnues auparavant ainsi que les abus de privilèges des utilisateurs légitimes du système ; par contre, le comportement de référence n'étant jamais exhaustif, on s'expose à des risques de fausses alarmes (faux positifs). De plus, si des attaques ont été commises durant la phase d'apprentissage, elles seront considérées comme normales (risque de faux négatifs).

III.1.1.2 Approche Par Scénarios :

Des scénarios d'attaques sont construits et l'analyse des traces d'audit se fait à la recherche de ces scénarios. Parmi les méthodes proposées à ce jour à cet effet nous citons :

a) Les Systèmes Experts :

Le système expert comporte une base de règles qui décrit les attaques, les événements d'audit sont traduits en des faits qui ont une signification sémantique pour le Système Expert. Son moteur d'inférence décide alors si une attaque répertoriée s'est ou non produite. Cette méthode été utilisée dans [LUN 88]. Les outils récents ne l'utilisent plus.

b) Les Algorithmes Génétiques :

Ils sont utilisés pour rechercher des attaques dans des traces d'audit. Chaque individu de la population code un sous-ensemble particulier d'attaques qui sont potentiellement présentes dans les traces d'audit. la valeur d'un individu est proportionnelle au degré de réalisme de l'hypothèse qu'il code, au vu du fichier d'audit.

c) Pattern Matching :

Il s'agit là de la méthode la plus en vue actuellement. Des signatures d'attaques sont fournies, à des niveaux sémantiques divers selon les outils (de la suite d'appels système aux commandes passées par utilisateur). Divers algorithmes sont utilisés pour localiser ces signatures dans les traces d'audit (voir [DEB98] pour un exemple). Les outils IDIOT [CRO96], Stalker [HAY96], RealSecure ou NetRanger utilisent cette méthode.

On peut voir deux inconvénients à cette approche : on ne peut détecter que des attaques connues, et il faut remettre à jour la base de scénarios d'attaque très souvent.

III.1.2 Déploiement :

Il y a deux stratégies fondamentales de déploiement pour un produit IDS, basé-Hôte (Host-Based) et basé-réseau (Network-Based). Le placement d'un produit IDS sur le réseau détermine directement le type d'information qui peut être assemblée et analysée par l'IDS.

III.1.2.1 IDS Basé-Réseau (NIDS) :

Un NIDS évalue l'information capturée à partir des réseaux de communications. Il analyse les trames de paquets voyageant à travers le réseau, et peut aussi faire une analyse du trafic. Les paquets sont habituellement analysés par rapport aux attaques définies en fonction de leur contexte et de leur contenu.

Un NIDS comprend un software qui est installé sur des stations de travail dédiées placés à des emplacements critiques du réseau (ex : à l'extérieur du Firewall, devant un serveur Web ou devant un serveur de messagerie). Celui ci «sniff » c'est-à-dire qu'il capture et lit les trames qui traversent le réseau.

III.1.2.2 IDS Basé-Hôte (HIDS) :

Un HIDS évalue l'information trouvée sur différents types d'ordinateurs. Cela peut inclure les contenus de systèmes d'exploitation, des fichiers système, et d'application, ainsi que d'autres logs. Les machines hôtes peuvent inclure des stations de travail utilisateurs, des périphériques, des serveurs spécialisés, ou des composants réseaux (tels que les Firewalls, les routeurs…).

Un HIDS utilise des modules software qui sont installés sur chaque hôte contrôlé, ces modules accèdent et lisent les fichiers logs et les enregistrements d'audit intéressants.

III.1.3 Comportement En Cas d'Attaque Détectée :

Le comportement d'un outil de détection d'intrusion face à la suspicion d'attaque qu'il est en mesure de révéler est une fonctionnalité qui peut s'avérer importante dans le choix d'un produit, il peut se contenter de déclencher une alarme (réponse passive), et/ou prendre des mesures visant à stopper une attaque (réponse active).

III.3.1 Réponse Passive :

C'est le minimum que l'on puisse attendre d'un IDS en matière de comportement en cas d'attaque détectée, la majorité des produits apportent une réponse passive à l'intrusion. Cette réponse se traduit par la génération d'une alarme sous forme de :

- Message sur la console système.
- Message Syslog.
- Courrier électronique, voir même alerte sur un beeper.
- Génération de rapport.

De toutes les manières, c'est à l'administrateur système de prendre les mesures qui s'imposent face à la menace d'intrusion révélée.

III.3.2 Réponse Active :

Les outils commerciaux récents apportent de plus en plus de réponses actives à la détection d'une intrusion. Grâce à une inter-operabilité grandissante avec d'autres produits de

sécurité (Firewalls, routeurs), les IDS sont en mesure d'offrir automatiquement des contre-réactions aux attaques. Ces mesures réactives sont notamment :

−Fermeture de sessions suspectes.

−Reconfiguration «à la volée » d'un routeur et/ou d'un Firewall afin de filtrer un flux suspect.

Cette caractéristique apporte une solution efficace pour se prémunir des dangers que représentent les attaques en déni du service.

III.1.4 Sources Des Données à Analyser :

Les sources de données à analyser sont une caractéristique essentielle des systèmes de détection d'intrusions. Les données proviennent, soit de fichiers générés par le système d'exploitation, soit de fichiers générés par des applications, soit encore d'informations obtenues en écoutant le trafic sur le réseau.

III.1.4.1 Sources D'Information Système (Audit Système) :

Un système d'exploitation propose plusieurs sources d'information :

−Historique des commandes systèmes : tous les systèmes d'exploitation fournissent des commandes pour avoir un « instantané » de ce qui se passe. Ainsi, sous UNIX, des commandes telles que *ps*, *pstat* ou *vmstat* fournissent des Informations précises sur les événements système.

−*Accounting* : *l'accounting* fournit de l'information sur l'usage des ressources partagées par les utilisateurs (temps CPU, mémoire, espace disque,…) les modules statistiques et neuronaux [DEB 92] utilise cette source d'information.

−Système d'audit de sécurité : tous les systèmes d'exploitation proposent ce service pour définir des événements, les associer à des utilisateurs et assurer leurs collecte dans un fichier d'audit. On peut donc potentiellement disposer d'informations sur tout ce que font les utilisateurs : accès en lecture à un fichier, exécution d'une application... cette source est utilisée, par exemple, par Gatassa.

Les outils utilisant ces sources de données sont les HIDS.

III.1.4.2 Sources D'Information Applicatives :

Les grandes catégories d'applications savent toutes générer des informations sur l'utilisation qui en est faite. C'est le cas des fichiers de logs générés par les serveurs FTP et les serveurs Web. Peu de systèmes de détection d'intrusions les utilisent. On peut toute fois citer l'outil webstakler.

III.1.4.3 Sources D'Information Réseau :

Des dispositifs matériels ou logiciels (sniffers) permettent de capturer le trafic réseau. Cette source d'information est intéressante car elle permet de rechercher les attaques en déni de service qui se passent au niveau réseau et les tentatives de pénétration à distance. Néanmoins, il est difficile de savoir qui est à l'origine de l'attaque car il est facile de masquer son identité en utilisant le *spoofing*. Presque tous les outils (commerciaux) récents utilisent cette source d'information. les outils utilisant ces sources de données sont les NIDS.

III.1.5 Fréquence D'Utilisation :

La dernière caractéristique des IDS est leur fréquence d'utilisation : périodique ou continue.

III.1.5.1 Surveillance Périodique :

Dans un contexte peu sensible, on peut se contenter d'une analyse périodique des fichiers d'audit à la recherche d'éventuelles intrusions passées. On peut, par exemple, choisir une analyse journalière, programmée la nuit afin de ne pas gêner les utilisateurs.

III.1.5.2 Surveillance Continue :

Dans un contexte sensible ce mode de fonctionnement est en effet justifié. Mais dans certains cas, le dimensionnement du système devra être effectue en conséquence, car le coût d'un calcul d'une analyse à la volée est loin d'être négligeable.

III.2 Classification selon [AXE00]:

Or que Axelsson [AXE00] a une vue un peut plus différente. Pour lui La partie centrale d'un système de détection d'intrusion est le *détecteur* et son *principe de fonctionnement* fondamental. Par conséquent les IDS sont classées selon lui en deux groupes: le premier traite des *principes de détection*, et le deuxième traite des *caractéristiques du système*.

- Taxonomie Des Principes De Détection D'intrusion: La taxonomie décrite de manière vague ci-dessous est prévue pour former une hiérarchie, tel montrée dans le tableau suivant. (voir Annexe IIa)

TYPE	Apprentissage	Outils Math.	Méthodes	Exemples d'IDS
Anomalies	Autodidacte	Séries Non Temporelles	Modélisation par Règles	W&S
			Statistiques Descriptives	IDES, NIDES, EMERALD, Nao, Haystack
		Séries Temporelles	ANN	Hyperview
	Programmé	Statistique descriptive	Statistiques Simples	MIDAS, NADIR, Haystack
			Règles Simples	NSM
			Seuil	ComputerWatch
		défaut nié	Séries à Etat	DPEM, JANUS, Bro
Signature	Programmé	Modélisation par Etats	Transition d'Etats	USTAT
			Réseaux de Pétri	IDIOT
		Système Expert		NIDES, EMERALD, MIDAS, DIDS
		Reconnaissance de Chaînes		NSM
		Règles Simples		NADIR, ASAX, Bro, JiNao, Haystack
Signature inspirée	Autodidacte	Sélection Automatique		Ripper

Tableau II.1 : *Classification des principes de détection.*

- Taxonomie selon les caractéristiques des systèmes : cette taxonomie classifie les IDSs selon leurs caractéristiques. Ces caractéristiques sont : le *Temps de Détection*, la *Granularité*, la *Source d'Audit*, le *Temps de Réponse*, le *Traitement des Données*, la *Collecte des Données,* le *Niveau de Sécurité*, l'*Interopérabilité.* (voir Tableau 1 de l'Annexe IIb).

Le travail d'*Axelsson* mène aux conclusions suivantes :

- La construction d'une taxonomie des principes de détection d'intrusion s'avère être un exercice fructueux qui offre beaucoup de perspectives dans le domaine.

- On s'aperçoit qu'il y'a un manque de recherche dans les taxonomies et les modèles du comportement intrusif et normal.
- En terme plus général, un système basé signature avec en plus un modèle explicite du comportement normal et un système basés anomalie avec un meilleur modèle d'intrusion/attaques forment un grand intérêt.
- En outre, quand nous divisons les détecteurs courants en trois groupes selon la difficulté du problème qu'ils traitent, il serait intéressant de voir à quel degré ceux-ci peuvent résister. Ces problèmes sont beaucoup plus difficiles à résoudre, particulièrement en raison des attaquants qui sont de plus en plus avancés et qui peuvent éviter d'être détectés.

III.3 Classification de S.Kumar [KUM95b]:

C'est l'une des classifications les plus complètes (Annexe IIa).

III.4 Classification de Smaha [SMA88]:

Ce schéma de classification se base sur les types d'intrusion et qui classifie les intrusions en six types :

- *Tentative de Cambriolage* : souvent détecté par des profils ou des violations atypiques des contraintes de sécurité.
- *Attaque de mascarade* : souvent détecté par des profils ou des violations atypiques des contraintes de sécurité.
- *Pénétration dans le système de commande de sécurité* : habituellement détecté par la surveillance pour les modèles spécifiques de l'activité.
- *Fuite* : souvent détecté par utilisation atypique des ressources d'entrées /sorties.
- *Déni de service* : souvent détecté par utilisation atypique des ressources du système.
- *Utilisation malveillante* : souvent détecté par des profils atypiques de comportement, des violations des contraintes de sécurité, ou l'utilisation des privilèges spéciaux.

IV.- UN MODELE GENERIQUE DE DETECTION D'INTRUSION

En 1987, *Dorothy Denning*, a établi un modèle de détection d'intrusion qui est indépendant du système, du type d'entrée, et des intrusions spécifiques à surveiller [DEN87]. Le *Générateur d'Evénement* (Event Generator) est générique; les événements actuels peuvent être des enregistrement d'audit, des paquets réseau, ou n'importe quelle autre activité observable. Ces événements servent de base à la détection d'anomalie dans le système. Le *Profil d'Activité* (Activity Profile) est l'état global du détecteur d'intrusion. Il contient les variables qui calculent le comportement du système en utilisant des mesures statistiques prédéfinies. Chaque variable est associée à des spécifications de modèle qui servent à filtrer des enregistrements d'événement. Les enregistrements assortis fournissent des données pour mettre à jour leurs valeurs. Chaque variable est associée à l'une des mesures statistiques établies dans le système, et est responsable de la mise à jour de son état en se basant sur l'information contenue dans les enregistrements d'événement assortis.

Le *Profil d'Activité* peut également produire dynamiquement de nouveaux profils pour les sujets nouvellement créés en se basant sur des calibres de modèle (Si de nouveaux utilisateurs sont ajoutés au système, ou de nouveaux fichiers sont créés, des calibres de profils sont instanciers pour eux). Le *Profil d'Activité* peut également produire des enregistrements d'anomalie quand certaines variables statistiques prennent des valeurs anormales. L'*Ensemble de Règle* (Rule Set) représente un mécanisme générique d'inférence et utilise des enregistrements d'événement,

des enregistrements d'anomalie, et des expirations de temps, pour commander l'activité des autres composants et pour mettre à jour leur état. Cependant, *Denning* [DEN87] utilise des systèmes basés sur les règles pour expliquer le mécanisme d'inférence et la nature de l'interaction avec les autres composants.

Comparaison avec d'autres systèmes :

Les différences primaires entre le modèle générique décrit ici et les systèmes actuels décrits précédemment sont :

- Comment les règles comportant l'*Ensemble de Règle* sont déterminées.
- Si l'*Ensemble de Règle* est codé *a priori* ou s'il peut s'adapter et se modifier selon le type de l'intrusion.
- La nature de l'interaction entre l'*Ensemble de Règle* et le *Profil d'Activité*.

Cependant la difficulté qui apparaît dans la majeure partie des systèmes construits actuellement, réside dans le faite de formuler de bonnes métriques statistiques pour identifier des intrusions, calculer leurs valeurs, et identifier des anomalies dans ces valeurs. Conceptuellement, le module *Profil d'Activité* détecte des anomalies, alors que le module *Ensemble de règle* effectue la détection d'abus. Différentes techniques et méthodes peuvent être substituées à ces modules sans changer sensiblement la vue conceptuelle.

Cependant, quelques nouvelles techniques de détection d'anomalie ne tracent pas bien dans les détails internes du *Profil d'Activité*. Par exemple, l'approche réseau de neurone pour la détection d'anomalie ne s'adapte pas facilement au cadre des variables et au calcul de nombre pour une valeur d'anomalie. L'apprentissage et l'adaptation des ensembles et des profils de règle ne sont pas bien modelés. Les approches très récentes tel l'approche basée modèle sont trop différentes pour intégrer directement ce cadre.

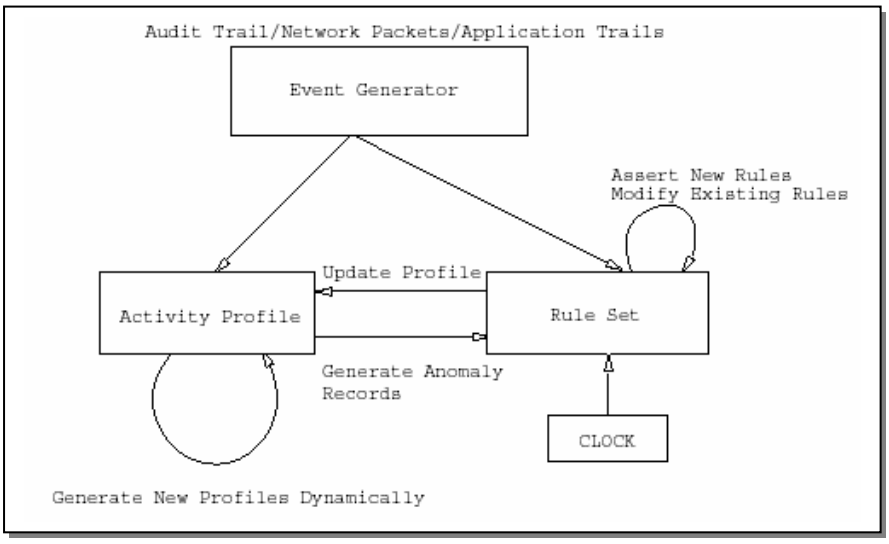


Figure II.7 : *Un Modèle Générique de Détection d'Intrusion.*

V- QUELQUES IDS :

Plusieurs systèmes de détection d'intrusion ont été proposés et mis en application. La plupart d'entre eux dérive du modèle statistique de détection d'intrusion *de Dorothy Denning*

[DEN87]. Certains d'entre eux, par exemple NIDX [BAU88], Haystack [SMA88], IDES [LUN89], MIDAS [SEB88], *Wisdom & Sense* [LIE89], et CMDS [PRO94] utilisent comme entrée une vérification rétrospective. D'autres, par exemple GENTIL [MAC90], [HEA90] et NSM [HEB91] essaient pour détecter des intrusions l'analyse des logs sur l'écoulement d'information dans un réseau. D'autres, comme DIDS [SNA91] ont augmenté la portée de la détection en distribuant la détection d'anomalie à travers un réseau hétérogène en analysant de façon centraliser des résultats partiels de ces sources distribuées pour détecter les intrusions potentielles qui peuvent être manquées par l'analyse individuelle de chaque source.

Parmi les approches non statistiques de la détection d'intrusion figure le travail de *Teng* [TCL90] qui analyse différents *audits* d'utilisateur et essaye d'impliquer les rapports séquentiels entre les événements; pour modéliser un réseau de neurones du comportement par *Simonian* et *Al.* [FOX90].

Les approches pour abuser de la détection d'intrusion comprend des approches basée langage pour représenter et détecter des intrusions telles qu'ASAX [HAB92], développant une interface de programmation d'application, comme dans STALKER [SMA95], systèmes experts tels que MIDAS [SEB88] et NIDX [BAU88], et machines d'état de niveau élevé pour coder les signatures telles que STAT [POR92] et USTAT [ILG92].

VI- LES WIRELESS IDS

Les IDS sont traditionnellement développés pour des systèmes filaires, mais récemment avec l'évolution et le grand déploiement des réseaux sans fil l'idée de *Wireless IDS* ou WIDS a émergée afin d'affronter les problèmes d'intrusions dans les réseaux sans fil.[FAR03a]

Les WIDS sont similaires aux IDS filaires mis à part quelques spécificités liées au déploiement.

Parmi les WIDS on cite: *AirDefense RogueWatch, Airdefense Guard, ISS RealSecure Server Sensor, Wireless Scanner, AirSnort, WIDZ.*

VI.1 Architecture

Les WIDS peuvent être *centralisés* ou *décentralisés* ; les WIDS Centralisés sont formés d'une combinaison de capteurs individuels, qui collectent et diffusent toutes les données 802.11 vers un système de gestion central ou sont stocker et traiter les données. Les WIDS Décentralisés comprend plusieurs unités qui collectent, traitent les informations, mais cette approche est mal adaptée à des WLAN de grande ampleur car elle induit de grand coût de gestion.

Un aspect essentiel pour l'implémentation des WIDS est de déployer des capteurs à chaque point d'accès, et ceci pour avoir plus d'information et aussi la possibilité de localiser géographiquement l'attaquant.

VI.2 Réponse physique

La détection de l'endroit physique est un aspect primordial des WIDS. Les attaques 802.11 sont souvent effectuées à proximité d'un WAP (*Wireless Access Point*) et peuvent être exécutées dans un *timeframe* extrêmement court. Par conséquent, la réponse aux attaques doit être non seulement logique, comme les IDSs standard (c.-à-d. bloquer les adresses IP interdites), mais également elle doit incorporer le déploiement physique des individus pour identifier l'attaquant. À la différence des attaques filaires où l'intrus est habituellement à de grandes distances physiques du réseau de la victime, les attaquants sans fil sont souvent dans les lieux locaux [COL05]. Les

WIDS contribuent en détectant l'endroit de l'attaquant en fournissant au moins une évaluation générale de son endroit physique. En corrélant les données 802.11 capturées avec l'endroit des sondes aussi bien que l'endroit du WAP victime, l'endroit physique de l'attaquant peut facilement être identifié. Une approche bien plus ambitieuse pour l'identification de l'endroit physique serait d'utiliser des antennes directionnelles pour trianguláriser la source du signal 802.11 de l'attaquant [LAC03]. Une fois que l'endroit physique a été rétréci, une équipe de réponse équipée d'outils comme *Kismet* ou *Airopeek* peut balayer le secteur général identifié par l'IDS pour rétrécir plus loin la recherche des attaquants. Avec cette approche d'identification (employant les IDS et les outils de scanne), l'équipe de réponse physique devrait pouvoir identifier et arrêter les attaquants rapidement et efficacement.

VI.3 Renforcement de la Politique

Les WIDS ne détectent pas seulement des attaquants, ils peuvent également aider au renforcement de la politique de sécurité. Avec une politique sans fil forte [FAR03b] et un renforcement approprié, un réseau sans fil peut être aussi sure qu'un réseau filaire et le WIDS peut aider au renforcement d'une telle politique.

Le WIDS peut également tout en respectant la politique, maximiser l'attribution des ressources humaines. Car les IDS peuvent automatiser certaines des fonctions que des humains ont l'habitude d'accomplir manuellement, telle la surveillance des WAPs arrogants.

VI.4 Détection Des Menaces

Les WIDS peuvent également faciliter la détection d'un certain nombre d'attaques. Ils peuvent détecter plusieurs attaques sans fil standard (ou non) [LUR03].

Les Hackers emploient généralement des logiciels de scannage afin d'identifier des WAPs cibles. Les intrus ou les individus curieux utiliseront des outils tels que *Netstumbler* ou *Kismet* pour tracer l'environnement du WAP. Utilisé en même temps qu'un système GPS ces balayages localisent non seulement les WAPs, mais notent également leurs coordonnées géographiques. Ces outils sont devenus si populaires qu'il y a des sites web consacrés à tracer la géographie des WAPs du monde entier. Les WIDS peuvent détecter ces balayages.

Les WIDS peuvent également détecter quelques attaques DOS. Les DOS sont relativement liées aux réseaux sans fil et se produisent de la perte du signal due à un conflit de fréquence ou à un bâtiment. Les intrus peuvent attaquer le WLAN avec l'intention de lui faire faire un Déni de service. Les WIDS peuvent détecter plusieurs attaques DOS, tel que des demandes d'authentification en flooding ou des trames de dissociation.

