Contribution à la sécurité du PDA : IDS Embarqué (EIDS)

Abdelkader Belkhir, Mohamed Djamedl Naci, Abderrezak Rachedi

Contribution à la sécurité du PDA : IDS Embarqué (« EIDS »).

Abdelkader Belkhir[α], M[ed] Djamel Naci[β] *and* Abderrezak Rachedi[α].
[α]*USTHB, Faculté Electronique & Informatique ;Laboratoire des Systèmes Informatiques, Département Informatique BP 32 El-Alia Alger ALGERIE.*
E-Mail : belkhir@wissal.dz , rachedi.abderrezak@gmail.com .
[β]*LLB, Laboratoire des Logiciels de Base ; Centre de Recherche sur l'Information Scientifique et Technique; CERIST, 3, Rue des frères Aissou, B.P 143 Ben Aknoun, 16030 Alger ALGERIE .*
E-Mail: naci_djamel@yahoo.fr , naci_djamel@mail.cerist.dz .

RÉSUMÉ. La sécurité informatique contribue à la préservation, l'intégrité, la confidentialité ainsi qu'à la non répudiation de l'information. Son intérêt est grandissant surtout dans un environnement sans fil et mobile et la solution ne saurait être ponctuelle ou périodique. Il est nécessaire d'établir un diagnostic en temps réel afin de parer à toute éventualité d'attaque. A cet effet, la solution développée consiste en la mise en œuvre d'un IDS embarqué capable de contrôler l'activité réseau ainsi que l'intégrité du système d'un terminal mobile. C'est un système Multi-Modules (Agents ou Composants) qui préserve sa modularité, son extension et sa propre sécurité ainsi que son indépendance vis à vis des plates-formes. En plus, le fait d'assurer la sécurité de ces terminaux renforcerai et accroîtrai la confiance des gens et augmenterai le nombre d'utilisateurs et de ce fait assurer la réussite économique et technologique de ces produits (PDA), qui vont intégrés les réseaux de 3[ieme] Génération (UMTS, IMT2000, CDMA2000).

KEYWORDS: IDS, PDA, intrusion, integrity, embedded system.

1. Introduction

L'évolution technologique fait du PDA un objet communicant centrique par sa capacité de communication et sa puissance de calcul. En effet, le PDA introduit une aisance d'intégration technologique dans la vie quotidienne permettant l'indépendance et la mobilité de l'utilisateur et l'usage d'un terminal intégré (*le tous en un*). Ainsi, la communication peut se faire à travers des réseaux ad hoc ou via des réseaux classiques [14]. C'est pour cela qu'ils sont réputés pour être fortement connectés (utilisation des différentes voix de communications).

A l'opposé, les PDA introduisent une nouvelle problématique de sécurité [8][19]. En effet, l'*oubli* ou la *perte* d'un PDA est un fait ordinaire. Par conséquent, il constituera un nouveau maillon faible de la chaîne de sécurité d'un système informatique. Il peut être utilisé comme un *canal* d'intrusion ou une *source* d'information dans un environnement de réseau d'entreprise. Ainsi, on se trouve face à un nouveau challenge de sécurité. Il s'agit d'assurer à la fois la protection et la sécurisation de ces objets communicants.

La sécurité du *système d'exploitation* assure le bon fonctionnement de votre machine [4][18]. Elle protège l'information stockée de la *perte*, de tout éventuel *changement indésirable* volontaire ou accidentel ou de lecture ou de modification par un tiers non autorisé. L'implantation et la maintenance de la sécurité ne sont pas une mince affaire. Beaucoup de structures disposent de sites et de plates formes multiples, de réseaux de provenances diverses, avec des liaisons vers des réseaux externes. Ce type de configuration est de plus en plus courant et ne fait qu'accroître l'importance des besoins en matière de sécurité et la complexité des solutions requises. Il ne faut pas oublier qu'une chaîne possède la solidité de son maillon le plus faible.

La section 2 passe en revue les problèmes de sécurité dans l'environnement des PDA et cela afin d'argumenter nos choix (types d'attaques auxquels sont sujets les réseaux mobiles sans fil en particulier pour les PDA); la section 3 se focalisera sur les détails conceptuels et techniques de notre IDS (*Intrusion Detection System*) embarqué, qui permettra de sécuriser le PDA. Il sera décrit par ses composants (modules, agents) et leurs interactions qui réalise la fonctionnalité de ce système. Les détails techniques seront introduits par des scénarios de comportement évoqués dans la partie *Annexe*. Enfin la section 4 énoncera quelques conclusions, perspectives et travaux en cours pour l'extension et l'amélioration de l'EIDS.

