Sécurisation de l'environnement mobile

Combinaison du Framework MPSS et le Firewall ALSD

Securing mobile environment Combination of MPSS Framework with ALSD Firewall

Najim Ammari[1], Norelislam El Hami[2], Almokhtar Ait El Mrabti[1], Anas Abou El Kalam[1], Abdellah Ait Ouahman[1]

[1] Laboratoire OSCARS, Ecole nationale des sciences appliquées Marrakech, université Cadi Ayyad, Maroc, najim.ammari@gmail.com, mokhtarmrabti@gmail.com, elkalam@hotmail.fr, aitouahman@yahoo.fr
[2] Ecole nationale des sciences appliquées Kenitra, université Ibn Toufail, Maroc, norelislam@outlook.com

RÉSUMÉ. L'objectif principale de cette étude est la définition d'une politique globale pour sécuriser l'environnement mobile, par la mise en place des procédures et des mécanismes de sécurités et de protection des dispositifs mobiles qui répondent mieux aux attentes des utilisateurs, que ce soit au niveau du trafic dans les réseaux mobiles, ou bien au niveaux des applications mobiles.
Au niveau réseaux mobiles : L'étude s'intéresse principalement à limiter la propagation des malwares via SMS / MMS et e-mails. Il décrit les étapes menant à identifier, analyser et sécuriser le trafic dans les réseaux mobiles. A cet effet, un Framework MPSS (Mobile Phone Security Scheme) a été utilisé pour faire partie de l'infrastructure de l'opérateur télécom du réseau mobile. MPSS vise à augmenter le niveau de sécurité de l'information à travers le réseau de l'opérateur télécom et résoudre les problèmes liés aux ressources limitées sur les appareils mobiles.
Au niveau des applications mobiles : L'étude propose un Firewall ALSD (Anti-Leak of Sensitive Data), permettant une protection fiable contre les fuites des données personnelles et professionnelles sensibles sur les dispositifs mobiles, ainsi il permet de notifier l'utilisateur. Cette solution intégrée au système d'exploitation mobile repose sur une analyse automatisée des applications mobiles du store des plateformes mobiles (Play Store, App Store …) ; Ce firewall permet de contrôler et de bloquer les requêtes malveillantes sur les données sensibles existantes dans le dispositif mobile tout en assurant le bon fonctionnement des applications installées sur le mobile.
ABSTRACT. The main objective of this study is to definite a global policy to secure the mobile environment, by setting up procedures and mechanisms for the security and protection of mobile devices Which meets the user's needs, whether in terms of mobile networks traffic or at mobile applications level.
At mobile networks level: The study focuses on limiting the malware spread via SMS, MMS and emails. It describes the steps involved identifying, analyzing and securing mobile network traffic. To this effect, the MPSS Framework (Mobile Phone Security Scheme) has been used to be part of the mobile telecom operator's infrastructure. MPSS aims to increase the level of information security through the telecom operator's network and to solve problems related to limited resources on mobile devices.
At the mobile applications level: The study proposes the ALSD Firewall (Anti-Leak of Sensitive Data), allowing reliable protection against leakage of sensitive personal and professional data on mobile devices, thus notifying the user. This solution, integrated into the mobile OS, is based on the mobile applications automated analysis of the mobile platform store (Play Store, App Store ...); This firewall allows control and block malicious requests on sensitive data while ensuring the proper functioning of the applications installed on the mobile.
MOTS-CLÉS. Sécurité mobile, propagation des malwares via SMS/MMS, sécurité des données sensibles, applications mobiles, Firewall ALSD, Framework MPSS, Android OS.
KEYWORDS. Mobile security, malware propagation via SMS / MMS, sensitive data security, mobile applications, ALSD firewall, MPSS framework, Android OS.

1. Introduction

Avec l'évolution des téléphones mobiles utilisables n'importe où, leur nombre a considérablement augmenté au cours de ces dernières années, en plus d'une tendance croissante de fonctionnalités et de performances couplés avec la croissance rapide de nombre d'applications mobiles. En l'absence quasi totale de mécanismes et de solutions de sécurité dans la plupart de ces installations en plus des problèmes liés aux ressources matérielles limités (processeur, RAM et batterie) et des logiciels (Faiblesses au

niveau systèmes d'exploitation et des problèmes de sécurité d'applications mobiles), à cet égard, la plupart des risques sont semblables à ceux des chevaux de Troie, aux traditionnel spyware, et à celle des applications conçues non sécurisée exposant la vie privé des utilisateurs au divulgation. Le dispositif mobile est exposé aux menaces liées à un risque accru dans un monde où l'appareil mobile devient une cible facile pour différentes attaques : les menaces et les attaques ciblant les appareils mobiles ont augmenté de 614% en un an et le nombre de logiciels malveillants a augmenté, passant de 38 689 à 276 259 en un an [1].