Le spoofing d'adresse MAC, peut être employé par un attaquant pour se déguiser face à un WAP ou un client sans fil. (Le spoofing d'adresse MAC est également employé dans plusieurs outils tel que *HostAP* et *WLAN-jack)*. Les WIDS peuvent détecter la présence du spoofing d'adresse MAC par différentes manières, y compris l'analyse du numéro de séquence [WRI03]. Les WIDS ont également la capacité de reconnaître les réseaux ad-hoc (une configuration commune qui permet potentiellement à des intrus d'exploiter un dispositif sans fil). Les WIDS peuvent aussi détecter des menaces uniques et non standard par l'utilisation des règles développées par les utilisateurs.

VI.5 Inconvénients des WIDS

La détection sans fil d'intrusion est une technologie plutôt nouvelle ; une grande attention devrait être prise avant d'appliquer n'importe quelle nouvelle technologie à un réseau

opérationnel. Il peut y avoir des bogues, ou des vulnérabilités qui pourraient potentiellement affaiblir la sécurité du WLAN. Cependant la technologie des WIDS se développe rapidement.

Le grand coût des solutions du marché peut être prohibitive. Dans ce cas, une solution propriétaire peut être développée, mais cette approche peut aussi bien être coûteuse en raison du capital humain qui peut être exigé pour développer une telle solution. En outre, le coût d'une solution WIDS (achetée ou propriétaire) augmentera en même temps que la taille du WLAN à surveiller, en raison du nombre de sondes déployées. Par conséquent, plus le WLAN est grand, plus le déploiement du WIDS sera plus cher.

Un WIDS est aussi efficace que les individus qui analysent et répondent aux données recueillies par le système. Les WIDS, comme les IDS standard, peuvent exiger de vastes ressources humaines pour analyser et répondre aux menaces détectées. En fait, il peuvent exiger plus de ressources humaines que les IDS standard parce qu'avec ces derniers, les individus auront à s'occuper des deux aspects : logiques (les données d'alertes) et physiques (trouver et attraper les intrus) d'une attaque. Tandis que la technologie est toujours relativement nouvelle, les coûts peuvent être prohibitifs, et les dépenses pour le capital humain peuvent être plus hautes que ce des IDS standard.

VII- CONCLUSION :

La technologie des IDS est en constante évolution et ne devrait pas être considérée comme défense complète. Cependant elle peut jouer un rôle significatif dans une architecture globale de sécurité.

Quand l'IDS est correctement déployé, il peut fournir des avertissements indiquant qu'un système est soumis à des attaques, même si le système n'est pas vulnérable à l'attaque spécifique. Cet avertissement peut être employé pour changer le maintien défensif de l'installation pour accomplir une plus grande résistance à l'attaque. En outre, les IDS peuvent être employées pour confirmer la configuration et le fonctionnement d'autres mécanismes de sécurité tels que des par-feu.

Selon les classifications étudiées plusieurs types d'IDS apparaissent; mais face au niveau élevé et à la grande complexité des attaques, la solution la plus pratique est d'avoir des IDS hybrides. Ces derniers combinent les avantages de tous les types d'IDS, pour combler leurs faiblesses et contrer au mieux les différentes attaques.

Avec le grand succès des réseaux sans fil, les terminaux mobiles deviennent des cibles aux différents types d'attaques, d'où la nécessité de les protéger comme tous autres éléments d'un système informatique. Cette protection exige le déploiement de nouvelles solutions de sécurité pour les plateformes de ces terminaux, ou l'adaptation des techniques de sécurité déjà existantes.

C'est dans ce contexte qu'on a proposé une solution d'IDS hybride pour les clients mobiles sans fil, nommé EIDS [BEL04]. Cette solution sera expliquée dans le chapitre suivant.

Chapitre III:

EIDS -
Un IDS Hybride Embarqué

EIDS - Un IDS Hybride Embarqué

I. Introduction.

Face au grand succès qu'a connu le monde des télécommunications mobiles, le marché des terminaux mobiles a explosé. La guerre de la concurrence a poussée les constructeurs de ces terminaux à les rendre plus sophistiqués et plus proches des ordinateurs, ce qui en même temps les inscrivaient dans la liste des nouvelles cibles des attaquants. Et comme conséquences de nouvelles catégories d'attaques sont apparut menaçant ces terminaux, ainsi que les systèmes informatiques qui intégré ces terminaux.

Cela nous a motivé pour essayer de trouver une solution de sécurité, afin de protéger d'une part ces terminaux comme cible directe, et d'autre part contrer à leurs niveaux des attaques ciblant les systèmes informatiques qui les intègrent. Nous avons opté dans notre choix de solution sur les Systèmes de Détection d'intrusions, car ils apparaissent comme étant l'une des solution la plus complète et la mieux adaptée, vue la complexité des contraintes et attaques rencontrées.

Parmi les catégories d'IDS étudiées, il existe une catégorie qui utilise une approche hybride pour mieux profiter des avantages des différentes approches tout en comblants leurs inconvénients; et c'est dans cette classe que s'inscrit notre solution « EIDS » [BEL04]. Nous allons décrire cette solution de manière détaillée, pour pouvoir comprendre tous les aspects et les motivations de la solution proposés par ce travail. Du fait que la solution a pour but de renforcer l'EIDS.

II. EIDS: Embedded Intrusion Detection System. -*Conception & Implementation*-

II.2. Objectifs & Motivations

L'objectif de ce travail consiste à mettre en œuvre un système de détection d'intrusion «Light» pour les systèmes embarqués avec l'utilisation de l'approche comportemental. En définissant des modèles et schémas d'activités anormales ou suspects, et en prenant les mesures nécessaires pour mettre fin à ces attaques afin d'atteindre son but qui est d'assurer la sécurité informatique dans un environnement mobile, sans fil, et embarqué. Tout en précisant que le terme "Light" ne signifie pas faible ou réduit coté fonctionnalités, mais au contraire ce terme veut exprimer la notion de plateforme embarqué, avec des ressources réduites qu'il ne faut pas puiser inutilement, et donc que ce système devrait être optimisé, tout en n'alourdissant pas le système d'exploitation cible.

Car en plus de tous les risques d'attaques que les PC ordinaires subissent, les terminaux mobiles (Pochette, PDA, H/PC …) sont exposés aux dangers supplémentaires qu'apporte l'environnement mobile et sans fil. Ces problèmes peuvent argumenter la nécessité d'avoir plusieurs modules pour chaque classe de vulnérabilité. On peut exprimer ces vulnérabilités et les éventuels modules nécessaires en ces points :

✓ Ils sont petits de taille, et donc facile à perdre, chose qui peut avoir des conséquences graves si les terminaux contenaient des informations confidentielles et critiques, ou si vous bénéficiez des services de téléphonie, visiophonie ou d'accès Internet payants. Et donc la nécessité d'avoir un module d'authentification pour l'utilisation du terminal à la mise sous tension du terminal.

✓ Ils bénéficient de l'accès Internet, et qui dit Internet dit tous les formes d'attaques qu'on connait (vers, SYN-Flood, …). Et donc un besoin d'avoir un module de filtrage de paquets entrant d'Internet.

✓ Lorsqu'ils sont synchronisés avec nos PCs plusieurs données et fichiers sont transférés aux terminaux sans aucune vérification ou filtrage, chose qui représente un risque important d'infection par des virus et des trojans. C'est pourquoi un module de détection de trojans et de virus s'impose.

✓ Ces terminaux ont des systèmes d'exploitation (Windows CE, Linos, Windows PPC, Palm OS, …) et donc il faudrait penser à protéger ses systèmes et à garantir l'intégrité de leur fichiers systèmes.

✓ Les terminaux mobiles ont plusieurs ports d'accès physiques (port Infrarouge (IrDA), carte Ethernet (NE2000), connexion via modem (carte modem), accès sans fil (carte Wireless)), ce qui représente plusieurs sources de problèmes. D'où la nécessité d'avoir un filtrage pour chaque point d'accès.

✓ L'accès à ces fichiers doit d'avantage être protégé et contrôlé par des droits d'accès et des procédures d'authentification comme deuxième niveau de protection; car des données confidentielles peuvent être dérobées à l'insu du propriétaire.

✓ L'accès et la transmission sans fil et en lui même un grand point de vulnérabilité, car se support est physiquement le plus fragile à pirater. Et donc la nécessité d'avoir un module qui prend en charge les transmissions critiques via Wireless par un cryptage et décryptage de la transmission dans un environnement de réseau privé (d'entreprise)en premier lieu et dans tout le réseau UMTS ultérieurement.

✓ Aussi il faudrait à tout moment authentifier la personne à l'extrémité de la communication pour savoir si on n'est pas piraté.

Il faut remarquer que dans tous ces points la présence d'un module comportemental trouve tout son intérêt, car il interagit et agit avec tous les modules et donne un apport considérable.

II.3. Choix du modèle

La plate-forme sans fil nous oblige à intégrer les différentes technologies d'IDS [SPA98][GRA00][ZAM01] pour mieux renforcer la sécurité. Ainsi on a opté pour un modèle hybride, qui regroupe trois modèles d'IDS qui sont: le basé hôte, le basé réseau et le basé comportemental.

Le choix de ces trois modèles permettra à notre IDS de bénéficier des avantages de chaque type et de combler les inconvénients d'un type d'IDS par un autre type.

II.4. L'architecture de l'EIDS

On a évité l'architecture monolithique (mono-module centralisé) car elle diminue les performances du système (centralisation des calculs), et elle est vulnérable puisqu'elle se base sur une analyse centralisée qui représente un point de faille du système (si le module central responsable de l'analyse est attaqué tout le système (IDS) tombe en péril).

II.4.1. Architecture globale

Pour la conception de notre EIDS, on s'est inspiré des vulnérabilités et problèmes précédemment exposer pour mettre en œuvre le schéma conceptuel suivant.

L'architecture globale de l'EIDS parait comme une architecture multi-modules indépendants et communiquant entre eux des informations spéciales.

Chaque module est indépendant pour un but d'efficacité global; qui signifie que si un module est altéré ou atteint par une attaque quelconque; l'ensemble de l'EIDS continue à fonctionner.

C'est un IDS léger par les fonctionnalités de ses modules qui doivent être optimales et minimales, afin de remédier aux contraintes de ces terminaux. Ces derniers qui ont une contrainte d'espace de stockage, de durée de batterie limité; et donc il faudrait des tailles de code réduit au maximum, de petits fichiers log générés et moins de calcul (temps CPU).

L'EIDS est composée de modules de détection et d'administration. Les sondes sont chargées de repérer les attaques et de déclencher les actions correspondantes. Les modules d'administration permettent la programmation et la gestion des sondes via un canal sécurisé. Une attaque est identifiée par des caractéristiques du trafic réseau correspondant aux modèles décrits dans une base de signature. Parmi ces attaques nous citerons les attaques par déni de service. Il y a des modules complémentaires qui observent les journaux d'activités ainsi que les fichiers critiques pour détecter toute activité suspecte et déclencher si nécessaire les actions préventives correspondantes.

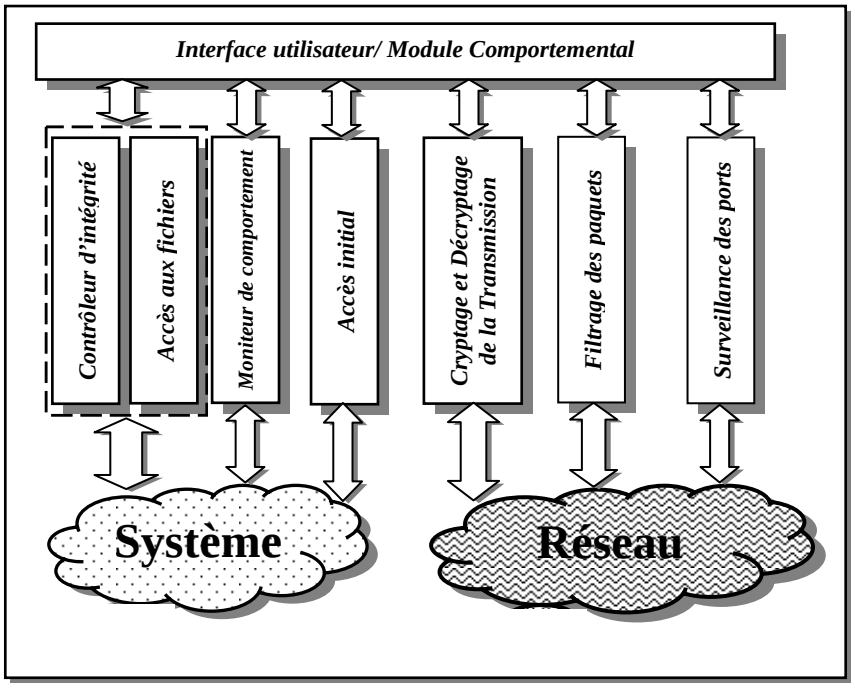


Figure III.1 : *Architecture Globale de EIDS*

II.4.2. Les modules de l'EIDS

Notre système est à base de modules qui peuvent être vu comme *agents mixtes*: *cognitifs* et *réactifs*. Initialement, chaque module possède ses connaissances qu'il enrichit dans le temps avec des informations qu'il collecte, et celles émanant des autres modules. Il est composé de huit *Modules* qui collaborent à la réalisation de notre système de détection d'intrusion:

- Module Controle_d'Integrité.
- Module Filtrage_Paquet.
- Module Surveillance_Ports.
- Module Accés_Initial.
- Module Crypt/Decrypt_Transmission.
- Module Accés_Fichiers.
- Module Interface_Utilisateur (UI).
- Module Comportemental.

Ces modules collaborent entre eux et partagent des connaissances pour renforcer le rôle de surveillance et de défense. La figure ci dessus [*Figure III.1*] montre ces différents modules et leur positionnement vis à vis du flux réseau, du système et de l'utilisateur.

A noter qu'une version de notre EIDS a été implémentée dans un environnement *Windows CE* [MUR98] en utilisant le langage *Embedded Visual Tools C++3.0* destiné aux Pockets PC (Compaq *iPaq 3700*, munie d'une carte Wireless *WL 110*). Les modules ont été implémentés en exploitant les possibilités multithreading offertes par le système *Windows CE*.

II.4.2.1. Module Contrôle_d'Integrité

Ce module offre une protection système en garantissant l'intégrité des fichiers de ce dernier; il permet en plus de détecter des codes d'applications malicieuses ou des virus connus.

Initialement, à l'installation de l'EIDS ce module conçoit une base de données de référence en calculant les signatures numériques de tous ou de certains fichiers spécifies par l'administrateur; puis périodiquement ou à la demande une analyse totale des fichiers systèmes critiques (*.SYS, *.DLL,…) est lancée, en calculant à chaque fois les signatures des fichiers à analyser et en les comparant aux signatures initiaux (de référence) faite à l'installation de l'EIDS. Si une variation de signature est détectée, ce module émet une alerte signalant qu'un fichier a été altéré, et fournit des informations sur ce fichier afin de pouvoir réparer plus facilement les dégâts.

Ces signatures de référence sont stockées dans une base de données avec d'éventuelles informations sur les fichiers (path, taille, date de création et de dernière modification, algorithme de hash utilisé, valeur de signature…). Ces informations concernent :

- *Chemin complet du fichier* : qui constitue une clé de recherche dans la base de données.
- *Signature numérique du fichier* : qui selon l'algorithme de signature contiendra la signature qui va être comparée.
- *Type de l'algorithme utilisé pour la signature* : le choix est entre MD5 et SHA suivant la configuration de l'administrateur.
- *Taille* : afin d'avoir un autre critère de surveillance.
- *Date d'accès et de dernière modification* : pour s'avoir à quand remonte la modification d'une part, et pour avoir plus d'information nécessaire pour les autres modules (module comportemental).
- *Nombre d'accès* : l'explication du but de ce champ est expliquée ultérieurement dans le module comportemental, car il aide aux calculs statistiques et à l'audit de l'utilisateur.

S'ajoute à cette base de données une seconde base, qui aidera le module à surveiller et détecter les éventuelles altérations sur des fichiers, et à dévoiler la présence de virus sur l'hôte (dans l'esprit que le terminal mobile du fait qu'il se synchronise avec des PC, devient facilement un porteurs de virus, et donc mieux vaut prévoir une attaque avant qu'elle agisse que d'essayer de réparer les dégâts). Cette dernière Bases de Donnée est dynamique et admet des mises à jour pour les identités des nouveaux virus.

Ce module assure aussi le contrôle d'intégrité de fichiers de données personnels ou confidentiels à notre choix, il suffit seulement de le spécifier pour qu'il soit pris en compte.

Au calcul de chaque signature ce module compare cette dernière aux signatures correspondant à des codes malicieux et virus connus qui sont stockées dans la seconde base de données dynamique qui est mise à jour régulièrement avec des signatures de nouveaux virus.

Par défaut l'analyse est lancée périodiquement, mais elle peut à tout moment être lancée pour des cas spéciaux de vérification globale ou spécifique. (Le cas de détection de ports spéciaux qui sont ouvert TELNET ou FTP… (Vol ou modification d'informations)).

Pour le choix des algorithmes de hash, on a opté pour les deux algorithmes SHA et MD5 qui ont fait leur preuve de puissance [SCH94].

Des fichiers de rapports sont génères à la détection d'altération quelconque. Ces fichiers sont mis à jour pour garder des traces en vue de détecter des attaques à distance, et pour être utilisés par d'autres modules. Ainsi que des rapports d'alertes sont envoyés au module Comportemental pour l'aider à décider.

Ce module interagit avec le module Cryptage/Décryptage pour inclure la possibilité de crypter et décrypter des fichiers confidentiels en but de les protéger; en fournissant un mot de passe jouant le rôle de clé de cryptage. Ainsi qu'il interagit avec le module Accès_Fichier à travers le module comportemental lors de la détection d'une tentative de modification de fichier non autorisée.

Et voici un schéma qui décrit l'architecture et le fonctionnement de ce module :

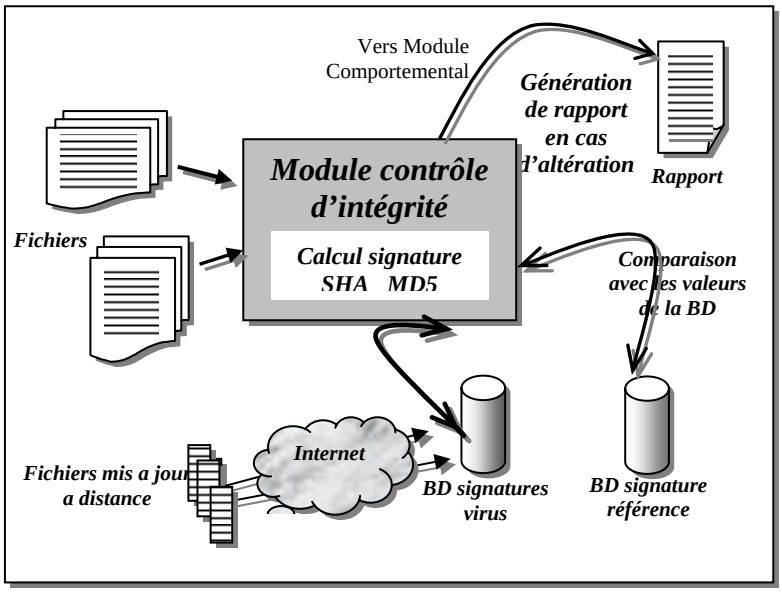
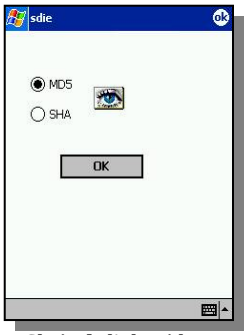


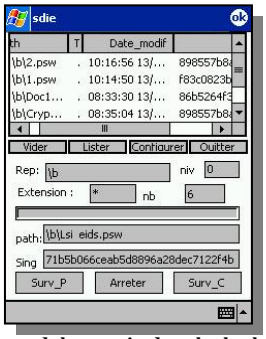
Figure III.2 : *Module contrôle d'intégrité*

Pour illustrer nos propos, voici un scénario d'action des modules cités :

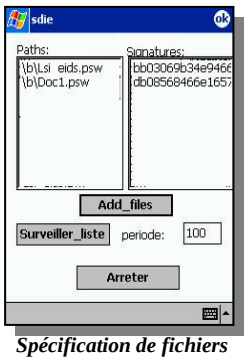


Choix de l'algorithme de signature

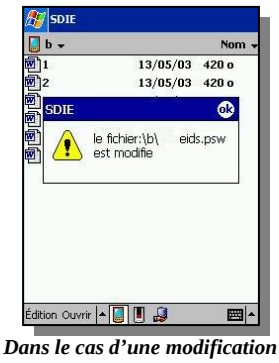
On précise un niveau de protection



Le module entrain de calculer les signatures de tous les fichiers



Spécification de fichiers personnels à surveiller



Dans le cas d'une modification l'EIDS nous alerte en précisant le fichier altéré et l'agent accès est lancé pour l'authentification

Un fichier log est généré avec toutes les informations utiles

Un deuxième mécanisme est implémenté pour avoir la protection temps réel, qui consiste à choisir un niveau de protection sur une échelle de 4 niveaux :

- ✓ Niv_0 : protection nulle.
- ✓ Niv_1 : protection contre les modifications.
- ✓ Niv_2 : cryptage de fichier.
- ✓ Niv_3 : protection contre la modification, la suppression.

Les niv_0, niv_1, niv_3 sont implémentés en adaptant périodiquement les attributs des fichiers spécifiés sous les modes «Read Only» et «Hidden + Read Only». Cette technique trouve toute sa puissance dans cette plateforme du moment que la possibilité de changement d'attributs n'est pas implémentée dans l'interface graphique de Windows PPC et le fait d'effectuer se travail périodiquement avec une petite période qui permet de contourner la possibilité de changement manuel d'attribut via l'interface graphique pour les H/PC; qui veut dire que cette solution est maintenue même si au futur on intègre la possibilité de changement d'attributs via l'interface.

Le niv_2 protége les fichiers en les cryptant en utilisant la puissance des algorithmes RC4 géré par la CAPI (CryptoAPI).

II.4.2.1. Module Filtrage_Paquet

Les terminaux mobiles disposent de plusieurs ports d'accès à l'environnement extérieur, parmi eux, l'accès filaire (Modem (SLIP, UniModem, PPTP…), carte Ethernet,…); l'accès infrarouge (port IrDA); et l'accès sans fil (carte Wireless). Tous ces ports d'accès sont des points de vulnérabilité surtout l'accès sans fil, qui permet à n'importe qui de se connecter et de s'introduire à l'intérieur du terminal puisant ainsi de toutes les données disponibles dans le terminal. Et comme ces terminaux ont été crées pour inclure la norme UMTS, ils bénéficient de la connexion Internet sans fil (à 2Mb/s) qui est un grand point d'intrusion.