2. Sécurité *Vs* Mobilité

La forte inter-connectivité des réseaux facilite le travail en groupe mais expose les ressources du système informatique à différentes attaques au quotidien [4]. De plus, la *mobilité* induit un mode de travail sans contrainte d'espace; elle met en avant l'enjeu de la sécurité dont les conséquences peuvent être néfastes pour tout système informatique propriétaire. Il s'agit de préserver cette connectivité et fluidité de travail coopératif sans mettre en péril la sécurité du système informatique. La *communication sans fil est vulnérable* car son *support physique* est *public* [3][18]. En effet, un programme renifleur (d'écoute)[2] de paquets facilite le filtrage et le tri des communications afin de trouver et évaluer un type de trafic bien défini. De plus, le vol d'adresse (*spoofing*) est un autre moyen d'attaque: quelqu'un se trouvant sur un nœud réseau peut se faire passer pour un nœud reconnu d'un autre réseau. Cela se fait en introduisant de fausses adresses dans des paquets IP et en envoyant ces paquets vers le réseau cible. Par ailleurs, des attaques par *refus* (déni) de service peuvent être l'œuvre d'un agresseur déconnectant une session: tout trafic venant d'un poste bien particulier sur un réseau peut être interrompu. D'autre part, la *synchronisation* d'un PDA avec un PC peut être une source de virus à partir du PDA (notion de *porteur de virus*). Le PDA possède son propre *système d'exploitation* [15], ce qui nécessite un système de protection de ce système qui garantit l'*intégrité* de ses fichiers. En plus des risques de *vol* et de *perte* des PDAs qui nécessite un mécanisme d'*authentification* et d'*identification* pour utiliser ce PDA. De plus, les intrusions dans un réseau privé sans interconnexion physique à ce dernier (attaques via support de fréquence).

A cet égard, il s'agit de préserver cette *intégration* de l'objet communicant (PDA) au sein du réseau tout en veillant à *sa propre sécurité*. Pour cela, et vu la complexité et la diversité des menaces posées dans cet environnement on utilisera conjointement les points décrits précédemment pour développer et renforcer la sécurité du système informatique : en implémentant un *IDS Embarqué*.

3. IDS Embarqué sur PDA

Il offre un service de détection et de réponse aux attaques en temps réel. Grâce à sa surveillance du trafic réseau en temps réel, l'IDS permet d'identifier toute anomalie et stoppe immédiatement les activités non autorisées [5][10].

Pour réaliser une supervision efficace, il convient d'agir conjointement selon trois axes:

Audit interne et tests d'intrusion réguliers pour évaluer les vulnérabilités.
Contrôle permanent de l'intégrité des services en lignes.
Détection d'intrusion en temps réel.

La détection d'intrusion est définie comme: ' *la capacité à identifier les individus utilisant un système informatique sans autorisation et ceux qui ont accès légitime au système mais abusent de leurs privilèges*'. On pourra lui ajouter les tentatives d'utilisation d'un système informatique sans autorisation. Les intrus (ou attaquants) peuvent être vus comme intrus externe, déguisé ou par abus. Ces mêmes intrus peuvent avoir différentes motivations allant de la simple curiosité à l'espionnage en passant par le vandalisme.

3.1. Critères et choix

Les systèmes de détection d'intrusion peuvent être classés [figure 1] [21][6][9] selon la *méthode* de *détection* en une approche *comportementale*, ou par *scénario* ou selon les *sources* des *données* analysées en une approche basée *application*, *hôte* ou *réseau*. Par ailleurs, L'IDS peut supporter le mode de détection en *différé* ou en *temps réel*, il peut être *passif* (alarme) ou *actif*. Toutes ces caractéristiques et critères de classification permettent de définir la conception et le fonctionnement de l'IDS. Elles sont relativement orthogonales, leur intégration dans un même système permettra d'assurer une plus grande sécurité.

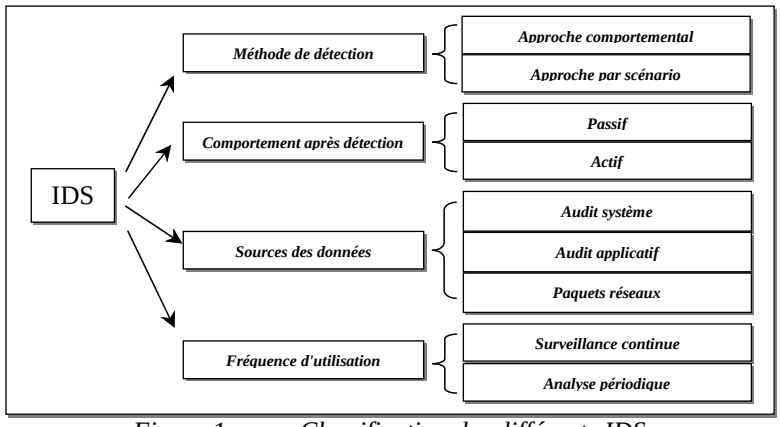


Figure 1 - Classification des différents IDS

Notre approche consiste à mettre en œuvre un IDS capable d'assurer la sécurité d'un PDA et son intégration sécurisée dans un réseau (filaire ou sans fil) sans nuire à ces ressources limitées (IDS light). Tenant compte de la diversité et de la complexité des risques et menaces liées à cet environnement (mobile, sans fil, à ressources réduites), notre architecture se doit être *hybride* et *optimal* pour remédier aux différentes menaces. Il sera *hybride* : basé hôte, basé réseau et basé cible. L'architecture s'articulera sur l'approche *Multi-Modules* (pour ne pas dire *Multi-Agents* ou *Multi-Composants*) où chaque *Module* effectuera une tâche bien déterminée tout en collaborant avec les autres *Modules*. (le terme *Module* est utiliser au lieu d'*Agent* ou *Composant* pour préserver l'aspect d'indépendance de la conception vis à vis des plates-formes et vis à vis des approches de modélisation, il représente une *Abstraction* des deux autres termes).