Face à ces défis, de nombreux efforts ont été consacrés à la sécurité de ces appareils mobiles en raison de la complexité des problèmes de sécurité et leur importance dans la vie personnelle et le monde des affaires.

Ce travail vise à élaborer dans un premier temps un nouveau Framework pour limiter la propagation de logiciels malveillants via SMS / MMS et emails dans trafic réseau de l'opérateur. Dans un deuxième temps ce travail vise à concevoir un firewall destiné aux dispositifs mobiles nommé Firewall Anti-Leak of Sensitive Data (ALSD) afin de protéger les données personnelles et professionnelles. Ce firewall est intégré au système d'exploitation mobile, basé sur l'analyse automatisée des applications du store qui présente l'emplacement de toutes les applications existantes sur le marché des applications mobiles. Ce firewall permet de contrôler et bloquer les requêtes malveillantes sur les données sensibles existantes dans le mobile tout en assurant le bon fonctionnement de l'application en question.

Notre contribution consiste aussi à combiné ces deux composants pour assurer une sécurité forte de l'environnement mobile que ce soit au niveau trafic réseau ou bien au niveau applicatif.

2. Framework Mobile Phone Security Scheme (MPSS)

La majorité des études publiées dans le domaine de la propagation des logiciels malveillants [2,3,4,5] ont mis l'accent sur l'analyse des virus et des vers se propageant par messagerie. Cependant, très peu de travaux [6,7] ont présenté une solution homogène et complète pour minimiser les risques de cette prorogation.

Notre principale motivation est donc d'y remédier en proposant une solution globale et homogène qui permet de limiter l'impact de la propagation des logiciels malveillants par SMS/MMS et par messagerie email et ce malgré les limitations technologiques des appareils mobiles.

Afin de limiter les impacts des logiciels malveillants et compte tenu des difficultés d'appréhension de la problématique de la propagation, nous proposons le Framework Mobile Phone Security Scheme MPSS qui relate le cadre d'application de notre solution et décrit les étapes à mettre en œuvre.

Pour assurer la sécurité de l'appareil mobile, le Framework MPSS propose une solution de sécurité installée, dans sa globalité, dans le réseau local de l'opérateur télécom.