D'où la nécessité d'avoir un module de filtrage des paquets entrants pour maîtriser et connaître le flux entrant. Ce filtrage doit être implémenté pour chaque interface d'accès (Wireless, Ethernet, IrDA …); et doit agir en toute légèreté pour ne pas alourdir les taches systèmes.

Ce filtrage est basé sur la détection et le rejet des paquets anormaux [FRE00] et ceux émanant de source inconnu (filtrage basé adresse, basé scénario); et l'émission d'une alerte à l'utilisateur à travers le module comportemental (pour qu'au pire des cas il débranche sa carte d'accès à distance) pour arrêter l'attaque; en plus de la génération des fichiers log pour la détection des scénarios d'attaques complexes (liée à l'utilisation de services web, FTP, SMTP,…). Ce filtrage touche les paquets IP; TCP et UDP; et rassemble les fragments dans un buffer avant de les analyser. Cette analyse se base sur l'article [FRE00] qui classe les paquets anormaux en cinq catégories d'anomalies :

1. Anomalie au niveau des @IP.

2. Anomalie au niveau paquets TCP.
3. Anomalie au niveau paquets UDP.
4. Anomalie au niveau paquets ICMP.
5. Anomalie de fragmentation.

La première catégorie concerne le fait que certaines adresses IP on été réservées par IANA (Internet Assigned Numbers Authority) comme étant des adresses à usage privé (usage interne des réseaux) et qu'on ne doit pas trouver ces adresses dans Internet. (RFC1918):

[10.0.0.0–10.255.255.255], [172.16.0.0–172.31.255.255], [192.168.0.0–192.168.255.255].

En plus des paquets avec : *@IP_Source == @IP_Destination* ; ces deux failles sont exploitées par les hackers dans les attaques de type «IP Spoofing» et «Land» [FRE00].

La deuxième catégorie concerne les combinaisons illégales des *flags* des paquets TCP :

- SYN +FIN utiliser par les Hackers pour scanner des ports.
- SYN+FIN+PSH; SYN+FIN+RST; SYN+FIN+RST+PSH qui sont des variantes de SYN+FIN.
- Les paquets avec seulement l'indicateur FIN, utilisés par des scanners de ports.
- Les paquets sans aucun indicateur.
- Les paquets avec les deux bits réservés actifs.
- Tous paquets avec combinaisons de jetons autres que celle-ci:
  - SYN. SYN+ACK et ACK.
  - ACK toujours mis; à part pour paquet SYN initial.
  - FIN+ACK et ACK pour l'arrêt de connexion.
  - RST+ACK pour l'arrêt immédiat de la connexion.
  - PSH et/ou URG sont facultative.

En plus des paquets TCP avec:

- Une source ou destination égale à 0.
- Numéro d'acquittement mis à 0 et l'indicateur ACK configuré.
- SYN seulement et contenant des données.
- @Dest de broadcast.

La troisième catégorie traite des numéros de ports dans les paquets UDP: *Port_Source* ou *Port_Destination == 0*.

La quatrième catégorie est celle des anomalies au niveau des paquets ICMP; il faut se méfier des message de redirection vers l'hôte lui même; car se type de message ICMP est utilisé entre les routeurs pour s'échanger des informations de routage dynamique et donc n'importe qui peut exploité ses message afin d'embrouiller ou de détourner la route des messages, comme le fait l'attaque «WinFreeze». Aussi les paquets de demande d'écho ICMP qui ont des entêtes de plus de 8 octets et une charge utile de plus de 56 octets sont considérés suspectes.

La cinquième catégorie englobe toutes les formes de paquets suspects d'appartenir à des attaques par fragmentation; la fragmentation parait comme une méthode pour dissimuler les paquets anormaux précédemment exposés du fait qu'un fragment est un paquet à part entière; et donc comme exemple d'attaque par fragmentation est de constituer un paquet pour l'attaque Land en mettant l'*@IP_Source == @IP_Destination*, puis à fragmenter ce paquet en deux paquets au niveau de la séparation des deux champs @IP et falsifier les valeurs des offsets (utilisées pour le réassemblage); et comme cela au réassemblage il y'aura un recouvrement des deux fragment qui donnera un paquet interdit. Dans d'autre cas la fragmentation excessif de paquets énormes est utilisé pour rendre les système inactif (en puisant des temps CPU au réassemblage); comme le cas de l'attaque «Ping of Death» qui crée un paquet de demande d'écho ICMP qui est plus grand que la taille maximal d'un paquet, 65535 octets.

Ce module capture un paquet, procède à son analyse en déterminant son type (TCP, UDP,…) et son entête en vue de détecter d'éventuelles anomalies qui sont considérées comme étant des signes d'attaques :

– Les paquets provenant d'adresses IP non autorisées et qui sont enregistrées dans une liste à travers l'agent interface utilisateur.

– Attaque par déni de services (SYN-FLOODING); on garde trace de tous les paquets de demande de connexion. On dispose d'un compteur des paquets SYN captés, il est décrémenté de 1 à chaque fois qu'un paquet d'acquittement (ACK) est reçu. Dès que ce compteur atteint un seuil fixé par l'administrateur (en prenant en considération l'importance du réseau et les besoins de sécurité), une alerte est générée pour avertir l'administrateur de l'événement.

– Paquets anormaux : plusieurs attaques sont commises en envoyant des paquets TCP/IP avec des entêtes non saines [FRE00].

Le module filtrage des paquets garde trace de toute l'activité réseau dans deux fichiers, l'un contient le trafic réseau et l'autre contient les alertes survenues (l'heure, type d'attaque, adresses source, adresse destination, port source, port destination). Le module peut être réactif pour fermer une connexion TCP/IP en envoyant un paquet avec le flag RST positionné. Il utilise les capacités réelles du système hôte, il fait appel à l'agent SNMP pour récupérer le résultat de l'audit de cet agent.

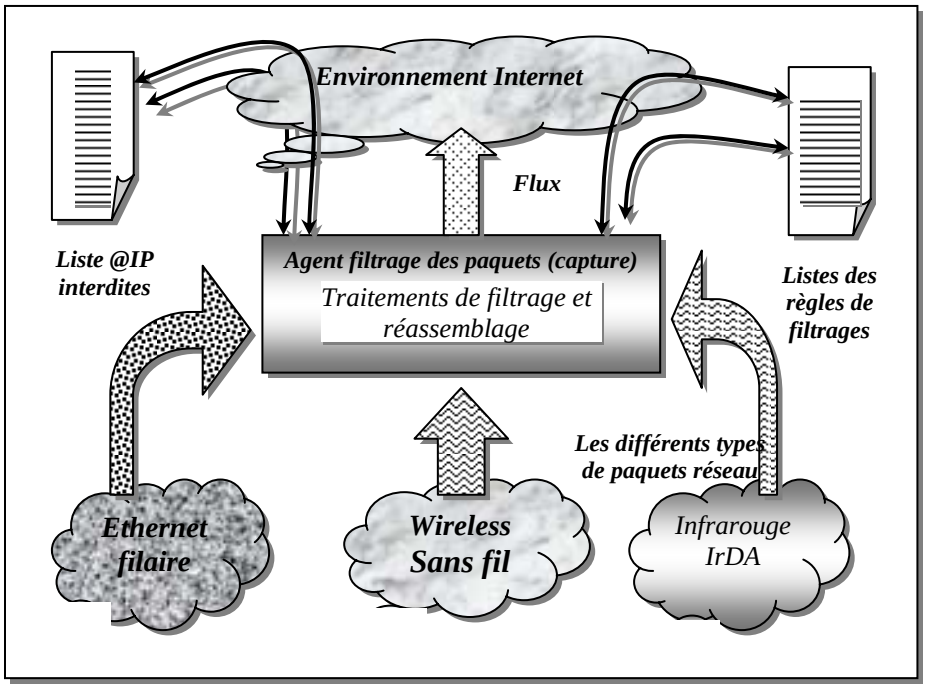
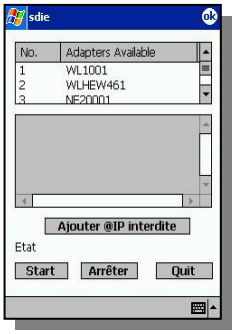
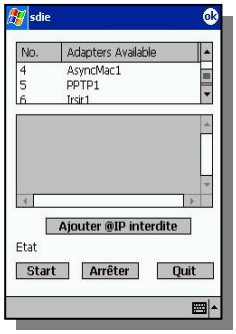


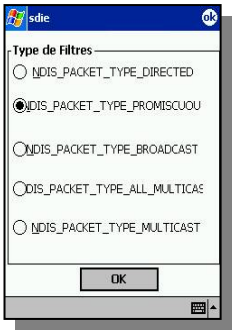
Figure III.4 : *Module filtrage des paquets*

Et voici un scénario de capture et de filtrage, avec l'étape de configuration pour choisir l'adaptateur réseau et le mode de filtrage puis le lancement de la capture et le filtrage.

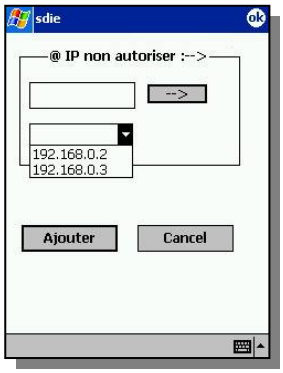




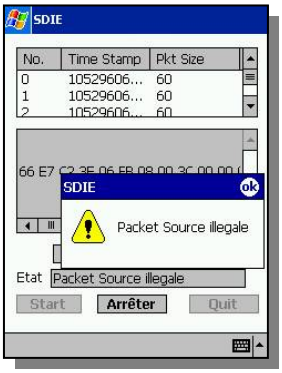
Choix de l'adaptateur (le port à filtrer: IrDA, WiFi, Ethernet, Async ;…)



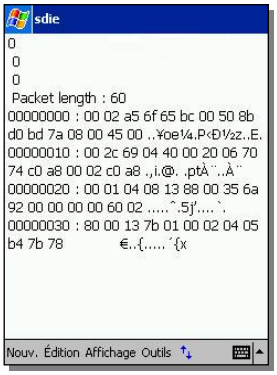
Choix du mode de filtrage



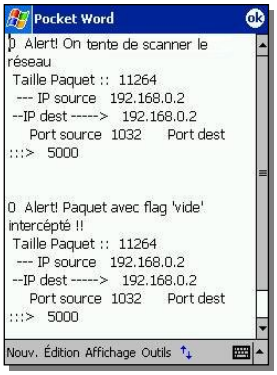
Configuration du filtrage basé adresse IP



Capture& filtrage. Détection de paquet de source illégale



Fichier historique du flux



Un fichier log est généré contenant les différents alertes du filtreur

II.4.2.3. Module Surveillance_Ports

Ce module est un scanner de ports, qui permet la détection des trojans qui peuvent être téléchargés ou transférés discrètement des PCs, et pour la détection des attaques à distance.

Il détecte les ports ouverts et les compare à une liste dont il dispose; cette liste peut être configuré par l'administrateur et contient les ports saints liés à des applications personnelles utilisant ces ports.

Ce module émet des alarmes à d'autre modules (Contrôleur_Intégrite, Module Comportemental) si des ports spéciaux sont ouverts (FTP, Telnet, …) dans le cadre de détection d'un comportement suspect (vol de fichiers, falsification de données, …).

Si un port non spécifié (qui n'appartient pas à la liste de l'administrateur) est ouvert une alerte est émise et un rapport (qui sera comme historique) est généré pour être utilisé par d'autres modules (détection des comportements suspects).

En réaction à cela il peut fermer les ports malsains à la demande en émettant des paquets FIN. Ce module agit périodiquement ou à la demande d'un autre module.

Le scannage des ports [FYO00] est une méthode fréquemment utiliser par les hackers pour la détection de voies de communications ouvertes et exploitables sur des hôtes à distance. A l'origine c'était une méthode d'administration de réseaux et de maintenance de ses ressources; (SATAN, …), puis elle a été adoptée par les hackers comme un moyen efficace de préparation d'attaque.

Les scannage de ports admet plusieurs méthodes, et plusieurs techniques ont étés développées pour examiner les protocoles et les ports; par mis eux:[FYO00]

- ✓ TCP Connect() scanning.
- ✓ TCP SYN (half open) scanning.
- ✓ TCP FIN (stealth) scanning.
- ✓ TCP FTP proxy (bounce attack) scanning.
- ✓ SYN/FIN scanning avec fragmentation IP.
- ✓ UDP recevfrom() scanning.
- ✓ UDP raw ICMP port unreachable scanning.
- ✓ ICMP scanning (ping sweep).
- ✓ Reverse-ident scanning.

- *TCP Connect() scanning :* qui consiste à faire des appels systèmes «Connect()» avec plusieurs numéros de ports; si l'opération réussit le port est ouvert sinon le port est fermé (non accessible), puit on ferme la connexion.

Avantages :

- Pour implémenter cette technique on n'a besoin d'aucun privilège spécial.
- Méthode rapide si l'appel est fait une seule fois.

Inconvénient :

- Prend beaucoup de temps si on fait des séries d'appel Connect().
- Facilement détectable (par les fichiers log: une masse de connexions suivit de fermetures) et filtrable

- *TCP SYN (half open) scanning:* appelé aussi "scanning demi-ouvert" car au lieu d'ouvrir une connexion TCP complète, elle se contente d'envoyer un paquet SYN et d'attendre une réponse; si cette dernière est un SYN/ACK le port est ouvert sinon si c'est un RST le port est fermé. Après cela un paquet RST est émis pour fermer la connexion.

Avantages :

- Peu de cibles loggerons cette connexion.

Inconvénient :

- Exige les privilèges «root» pour construire les paquets SYN.

- *TCP FIN (stealth) scanning :* envoie des paquets FIN qui engendre une réponse RST de la part des ports fermés, et pas de réponse des ports ouvert. Il faut préciser que cette méthode ne marche pas avec des machines MicroSoft.

- *Fragmentation :* c'est une variation d'autres techniques; qui consiste à diviser le paquet espion en plusieurs fragments IP, pour outrepasser les filtres.

- *TCP Reverse-ident scanning :* elle exploite le protocole «ident» (RFC1413) qui permet de révéler le nom de l'utilisateur propriétaire de n'importe quel processus relié par TCP. Elle consiste à ce connecté à un port et puis exécuté *ident* pour connaître le propriétaire.

- *TCP FTP Proxy (bounce attack) scanning:* Elle exploit la possibilité du protocole FTP (RFC959) à traverser les serveurs proxy. On initie un «User-DTP» (Data Transfer Protocol) passif et on le met en écoute du système cible sur un certain numéros de port ; puis on essaye de listé le répertoire actuel. Si le port spécifié de l'hôte cible est ouvert, le serveur DTR envoie une réponse 150 ou 226; sinon une réponse «*425: can't build data connexion*» est reçut.

Inconvénients :

- Lenteur.
- Certain serveurs FTP ont désactivé cette possibilité de proxy.

- *UDP raw ICMP port unreachable scanning:* cette technique utilisant le protocole UDP ou les ports ouverts ne sont pas obligés d'envoyer un acknowlegment en réponse à une demande, et ou les ports fermés n'envoient même pas de paquet d'erreur. Mais la plus part des hôtes renvoient une erreur ICMP_PORT_UNREACH quand le port UDP est fermé ; ainsi on peut connaître qu'un port est fermé. Il faut en plus que ce scanneur implémente une retransmission des paquets qui pourraient être perdus (car le protocole UDP ne garantie pas l'arrivé des messages UDP ou erreurs ICMP).

Inconvénients :

- Privilège «root» pour avoir la possibilité d'utiliser les raw ICMP sockets, nécessaire pour la lecture des ports inaccessibles.

- *UDP recevfrom() scanning :* faire des *write()* qui échoue ou interpréter les codes de retour de la fonction *recevfrom()* qui retourne EAGAIN (*«Try Again», errno 13*) si l'erreur ICMP n'a pas été reçue et ECONNREFUSED (*«Connection refused», errno111*) si oui.

- *ICMP echo scanning (ping sweep):* qui consiste à pinger les hôtes d'un réseau pour détecter ceux qui sont en marche.

Exemples de scanneurs connus : [FYO00] *strobe* (de Juliun Assange); *netcat* (de *Hobbit*); *stcp* (d'Uriel Mainmon); *pscan* (de Pluvius); *ident-scan* (de Dare Goldsmith); *SATAN* (de Wietse Venema); *nmap* (de Fyodor)….

L'implémentation de la technique "*TCP Connect () scanning*" ce fait en créant des sockets avec des numéros de port allant de 0 à 65535 pour un scannage complet, ou un numéros précis pour des ports spécifique. Puis en exécutant l'appel system Connect (), et en attendant la réponse pendant un certain laps de temps. Si une réponse aboutit on juge que le port est ouvert et donc on peut décider de fermer le port par un CloseSocket, sinon il est fermé. La contrainte de cette méthode est qu'elle alourdit beaucoup le système. Pour cela on a opter pour une autre solution plus efficace qui exploite les fonctionnalités de la DLL (INTMIB1.dll) et des propriétés du protocole SNMP (Network Managent protocole), on Utilise les deux fonctions (*SnmpEXtensionInit()*) pour initialiser l'agent SNMP et (*SnmpEXtensionquery()*) pour récupérer le résultat de l'audit de cet agent.

Cette 'dll' nous permet d'avoir tous les ports ouvert, et donc il nous faut disposer épose d'un liste (BD) des ports sains, qui sont insérés dans la base au moment d'installation d'application et qui sont considérés comme sains. Ce mécanisme nous permet, en plus de détecter des ports ouverts, de bénéficier d'information supplémentaire comme l'@IP qui peuvent aider les autres modules à la construction de leur base de connaissance (comme le module de filtrage qui va insérer ces adresses IP dans sa liste noir d'@IP).

C'est un module tems réel et ouvert du fait qu'on peut spécifier les ports sains.

II.4.2.4. Module Accés_Initial

L'existence de ce module s'inspire du fait que les terminaux mobiles peuvent être facilement volés ou perdus, car ils sont petits de taille (terminaux de poches). Son rôle consiste à protéger l'utilisation du terminal (ou l'accès au service de ce terminal) par une procédure d'authentification par mot de passe (avec un nombre limité de tentatives afin d'éviter les perceurs de mots de passe), et par un questionnaire comme un deuxième niveau d'authentification qui s'ajoute au mot de passe ; ce dernier peut être facilement divulgué. Le questionnaire est constitué d'une manière évolutive, en commençant par une liste initiale de questions posées à l'installation de l'IDS; et qui au fur et à mesure s'enrichit d'avantage par des informations collectées en collaboration avec le module moniteur de comportement. Le questionnaire est étudié de façon à ce qu'il récolte des informations individuelles, personnelles, et suffisant à l'authentification.

Ce module permet d'une part, de protéger les documents confidentiels contenus à l'intérieur du terminal, et d'autre part d'empêcher les voleurs d'utiliser les services de téléphonie et de connexion Internet au détriment du propriétaire. La procédure d'authentification périodique (selon la configuration) demande une éventuelle information personnelle; si la réponse est fausse le terminal est éteint et verrouillé automatiquement. Ce module interagit avec d'autres modules lorsque ces derniers émettent des alertes de soupçons sur l'action en cours pour les besoins d'authentification. Il est à noter que les informations récoltées sont stockées dans la même base de données utilisée par le module *moniteur de comportement* pour la similitude des informations stockées. Nous préconisons que ce module doit être intégré dans le système d'exploitation, car ces terminaux peuvent être réinitialisés, et par conséquent il y aura la perte de toute application (EIDS) et données (base de données) sur le terminal. Le même cas de figure peut être obtenu dans le cas où la batterie se vide entièrement.

II.4.2.5. Module Crypt/Decrypt_Transmission

On implémente ce module dans un environnement de réseau privé afin qu'il nous permette de faire une transmission, un transfert de fichier, ou une communication sans fils en toute sécurité; et cela en ajoutant au cryptage offert par l'interface réseau sans fil (le protocole de cryptage «WEP» pour les cartes Wireless) notre algorithme de cryptage comme deuxième couche de protection. Et cela pour éviter le risque de piratage, car la liaison (support) sans fil est l'une des plus faibles supports, et l'une des plus difficile à protéger (physiquement). Sachant que dans un environnement d'entreprise, la confidentialité des données transmises est cruciale. On ajoute donc un algorithme de cryptage, qui change dynamiquement de clé (algorithme à clé public). Le cryptage est conçu en exploitant les possibilités de la CryptoAPI.