3.2. EIDS (Embedded Intrusion Detection System)

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. C'est un IDS léger qui veut dire que les fonctionnalités de ses modules sont optimisées en conformité avec l'environnement des Pockets PC; ces derniers ont une contrainte d'espace de stockage, de durée de batterie limité; et donc il faudrait des tailles de code réduit, de petits fichiers log générés et moins de calcul (temps CPU).

3.2.1. Architecture & Implémentation

Notre système est à base de modules qui peuvent être vu comme *agents mixtes* [11]: *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 contrôleur d'intégrité,

module accès aux fichiers, module accès initial, module moniteur de comportement, module cryptage/décryptage, module filtrage des paquets, module surveillance des ports, module interface utilisateur. Ces modules collaborent entre eux et partagent des connaissances pour renforcer le rôle de surveillance et de défense. La figure ci dessous [*Figure 2*] montre ces différents modules et leur positionnement vis à vis du flux du réseau, du système et de l'utilisateur.

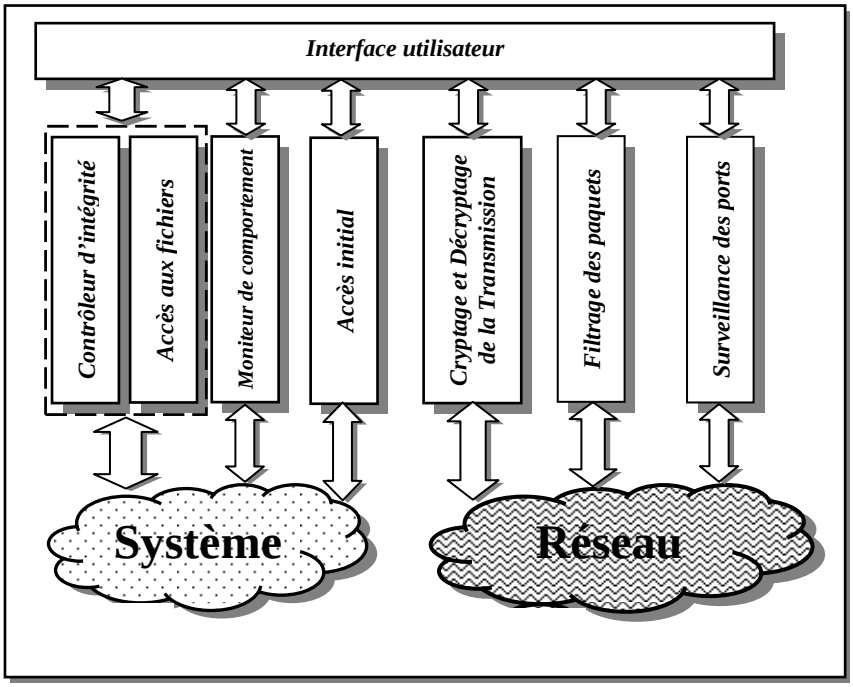


Figure 2 -Architecture de l'IDS Embarqué

Une version de notre EIDS a été implémentée dans un environnement *Windows CE* [15] 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*..(voir dans l'annexe les scénarios d'exécution).

3.2.2. Module contrôle d'intégrité

C'est un scanner lancé périodiquement ou à la demande pour détecter tout changement survenu dans le système à partir d'informations stockées sur le disque telles que : fichier **.DLL*, **.EXE*, **.SYS* …. Cette vérification utilise un algorithme de checksum {SHA, MD5}[17] en passant par la date de dernière modification et la taille. Ce module aide l'administrateur à localiser les fichiers modifiés en cas d'attaque réussie pour pouvoir rétablir le système. 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. Ses 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 utiliser, valeur de signature…). Ce module assure aussi le contrôle d'intégrité des fichiers de données personnels, il suffit seulement de les spécifier pour qu'il soit pris en compte. Au calcul de chaque signature ce module compare cette dernière à des signatures correspondant à des codes malicieux et virus connus qui sont stockées dans une seconde base de données dynamique qui est mise à jour régulièrement avec des signatures de nouveaux virus. Des fichiers de rapports (*logs*) sont génères à la détection d'altérations 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. Notre système signe ses propres fichiers pour préserver son intégrité.

