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.