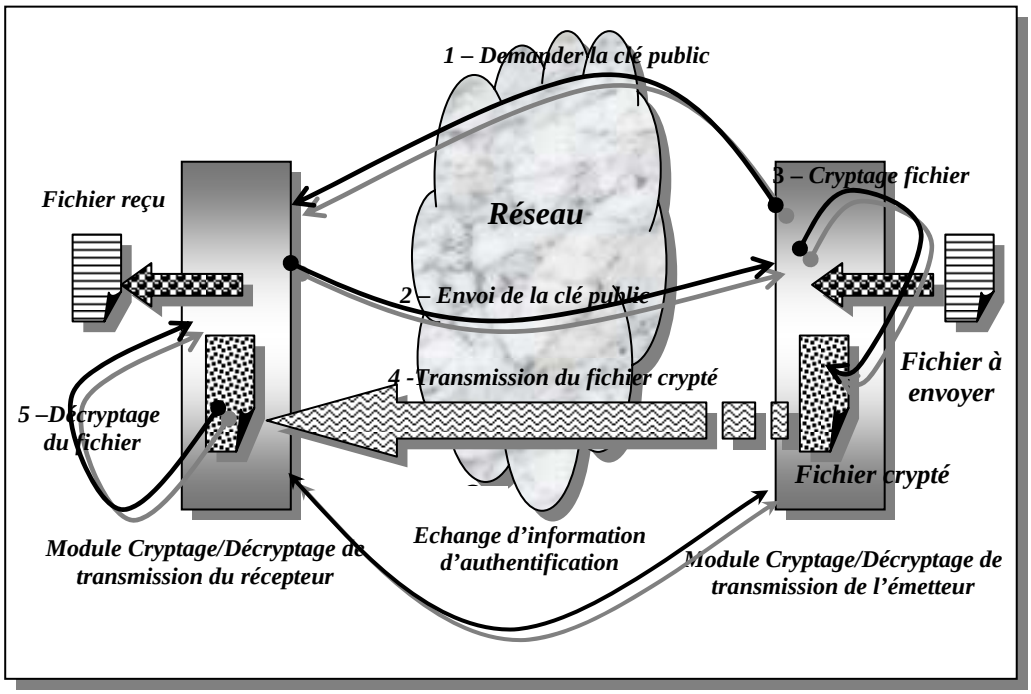


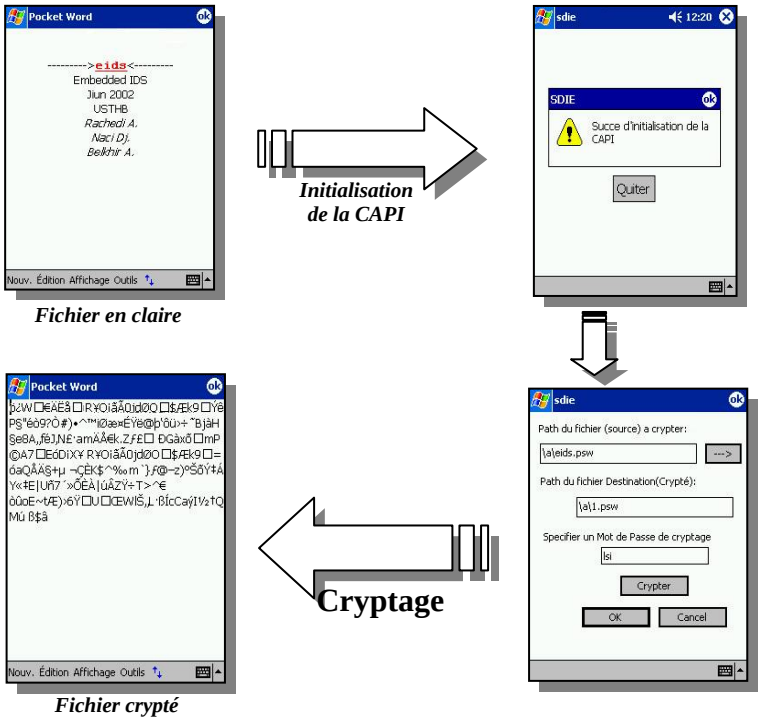
Figure III.5 : *Module Cryptage/Décryptage de la transmission*

Si l'utilisateur désire envoyer des fichiers, ou faire une communication sécurisée, il actionne ce modulesélection du fichier à envoyer, ce module demande à connaître la destination afin d'aller se connecter à ce dernier pour amener la clé publique de cryptage ; et c'est avec cette clé que le module Crypt/Decrypt_transmission crypte le fichier spécifié. Après cela le module se reconnecte et envoie le fichier crypté; arrivé à destination se dernier est décrypté en utilisant la clé secrète du destinataire et le fichiers est prêt à être exploité.

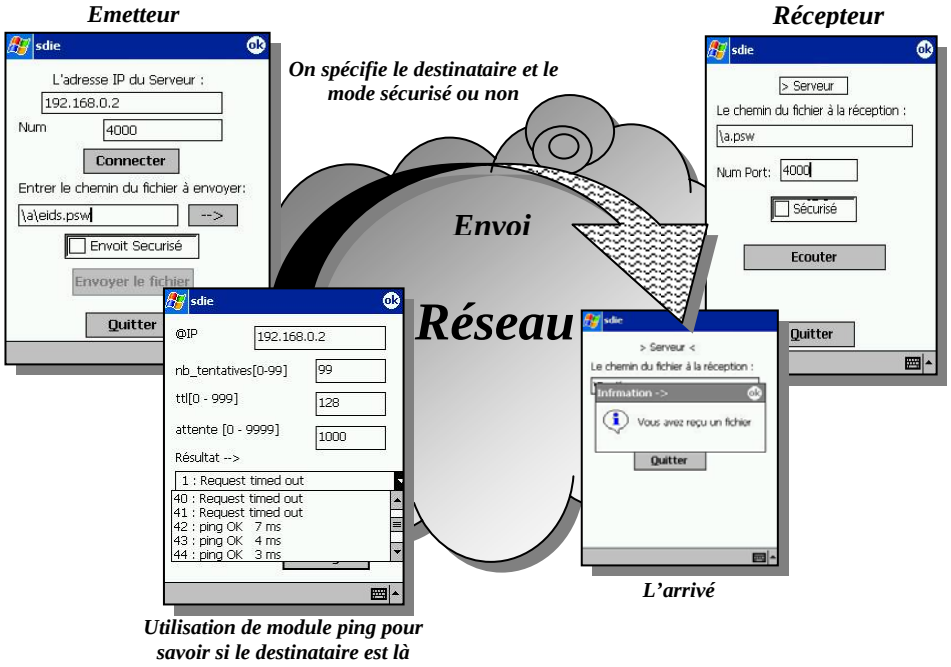
L'émetteur se reconnecte pour l'envoi du fichier car il utilise un deuxième canal de transmission pour le transfert et laisse le premier pour les commandes ou les données d'authentification. Il ne faut pas bien sûr oublier de configurer l'option de cryptage au niveau interface réseau (en activant l'option WEP par exemple).

Ce module gère aussi les transmissions filaires; mais pour le port infrarouge on estime qu'il n'exige pas une grande précaution car la connexion demande l'avis du récepteur d'une part, et d'autre part demande que les ports soient alignés et rapprochés.

Voici un exemple du module cryptage/Décryptage.



Tandis que la transmission locale se fait via un module de transfert qui supporte l'option transfert crypté



II.4.2.5. Module Accé_fichiers

Ce module est d'une grande utilité, à l'événement d'accès ou d'ouverture d'un fichier une boite de dialogue surgit et s'affiche pour vérifier et authentifier les droits d'accès à ce fichier. Si la procédure de vérification des permissions réussit le fichier est décrypté et est ouvert à celui qui veut y accéder. Bien sur cette opération est configurée au besoin du propriétaire du fichier.

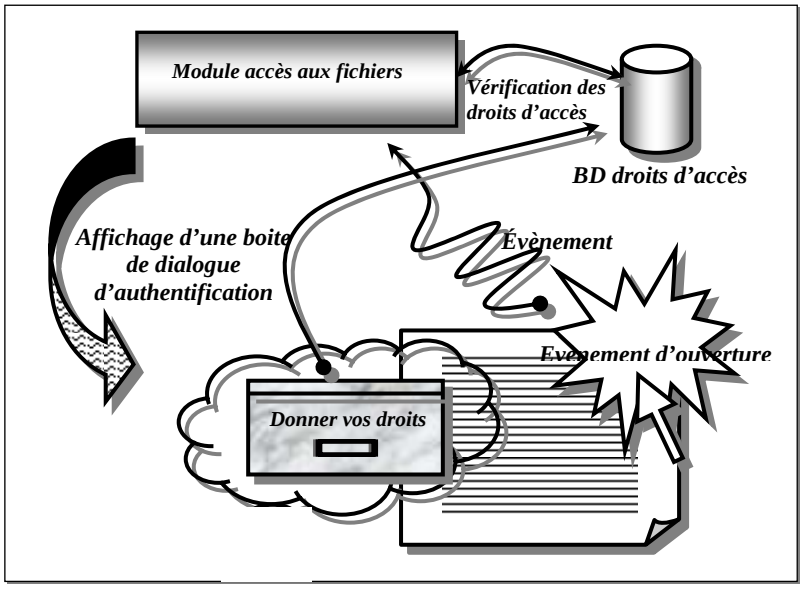


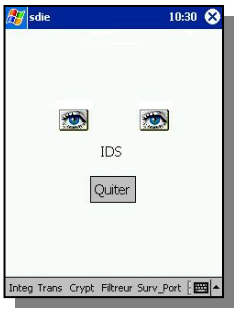
Figure III.7 : *Module accès aux fichiers*

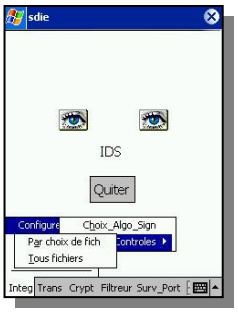
Ce module permet de protéger les données confidentielles et les fichiers système critiques (et surtout les fichiers de notre EIDS). Il doit impérativement être inclut dans le système d'exploitation car les événements et messages système spécifiés (de Windows) ne sont pas documentées.

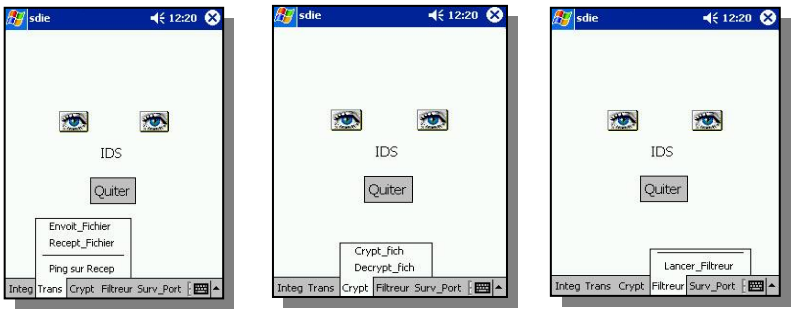
II.4.8. Module Interface_Utilisateur :

Ce module permet d'établir une interaction avec l'utilisateur, il a la charge de lancer, arrêter et configurer les autres modules. Il interagit directement avec l'utilisateur pour la configuration, la consultation des données récoltées à partir d'autres modules. Il est configurable dans le sens où l'administrateur peut définir la liste des fichiers à surveiller, les adresses IP des utilisateurs indésirables.

C'est le module qui permet l'accès et l'administration ou la configuration de tous les autres modules;







II.4.9. Module Comportemental

Il faut remarquer que la présence d'un module comportemental trouve tout son intérêt, car il interagit et agit avec tous les modules et donne un apport considérable. Tous les modules représentent pour ce dernier des sources (sondes) de données cruciales, ainsi que des modules de réaction dans le cas ou le module comportemental décide qu'une action est suspecte. Chaque module pris indépendamment est destiné à une classe de vulnérabilité précise, préalablement recensée. Les attaques plus complexes, qui diversifient leurs champ d'action ou qui sont nouvelles ne sont pas détecté par ces modules. C'est la qu'intervient le rôle du module comportemental qui est en relation avec tous les modules; pour faire corréler toutes les activités au niveau de ces modules pour déceler des intrusions complexe ou nouvelles.

Ce module n'a pas été implémenté dans le travail [BEL04], chose qui motive notre travail actuel.

III. Conclusion.

EIDS est un système modulaire, chaque module peut être implémenté comme *Agent Mobile* sur des plateformes appropriées (FIPA, AGLET, AGENTA, MADKIT) afin de bénéficier de la puissance de leurs mobilité et d'étendre la solution pour la sécurisation d'un réseau (filaire, Wireless); ou comme *Composant* pour pouvoir adapter chaque composant selon les besoins spécifiques des entreprises.

Le système qu'on vient d'exposer sa conception est un système à base de plusieurs modules indépendants, qui interagissent comme un seul, tous ces modules ont le même but, c'est de protéger les unités mobiles (PPC, HPC,…), tout en évitant l'effondrement de tous le système si l'un de ces modules est attaqué.

Ce système est léger «light» pour remédier aux besoins de la plate-forme en matière de ressources. Il est évolutif par ces possibilités de configurations, de mis à jour de ses bases de données et de connaissances. Il est hybride car il marie plusieurs modèles d'IDS pour exploiter au mieux leurs avantages et pour combler leurs faiblesses respectifs.

La structure modulaire de notre système le préserve d'écroulement, car les modules sont autonomes: il faut attaquer tous les modules pour corrompre le système de détection d'intrusion. Par ailleurs, il intègre l'ensemble des stratégies d'attaque. Par analogie à la brosse à dents; on dira que cette brosse préserve les dents mais s'use en même temps. De même les chiffres peuvent être cassés par le temps, les scénarios d'attaques peuvent évoluer et par là même échapper aux techniques de détection. Une solution préconisée consiste à faire évoluer les solutions de sécurité (les agents génétiques et les solutions de la Vie Artificielle) au même titre que le changement périodique de brosse à dents.

Cette solution essaie de combiner plusieurs techniques et approches d'IDS, tout en respectant les spécificités des environnements mobiles sans fil. Mais elle admet des manques et faiblesses, qui peuvent être fortement améliorés par l'ajout d'un module comportemental.

Notre présent travail porte essentiellement sur la mise en oeuvre du module comportemental qui représente pour les terminaux mobile un module crucial, car ces derniers sont sensé avoir des propriétaires uniques chose qui représente une source importante d'information. Ce module s'intéresse principalement au facteur humain, qui représente un des plus important maillon de la chaîne de sécurité. Il essai de déceler un comportement suspecte en vue de la détection d'attaques récentes et non préalablement recensées. Ainsi qu'il tente de remédier aux problèmes liés aux vols de terminaux et à l'usurpation d'identité. Ce module interagit avec tous les autres modules de l'EIDS, pour la collecte d'informations, et pour la réaction contre des attaques.

La conception et la réalisation de ce module seront détaillées dans le chapitre suivant.

Chapitre IV:

Le Module Comportemental de l'EIDS

-La Solution-

Le Module Comportemental de l'EIDS
- La Solution -

I. Introduction.

Malgré que l'EIDS a été conçu pour protéger les terminaux mobiles contre divers scénarios d'attaques et vulnérabilités. On a constaté que beaucoup d'informations ne sont pas exploitées. Aussi la réaction de l'EIDS se dégrade à l'apparition de nouvelles attaques.

Cela nous a motivé à renforcer notre EIDS, par l'ajout et la mise en œuvre du module comportemental. Ce module qui va représenter une nouvelle couche de sécurité, et qui va renforcer la réaction de l'EIDS.

C'est l'apport de ce travail, en proposant un modèle d'action du module comportemental, afin d'exploiter au mieux les informations émanant des différents modules de l'EIDS (logs, rapport, traces,…).

En s'intéressera au noyau de notre solution qui est le module comportemental, en décrivant notre approche et notre apport pour la réalisation de ce dernier.

II. Le Module Comportemental de l'EIDS.

II.1. Introduction

Dans l'architecture Multi Modulaire de l'EIDS décrite précédemment ; le module comportemental représente le cœur de l'EIDS du fait qu'il interagit avec tous les autres modules, soit pour la collecte d'information soit pour la réaction globale de l'EIDS.

Dans cette section nous allons décrire nos motivations pour l'intégration d'un tel module, ainsi que son importance; puis on discutera de son principe de travail, et l'approche qui a été adopté pour sa conception.

II.2. Motivations

« Pourquoi un module comportemental pour l'EIDS ? ».

En plus de tous les bénéfices dont jouissent les IDS comportementaux en ce qui concerne leur capacité potentielle à détecter des formes d'attaques non préalablement connues (non recensées); ils offrent aussi la possibilité de reconnaître un comportement anormal, que ce soit celui de l'utilisateur humain (légitime ou pas) ou celui d'un programme intrus qui attaque le système de la machine (virus, ver, trojan,…).

Dans notre cas, les clients mobiles sont à utilisation personnelle ; ils appartiennent à une seule personne qu'elle l'utilise de manière exclusive. Et du fait de leur petite dimension ils peuvent être facilement volé ou perdu. Le module comportemental trouve

toute sa valeur et sa raison d'être du fait qu'il peut facilement tracer le comportement de son utilisateur.

On essai par ce module de profiter du fait que l'usager du terminal mobile est unique (avantage de l'unicité du propriétaire).

II.3. La Solution – Modèle Statistique

Un module comportemental surveille le *comportement* de l'utilisateur du client mobile, en lui élaborant et en lui calculant un *profil*. Mais que ce qu'un comportement?

Le Comportement :

Le *Comportement* peut être décrit, dans notre cas, comme l'ensemble des actions ou activités et habitudes journalières qu'effectue un utilisateur; ces activités sont de nature divers; allant des horaires d'utilisation du terminal, aux applications utilisées, et leurs fréquences, au taux de mémoire consommé, des entrées sorties effectuées, des événements systèmes générés, des ports ouvert, des sites visités,…. Devant la grande diversité des ces données en remarque cependant un certain phénomène d'habitude qui caractérise la différence de comportement entre les hommes; bien que ce comportement n'est pas figé et n'est pas statique; chose qui impose d'avoir un mécanisme de recalcule et de suivi d'évolution du comportement.

Toutes ces données à caractère hétérogène représentent les données d'entrées à l'élaboration et au calcul du *profil* utilisateur

Le Profil :

C'est l'ensemble des valeurs et critères qui représente de manière unique une personne.

Un changement du Comportement d'un utilisateur est caractérisé par une variation du profil et de sa valeur.

Dans notre cas on a voulu profiter de tous ces paramètres et données de nature hétérogène, et donc il fallait trouver une manière de représentation et c'est la qu'intervient l'apport de l'approche choisie. Car parmi les approches demeure celle de l'*approche statistique*.

L'approche Statistique :

Vu qu'une approche statistique est connue pour être robuste, et d'aboutir rapidement à des implémentations afin de valider ces méthodes ; nous avons opté pour cette dernière.

Comme les terminaux mobiles (Pockets) sont personnels, le profil utilisateur est unique et représente un moyen efficace pour l'authentification du propriétaire; et donc une approche statistique s'avers fort intéressante. Car les valeurs statistiques bénéficierons d'une certaine période de stabilité qui donnera une image claire de l'utilisateur et de son profil.

Le module comportemental est implémenté de sorte qu'il calcule et constitue le profil du propriétaire par des informations de base collectées à l'installation de l'EIDS en collaboration avec tous les autres modules, et puis à fur et à mesure il récolte de nouvelles

données en auditant le système et l'utilisateur, pour gérer les variations normales du comportement; tout cela en faisant des calculs statistiques de manière périodique. Lors de ces calculs périodiques on pourra avoir la variation du profil courant par rapport au profil initial.

Notre schéma va associer à chaque critère ou événement une variable aléatoire:

$$\{X_1, X_2, \ldots \ldots, X_n\}$$

avec: X_i représentant une Norme Statistique (Moyenne, Variance…)

Ces variables représentent la moyenne des valeurs récoltées initialement pendant une période d'apprentissage puis mis à jour périodiquement avec le temps, sur différentes entités.

Exemple :

X1——————————► temps d'utilisation CPU.

X2——————————► temps de connexion à quelques ports spéciaux.

:

:

:

Xn——————————► applications utilisées.

Et donc périodiquement de nouvelles valeurs sont calculées pour avoir les nouvelles moyennes auxquelles sont comparées les variances statistiques des valeurs précédentes, pour vérifier si les nouvelles valeurs excédent les seuils des variances; si c'est le cas une alerte est émise au module d'*Accé_Initial* pour qu'il procède à l'authentification du présent utilisateur.

Mais le problème est que le profil est décrit par toutes ces information ou variables aléatoires hétérogènes. Il faudrait chercher un modèle statistique qui nous permettrai de prendre en considération en même temps toutes ces variables et pouvoir avoir un modèle calculable afin d'effectuer la comparaison des profils et leurs mise à jour.

On s'est inspiré des travaux [STO03a][STO03b][STO04]. Dans un autre contexte, ou les auteurs proposent des filtres emails en se basant sur une approche comportementale. Nous choisissons l'*histogramme* et les fonctions statistiques de calcul sur ces derniers.

On représente un profil par un histogramme, ou chaque colonne représente la fréquence calculée d'une certaine variable aléatoire à un instant donné.

Un *Profil* à l'instant t = Histogramme à l'instant t de toutes les variables. Et pour faire la comparaison avec d'autres profils à d'autres instant ou des profils d'autres utilisateurs il suffit d'appliquer les fonctions statistiques de comparaison d'histogrammes qui sont : les distances d'histogrammes.

Une *fonction de distance* est employée pour mesurer la dissimilitude d'histogramme. Pour chaque paire d'histogrammes, h_1, h_2, il y a une distance correspondante, $D(h_1, h_2)$, appelée distance entre h_1, h_2. La fonction de distance est *positive*, *symétrique* et vaut 0 pour

les histogrammes identiques. La dissimilitude est proportionnelle à la distance. Nous avons adapté certaines des fonctions de distance généralement connues: *intersection simplifiée d'histogramme* (L1-form), *distance euclidienne* (L2-form), *distance Quadratique* et *distance de Mahalanobis*. Ces mesures standard ont été modifiées pour être plus appropriées à l'analyse de comportement de l'utilisateur. Leurs formules sont :

L1-form: $D_1(h_1, h_2) = \sum_{i=0}^{n-1} |h_1[i] - h_2[i]|$

L2-form: $D_2(h_1, h_2) = \sum_{i=0}^{n-1} (h_1[i] - h_2[i])^2$

Quadratique: $D_3(h_1, h_2) = (h_1 - h_2)^t A(h_1 - h_2)$

Ou :

n : est nombre de colonnes de l'histogramme.

A : est la matrice ou a_{ij} dénotent la similarité entre la colonne i et la colonne j.

$a_{ij} = |i - j| + 1$

La distance *Mahalanobis* est un cas spécial de la distance quadratique ou A est donner par l'inverse de la matrice de covariance.

Mahalanoubis : $D_4(h_1, h) = (h_1 - h)^t A(h_1 - h)$

Avec : $A = B^{-1}, b_{ii} = Cov(h[i], h[i]) = Var(h[i]) = \sigma_i^2$

$$B = \begin{bmatrix} \sigma_0^2 & 0 & K & 0 \\ 0 & \sigma_1^2 & K & 0 \\ M & M & O & \\ 0 & K & 0 & \sigma_{n-1}^2 \end{bmatrix}$$

On aura donc : $D_4(h_1, h) = \sum_{i=0}^{n-1} \left((h_1[i] - h[i])^2 / \sigma_i^2 \right)$ avec h l'histogramme du profil de référence et h_1 le profil récent.

Aussi pour renforcer le niveau de représentation de notre profil; on définit ce dernier comme étant la composition de quatre histogrammes pour chaque période de la journée; et on a divisé la journée en quatre périodes qui sont le *Matin*, l'*Apres Midi*, le *Soir* et le *Nuit*, car généralement chacune de ces périodes est connue par un comportement globale spécifique (des habitudes); et cela représente un critère en plus qui renforcera le traçage de l'utilisateur. Exemple si un utilisateur à toujours l'habitude de travailler que la nuit, alors si on détecte des activités l'après midi cela est suspect.

Donc : *profil* = Histogramme = { Histogramme Matin,
Histogramme Apres Midi,
Histogramme Soir,
Histogramme Nuit }

Le module comportemental passe à son installation par une période d'apprentissage ; ou il récolte ses informations en interagissant avec tous les autres modules (*Controleur_intégrité, Accé_initial, Accé_fichiers, Surveillance_ports*, …). Le but étant la constitution des histogrammes des profils de référence. A la mise en place du module comportemental, une période d'apprentissage sert à la constitution du profil de reference du propriétaire. Apres une certaine période d'apprentissage déterminée de manière empirique, ce module commence à agir en temps réel. Il recalcule des nouveaux profils instantanées, et les compare au profils de référence, en utilisant les quatre fonctions de distances. Comme le comportement des utilisateurs à travers leurs profiles n'est pas statique, périodiquement une procédure de mise à jour du profil est appliqué en recalculant un nouveau histogramme résultant de la combinaison de l'histogramme de référence avec un histogramme temporaire d'une certaine période récente (moyen des deux histogrammes).