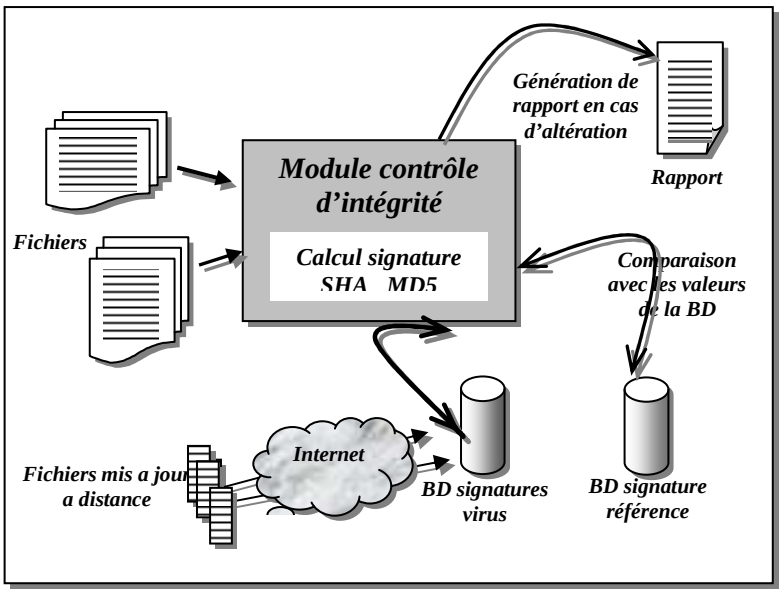


Figure 3 -Module contrôle d'intégrité

3.2.3. Module filtrage des paquets

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)[15]. 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. D'où la nécessité d'avoir un module de filtrage des paquets entrants pour maîtriser et connaître (analyser) 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 [12] et ceux émanant de source inconnu (filtrage basé adresse, basé scénario). Et l'émission d'une alerte à l'utilisateur 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'attaque complexes (liée à l'utilisation de services web, FTP, SMTP,…).

Dès la capture d'un paquet, ce module procède à son analyse sur les paquets 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 par l'agent interface utilisateur.
- Attaque par déni de services (SYNFLOODING); 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 [12] (port source ou destination nul, bit SYN positionné contenant des données, bits SYN et FIN positionnés, URL dépassant 4KO,…).

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.

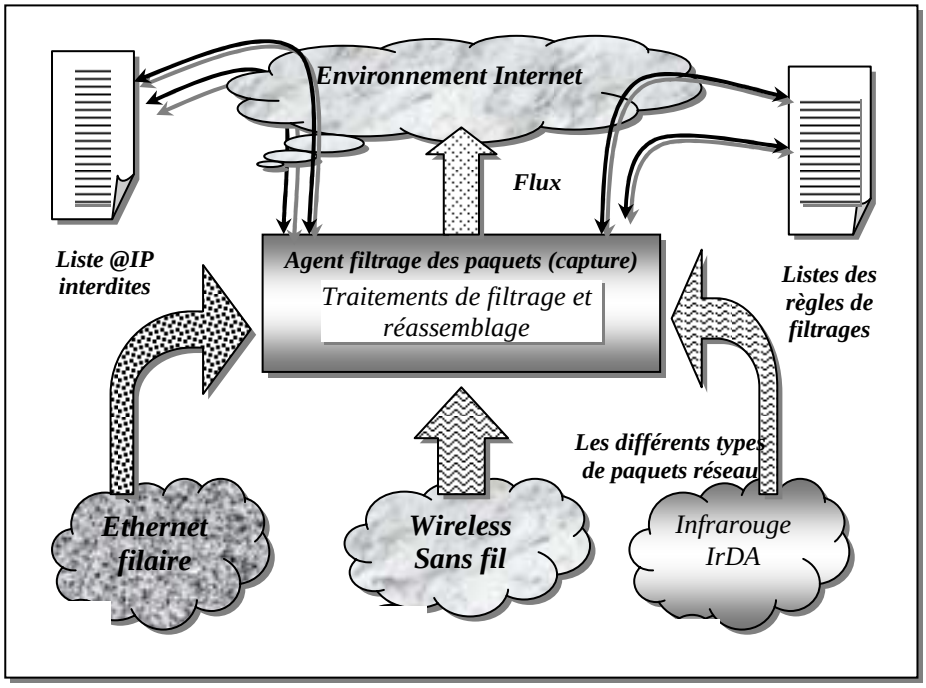


Figure 4 -Module filtrage des paquets

3.2.4. Module surveillance des ports

Le scannage des ports [13] 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.

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 d'intégrité*) 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 listé 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).Ce module agit périodiquement ou à la demande d'un autre module; il peut fermer les ports malsains à la demande en émettant des paquets FIN.

3.2.5. Module Accès 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 (IDS) 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.

3.2.6. Module Cryptage/Décryptage de la 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 à clé publique [17] comme deuxième couche de protection. Ceci est motivé par le fait que la liaison sans fil est l'une des plus faibles supports, et l'une des plus difficile à protéger (physiquement) [20]. Sachant que dans un environnement de société, la confidentialité des données transmises est cruciale. Notre protocole de cryptage est conçu en exploitant les possibilités de la CryptoAPI [15].