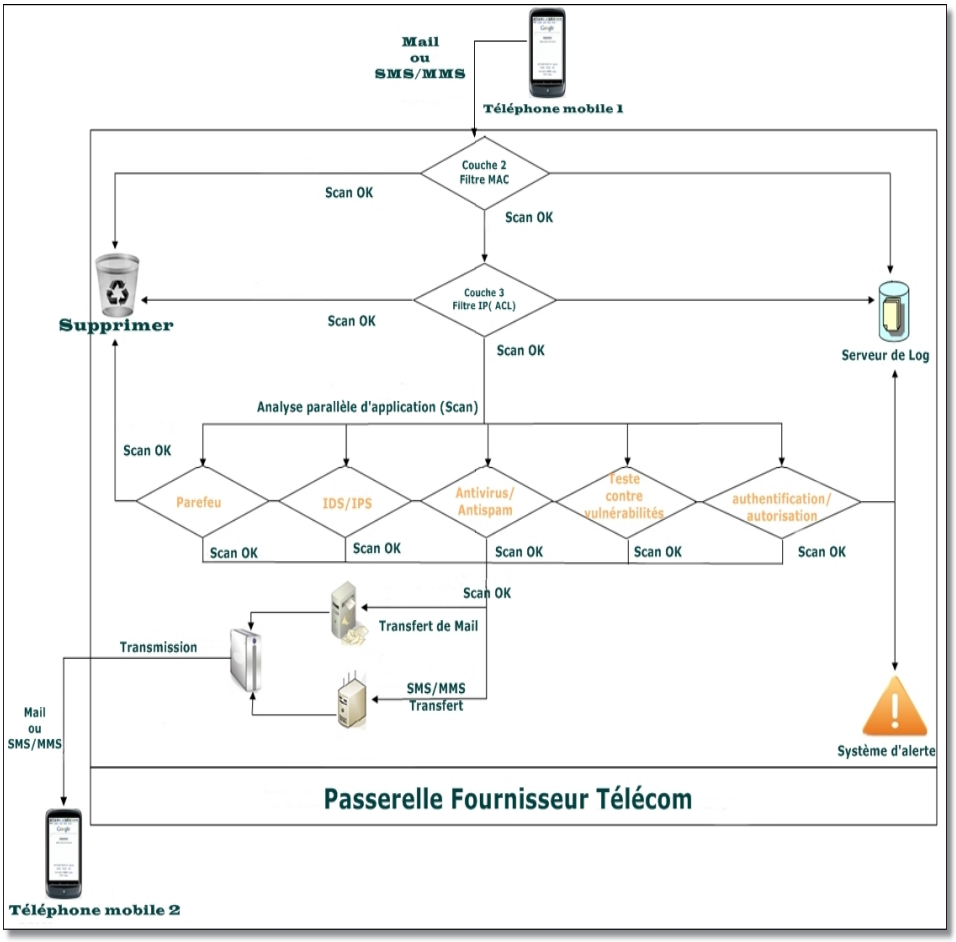

Figure 2.1. *Mode de fonctionnement du Framework MPSS*

De ce fait, l'ensemble des données (courrier, SMS/MMS, données internet...) peuvent être analysées et désinfectées à l'intérieur de cette passerelle constitué par l'opérateur mobile, en utilisant son module de sécurité composé de firewall, d'anti-malware et des IDS/IPS [8]. Toutes ces données peuvent être traitées et désinfectées à l'intérieur de la passerelle du même fournisseur mobile, en se basant sur son infrastructure de sécurité.

Ce passage obligé par la plateforme de l'opérateur télécom nous aidera à bloquer toute diffusion ou propagation des malwares entre deux appareils mobiles, car même dans le cas d'une infection de l'appareil, les malwares seront désinfectés lors du premier passage au niveau de la passerelle de l'opérateur.

Pour une meilleure efficacité, cette solution doit être mutualisée entre deux opérateurs télécoms (ou même plus) afin de bloquer toute propagation de programmes malveillants entre les réseaux de ces deux opérateurs.

La passerelle de sécurité de chaque fournisseur de service mobile contiendra tous les éléments de sécurité nécessaires (pare-feu redondants, antivirus, anti-spam, anti-malware, système anti-intrusion, outil de test de vulnérabilités, reverse proxy, serveur VPN...) pour bloquer la propagation des programmes malveillants entre les réseaux de ces opérateurs.

Le schéma suivant décrit le mode de fonctionnement du Framework MPSS une fois implémenté au niveau du réseau LAN de l'opérateur de télécom :

Quand un utilisateur d'un téléphone mobile 1 envoie un SMS/MMS (ou l'e-mail) à un utilisateur d'un téléphone mobile 2, la passerelle de l'opérateur effectue les trois tests suivants :

1. Scan au niveau de la couche 2 : si l'adresse MAC de l'appareil l'émetteur est autorisée à ce niveau, la trame se déplace à l'étape suivante. Sinon, la trame sera abandonnée et un message d'alerte sera envoyé au serveur log par une alarme SNMP pour assurer la fonction de la traçabilité.

2. Scan au niveau de la couche 3 : à ce niveau, seuls les paquets des mobiles dont les adresses IP ne sont pas interdites par le firewall de la passerelle peuvent être sont traités. Ce filtre basé sur les access-lists (ACL) permet le blocage des paquets au niveau de la couche réseau, avant qu'ils soient routés.

3. Une fois les données sont validées par ces deux scans, elles passeront à la phase de l'analyse applicative. Une analyse en parallèle sera effectuée par le firewall, l'anti-malware, l'IPS et le serveur d'authentification. Le but de ce scan en parallèle (au niveau de la couche 7 du modèle OSI) est de réduire le temps de scan et par conséquent minimiser la latence globale. Dans cette phase, un système d'avertissement et de notification informe l'utilisateur de la détection d'un problème ou incident de sécurité.

Après avoir réussi ces trois niveaux d'analyses, le SMS/MMS (ou l'e-mail) sera accepté pour être livré au serveur SMS/MMS (ou au serveur de messagerie), puis transmis à l'appareil mobile de destination.