III. Conclusion.

Ce travail est une petite contribution qui vise à protéger au mieux les terminaux mobiles sans fil ; et cela en renforçant l'EIDS, par l'aspect comportemental.

Par ce travail on a voulu explorer le domaine des approches comportementales; on a voulu en profiter au maximum du fait que ces terminaux soient à utilisation personnelle, pour les protéger contre les divers problèmes qui les menace.

Cette proposition n'est en aucun lieu la solution idéale qui assure le degré de sécurité 100%, mais elle représente une tentative de renforcement.

Néanmoins il faut préciser que l'approche proposée pour la conception du module comportemental est générique, et ne ce limite pas qu'aux terminaux mobiles. Elle peut être appliqué à la sécurisation d'un réseau d'entreprise.

Chapitre V:

Tests

&

Résultats

Tests & Résultats

Afin de valider notre apport concernant le modèle du module comportemental, nous avons effectué des tests; que nous allons décrire ainsi que leurs analyses.

I. Logique des tests

Afin de valider notre apport il fallait effectuer des tests, on ne dispose pas d'un modèle prédéfini de test; c'est pourquoi on a réfléchi sur les batteries de tests suivants.

Nos tests se divisent en deux classes selon nos besoins ; car on veut d'abord par ces tests prouver que notre profil de référence (l'histogramme de référence) tel calculé représente bien notre utilisateur; et qu'il est, une fois calculé, uniforme et cohérent aux activités, habitudes et événements de notre utilisateur. C'est pour cela qu'au départ nos tests prouveront ce critère. Et en second lieu on va tester la puissance de détection par une autre logique de tests.

A noter que les tests se sont déroulés au sein des laboratoires du Centre de Recherche en Information scientifique et Technique (CERIST).

Dans le premier scénario de test, on prend un échantillon de vingt personnes qui utilisent leurs PC de manière exclusive et on étudiera l'homogénéité de notre profil, en calculant pour chaque utilisateur son profil de référence puis on prendra plusieurs périodes ou on va calculer des profils temporaires et on comparera ces derniers avec le profil de référence de chaque utilisateur et on verra le comportement des résultats des distances (qui doit être homogène et non alarmant).

Dans le second scénario on va essayer d'étudier le comportement de notre IDS vis-à-vis d'attaque par changement d'utilisateur et cela en permutant les utilisateurs sur les PC. Et on calculera à nouveau les profils temporaires où un utilisateur non légitime utilise le PC d'un autre et on calcule les distances et en regarde le comportement de ces distances.

En même temps ces tests ont révélé être un moyen pour aider à décider du niveau d'une alerte d'intrusion et cela dans la détermination des seuil d'alertes.

Pour effectuer ces tests on a prélevé une vingtaine de fichiers Logs (en exploitant les fonctionnalités d'audit offertes par le système) de différents utilisateurs tel que chaque utilisateur utilise son PC de manière exclusive; et pour chaque utilisateur on extrait de son fichier log le profil référentiel selon les quatre périodes (Matin, Après Midi, Soir, Nuit), et on extrait aussi les différents profils temporaires pour la comparaison.

Outre que prouver la méthode, ces tests vont nous aider à répondre aux questions:

- *Les histogrammes reflètent t'ils exactement le comportement d'un utilisateur* ?

- *Quels sont les meilleurs seuils pour la détection (minimiser les faux positifs)* ?

- *Quelle est la meilleure distance de calcul* ?

- *Quels sont les paramètres influant dans l'analyse (la période d'apprentissage, la stabilité du profil…)* ?

Pour effectuer ces tests nous avons mis en œuvre le module comportemental en utilisant l'environnement MicroSoft Visual Studio .Net et MicroSoft SQL Server 2000. Ce module Implémente le modèle statistique choisi et nous a permis par la suite d'effectuer nos tests de validation

II. Représentation du profil en histogramme

Le profil est représenté dans notre système par un ensemble d'histogrammes, et est issu des différents fichiers log de l'observateur d'événement (*Application*, *Système*). Chaque histogramme représente les fréquences des événements issus d'un fichier log (*Application*, *Système*) et lors d'une période donnée (*Matin*, *Après Midi*, *Soir, Nuit*).

Voici un exemple d'histogramme représentant un profil référentiel tel affiché par notre application :

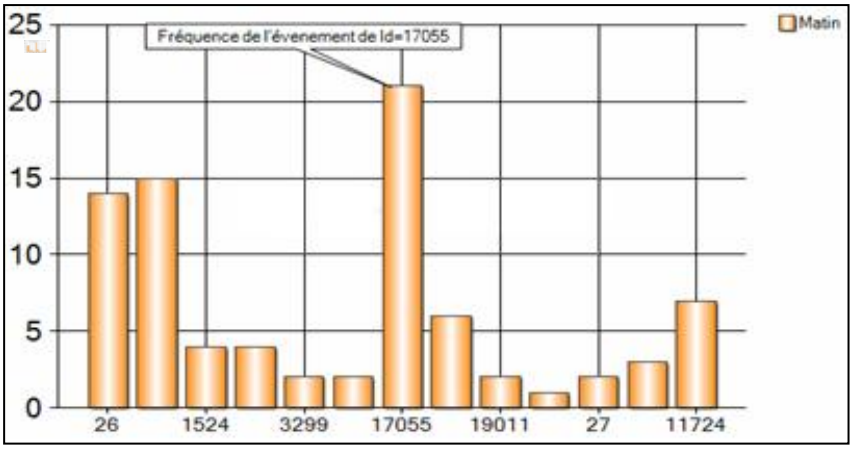


Figure IV.1 : *Profil référentiel Source «Application» et période «Matin»*

Cet histogramme a comme coordonnées (*x,y*) pour (les ID Event, fréquences d'occurrences). Les identificateurs représentent des numéros d'événements Système, tel défini par MicroSoft Windows.

III. La période d'apprentissage

Les profils référentiels utilisés sont établis en exploitant des fichiers texte exportés à partir de l'observateur d'évènements (Fichiers logs du Système d'Exploitation). En interagissant avec le mécanisme d'audit du système d'exploitation on gagne en précision. Dans ce cas la période d'apprentissage de chaque profil est déterminée à partir du ficher log, et est représentée par la durée entre la date minimale et la date maximale apparentes dans ce fichier.

Dans notre cas on prend :

User1 : 1mois (moyenne)

User2 : 4 mois (longe)

User3 : 1 semaine (courte)

User4 : 3 mois (longe)

User5 : 2 mois (moyenne)

User6 : 2 mois (moyenne)

User7 : 1 mois (moyenne)

Différentes périodes ont été choisit et cela afin de voir la réaction de notre module comportemental face à différentes périodes d'apprentissage. Nous avons choisi une période d'apprentissage longue (user 2, 4), moyenne (user 1, 5, 6, 7), et courte (user 3) ; afin de mieux étudier le comportement de notre module vis-à-vis du choix des périodes d'apprentissages.

IV. Scénario des Tests

Pour chaque utilisateur on a effectué 10 tests de façon à ce que le profil référentiel représente tout le contenu du fichier log mais pour une période précise (Matin, Après Midi, Soir, Nuit); de ce fait le profil référentiel est divisé en quatre profils. Le profil temporaire quant à lui n'est que les évènements d'une journée de ce fichier pour une période spécifique par exemple «Matin».

Dans chaque test, on compare un profil temporaire et un profil référentiel suivant la période et la source du fichier log (*Application*, *Système*) pour un même utilisateur. Tous ces tests sont effectués pour chaque distance.

Prenant par exemple le profil référentiel pour la période *«Matin»*, et la source *«Application»*, de l'utilisateur «*User1»* sous forme d'histogramme :

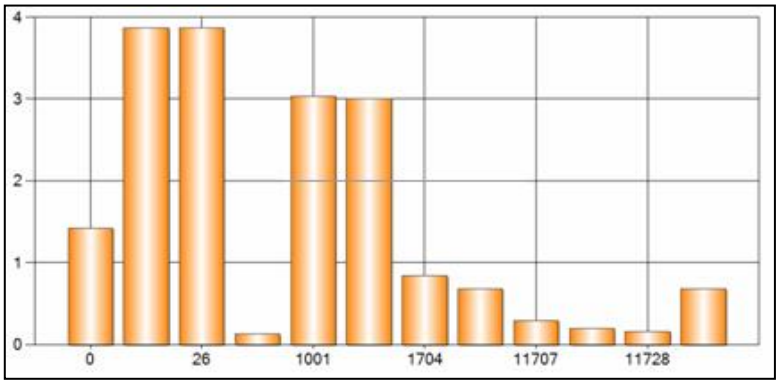


Figure IV.2 : *Histogramme du profil référentiel du User1 période Matin et source Application*

Ce dernier est comparé au profil temporaire du ***User1*** qui est le suivant :

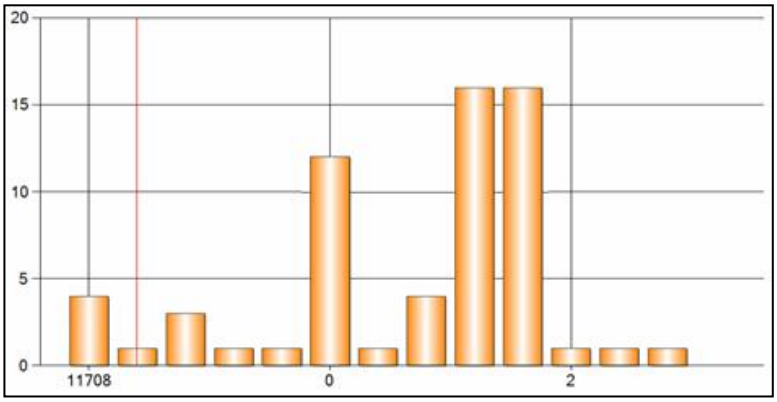


Figure IV.3 : *Histogramme d'un profil temporaire du User1 période Matin et source Application*

En comparant ces deux histogrammes, on trouve pour les distances *«Euclidienne Forme L1»* et *«Euclidienne Forme L2»* respectivement les valeurs **58,6102** et **468,35**.

Dans ce qui suit, on va exposer tous les tests réalisés dans des tableaux pour les distances *Euclidienne Forme1* et *Forme L2*, et la *Quadratique*. Et à la fin on donnera l'analyse de ces tests et ce qu'on a pu tirer comme résultats concernant le seuil d'alerte, les paramètres influant sur l'analyse, la meilleure distance de calcul…etc.

Tableau 1 : Test de la distance Euclidienne Forme L1 sur des profils propres aux utilisateurs

		Test1				Test2				Test3				Test4				Test5				Test6			
		matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit
User1	App	18	17	13.7	1.38	26	5	7.72	1.38	18,9	9	2.72	3.38	18	18	1.27	1.38	20	6 .99	1.27	6.61	16	1.99	1.27	2.61
	Sys	21.5	1.35	14.2	3.3	31.4	33.6	11.7	7.76	16.4	22.3	2.72	15.6	45.5	15.3	2.27	4.66	16.4	10.3	3.72	18.3	19.4	16.3	40.2	
User2	App	16.4	17.8			16.3	17.8			4.36	14.1			8.64	23.6			20.3	7.63			3.36	15.2		
	Sys	92.1	2.90			89.1	6.09			89.2				93.1	3.90			97.1	0.09			92.1	0.90		
User3	App	32.6	7.33	15.4	24.3	32.3	26.3	12.5	3.66	10.6	16.3	25.1	16.3	11.3	26.5	7.42	3.66	16.3	27.6	28.6	31.6	16.3	13.3	40.1	
	Sys	24.6	45.1	59.2	55.2	44.6	43.2	66.7	43.2	44.6	36.7	28.1	33.9	39.6	38.9	29	55	44.6	43.4	66.1	31.2	24 .3	27.4	20.5	
User4	App	1.93	2.48			2.93	2.48			10.2	2.48			0.61	3.37			1.93	10.7			1.61	2.48		
	Sys	4.53	11.7			5.82	9.72			4.53	29.0			3.33	11.7			5.64	14.9			4.33	11.9		
User5	App	10	12.3	7.24	3	9.00	12.3	6.91	3.66	17.6	12.8	5.92	9.44	9.00	12.3	4.58	3.11	9.00	11.3	4.08	8.99	16.5	27.5	4.08	3.01
	Sys	9.34	19.9	7.37	2.75	3.65	17.9	6.35	3.25	7.65	18.9	3	2.75	10.9	20.9	2.5		11.5	18.9	3.62		20.2	21.5	6.62	
User6	App	13.7	68.6	16.5		22.1	11.3	3		4.15	11.1			14.3	10.2			4.15	5.75			13.1	11.2		
	Sys	13.6	68.8			13.6	20.6			8.5	23.6			8	28.6			15.6	11.6			6.12	35.6		
User7	App	6.6	13.1	7.64	0.15	7.5	8.39	5.00	0.15	9.19	11.1	1.7	0.15	8.99	43.8	1.7	1.84	9.99	30.9	1.7	0.15	4.6	8.1	7.64	
	Sys	43.7	42.5	65.0	3.66	38.3	37.5	83.2	0.66	19.6	48.7	30.5		36.0	49.1	29.4	5.33	48	53.3	22.4	1.35	52.0	42.3	25.4	1.33

		Test7				Test8				Test9				Test10			
		matin	Après midi	Soir	Nuit	matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit
User1	Application	18	6.99	2.72	2.61	21	1.99	2.27	1.38	11.00	2.98	2.72	1.38	22	5	7.72	1.38
	Système	54.49	31.64	2.72	2.36	17.5	52.24	13.72		2.5	12.35	11.27		13.45	1.35	5.27	
User2	Application	23.63	0.80			9.63	12.19			8.63	16.81			5.63	11.19		
	Système	94 .01	2.90			93.01	2.90			81.11	1.901			90.01	1.907		
User3	Application																
	Système																
User4	Application	0.61	3.48			6.61	9.15			8.61	2.48			5.61	2.48		
	Système	13.61	13.19			3.64	11.33			6.92	9.69			15.35	8.58		
User5	Application	25.3	25.82	4.91		10.6	20.37	7.27		10.001	12.82	8.41		22.35	22.24	4.08	
	Système	7.15	18.93	2.75		13.7	23.93	2.5		5.03	26.93	5.625		6.46	34.93	3.5	
User6	Application	4.84	10.5			13.15	9.5			6.84	7.25			4.84	7.875		
	Système	4.5	47			13.62	51 .31			16.12	52.34			15.5	54.8		
User7	Application	9.8	8.1	23.35	0.15	8.1	7.10	1.70	0.15	6.9	14.10	3.70		6.8	16.49	1.70	
	Système	46.15	79.2	30.49	3.66	20.30	48.64	38.7		70.1	51.2	34.50		51.6	51.02	57.06	

Tableau 1 : Test de la distance Euclidienne Forme L1 sur des profils propres aux utilisateurs (suite).

		Test1				Test2				Test3				Test4				Test5				Test6			
		Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit
User1	App	67.4	68.8	17.6	0.48	35.1	60.4	14.2	3.71	36.9	64.7	2.83	0.48	35.2	4 .01	2.83	10.9	36.1	5.54	0.16	1.71	33 .8	14.5	0.61	1.71
	Sys	399	173	180	99.2	402	181	245	84.7	341	133	158	130	714	144	208	167	971	132	158	336	420	29.4	172	90.9
User2	App	9.71	15.2	57.3	0.01	546	60.5	0.17	0.01	24.8	345	0.01	0.19	35.3	137	0.01	0.19	24.8	58.7	0.01	0.19	37.2	59.7	0.01	0.01
	Sys	617	2.28	1.85	1.45	750	3.74	0.92	1.11	771	6.15	1.85	1.45	846	33.5	9.57	2.6	808	10.4	1.85	0.45	755	3.35	0.96	1.45
User3	App	427	50.9	46.9	112	238	1028	94.3	705	38	197	540	145	78.3	704	42.3	13.4	79.6	4.33	453	321				
	Sys	241	350	539	2279	4442	395	3018	2259	65.5	705	537	3615	230	220	530	3615	272	328	233	2510				
User4	App	15.7	13			9.15	18.5			9.15	18.5			9.15	40.1			9.15	13			9.15	13.9		
	Sys	1.25	19.2			1.25	15.8			2.46	11.5			5.38	10.9			3.05	101			2.33	11.3		
User5	App	52.3	20.8	15.3		19.5	12.3	14.9		463	11.3	4.14		60.2	12.4	4.41		164	20.8	15.3		51.2	58.2	17.8	
	Sys	7.46	16.7	0.66		1.83	17.9	1.16		8.40	6.07	0.66		4.33	15.2	4.53		70	14.9	4.53		2.40	10.6	0.66	
User6	App	11.9	20.5			3.09	22.4			24.5	21.1			2.4	20			47.2	5.17			23.8	21.1		
	Sys	23.2	843			8.24	768			8.11	850			29.7	772			5.86	861			2.86	716		
User7	App	7	8.20	0.39		6.7	8.5	91.3		6.9	8.5	0.39		7.6	114	32.8		21.3	5.20	0.39		10.3	4.20	0.39	
	Sys	453	201	1065		474	757	1003		104	255	265		183	442	220		368	331	107		484	330	134	

Tableau 2 : Test de la distance Euclidienne Forme L2 sur des profils propres aux utilisateurs.

		Test7				Test8				Test9				Test10			
		Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit
User1	App	35.2	4.00	0.61	0.48	43 .1	2.99	0.16	0.48	79.7	4.00	0.16	0.48	50 .2	2.55	2.83	0.48
	Sys	779	113.4	73.5	1031	670	29.4	1061	2034	612	477	172	1023	288	1211	1123	150
User2	App	37.2	45.9	0.017	0.017	37.3	75.8	0.17	0.017	8.81	23.4	0.17	0.74	6.2	50.5	0.017	0.017
	Sys	784	2.28	0.96	1.11	791	4.09	8.77	1.28	858	1.81	0.92	1.28	791	2.78	1.85	1.11
User3	App																
	Sys																
User4	App	0.15	13.06			9.15	13.02			9.15	13.06			14.52	13.06		
	Sys	1.95	17.7			2.46	11.4			4.64	11.8			0.87	17.6		
User5	App	53.7	65.06	4.61		64.83	12.32	4.14		20.11	12.60	14.9		19.51	12.33	15.31	
	Sys	8.46	7.54	2.16		6.58	10.25	2.78		14.08	5.72	1.78		31.21	7.07	8.91	
User6	App	2.40	20.4			34.9	9.79			27.7	20.4			3.05	8.17		
	Sys	8.74	689			38.46	81299			24.7	751			5.11	27846		
User7	App	8.5	19.10	13.5		9.9	32	0.39		6.7	35.5	32.8		3.10	21.3	0.39	
	Sys	395	314	247		99.05	353	549		826	393	517		531	236	523	

Tableau 2 : Test de la distance Euclidienne Forme L2 sur des profils propres aux utilisateurs (suite).

		Test1				Test2				Test3				Test4			
		Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit
User1	App	39	35.27			87.7	23.72			79.7	81.45			50 .2	28.72		
	Sys	42.78	128.1			57.21	54.82			57.35	54.67			139.5	57.55		
User2	App	95.63	31.19			33.39	86.37			36.51	29.87			40.51	31.41		
	Sys	127.88	59.03			147.8	77.5			124.9	39.77			109.1	88.43		
User3	App	55.66	88.99	56.42	65.33	104	65.99	51.42	62.33	52.66	117.6	74.42	67.32	71.33	60.66	57.57	65.33
	Sys	173.3	57.13	51.45	62.33	61.14	46.99	58.45	80.21	43.74	72.99	35	64.2	51.71	48.66	62.03	36.55
User4	App	16.93	131.4	-	-	78.4	38.15	-	-	38.9	66.15	-	-	130.3	13.37	-	-
	Sys	23.53	11.55			9.71	108.9			16.84	12.99			105.4	24.97		
User5	App	32.16	34.96	26.25		33.16	25.45	9.08		31.51	26.31	10.91		30.16	30.93	13.03	
	Sys	21.71	38.7	43.3		160.3	34.41	61.2		47.03	87.48	13.03		42.71	53.71	22.32	
User6	App	47.30	60.68	63.77		36.07	58.68	68.91		163	55.43	42.13		53.30	18.62	45.62	
	Sys	39.07	89.43	34.5		55.87	80.43	58		43.57	207.8	43.5		328	76.68	41	
User7	App	37.27	26.3	42		18.99	30.2	15.52		27.19	43.8	131		20 .29	18.7	47	
	Sys	60.53	86.35	116.7		61.15	95..78	63.2		76.15	62.5	55.81		68.84	57.5	56.42	

Tableau 3 : Test de la distance Euclidienne Forme L1 sur des profils temporaire non propres aux utilisateurs légitimes.

		Test1				Test2				Test3				Test4			
		Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit	Matin	Après midi	Soir	Nuit
User1	App	85.8	548.7			86.8	256			96.03	99			124.8	71.24		
	Sys	418.8	651.3			708.4				548	1035			1240	2030		
User2	App	412.3	139.8			464.7	146.2			465.1	199.1			397	201.1		
	Sys	1555	830			13561	740			1574	955			833.9	733.1		
User3	App	482.66	1158	516.4	521.1	1134	865.7	74.42	1502	469.6	1523	768.2	1548	907.3	60.66	518.5	1533
	Sys	21957	429.1	693	1501	960.3	371.9	780.3	1956	294.6	1071	552.	1574	359.8	371	1503	571.3
User4	App	41.78	3734	-	-	1315	241.5	-	-	243.7	907.2	-	-	3733	220.7	-	-
	Sys	94.4	14.72			7.55	3086			29	22.81			3079	92.45		
User5	App	121.96	129.5	368.5		156.9	208.8	29.14		86.02	237.8	52.97		119.9	372.5	70.03	
	Sys	70.9	739.2	502.1		1351	179.9	634.5		471.4	1280	47.57		413.6	362.3	89.39	
User6	App	319.24	454.3	341.2		268.6	433.2	587.8		12903	238.2	213.3		1286	57.33	187.9	
	Sys	118.5	1888	738.2		555.9	1598	1325		754.7	13720	1305		1032	882.4	752.2	
User7	App	288.8	89.7	213.5		55.50	118.8	54.21		103.3	256	1524		62	2108	227	
	Sys	589.1	540.8	2534		599.4	1727	781.8		647.9	450	479.7		709.1	425	369.3	

Tableau 4 : Test de la distance Euclidienne Forme L2 sur des profils temporaire non propres aux utilisateurs légitimes.