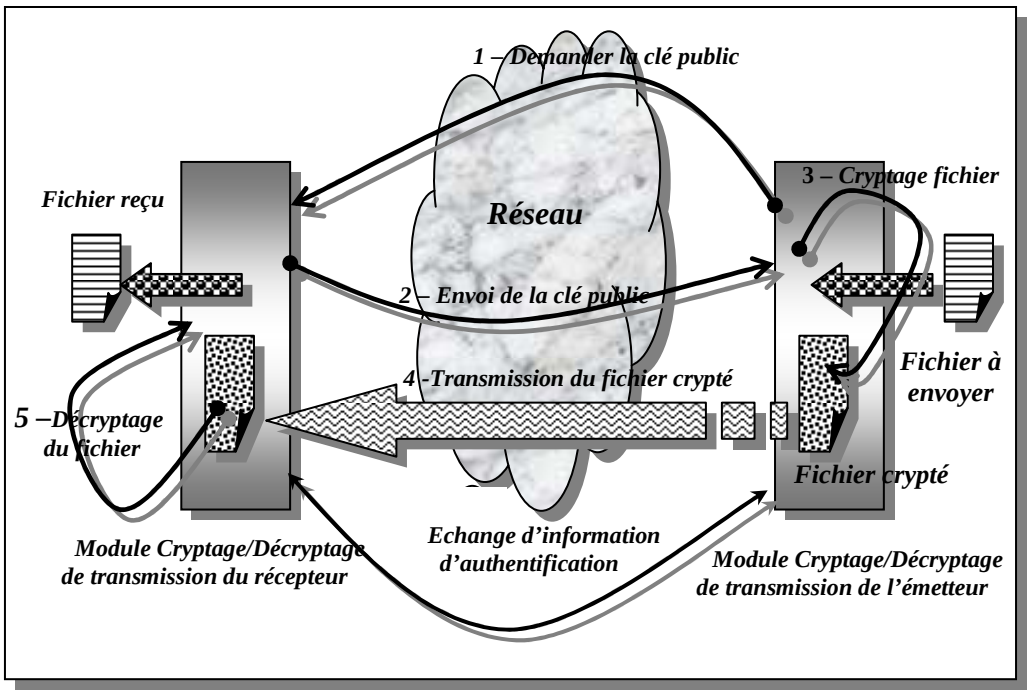


Figure 5 -Module Cryptage/Décryptage de la transmission

Ce module offre à l'utilisateur d'envoyer des fichiers, ou d'établir une communication sécurisée. Après que l'utilisateur ait choisi le fichier à envoyer et sa destination; il se connecte à la destination pour amener la clé publique de cryptage du fichier spécifié. Ensuite, il se reconnecte sur un deuxième canal 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.

REMARQUE. — 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 elle exige que les ports soient alignés et rapprochés.

3.2.7. Module moniteur de comportement

Comme les terminaux mobiles (Pocket PC) sont personnels, le profil utilisateur est unique et représente un moyen efficace pour l'authentification du propriétaire. Il est implémenté en constituant le profil du propriétaire par des informations de base collectées à l'installation de l'IDS en collaboration avec le module Accès initial. Ensuite, il récolte de nouvelles données en auditant le système et l'utilisateur, cela tout en faisant des calculs statistiques périodiquement pour avoir la variation du profil courant par rapport au profil initial. Ceci est fait en déterminant des variables aléatoires telles que le temps d'utilisation CPU, le temps de connexion à quelques ports spéciaux, applications utilisées. 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. Et donc périodiquement de nouvelles valeurs sont calculées pour avoir les nouvelles moyennes aux quelles sont comparées les variances statistiques des valeurs précédentes. Le franchissement du seuil de variance permet de déclencher une alerte vers le module *Accès initial* afin qu'il procède à l'authentification de l'utilisateur. Toutes les informations récoltées sont stockées dans une base de données du profil. Ce module interagit avec d'autres modules: module Accès aux fichiers, module Surveillance des ports, …).

3.2.8. Module Accès aux 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 les droits d'accès à ce fichier et authentifier donc celui qui veut y accéder en collaboration avec l'agent comportemental.

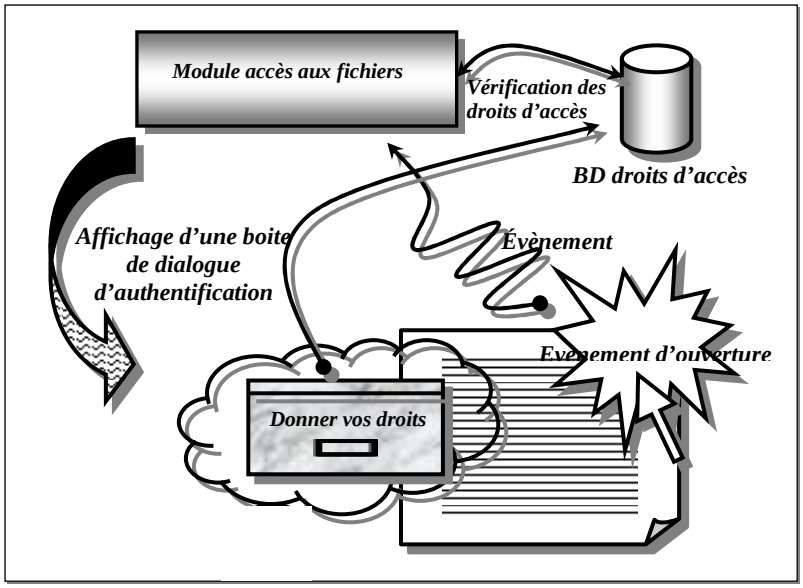


Figure 5 -Module accès aux fichiers

Contribution à la sécurité du PDA (EIDS)

Si la procédure de vérification des permissions réussit le fichier est décrypté et est ouvert à l'utilisateur. Ce module permet de protéger les données confidentielles et les fichiers système critiques (et surtout les fichiers de notre IDS).