Ainsi, l'utilisation de cette solution centrale basée sur l'offre de service de l'opérateur télécom permet d'assurer une autonomie et une protection optimale pour les utilisateurs de téléphones mobiles sans grand effort ou investissement de leur côté.

Notons que cette analyse sera effectuée par le fournisseur d'accès à tous ses abonnés avec un délai optimisé de deux façons :

1. Une analyse manuelle demandée par l'utilisateur en invoquant un service en ligne de son fournisseur.

2. Un scan/désinfection automatique à l'aide de la solution de sécurité centralisée basée sur la plateforme de l'opérateur à chaque passage par réseau.

3. Firewall ALSD

Au troisième trimestre de 2015, les ventes mondiales des smartphones ont atteint 355,2 millions soit une hausse de 6,8% [9], les smartphones équipés des systèmes Android représentent 81,2% [10], les Appareils Android ont gagné une énorme part de marché en raison de l'architecture ouverte d'Android,

et la popularité de son API de développement. Le succès de cette plateforme est accompagné avec une forte hausse des logiciels malveillants les applications Android, ce qui fait que notre solution sera destinée principalement à la plateforme mobile Android.

Android a mis en place un modèle de sécurité très simple, il est basé sur le principe qu'une application ne peut accéder qu'aux seules ressources expressément autorisées par l'utilisateur, ce model délègue à l'utilisateur la prise de décision d'accepter ou non une application potentiellement malveillante, et d'assumer tous la responsabilité.

L'article « solution d'analyse automatisée de markets Android » [11] propose des informations relatives à l'impact des applications sur le dispositif mobile, stockés sur une base de donnés distribuée, et résulte d'une analyse statique et dynamique de tous les applications du Play Store d'Android (figure 3.1). Les utilisateurs prennent leur décision d'accorder des permissions ou non à une application donnée en se basant sur ces informations, notre contribution consiste à automatiser cette opération « la prise de décision est faite par notre firewall ALSD au lieu de l'utilisateur »

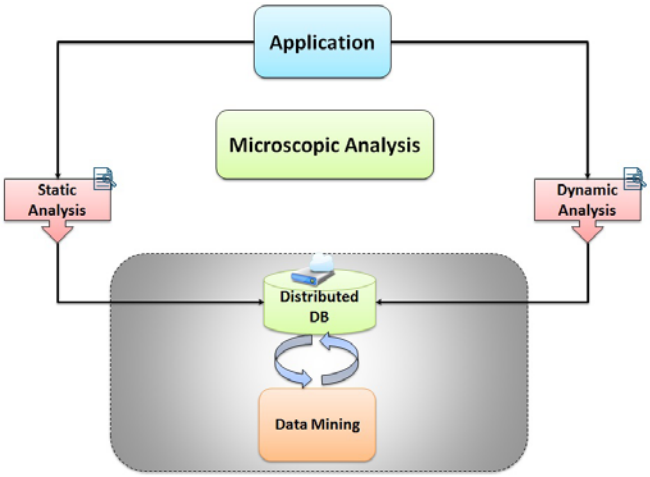

Figure 3.1. *Les étapes d'analyse par Hooker*

Cette partie représente une étude théorique sur la modélisation du firewall ALSD, et la démarche pour l'intégrer dans le système d'exploitation Android.

3.1. *Conception du Firewall ALSD*

Malgré toute la pertinence et la précision des permissions disponibles pour l'utilisateur avant d'installer n'importe quelle application, elles ne répondent pas aux problèmes liés aux risques de sécurité qui se posent avant d'accepter l'installation ou non d'une application. Les questions les plus importantes sont les suivantes : Qu'est-ce qui prouve que cette application n'utilise pas ces permissions pour exfiltrer les données sensibles sur un serveur distant ? Que fait cette application avec les ressources auxquelles elle a demandé des autorisations d'accès ? Va-t-il abuser de ces autorisations ?

Pour répondre à ces questions, nous avons mis en place un firewall appelé ALSD (Anti-Leak of Sensitive Data) qui prend en charge la surveillance et la protection des données sensibles. Ce firewall utilisera les résultats des analyses effectuées par le système Hooker [11] :

- Analyse statique basée sur l'étude du code source de l'application et inversement ;
- Analyse dynamique basée sur l'étude de l'application au cours de son exécution.

Le firewall ALSD doit être implanté dans le système d'exploitation Android (voir figure 3.2). Il doit avoir un impact minimum sur les performances du système et reste transparent pour l'utilisateur et les applications même si leurs requêtes sont interceptées.