		Test1		Test2		Test3		Test4		Test5		Test6	
		Matin	Après midi	Matin	Après midi	Matin	Après midi	Matin	Après midi	Matin	Après midi	Matin	Après midi
User1	App	586.25	0.56	34.05	59.92	1548.5	16227.9	875.07	33.04	856.04	34.61	1600.04	546.5
	Sys	45361.32	21838.9	11614.5	7419.99	33272.03	304.78	1565.68	270.21	5585.92	3499.4	73791.76	15877.18
User2	App	232.08	1919.13	327.03	323.65	232.08	486.76	87.47	785.33	295.46	221.17	63.14	1104.32
	Sys	45257.69	170.93	37217	11.20	54523 .97	27.25	55168.72	197.20	52149.22	51.37	51217.85	5243.14
User3	App	866.11	3280.72	750.94	717.53	2.61	51424.48	204.35	3280.72	5689.70	20.42	4825.42	25074.48
	Sys	889.37	13689.83	1242.08	172610.33	775675.05	184287,09	6218.35	5512.41	194620.76	6218.35	33524.13	3768,82
User4	App	0.085	9.37	5.61	9.11	6.61	8.22	0.61	8.86	1213.5	11.44	213.32	213.43
	Sys	5.97	234.83	441.43	51.13	5.19	167.01	44.64	76.86	6.42	120.97	6.79	1670.01
User5	App	557.91	950.92	175.99	780.12	198.98	212.81	620.51	111.60	588.1	22.78	710.07	114.16
	Sys	0.84	161.46	39.95	161.86	119.02	486.72	37.06	1287.91	10149.47	12098.6	1347.46	239.05
User6	App	157.14	39.68	3.77	343.09	265.08	49.32	92.88	39.56	37.95	179.92	60.76	24288.73
	Sys	259.72	27520.09	161.46	1881.23	218.65	19711.87	275.34	14628.89	102.54	12321.37	125.01	1187.86
User7	App	23.03	48.82	35.92	387.63	19.15	72.61	65.45	179.47	45.22	2768.98	4430.37	164.65
	Sys	6195.56	2770.86	8666.69	10773.78	1447.52	21620.06	2430.4	1786.74	12281.96	9332.62	22416.21	420.94

Tableau 5 : Test de la distance quadratique sur des profils propres aux utilisateurs.

		Test1		Test2		Test3		Test4		Test5		Test6	
		Matin	Après midi	Matin	Après midi	Matin	Après midi	Matin	Après midi	Matin	Après midi	Matin	Après midi
User1	App	287.9	15807 ,7	192 ,33	2205.23	7889.03	548.43	211.98	5321.67	26.64	342.74	7540.9	12432.98
	Sys	2128.86	11983 ,32	1687.14	865.87	12660.88	32834.04	4385.85	1254.71	1265.98	12764.39	1273.43	5321,12
User2	App	341.21	2103.67	3243.23	623. 35	8232.01	330.54	921.85	98.33	1085.43	2024.32	164.28	154.22
	Sys	569.75	286 .87	4814,34	78211.20	69523.23	1643.92	3162.48	56.33	2186.43	9375.38	3298.03	21984.75
User3	App	18.43	4267.48	243.56	2134.76	3212.64	63875.98	4383.53	6873.43	154.76	978.66	321.87	2109.65
	Sys	395.82	12874.76	2476.20	2344.92	55875.32	1798.04	24869.76	923.08	33120.25	432.66	5398.84	453.98
User4	App	39.57	125.43	910.65	96.81	36.70	125.42	68.75	76.54	45.23	2.87	2.39	41.36
	Sys	11.68	0.44	32.32	167.01	11.68	58.20	59.81	15366.87	14.38	795.87	1238.36	205.93
User5	App	213.44	132.36	1354.98	87.88	2187.29	102.54	2437.64	184.73	521.95	661.38	183.72	21984.9
	Sys	32125.43	321.54	145.63	2739.68	1409.81	362.09	677.42	114.75	9.76	43213.7	9863.8	142.54
User6	App	175.41	209.85	98.07	343.09	175.41	499.56	746.22	238.57	166.49	324.56	77.03	23.54
	Sys	10.99	2994.82	9.24	27294.08	4.31	32.25.58	76.97	2642.76	44.47	21537.54	664.70	17013.30
User7	App	751.71	139.23	147.30	965.27	790.20	66.17	49.10	965.23	50.10	771.07	452.40	2139.03
	Sys	1131.29	13449,36	81.75	17010,70	896.46	15782,16	1294.11	16563,08	904.32	321,28	1294.15	31878,12

Tableau 6 : Test de la distance quadratique sur des profils temporaire non propres aux utilisateurs légitimes.

V. Analyse des tests

Avant de commencer à commenter les tests qu'on a effectués, il faut d'abord préciser que l'échantillon des utilisateurs que nous avons pris travaillent dans une entreprise (CERIST) où la charge du travail (volume horaire des utilisateurs) est principalement dans la période «*Matinale*» et «Après Midi».

V.1 Les tests de la distance euclidienne Forme L1

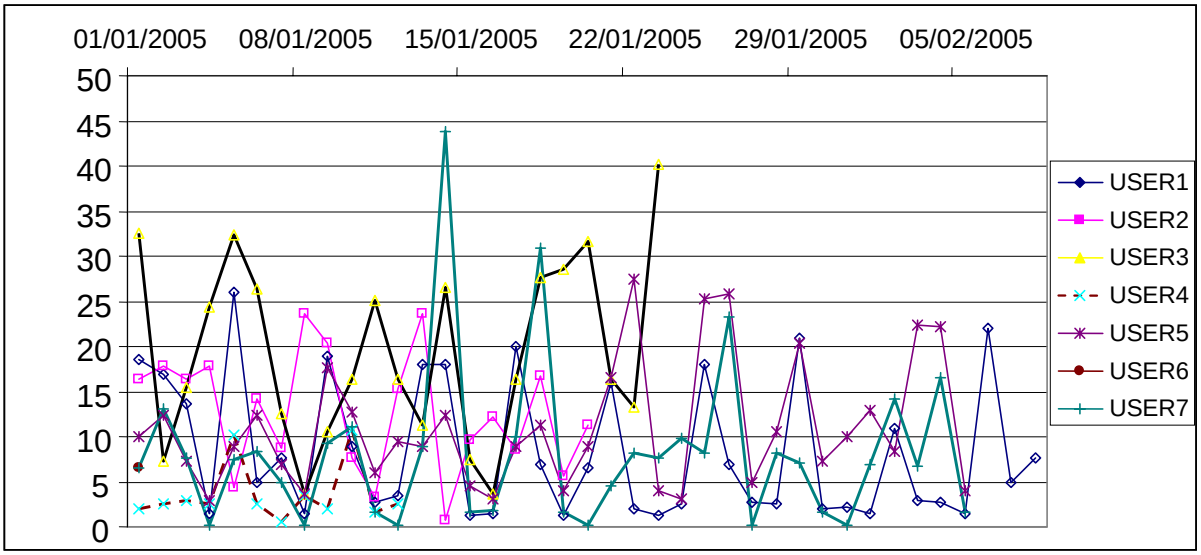


Figure IV.4 : *Résultat des différentes analyses de la Forme L1 de tous les utilisateurs pour la source Application.*

Pour la distance *Euclidienne formeL1* (tableau 1), on remarque que la majorité des résultats d'analyse des utilisateurs sont homogènes (Figure IV.4), en d'autre terme ces résultats sont à peu prés dans la même plage de valeurs entre 0 et 30, et à cause de la longueur de la période d'apprentissage on trouve des résultats supérieurs à 30 pour les utilisateurs: *User7* (4 mois), *User3* (une semaine).

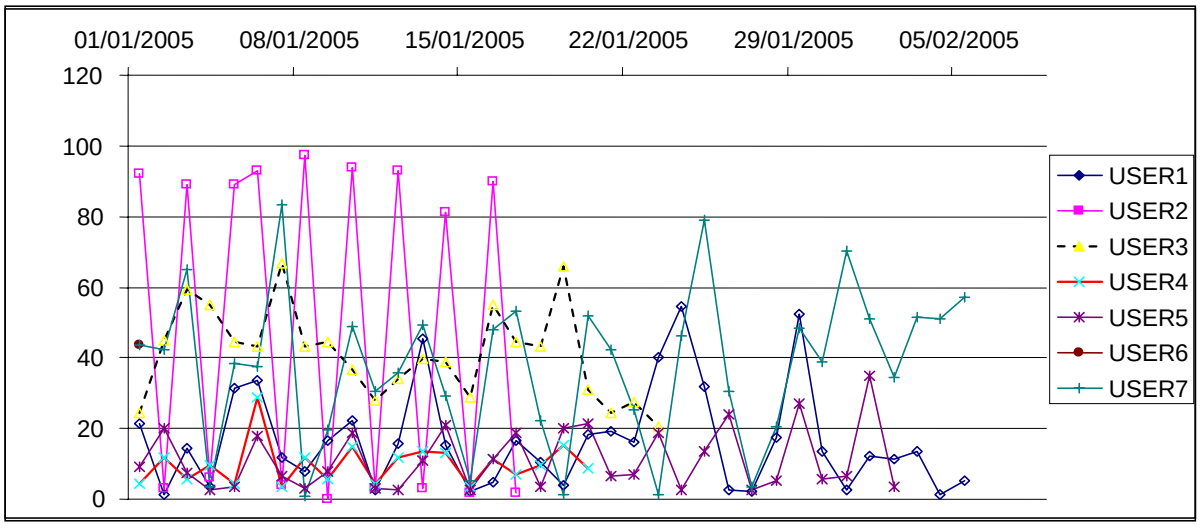


Figure IV.5 : *Résultat des tests de la distance Forme L1 sur la source Système*

La figure IV.5 représente les résultats de la source Système (distance euclidienne Forme L1) du tableau 1, comme on a déjà expliqué, ces résultats sont issus d'une analyse sur le

comportement des utilisateurs légitimes, et ceci pour observer la variance de ces résultats (intervalle ou bornes des résultats) dans le but de définir un seuil pour cette distance.

Dans cette figure les résultats varient entre 0 et 97.1, on peut même filtrer ces résultats puisque les utilisateurs : *User1*, *User3*, *User4*, *User5*, *User6*, varient avec des valeurs proches et inférieurs à 60, alors que *User7* et *User2* ont des valeurs très grandes (à cause de l'instabilité de leur profil).

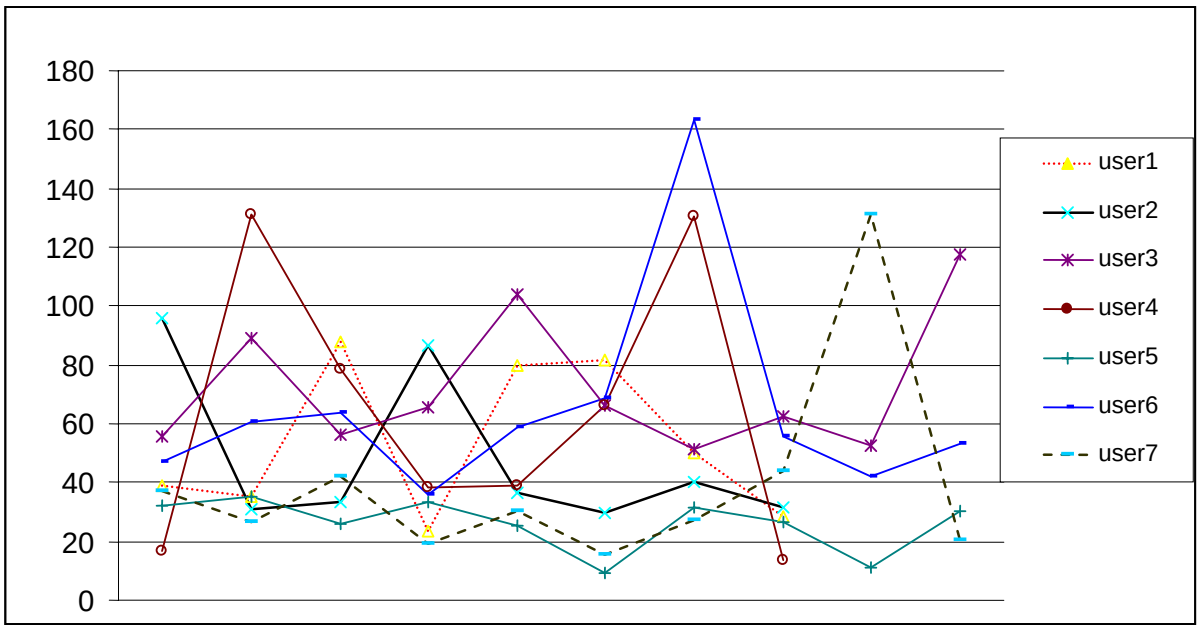


Figure IV.6 : *Graphe des résultats pour la détection des comportements anormaux (Application – Matin)*

La Figure IV.6 résume les résultats de la fonction euclidienne Forme L1 pour la source *Application* du tableau 3, ces résultats sont considérés comme des intrusions car ils sont issus d'une comparaison entre le profil référentiel d'un utilisateur avec des profils temporaires d'autres utilisateurs.

On ne peut comparer les résultats de l'analyse du comportement normal (Figure IV.4) avec les résultats de l'analyse des comportements sensés être des cas d'intrusions (Figure IV.6), et cela pour la simple raison que toutes les périodes (Matin, Après Midi, Soir, Nuit) sont inclus dans ces résultats, en d'autre terme le seuil de la période matin ne peut être pris comme seuil pour les autre périodes et vis versa (par exemple le profil matin n'est pas nécessairement le même que celui de l'après midi).

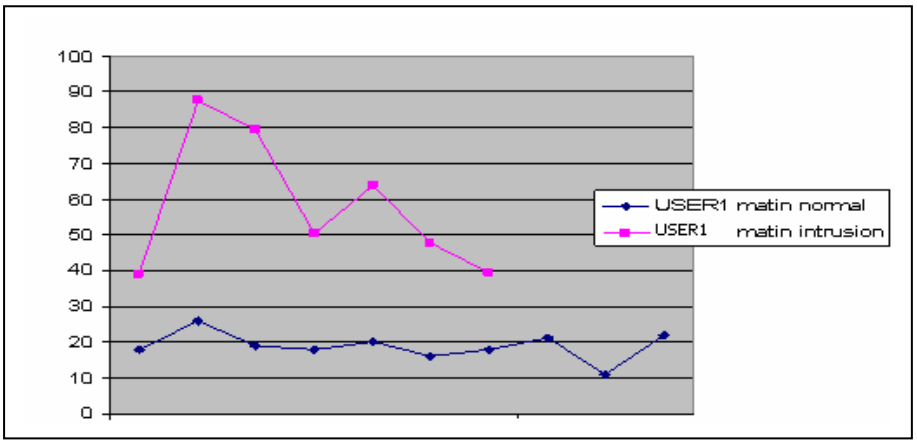


Figure IV.7 : *Graphe de comparaison des résultats d'un comportement normal de User1 avec des résultats d'intrusions sur User1 (Matin - Application).*

Dans la Figure IV.7 on peut voir deux graphes de l'utilisateur *User1* (Application - Matin), tous les deux sont des résultats de la Forme L1, mais l'un issu d'une analyse du profil temporaire du *User1* (c'est *User1* qui a exploité la machine), et l'autre d'un comportement anormal (c'est un autre utilisateur qui a exploité la session de *User1*); en analysant ces résultats on voit que le comportement anormal génère des résultats très grands par rapport aux résultats de l'analyse de *User1*. Un seuil de détection serait entre la valeur maximal du comportement normal et la valeur minimal du comportement anormal.

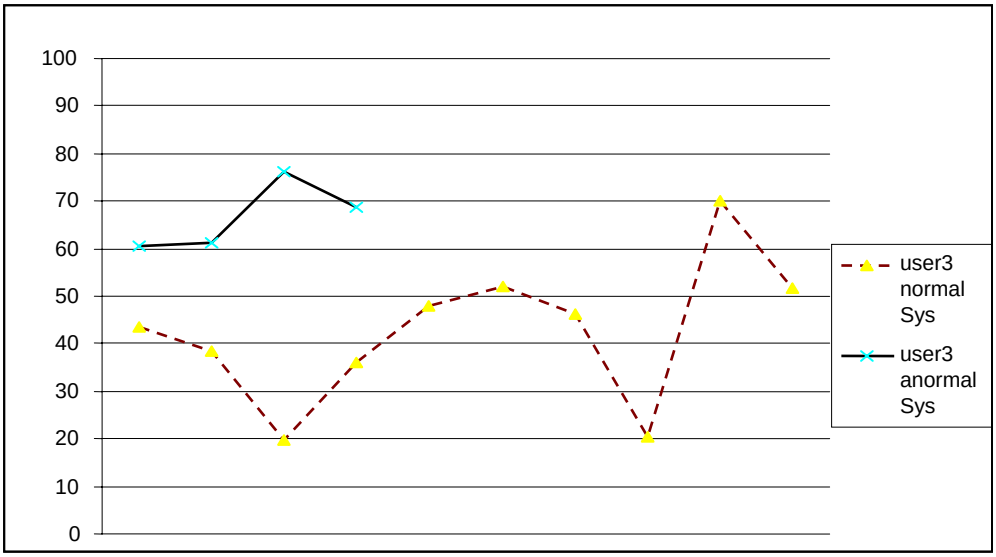


Figure IV.8 : *Graphe de comparaison des résultats de la distance Euclidienne Forme L1 entre User3 normal User3 anormal (Matin - Système).*

On remarque dans la Figure IV.8 que seul la valeur maximal 70,1 du profil Système Matin de *User3* se trouve dans la même plage de valeurs que le comportement anormal, si on prend cette valeur comme seuil, trois valeurs des résultats anormaux seront considérés comme normaux; un meilleur choix du seuil serait probablement de pendre une valeur inférieure à 70,1. Dans ce cas les résultats anormaux seront considérés comme intrusion.

V.2 La distance Euclidienne Forme L2

Pour cette distance on est arrivé aux mêmes remarques que la première distance.

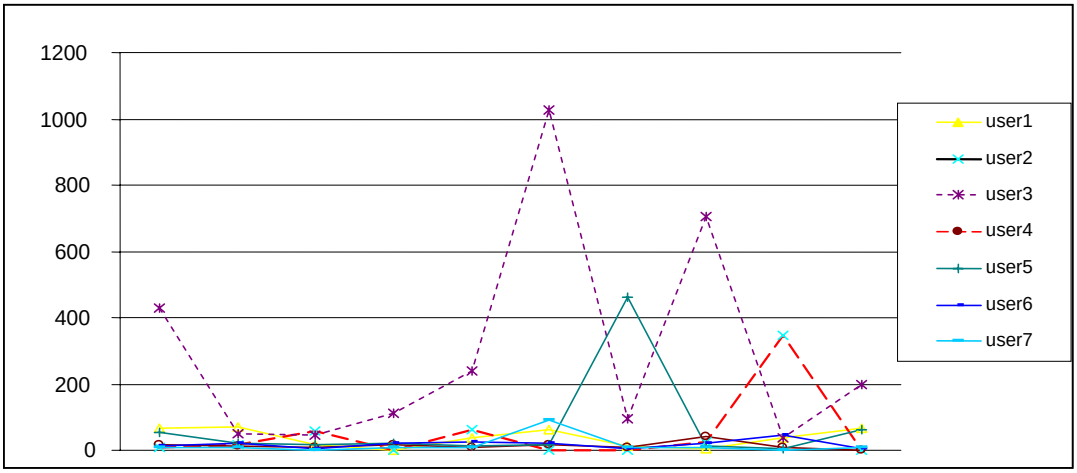


Figure IV.9 : *Graphes des différents tests effectués sur les utilisateurs (Application Matin) avec le Distance L2.*

Dans la Figure IV.9 on remarque que la majorité des profils varient sur la même plage de valeurs (inférieur à 61), et trois utilisateurs (*User2*, *User3*, *User5*) ont des résultats énormes, on peut expliquer cela par la longueur de leurs périodes d'apprentissage qui est très importante 2mois, 4mois et 4 mois respectivement.

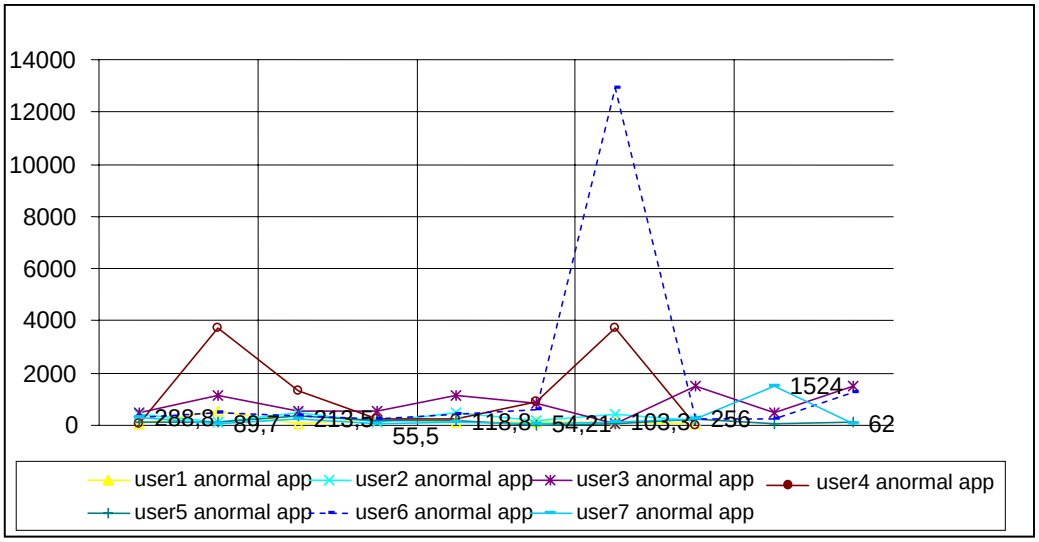


Figure IV.10 : *Résultats pour la détection des comportements anormaux (Application – Après midi).*

Cette Figure IV.10 résume les comportements anormaux détectés grâce la fonction euclidienne Forme L2, et cela pour tous les utilisateurs dans les différentes périodes.