3.2.9. 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.

4. Perspectives, Travaux en cours & Conclusion

EIDS est un système modulaire, chaque module peut être implémenté comme *Agent Mobile* sur des plateformes appropriées (FIPA, AGLET, AGENTA, MADKIT)[22] afin de bénéficier de la puissance de leurs mobilité et d'étendre la solution pour la sécurisation d'un réseau (filaire, Wireless), et ou on ajoutera des modules superviseurs chargés de l'extraction et de la collecte des informations sur tous le réseau ainsi que la coordination; ou comme *Composant* pour pouvoir adapter chaque composant selon les besoins spécifiques des entreprises suivant leurs politiques de sécurité.

En perspective et afin d'augmenter la sécurité propre de ce système, il est utile de doter les différents modules d'interfaces de communication inter-module *dynamique* à protocole d'authentification qui permettra d'éviter les cas d'attaque du système par déguisement (se faire prendre pour un module du système). Par ailleurs, dans le cas des réseaux sans fils (ad hoc, cellulaire) l'exploitation des informations de localisation permet au module comportemental (par le principe du profil spatial-géographique) de suspecter les cas de vols de terminaux.

Les travaux en cours portent essentiellement sur le perfectionnement 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.

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. D'autre part, la mobilité du code peut être vue comme une extension de notre système afin d'aboutir à un IDS qui contrôle l'ensemble du réseau. 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)[1] au même titre que le changement périodique de brosse à dents.

5. Références

[1] *State of Practice of Intrusion Detection Technologies*, J. Allen, A. Christie, W. Fithen, J. Mackhugh, J. Pickel, *Ed. Stoner Carnegie Mellon University*,2000 (http://www.sel.cmu.edu/publication/pubweb.html)

[2] *Sécurité Optimale*, Anonyme hacker, *CAMPUS PRESS*, 1999.

[3] *Your 802.11 Wireless Network has no Clothes*, W. Arbaugh, N. Shankar, Y. Wan, 30 March 2001, (http://www.cs.umd.edu/~waa/wireless.php,)

[4] *La sécurité ce n'est pas du bricolage*, J.L Archimbaud, 2001, (www.cnrs.fr).

[5] *Research in intrusion detection systems: a survey*, S. Axelsson, 1999, (www.guill.net/securite/),

[6] *An introduction to detection & assessment*, R. Bace, 2000, (www.icsa.net).

[7] *Contribution à la détection d'intrus*, A. Belkhir, A. Belkhirat, M. Adda, F. Guerrout, *Conférence maghrébine 7th MCSEAI*, pp 43-48, mai 2002.

[8] *Réseaux locaux sans fil: Aussi dangereux que séduisants*, C. Claveleira, *Revue de sécurité informatique CNRS*, N°40, Juin 2002.

[9] *Les systèmes de détection d'intrusion*, J.S. Balasubramaniyan, J.O. Garcia-Frenandez, D. Isacoff, E. Spafford, D. Zamboni, 2000, (www.gui.net/securite/ids.htm).

[10] *Les systèmes de détection d'intrusion*, E. Doceux, 2001, (http://guill.net /securite/ids.htm).

[11] *Les systèmes intelligents vers une intelligence collective*, J. Ferber, *Inter Editions Paris* 1995.

[12] *IP abnormal packets*, K. Frederick, 2000, (www.securityfocus/frames/?focus=ids&content=/focus/ids/articles/abnormal1.html).

[13] *The art of scanning ports*, I. Fyodor, 2000, (www.nmap.com/the_art_of_scanning_port.html).

[14] *Wireless LAN access Network for Mobile Operator*, A. Laurila, J. Mikkanen, J. Rinemaa, *IEEE Communications Magazine*, pp82-89, November 2001.

[15] *Inside Microsoft Windows CE*, J. Murray, *Microsoft Press*, 1998.

[16] *Introduction and basic concepts on the architecture*, Net group sec, polytechnic de torino (Italt), 2001, (netgroup-secu.polito.it/Introduction_and_basic_concepts_on_the_architecture.htm),

[17] *Cryptographie appliquée, protocoles algorithmes et codes sources*, B. Schneier, *International Thompson Publishing*, 1994.

[18] *Modern Operating Systems*, A.S. Tanenbaum, *Prentice Hall, Second Edition*, 2001.

[19] *Sécurité des réseaux sans fil*, P. Urien, *Revue de sécurité informatique CNRS*, N°40, Juin 2002.

[20] *Unsafe at any key size: an analysis of the WEP encapsulation*, J.Walker, *Tech Rep 03628E, IEEE 802.11 committee*, March 2000.