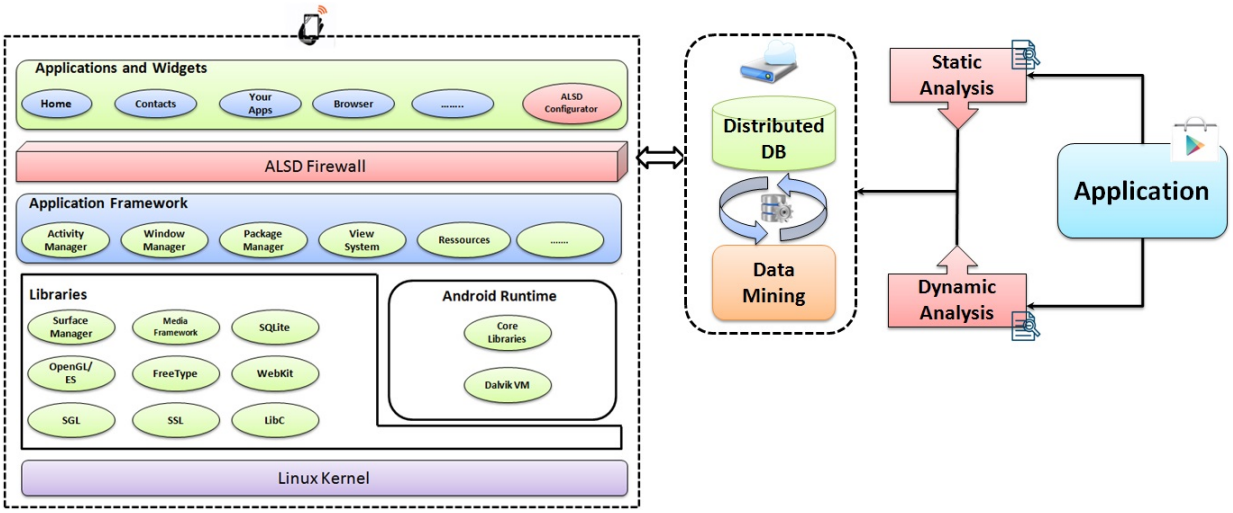

Figure 3.2. *OS Android avec le Firewall ALSD*

Pour garantir l'aspect temps réel de notre solution, nous devons modifier chaque manager qui permet à une application d'accéder aux données du système. Le grand inconvénient de cette solution est que nous éditons chaque partie du Framework qui permet l'accès aux données. Cette approche implique la création d'un composant spécial qui joue le rôle d'un manager appelé ALSD Firewall qui sera responsable des décisions concernant les données sensibles. Ce composant est implémenté comme un module du système Android qui sera lancé au démarrage du téléphone pour inclure son temps de chargement au temps globale de démarrage. Ce composant interagira avec la base distribuée Hooker [11] en utilisant un mode de requêtes à distance basé sur HTTPS. De plus, ALSD Firewall implémente l'algorithme présenté dans la figure ci-dessous.