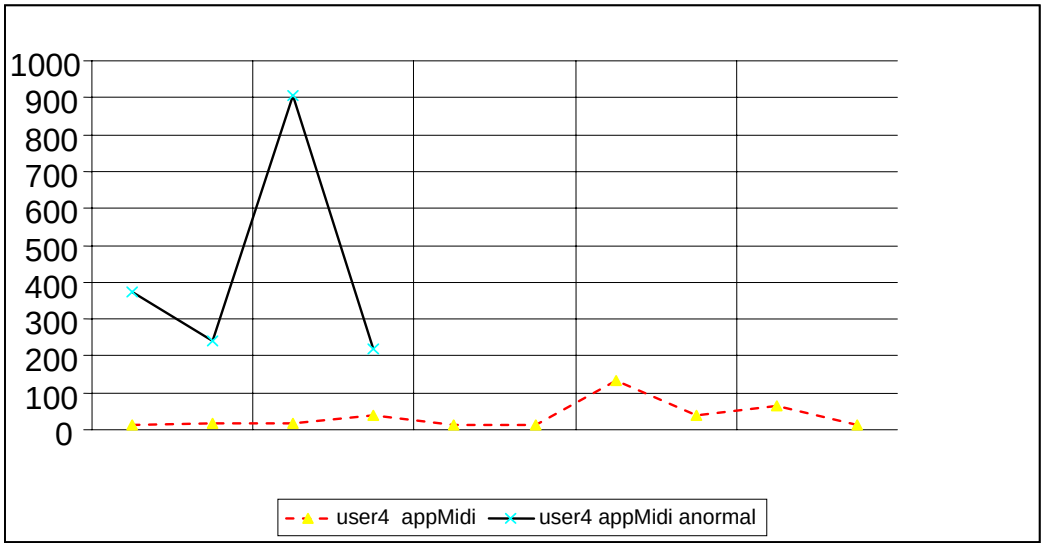


Figure IV.11 : *Graphe de comparaison entre User4 normal - User4 anormal (Après midi et Application).*

La Figure IV.11 nous montre l'efficacité de la fonction euclidienne Forme L2 sur le profil de *User4*, la courbe des résultats anormaux (issue d'une comparaison avec d'autres utilisateurs) est supérieure a celle des résultats d'analyses sur *User4*.

V.3 La Distance Quadratique

Les résultats des analyses avec cette distance se sont soldés par un échec (tableaux 5 et 6), puisque les résultats d'analyse sur les comportements normaux des utilisateurs ne diffèrent pas de ceux des comportements anormaux respectives pour chaque utilisateur. Ainsi donc les tests ont révélés l'inefficacité de cette distance dans la détection d'intrusion. Et ceci représente un résultat en soit.

V.4 Quelques Remarques

On remarque que *«User6»* dans l'observation du Profil *«Système» «Après midi»* a des valeurs incohérentes (dans le tableau 2). Cela est dû à l'instabilité de son profil. En effet lors de la période d'apprentissage, il y'a eu deux événements (les événements «51» et «26») qui se sont produits à deux reprises durant toute la période d'apprentissage et avec des valeurs très grandes.

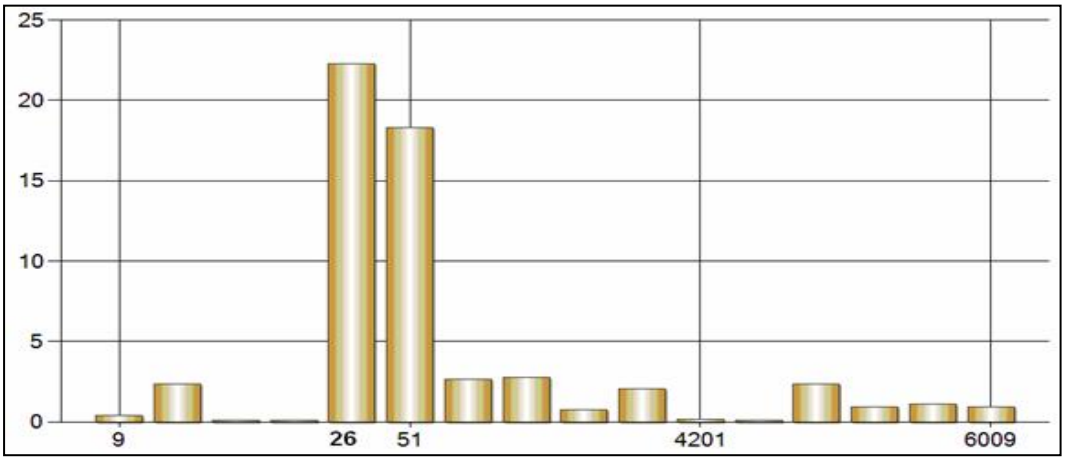


Figure IV.12 : *Profil référentiel Système - Après Midi de User6*

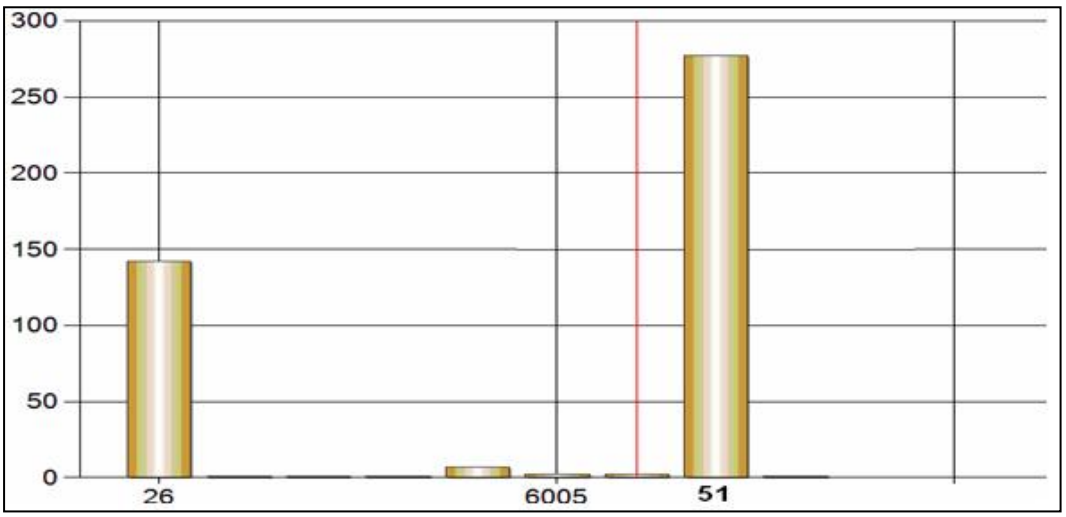


Figure IV.13 : *Profil temporaire Système - Après Midi de User6 le 25/4/2005*

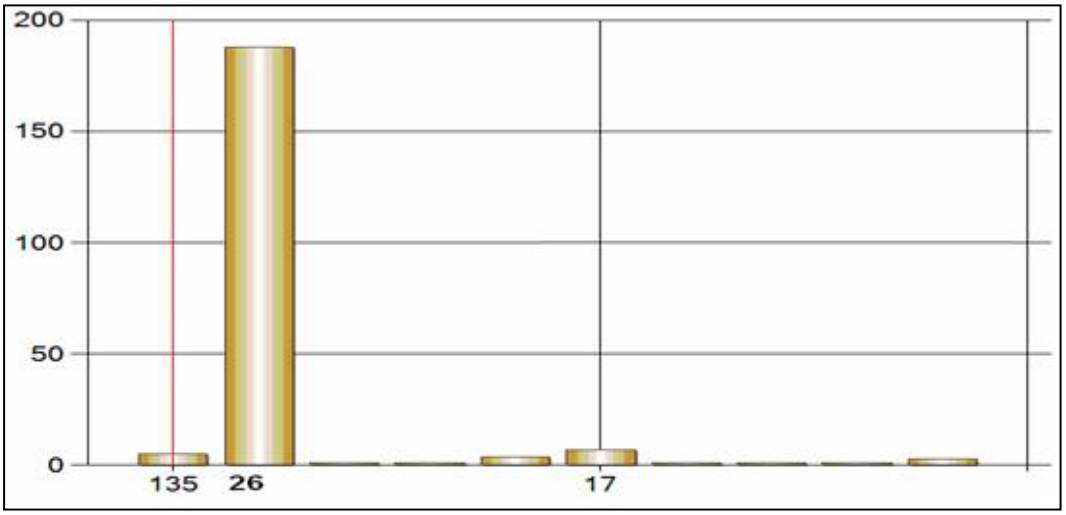


Figure IV.13 : *Profil temporaire Système - Après Midi de User6 le 19/4/2005.*

Les deux événements se sont produit avec des fréquences très grandes 155 et 188 pour l'événement 26 et 277 pour l'événement 51; et leurs sources sont Application POP UP pour l'événement 26 et Erreur CD ROM pour 51; et d'après l'histogramme du profil référentiel (Système - Après Midi) ces deux événements influes considérablement sur le comportement de *User6* (22,18 pour l'événement 26 et 18,55 pour l'événement 51), or ces événements ne se sont produits que deux fois durant toute la période d'apprentissage (un mois).

On peut affirmer que ces deux événements ne représentent pas un comportement normal de l'utilisateur, mais ils sont tout simplement générés suite à une anomalie lors de l'exploitation de la machine (exception et erreur Système), comme pour l'événement 51 qui n'est qu'une erreur du lecteur CD ROM.

Une autre observation sur les sous comportements **:** si un profil donné se compose d'un ensemble d'événements E qu'on divise selon la période de leurs occurrence lors de la période d'apprentissage on remarque le fait suivant :

Si la période d'apprentissage est très grande (par exemple quatre mois) on remarque qu'il y'a au moins deux sous ensembles d'événements Ei et Ej appartenant a E tels que pour tout i de Ei il n'existe pas j de Ej qui s'est produit au moins une fois dans le même jour que i.

Par exemple dans un profil référentiel de 4 mois, on peut trouver un ensemble d'événements qui s'est produit qu'au début de la période d'apprentissage (le premier mois par exemple), et un autre qui se produit que vers la fin de la période d'apprentissage, et tous les deux (ensembles) sont influant dans le profil référentiel (les poids des événements des deux ensembles sont importants), si on effectue l'analyse à partir d'un tel profil, les taux de faux positifs (fausse alerte) et faux négatifs seront très grands, puisque l'utilisateur a plusieurs comportements.

La seule explication de ces formations d'ensemble est que le profil de l'utilisateur a changé durant la période d'apprentissage qui est relativement longue. Pour évité un tel problème il faux prendre des périodes d'apprentissages qui ne sont pas longues (un mois par exemple) et effectuer une mise à jour des profils référentiels en cas de changement du comportement de l'utilisateur.

V.5 Contrainte sur la période d'apprentissage

La période d'apprentissage est la base de la détection comportementale, puisque cette période donne lieu à un profil sensé refléter le comportement de l'utilisateur, toute erreur ou événement externe qui arrive lors de cette période peut rendre ce profil incohérent.

Voici quelques contraintes qui doivent être respectées lors de l'établissement du profil (concernant la période d'apprentissage) :

- Lors de la période d'apprentissage il est impératif que l'utilisateur soit le *seul* a exploité la machine, sinon le profil ne reflétera pas que cet utilisateur. Car un profil est unique à chaque utilisateur.
- La *Duré* de la période d'apprentissage: la période d'apprentissage ne doit être ni très longue (quatre mois ou plus), ni très petite (une semaine) pour ne pas rendre le profil imprécis. Après observation et analyse plus la période est grande moins le Système est apte à différencier le comportement normal du comportement anormal. Par exemple voici un histogramme d'une période de quatre mois de *User4* :

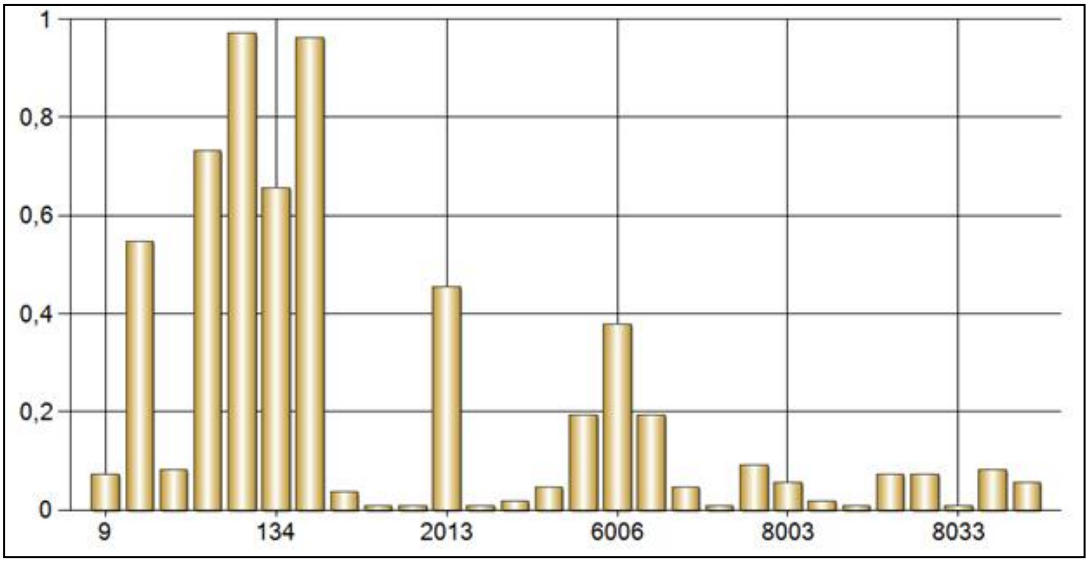


Figure IV.14 : *Profil de référence du User4 Système-Matin*

Dans cette figure la plus grande valeur est inférieur à 1 ; un tel profil ne peut être utilisé comme source d'analyse car on ne peut pas jugé le résultat de cette dernière.

En plus un profil trop petit aussi est considéré comme un problème, par exemple *User3* a un profil d'une semaine et voici un de ses histogrammes :

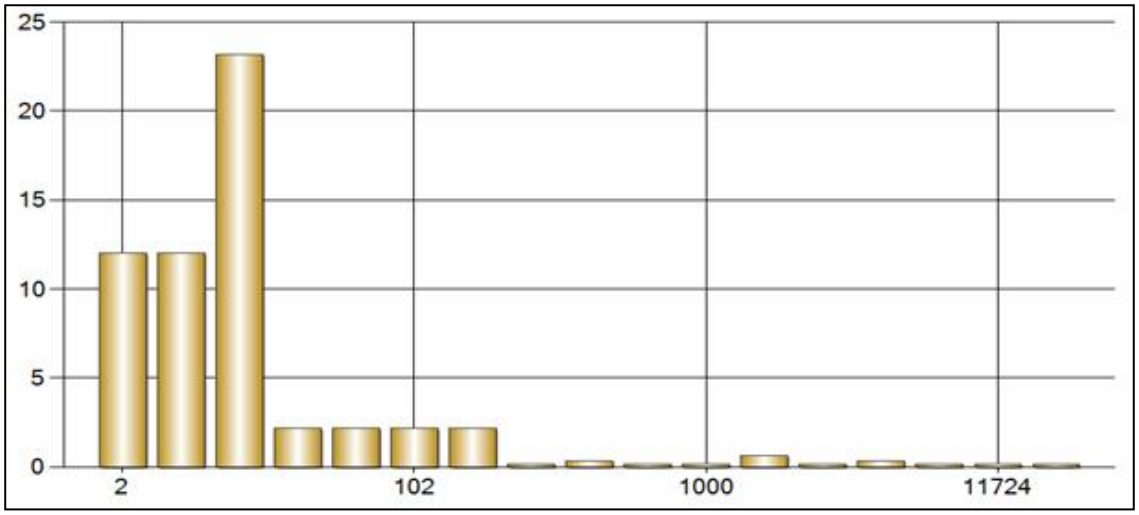


Figure IV.15 : *Application – Matin de User3.*

Là encore une semaine ne peut suffir pour établir un profil.

- Des événements de type erreur comme l'erreur du lecteur CDROM ne doivent pas être fréquentes car ces événements ne sont pas issus du comportement de l'utilisateurs, et leurs présences avec des poids élevés (fréquences importantes) risque d'influer sur l'analyse, ce qui pourrait rabaisser la capacité du système à détecter.

VI. Limite de cette méthode

Cette méthode présente quelques limites comme :

- *Ne détecte pas d'intrusion :*
  - Dans le cas où tous les événements du profil temporaire ont des fréquences très petites (Égaux à 1), ou le profil temporaire ne contient pas beaucoup d'événements (par exemple 3 événements).
  - Si le profil référentiel n'est pas cohérent (pas précis).
- *Faux positifs* : c'est-à-dire signaler une alerte alors qu'il n'y a pas eu d'intrusion; en général ce problème est un inconvénient de l'approche comportemental et représente à lui seul un axe de recherche.

Dans notre système la capacité de détection est étroitement liée au choix du seuil de détection et à la précision du profil référentiel.

VII. Conclusion :

Dans ce chapitre on a illustré le coté pratique de la méthode de détection comportementale, et ceci grâce aux tests, ce qui nous a permis d'avoir un point de vue global sur chaque distance.

A travers ces tests on peut constater que les deux distances *forme-L1* et *forme-L2* donnaient de bons résultats, contrairement aux distances Quadratique et Mahalanobis qui ne sont pas adaptées à ce contexte.

Malgré l'exploitation des histogrammes comme base pour l'établissement du profil, on ne peut pas dire que ce profil caractérise l'utilisateur (l'identifie) à 100% (problème de l'approche comportementale), mais on a un bon degrés de concordance; car il ne faut pas oublier que les autres modules de l'EIDS vont compléter ce profil afin de l'aider à décider des cas d'intrusion au cas ou il est indécis.

En ce qui concerne le seuil d'analyse, les tests ont révélés qu'il dépend non seulement de l'utilisateur et de la période (Matin, Après Midi, Soir, Nuit) mais aussi de la source des événements (Application, Réseau ou Système).

Conclusions, Perspectives & Extensions:

Conclusions, Perspectives & Extensions

Ce travail nous a permis d'aborder un domaine jusque la peu exploré des IDS qui est l'aspect comportementale, tout en le reliant avec la mouvance des technologies mobiles sans fil, ainsi que les aspects sociologiques des comportements humains.

L'EIDS ou « *Embedded Intrusion Detection System* » [BEL04] est un système de détection d'intrusion modulaire, destinée à la protection des terminaux mobiles sans fil. Il incorpore plusieurs fonctionnalités de sécurité mais il reste toute fois incomplet, d'où la nécessité de lui incorporer un module comportemental. Tout l'intérêt de l'ajout de ce module réside dans le fait que les terminaux sont à utilisation personnelle.

Par ce travail on a conçu le module comportemental qui représente pour les terminaux mobile un module crucial, car ces derniers sont sensé avoir des propriétaires uniques chose qui représente une source importante d'information. Ce module qui représente le cœur et le noyau de notre EIDS car il interagit avec tous les modules et offre un grand avantage à la fonctionnalité de détection.

Ce travail est une petite contribution qui vise à protéger au mieux les terminaux mobiles sans fil; et cela en renforçant l'EIDS, par l'aspect comportemental. Cet aspect qui consiste à avoir un module qui sonde et analyse le comportement d'un utilisateur en vu de constituer un profil de référence. Puis à essayer de détecter des variations brusques du comportement de l'utilisateur par rapport au profil de référence. L'approche entreprise dans ce travail, est l'approche statistique, qui est connu pour sa robustesse ainsi que pour l'aboutissement rapide à des applications. Dans l'approche statistique il fallait déterminer un modèle statistique qui coïncide avec le problème traité, et c'est le modèle des histogrammes et leurs distances qui a été choisi. Cette proposition n'est en aucun lieu la solution idéale qui assure le degré de sécurité 100%, mais elle représente une tentative de renforcement. Néanmoins il faut préciser que l'approche proposée pour la conception du module comportemental est générique, et ne se limite pas aux terminaux mobiles. Elle peut être appliqué à la sécurisation d'un réseau d'entreprise.

Comme perspectives à ce travail, nous proposons l'essai d'autres modèles et leur hybridation pour aboutir à de meilleurs résultats, pour des champs d'action plus larges. Des modèles tel que les réseaux de neurones et les algorithmes génétiques peuvent aider au filtrage et à l'analyse pertinente des données récoltées (du fait de la nature hétérogène de ces données).

Bibliographie:

Références:

[AND80]: J.P. Anderson; «*Computer Security Threat Monitoring and Surveillance*»; Rapport technique J.P. Anderson Co. Fort Washington, Pensylvania; Avril 1980.

[ADD01]: M. Adda, F. Guerrout, «*Contribution à la sécurité informatique, mise en œuvre d'un IDS*», Thèse d'ingéniorat à USTHB, Juin 2001.

[ALL01]: J. Allen, A. Christie, J. McHugh; «*Intrusion Detection: Implementation and Operational Issues*»; CrossTalk The Journal of Defense Software Engineering; www.stsc.hill.af.mil/index.html , Jan 2001.

[AMD98]: E. Amoroso, R. Kwapniewski; «*A Selection Criteria for Intrusion Detection Systems*». Proceedings of the 14th Annual Computer Security Applications Conference. IEEE Computer Society Press, December 1998.

[AND95a]: D. Anderson, T. Frivold, A. Valdes; «*Next-generation intrusion-detection expert system (NIDES)*»; Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, Menlo Parck, CA 94025-3493, USA, May 1995.

[AND95b]: D. Anderson, T.F. Lunt, H. Javitz, A. Tamaru, A. Valdes; «*Detecting unusual program behaviour using the statistical component of the next generation intrusion detection system (NIDES)*». Technical Report SRI-CSL-95-06, Computer Science Laboratory, SRI International, Menlo Park, CA, USA, May 1995.

[ANO99]: Hacker Anonyme, « *Sécurité Optimale* », CAMPUS Press, 1999.

[ANO00]: Hacker Anonyme, «*Comprendre les Attaques informatique*»; Ver 1.0, Janvier 2000.

[ANO02]: Anonyme, « *Maximum Security* », Que Publishing, December 2002.

[ARC00]: Archimbaud ; « *La sécurité informatique* », article CNRS, www.cnrs.fr/infosecu.html , 2000.

[AXE99]: S. Axelsson; «*The base-rate fallacy and its implications for the difficulty of intrusion detection*»; In 6th ACM Conference on Computer & Communications Security, pp.1-7, Kent Ridge Digital Labs, Singapore, 1-4 November 1999.

[AXE00]: S. Axelsson ; «*Intrusion Detection Systems: A Survey and Taxonomy*» ; Mars 2000.

[BAC00]: R. Bace; «*An Introduction to Intrusion Detection & Assesment.*» ; ICSA http://www.icsa.net/ , 2000.

[BAU88]: S.D. Bauer, M.E. Koblentz; «*NIDX – An Expert System for Real-Time Intrusion Detection*»; Proc. of the Computer Networking Symposium; pp: 98-106; IEEE, New York, Avril 1988.

[BEL04]: A.Belkhir, Dj. Naci, A. Rachedi ; «*Contribution à la sécurité du PDA : EIDS*» ; Proc. de 3iemme Conférence International sur la Sécurité & Architectures Réseaux SAR'04, La Londe, Cote d'Azur France. 21-25 Juin 2004.