[21] *Towards a Taxonomy of Intrusion Detection Systems*, A. Wespi, M. Dacier, H. Debar, *Computer Networks* 31, pages 805-822, 1999.

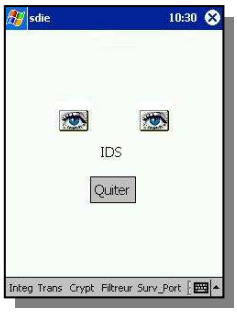
[22] *FIPA: The Foundation of Intelligent Physical Agents*, Fipa Organisation, 2002, (www.fipa.org).

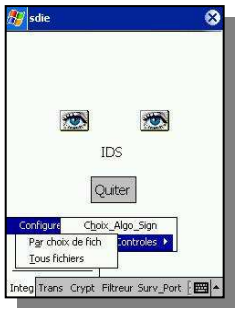
Annexe

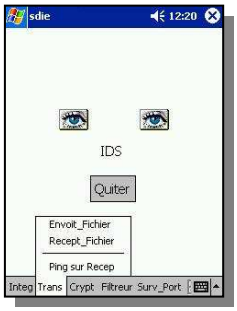
En voici des scénarios et des captures d'écran montrant notre EIDS en actions:

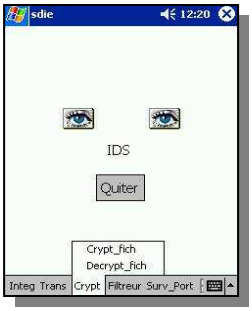
1. Module Interface Utilisateur:

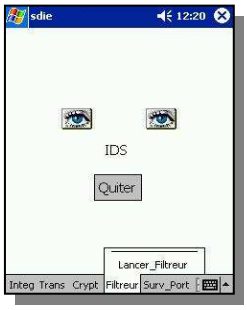
C'est le module qui permet l'accès et l'administration ou la configuration de tous les autres modules;



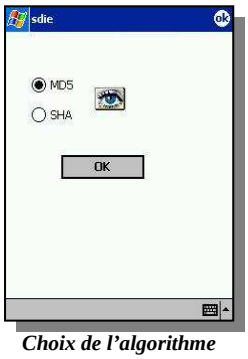






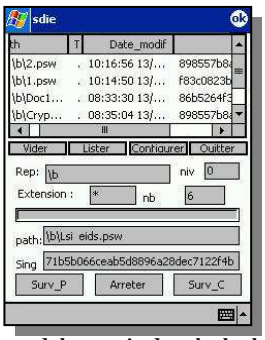


2. *Module Contrôleur d'intégrité & Accès Fichiers:*

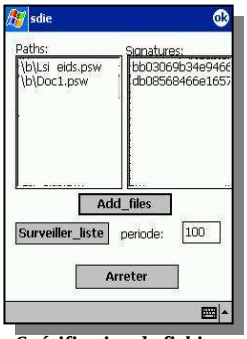


Choix de l'algorithme de signature

On précise un niveau de protection



Le module entrain de calculer les signatures de tous les fichiers



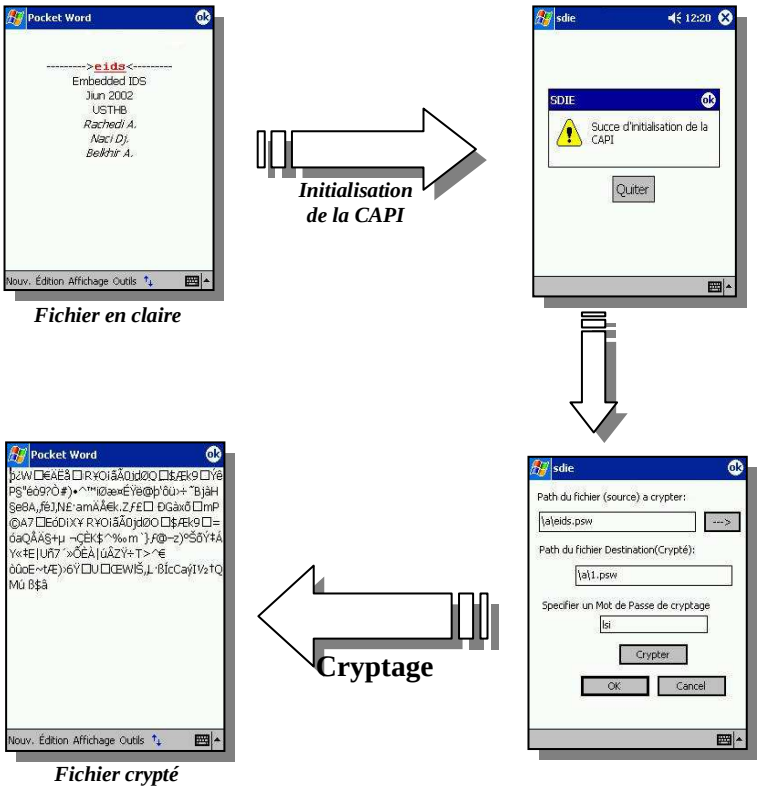
Spécification de fichiers personnel à surveiller