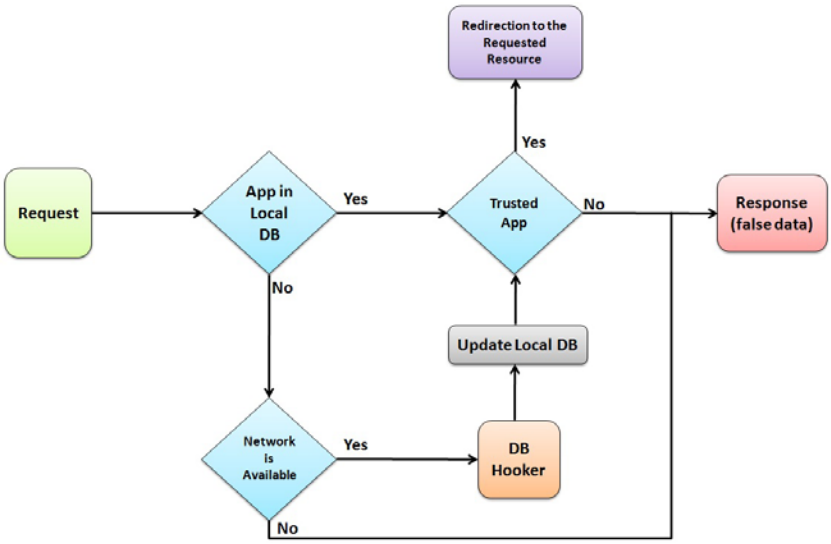

Figure 3.3. *Algorithme du Firewall ALSD*

Différents managers doivent être modifiés pour utiliser notre manager système ALSD pour permettre l'interception de toutes les requêtes. Prenant l'exemple d'interception des requêtes liées aux contacts, une application qui souhaite obtenir les registres d'informations de contact avec le provider Contacts-ContentProvider utilisé comme Singleton. Pour intercepter la requête, le ContactsContentProvider doit être modifié pour appeler notre composant ALSD avant de fournir une réponse. L'ALSD prendra une décision pour autoriser ou non l'accès aux contacts suivant les informations fournies par le système Hooker [11] sur l'application demandant l'accès aux contacts. Si la requête est refusée par ALSD, des fausses données de contact seront retournées à l'application pour assurer son fonctionnement normal, en utilisant le principe de withholding data [12]. ALSD utilisera le nom du package pour identifier chaque application afin de permettre une sécurité plus fine.

4. Conclusion

Notre travail est centralisé autour de l'étude des mécanismes de sécurité et de protection de l'environnement mobile ; dans le trafic réseau et au niveau applicatif par la sécurisation de la vie privée des utilisateurs des dispositifs mobiles.

Nous avons proposé une approche fondée sur l'infrastructure réseau du fournisseur mobile, pour remédier aux risques de sécurité SMS / MMS. Un nouveau Framework MPSS a été proposé et mis en œuvre dans le réseau de l'opérateur télécom.

Dans cet article, nous avons également présenté l'architecture générale du firewall ALSD, et la démarche son intégration dans un système d'exploitation mobile en se basant sur la plate-forme Android. Il offre une protection renforcée de la vie privée des utilisateurs. Ce firewall exploite les informations fournies par le système Hooker sur le degré d'impact d'une application sur le mobile.

La combinaison du Framework MPSS et firewall ALSD garanti une sécurité globale forte de l'environnement mobile tout entier.

Une étude devrait être menée sur les performances du firewall ALSD et le degré de son impact sur le système d'exploitation mobile.

Bibliographie

[1] Rapport de la société d'investissement KPCB : "Top 10 Mobile Internet Trends" : http://www.terminauxalternatifs.fr/, 2011.

[2] LAURENT BUTTI., Evolution de la propagation des malwares. Sécurité Informatique, 61, October 2007.

[3] MOORE D., SHANNON C., BROWN J., Code-red: a case study on the spread and victims of an internet worm. In ACM Internet Measurement Workshop, 2002.

[4] YONG LI., PAN HUI., DEPENG JIN., LI SU., LIEGUANG ZENG., "An Optimal Distributed Malware Defense System for Mobile Networks with Heterogeneous Devices"; Mesh and Ad Hoc Communications and Networks (SECON), 2011 8th Annual IEEE Communications Society Conference, p. 314 – 32, 2011.

[5] LIANG CAI., SRIDHAR MACHIRAJU., HAO CHEN., Defending against sensor-sniffing attacks on mobile phones, Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds, August 17-17, Barcelona, Spain, 2009.

[6] PAUL BARFORD., VINOD YEGNESWARAN., An Inside Look at Botnets.Special Workshop on Malware Detection, Advances in Information Security, 2006.

[7] LLOYD BRIDGES., The changing face of malware.Network Security, 1:17–20, January 2008.

[8] MOHAMED GHALLALI., "Mobile phones security: the spread of malware via MMS and Bluetooth, prevention methods. MoMM 2011: 256-259, Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia.

[9] CHIFFRES CLES., les ventes de mobiles et de smartphones, 2015, http://www.zdnet.fr/actualites/chiffres-cles-les-ventes-de-mobiles-et-de-smartphones-39789928.htm.

[10] CHIFFRES CLES., les OS pour smartphones, 2015, http://www.zdnet.fr/actualites/chiffres-cles-les-os-poursmartphones-39790245.htm

[11] VINCENT J., DUBIN T., PORQUE C., "Protection de la vie privée basée sur des ontologies dans un système Android". APVP 2012 (Atelier Protection de la Vie Privée, 3 eme edition), Ile de Groix, France, Jun 2012.

[12] HORNYACK P., HAN S., JUNG J., SCHECHTER S., WETHERALL D., These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In Proceedings of the 18th ACM conference on Computer and communications security, p. 639–652. ACM, 2011.