[BOL89]: M.I. Bolsky, D.G. Korn; «*The KornShell Command and Programming Language*»; Prentice Hall, Englewood Cliffs, New Jersey, 1989.

[CCR98]: Commission Consultative Des Radiocommunications, «*Introduction de l'UMTS en France*», Rapport N° 1 du 22/09/1998.

[CHA91]: E. Charniak; «*Bayesian Networks Without Tears*»; AI Magazine, pp 50-63; 1991.

[CHA97]: D. Chapman, D. Brent, E.D. Zwicky; «*Firewalls la sécurité sur Internet*»; OReilly International Thomson, 1997.

[CHE88]: P. Cheeseman, J. Kelly, M. Self, J. Stutz, W. Taylor, D. Freeman; «*Autoclass: A Bayesian Classification System*»; In Proc. of 5th International Conf. on Machine Learning, pp: 54-64; Morgan Kaufmann, June 1988.

[CHE91]: P. Cheeseman, R. Hanson, J. Stutz; «*Bayesian Classification with Correlation and Inheritance*»; In 12th International Joint Conference on Artificial Intelligence, IJCAI, August 1991.

[COL05]: E. Cole, R. Krutz, J.W. Conley; «*Network Security Bible*»; Wiley Publishing Inc. ISBN: 0-7645-7397-7; 2005.

[CRO96]: M. Crosbie, B. Dole, T. Ellis, I. Krsul, E. Spafford. «*IDIOT- Users Guide*». The COAST Project, Dept. of Computer Science, Purdue University, West Lafayette, IN, USA, Technical Report TR-96-050, 4 September 1996.

[CST96]: CST; « *Sécurité des réseaux, Analyse et mise en œuvre* », Centre de la sécurité des télécommunications Canada, www.cse.dnd.ca , Janvier1996

[CUF03]: A.Cuff ; «*Intrusion Detection Terminology*» ; Revue SecurityFocus, September 2003.

[DAN99]: T. Danse ; «*L'avenir des mobiles de la 3éme Génération*»; http://memoireinline.free.fr/thierrydanseUMTS.html , Août 1999.

[DEB92] : H. Debar, M. Becker, D. Siboni. «*A neural network component for an intrusion detection system*». In Proc. of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, pp: 240-250 May 1992. IEEE, IEEE Computer Society Press, Los Alamitos, CA, USA.

[DEB98]: H. Debar, M. Dacier,A. Wespi; «*Towards a Taxonomy of Intrusion Detection Systems*»; Internal RZ 3030, IBM Zurich Research Laboratory, Saumerstrasse 4, CH-8803 Ruschlikon, Swizerlan. June 1998.

[DEN87]: D.E. Denning; «*An Intrusion Detection Model*»; In IEEE Transactions on Software Engineering, n°2, pp 222; Februrary 1987.

[DEN01]: D.E. Denning; «*AAFID* »; http://www.guill.net , 2001

[DOA92]: J. Doak; «*Intrusion Detection: The Application of Feature Selection – a Comparison of Algorithms, and the Application of a Wide Area Network Analyzer*»; Master's Thesis, Departement of Computer Science, Univ. of California, Davis; 1992.

[DOD85]: Department of Defense (DoD); «*Trusted Computer System Evaluation Criteria (TCSEC)» ;* (DoD 5200.28-STD 1985). Fort Meade, MD: Department of Defense, URL: www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html 1985.

[DOW90]: C. Dowel, P. Ramstedt; «*The computer watch data reduction tool*»; In Proc. of the 13th National Computer Security Conference, Washington DC, USA, NIST, National Institute of Standards and Technology /National Computer Security Center. pp 99-108, October 1990.

[EGA75]: J.P. Egan, «*Signal Detection Theory and ROC Analysis*»;. Academic Press, 1975.

[FAR03a]: J. Farshchi, «*Wireless Intrusion Detection System*»;. www.SecurityFocus.com, Novembre 2003.

[FAR03b]: J. Farshchi, «*Wireless Network Policy Development*»; www.securityfocus.com/infocus/1732 , 2003.

[FLU01]: Fluhrer, Mantin, Shamir; «*Weaknesses in the Key Scheduling Algorithm of RC-4*»; www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps ; 2001.

[FOX90]: K.L. Fox, R.R. Henning, J.H. Reed, R. Simonian; «*A Neural Network Approach Towards Intrusion Detection*»; In Proc. of the 13th National Computer Security Conf., pp: 125-134, Washington, DC, October 1990.

[FRE00]: K. Frederick; «*IP abnormal packets*»; www.securityfocus/frames/?focus=ids&content= /focus/ids/articles/abnormal1.html , 2000.

[FYO00]: Fyodor, «*The Art of Scanning Port* », www.nmap.com/the_art_of_scanning_port.html , 2000

[GAR91]: T.D. Garvey, T.F. Lunt. «*Model based Intrusion Detection*»; In Proc. of the 14th National Computer Security Conference, pp: 372-385, October 1991.

[GIA92]: J.C. Giarratano; «*Clips Version 5.1 User's Guide*»; NASA, Lyndon B.Johnson Space Center, Information Systems Directorate, software Technology Branch, March 1992.

[GOL96]: I.Goldberg, D. Wagner, R. Thomans, E. Brewer. «*A secure environment for untrusted helper applications (confining the wily hacker)*». In Proc. of the 6th USENIX UNIX Security Symposium, USENIX Association, San Jose, California, USA, July 1996.

[GRA00]: R. Graham; « *Network Intrusion Detection System* »; http://www.robertgraham.com/pubs/network-intrusion-detection.txt ,2000

[HAB92]: J. Habra, B. Le Charlier, A. Mounji, I. Mathieu; «*ASAX: Software architecture and rule-based language for universal audit trail analysis*»; In Yves Deswarte et al., editors, Computer Security – Proc. of ESORICS 92, Vol.648 of LNCS, pp:435-450, Springer-Verlag; Toulouse, France, 23-25 November 1992.

[HEA90]: R. Heady, G. Luger, A. Maccabe, M. Servilla; «*The Architecture of a Network Level Intrusion Detection System*» ; rapport technique, Dépt. Informatique, Univ New Mexico ; Aout 1990.

[HEB90]: T. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, D. Wolber; «*A network security monitor*». In Proc. of the 1990 IEEE Symposium on Research in Security and Privacy, IEEE, IEEE Comput. Soc. Press, Los Alamitos, CA, USA, pp: 296-304; 1990.

[HEB91]: L.T. Heberlein, K.N. Levitt, B. Mukherjee; «*A Method to Detect Intrusive Activity in a Networked Environment* » ; Proc. of the 14th National Computer Security Conference, pp:362-371, October 1991.

[HEL93]: P. Helman, G. Liepins; «*Statistical foundations of audit trail analysis for the detection of computer misuse*». IEEE Transactions on Software Engineering, 19(9): 886-901, September 1993.

[HOC93]: J. Hochberg, K. Jackson, C. Stallings, J.F. McClary, D. DuBois, J. Ford; «*NADIR: An automated system for detecting network intrusion and misuse*»; Computers & Security, 12(3) pp:235-248, 1993.

[ILG92]: K. Ilgun. «*USTAT: A Real-Time Intrusion Detection System for UNIX*». Master's Thesis, Computer Science Department, University of California, Santa Barbara, July 1992.

[ILG93]: K. Ilgun; «*USTAT: A real-time intrusion detection system for UNIX*»; In Proc. of the 1993 IEEE Symposium on Security and Privacy, pp: 16-28, Oakland, California, IEEE Computer Society Press; 24-26 May 1993.

[ILG95]: K. Ilgun, R.A. Kemmerer, P.A. Porras; «*State transition analysis: A rule-based intrusion detection approach*». IEEE Transactions on Software Engineering, 21(3) pp:181-199, March 1995.

[INN01]: P. Innella; «*The Evolution of Intrusion detection Systems* »; www.securityfocus.com Nov 2001.

[ISO89]: Norme internationale ISO 7498-2, «*Système de traitement de l'information Interconnexion des systèmes ouvert*», Modèle de référence de base, Partie 2: Architecture de sécurité, 1989.

[JAC95]: K.A. Jackson, D.H. DuBois, C.A. Stallings; «*An expert system application for network intrusion detection*»; In Proc. of the 14th National Computer Security Conf. Pp 215-225, Washington, D.C., 1-4 October 1991.

[JOU97]: Y.F. Jou, F. Gong, C. Sargor, S. FelixWu, C.W. Rance. «*Architecture design of a scalable intrusion detection system for the emerging network infrastructure*». Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University,

Releigh, N.C, USA, April 1997.

[KEM94]: R.A. Kemmerer; «*Computer Security*»; Encyclopedia of Software Engineering: 1153-1164. New York, NY: John Wiley and Sons, 1994.

[KOR01]: M.R. Kortebi & H. Abdellah El Hadj ; «*Réalisation d'un outil détecteur de SNIFFER: IDS*», Thèse d'ingéniorat U.S.T.H.B., Septembre 2001.

[KRU04]: R.L. Krutz, R.D. Vines; «*The CISSP Prep Guide, 2nd Edition: Mastering the CISSP and ISSEP Exams* », Wiley Publishing Inc., Indianapolis; ISBN: 0-7645-59-15-X; 2004.

[KUM94a]: S. Kumar, E.H. Spafford; «*An application of pattern matching in intrusion detection*». Technical Report CSD-TR-94-013, The COAST Project, Dept. of Computer Sciences, Purdue University, West Lafayette, IN, USA, 17 June 1994.

[KUM94b] : S. Kumar, E.H. Spafford; «*A pattern matching model for misuse intrusion detection*». In Proc. of the 17th National Computer Security Conference, pp:11-21, Baltimore MD, USA, NIST, National Institute of Standards and Technology/National Computer Security Center. 1994.

[KUM95a]: S. Kumar, E.H. Spafford; «*A software architechture to support misuse intrusion detection*». Technical report, The COAST Project, Dept. of Comp. Sciences, Purdue Univ.,West Lafayette, IN, 47907-1398, USA, 17 March 1995.

[KUM95b]: S. Kumar ; «*Classification and Detection of Computer Intrusions*» ; Thèse PhD Univ. Purdue ; Aout 1995.

[LAC03]: Lackey, Roth, Goddard; «*Wireless Intrusion Detection*» ; www-1.ibm.com/services/strategy/files2/wireless_intrusion_detection.pdf ;2003

[LAN92]: L. Lankewicz; «*A Non-Parametric Pattern Recognition to Anomaly Detection*»; Thèse PhD Univ. Tulane; 1992.

[LEE99]: W. Lee. «*A data mining framework for building intrusion detection Models*». In IEEE Symposium on Security and Privacy, pp: 120-132, Berkeley, California,1999.

[LEG00]: G. LeGrand; «*LA MOBILITE*», www-rp.*lip*6.fr/~legrand/mobilite.html , 2000.

[LIE89]: G.E. Liepins, H.S. Vaccaro; «*Anomaly Detection: Purpose and Framework* »; Proc. of the 12th National Computer Security Conference; pp:495-504; Octobre 1989.

[LIP98]: R.P. Lippmann, I. Graf, S.L. Garfinkel, A.S. Gorton, K.R. Kendall, D.J. McClung, D.J. Weber, S.E. Webster, D. Wyschogrod, M.A. Zissman; «*The 1998 DARPA/AFRL off-line intrusion detection evaluation*»; Presented to The First Intl. Workshop on Recent Advances in Intrusion Detection (RAID-98), Lovain-la-Neuve, Belgium, No printed proceedings, pp 14-16 September 1998.

[LOS 87]: D. Longley, M. Shain ; «*Data and Computer Security : Dictionary of Standars, Concepts, and Terms*» ; Stockton Press, New York, 1987.

[LUD97]: M. Ludwig; « *Du Virus à l'Antivirus* », DUNOD, 1997.

[LUN88]: T.F. Lunt, R. Jagannathan, R. Lee, S. Listgarten, D.L. Edwards, P.G.Neumann, H.S. Javitz, A. Valdes; «*IDES: The enhenced prototype, A real-time intrusion detection system*»; Technical report SRI Project 4185-010, SRI-CSL-88-12, CSL SRI International, Computer Science Laboratory, SRI Intl. 333 Ravenswood Ave, Menlo Park, CA 94925-3493, USA, October 1988.

[LUN89]: T.F. Lunt, R. Jagannathan, R. Lee, S. Listgarten, A. Whitehurst, S. Listgarten; «*Knowledge based Intrusion Detection*»; Proc. of the Annual AI Systems in Government Conference, Washington, DC, Mars 1989.

[LUN92]: T.F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, C. Jalali, P.G. Neuman. «*A real-time intrusion-detection expert system (IDES)*». Technical Report Project 6784, CSL, SRI International, Computer Science Laboratory, SRI Intl. 333 Ravenswood Ave., Menlo Park, CA 94925-3493, USA, February 1992.

[LUN93]: T.F. Lunt, «*A Survey of Intrusion Detection Techniques*»; Computers and Security: 405-418; 12, 4 June 1993.

[LUR03]: LURHQ Threat Intelligence Group; «*Intrusion Detection: In Depth Analysis*»; www.lurhq.com/idsindepth.html ; 2003.

[MAC90]: A.B. Maccabe, R. McDonald, V. Anand. «*Learning How to Characterize Normal Behavior in Local Area Network*».1990.

[ME 99]: L. Mé ; «*Méthodes et Outils de la Détection d'intrusions*» ; Cours Supelec http://www.supelec-rennes.fr/rennes/si/equipe/lme/; 1999.

[MER04]: A.Mercier; «*La Gestion des Incidents de Sécurité de l'Information Numérique* » ; Cours CRIM; Octobre 2004.

[MOI]: A. Moitra; «*Real Time Audit Log Viewer And Analyzer*».

[MUK94]: B. Mukherjee, L.T. Heberlein, K.N. Levitt. «*Network intrusion detection*». IEEE Network, 8(3) pp:26-41, May/June 1994.

[MUR98]: J. Murray; «*Inside Microsoft Windows CE*»; Microsoft Press, 1998.

[NAC02]: Dj. Naci, A. Rachedi ; «*Système de Détection d'Intrusion sur plateforme Embarquée (Windows CE)*» ; Thèse d'ingéniorat U.S.T.H.B., Juin 2002.

[NAC05]: Dj. Naci ; «*Les Système de Détection d'Intrusion*» ; Cours Post Graduation Spécialisé en Sécurité Informatique LLB-CERIST Algérie ; 2005.

[NOR99]: S. Northcutt ; «*Network Intrusion Detection*» ; New Riders, Indianapolis, 1999.

[PAX88]: V. Paxon. «*Bro: A system for detecting network intruders in real-time*». In Proc. of the 7th USENIX Security Symposium, San Antonio, TX, USA, USENIX, USENIX Association. Corrected version, §7 overstated the traffic level on the FDDI ring by a factor of two. January 1988.

[PEA88]: J. Pearl; «*Probabilistic Reasoning in Expert Systems* »; Morgan Kaufman, San Mateo, California; 1988.

[PEI02]: C. Peikari, S. Fogie; «*Maximum Wireless Security* »; Sams Publishing. December 2002.

[POR92]: P.A. Porras, R.A. Kemmerer. «*Penetration State Transition Analysis – A Rule-based Intrusion Detection Approach*». In 8th Annual Computer Security Applications Conf. pp: 220-229. IEEE Computer Society press, November 30 – December 4, 1992.

[POR97]: P.A Porras, P.G Neumann. «*EMERALD: Event monitoring enabling responses to anomalous live disturbances*». In Proc of the 20th National Information Systems Security Conference, pp: 353-365, Baltimore, Maryland, USA, NIST, 7-10 October 1997.

[POR98]: P.A Porras, A. Valdes. «*Live traffic analysis of TCP/IP gateways*». In Proc. of the 1998 ISOC Symposium on Network and Distributed Systems Security, San Diego, California, 11ñ13 March 1998.

[PRO94]: P. Proctor; «*Audit Reduction and Computer Misuse Detection*». Talk given at the Sixth Annual Computer Security Incident Handling Workshop; 1994.

[PTA98]: T.H. Ptacek ; T.N. Newsham ; «*Insertion, Evasion, and Denial of Service : Eluding Network Intrusion Detection*» ; www.snort.org/IDSpaper.pdf Janvier 1998.

[PUJ98]: G. Pujolle, E. Morlait, D. Seret, D. Dormard, «*Réseaux et Télématique* », Tome II, Eyrolles, 2ieme édition 1998.

[SCH94]: B. Schneier; «*Cryptographie appliquée, protocoles, algorithmes et codes sources*»; International Thomson Publishing France, 1994.

[SEB88]: M. Sebring, E. Shellhouse, M.E. Hanna, R.A. Whitehurst; «*Expert systems in intrusion detection : A Case Study*»; In Proc. of 11th National Computer Security Conference, pp 74-81, Baltimore, Maryland, 17-20 October 1988.

[SEC01]: Anonyme ; «*La sécurité informatique* »; http://www.secinfo.com , 2001.

[SHE00]: T. Sheldon ; «*Guide pratique de la sécurité sous WindowsNT* », International Thomson Publishing France, 2000.

[SIE01]: SIEMENS, CERBERUS® , «*Technique de détection d'intrusion*».

[SIL94]: A. Silberchatz, P.B. Galvin, «*Operationg system Concepts*», Addition-Wesley USA, 1994.

[SMA88]: S.E. Smaha; «*Haystack: An Intrusion Detection System*»; 37-44. Proc. of the Fourth Aerospace Computer Security Applications Conference. Orlando, Florida, December 12-16, 1988. Washington, DC: IEEE Computer Society Press, 1989.

[SMA95]: S. Smaha; Talk given at third Computer Misuse and Anomaly Detection Workshop (CMAD III) in Sonoma, California; January 1995.

[SNA91]: S.R. Snapp, J. Brentano, G.V. Dias, T.L. Goan, L.T. Heberlein, C. Ho, K.N. Levitt, B. Mukherjee, S.E. Smaha, T. Grance, D.M. Teal, D. Mansur; «*DIDS Distributed Intrusion Detection System – Motivation, Architecture, and an Early Prototype* »; Proc. of the 14th National Computer Security Conference, pp:167-176, October 1991.

[SNA92a]: S.R. Snapp, S.E. Smaha; «*Signature Analysis Model definition and Formalism*»; In Proc. of the 4th Workshop on Computer Security Incident Handling. Denver, Colorado; August 1992.

[SNA92b]: S.R. Snapp, S.E. Smaha, D.M. Teal, T. Grance; «*The DIDS (distributed intrusion detection system) prototype*»; In Proc. of the Summer USENIX Conf. Pp 227-233, San Antonio, Texas, 8-12 Jun 1992.

[SPA88]: E.H. Spafford; «*The Internet Worm Program: An Analysis*»; (CSD-TR-823). West Lafayette, IN: Purdue University, 1988.

[SPA98]: E. Spafford, D. Zamboni; «*A framework and prototype for a distributed intrusion detection system*», Rapport technique 98-06 COAST Laboratory, Purdue University http://www.cs.purdue.edu/coast/coast-library.html, Mai 1998.

[STA96]: S. Stani ford Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K Levitt, C. Wee, R. Yip, and D. Zerkle; «*GrIDS -A graph based intrusion detection system for large networks*». In Proc. of the 19th National Information Systems Security Conference, 1996.

[STA98]: S. Staniford¡Chen, «*Common Intrusion Detection Framework*» ; 1998 ; http://seclab.cs.ucdavis.edu/cidf/

[STO03a]: S.J. Stolfo, S. Hershkop, K. Wang, O. Nimeskern, C. Hu; « *Combining Behavior Models to Secure Email Systems*»;.Colombia University, USA. 2003

[STO03b]: S.J. Stolfo, S. Hershkop, K. Wang, O. Nimeskern, C. Hu; «*Behavior Profiling of Email*»;. 1st NSF/NIJ Symposium on Intelligence & Security Informatics (ISI). Tucson, Arizona, USA. 2003.

[STO04]: S.J. Stolfo, S. Hershkop, K. Wang, O. Nimeskern, C. Hu; « *Detecting Viral Propagations Using Email Behavior Profiles*»;. Columbia University, USA. 2004

[SUN96]: A. Sundaram ; «*An Introduction to Intrusion Detection*» ; ACM Crossroads Student Magazine 1996.

[TAN90]: Tanenbaum, «*Les réseaux, Architectures, Protocoles et Applications* », InterEdition, Mai 1990.

[TCL90]: H.S. Teng, K. Chen, S.C. Lu; «*Security Audit Trail Analysis Using Inductively Generated Predictive Rules*»; In Proc. of 6th Conf. on Artificial Intelligence Applications, pp 24-29, IEEE, Piscataway, New Jersey, Marsh 1990.

[VAC89]: H.S. Vaccaro, G.E. Liepins; «*Detection of anomalous computer session activity*»; In Proc. of the 1989 IEEE Symposium on Security and Privacy, pp. 280-289, Oakland,

California, 1-3 May 1989.

[VEN92]: W. Venema; «*TCP WRAPPER: Network monitoring, access control and booby traps*»; In Proc. of the 3rd USENIX UNIX Security Symposium, pp:85-92, USENIX Association; Baltimore, Maryland, 14-16 September 1992.

[WAR79]: W. H. Ware; «*Security Controls for Computer Systems: Report of Defense Science Board, Task Force on Computer Security»;* Santa Monica, CA: The Rand Corporation, 1979.

[WAR99]: C. Warrender, S. Forrest, B. Perlmutter; «*Detecting intrusions using system calls: Alternative data models*». In IEEE Symposium on Security and Privacy, pp. 133-145, Berkeley, California, May 1999.

[WET93]: B.R. Wetmore; «*Paradigms for the Reduction of Audit Trails* ». Thèse de Mastère, Univ. de Californie, Davis; 1993.

[WHI96]: G. White, V. Pooch; «*Cooperating security managers: Distributed intrusion detection systems*»; Computers & Security, Vol. 15(No. 5) pp:441-450, Elsevier Science Ltd. 1996.

[WID03] : «*WIDZ- Wireless Intrusion Detection System*»; www.loud-fat-bloke.co.uk/articles/widz_design.pdf; 2003.

[WIN92]: P.H. Winston; «*Artificial Intelligence*»; Addison Wesley, Reading, Massachusetts, 3rd edition, 1992.

[WRI03]: J. Wright; «*Detecting Wireless LAN MAC Adress Spoofing*»; http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf ; Janvier 2003.

[ZAM98]: D. Zamboni, J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isacoff, E. Spafford, «*An Architecture for Intrusion Detection using Autonomous Agents*», Rapport Technique COAST n°47907-1398, 98/05. Juin 1998.

[ZAM01]: D. Zamboni; «*Autonomous Agent for Intrusion detection*»; http://www.guill.net/securite/ids.html , 2001