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

Un fichier log est généré avec tous les informations utiles

3. *Module Cryptage/Décryptage:*

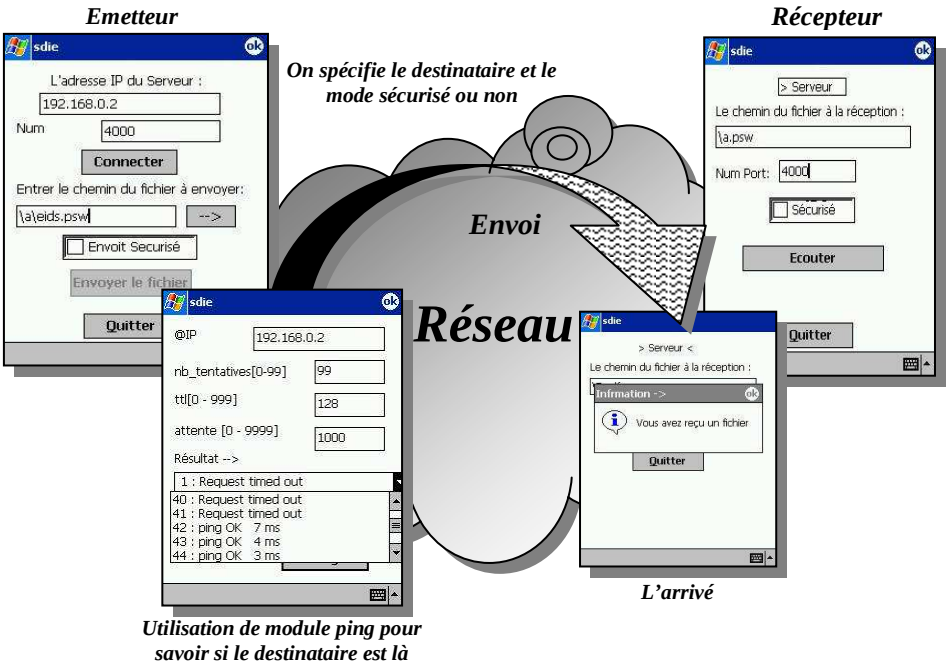
Voici un exemple du module cryptage/Décryptage.



Fichier en claire

Fichier crypté

4. Module Transfert fichier(& ping):

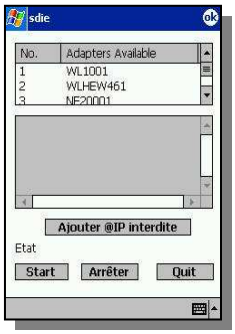


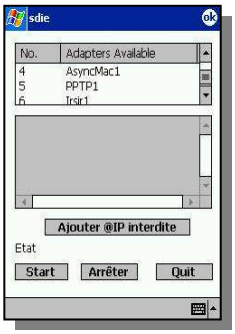
Utilisation de module ping pour savoir si le destinataire est là

L'arrivé

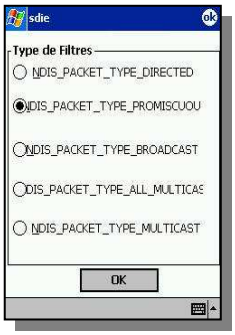
5. *Module Filtrage de Paquets:*

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

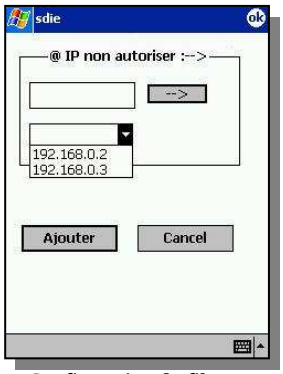




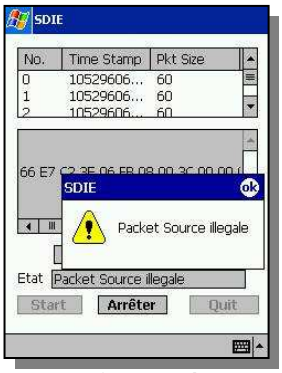
Choix de l'adaptateur (le port à filtrer: IrDA, WiFi, Ethernet, Async ;…)



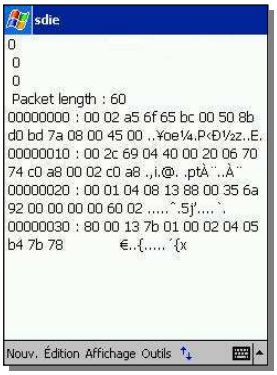
Choix du mode de filtrage



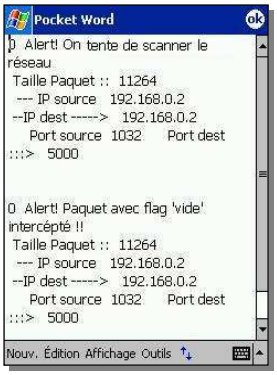
Configuration du filtrage basé adresse IP



Capture& filtrage. Détection de paquet de source illégale



Fichier historique du flux



Un fichier log est généré contenant les différents alertes du filtreur