République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Larbi Tébessi

Faculté des sciences exactes et sciences de la nature et de la vie

Département des mathématiques et de l'informatique

Mémoire de Master

Filière : Mathématiques/Informatique

Option : Réseaux et sécurité informatique

Thème

Sécurité D'appareils Mobiles

Présenté par : - FOUDIL NOUREDDINE
- NOUIRI FADI

Encadré par : MEKHAZNIA TAHAR

Promotion : Mai/2017

Jury de soutenance :

Président :	MENASSEL YAHIA	M.A.B	Université de Tébessa
Encadreur :	MKHAZNIA TAHER	M.C.A	Université de Tébessa
Examinateur :	AZZEDINE ABDELGAFOUR	M.A.A	Université de Tébessa

Promotion : 2016 – 2017

REMERCIEMENTS

Je remercie tout d'abord Dieu tout puissant, pour nous avoir guidés et éclairés sur la bonne voie du savoir afin d'avoir élaboré ce travail et atteindre les objectifs à atteindre.

Je remercie tous ceux qui, pour leurs encouragements, leur aide intellectuelle et matérielle, leurs conseils et leurs critiques, avoir contribué à la réalisation de ce travail.

Je tiens à remercier très fort Monsieur ***MEKHAZNIA TAHAR*** *de m'avoir assistée et guidée.*

Mes remerciements s'adressent également à mes jurys qui feront l'honneur d'évaluer notre travail

Dédicace

Je dédie ce modeste travail

A mes chers parents
Qui m'ont éclairé mon chemin et qui m'ont encouragé et soutenue toute au long de mes études.

A Ma grande mère
Elle m'a apporté de l'encourage tout le temps

A mes deux sœurAmani et Tasnim

A mon encadreur Mekhaznia Tahar
Qui ma guider et diriger tout au long de l'année scolaire.

A mon binôme foudil
Qu'ont à passer ensemble le meilleur et le mauvais, le facile et surtoutle difficile de notre projet.

A tous mes camarades de notre département.

A tous mes enseignants
Que je leur remercie a tous ses efforts.

Résumé

Titre : Sécurité des appareils mobiles

L'évolution et la nécessité des médias et des services mobiles et le besoin croissant de services numériques pour accomplir des tâches ont poussé vers l'utilisation des appareils mobiles. Les appareils mobiles sont souvent portables et équipés d'un écran tactile et utilisent un système d'exploitation selon le fabricant. Pour exécuter des applications, des jeux, et lire des films et des fichiers musicaux, ainsi de sauvegarder des diverses informations.

La malveillance au contexte de la mobilité liée à la performance des appareils mobiles, à mener à un problème de sécurité .dans ce mémoire nous intéressons à détailler les architectures de réseaux mobiles et les différents systèmes d'exploitations de mobiles, ainsi que les attaques aux mobiles.

Par la suite, on va effectuer une étude sur ces attaques, qui sont extrêmement difficiles à détecter par des techniques ordinaires, plus précisément le comportement des menaces et leurs scenarios dans l'environnement mobile. comment assurer la sécurité et la fiabilité de communication. C'est dans ce sens qu'on va présenter un état de l'art de sécurité des appareils mobile et le problème lié à la couverture réseau, ainsi qu'on va définir les différentes attaques et leur caractéristique en effectuant une étude comparative pour déterminer la méthode optimale de la sécurité mobile.

Mots clé : appareil mobile, sécurité, attaques, communication.

ABSTRACT

Title: Mobile Network security

The Evolution and the need for media and mobile services and the growing need for digital services for tasks led to the use of mobile devices. Mobile devices are often portable and equipped with a touch screen and use an operating system according to the manufacturer. To run applications, games, and read the movies and music files, so to back up various information.

Maliciousness in the context of mobility related to the performance of mobile devices, to lead to a security problem. In this memory we are interested in detailing the mobile network architectures and the various mobile operating systems, as well as the mobile attacks.

Afterwards, we'll perform a study on the attacks, which are extremely difficult to detect by ordinary techniques, specifically the behavior of threats and their scenarios in the mobile environment how to ensure the security and reliability of communication. It is in this sense that we're going to present a State of mobile device security art and the problem with network coverage, as we're going to define the different attacks and their characteristic by conducting a comparative study to determine the optimal method for the mobile security.

Key words: mobile device, security, attacks, communication.

الملخص

أدى التطور والحاجة إلى وسائل الإعلام وخدمات الهاتف النقال والحاجة المتزايدة لمهام الخدمات الرقمية إلى استخدام الأجهزة النقالة وغالبا ما تكون محمولة ومجهزة مع شاشة تعمل باللمس وتستخدم نظام تشغيل مزود من طرف الصانع لتشغيل التطبيقات والألعاب وتشغيل الأفلام وملفات الموسيقى وحفظ المعلومات المختلفة.

تتعرض هذه الهواتف النقالة المتصلة بالشبكة لمجموعة واسعة من الاختراقات المتفاوتة الخطورة لذلك أصبحت وسائل الأمن ضرورة ملحة للوقاية من مختلف الهجمات.

هذه المذكرة مهتمة بتفاصيل الأجهزة النقالة وطرق حمايتها من الاختراقات.

وفي وقت لاحق، سنقوم بإجراء دراسة عن مسألة السلامة وتحديدا مشكلة التواصل بين الأجهزة النقالة و كيفية ضمان سلامة و موثوقية الاتصال. ومن هذا المنطلق سنقدم دراسة تتعلق بأمن الأجهزة النقالة المتصلة بالشبكات كما سنقوم بدراسة مجموعة من الهجمات المختلفة عن طريق إجراء مقارنة لتحديد الطريقة المثلى للحماية و تبادل المعلومات بطريقة آمنة.

كلمات دلالية : أمن ، الهاتف النقال ، الهجمات ، الاتصالات

Table des matières :

Liste des figures :

CHAPITRE I

CHAPITRE II

CHAPITRE III

CHAPITRE IV

Liste des tableaux :

Introduction générale :

La nature des moyens de subsistance des populations en constante évolution et la nécessité des médias et des services mobiles. Permet une demande croissante pour les appareils mobiles et le besoin croissant de services numériques pour accomplir des tâches. Les appareils mobiles sont carrément, portables et équipés d'un écran tactile et utilisent un système d'exploitation selon le fabricant. Pour exécuter des applications, des jeux, et lire des films et des fichiers musicaux, ainsi de sauvegarder des diverses informations.

En effet, l'efficacité des appareils mobiles est liée au développement de ses systèmes d'exploitation parallèlement aux applications mobiles, car l'utilisateur a été amené aux changements, notamment en ce qui concerne la domination au sein des nouvelles technologies. En particulier, cela concerne Smartphones, tablettes et PDA[1].
L'utilisateur est libre d'accepter ou de refuser l'application Mais en raison de sécurité, il ne peut pas modifier la liste des permissions demandées (sauf à modifier l'application et à la résigner avec sa propre clé).

Les plateformes des appareils mobiles se constituent des permissions a priori spécifiques à l'operateur, qu'il s'agit d'un circuit de distribution comme un acteur majeur qui intervient dans le marché de la mobilité. La séparation entre les acteurs (logiciels, matériels, services…….) pose un grand risque dans la sécurité des appareils mobiles.

Il identifie trois principaux risques de sécurité pour les appareils mobiles modernes, sont ; La structuration du marché de la téléphonie, les failles logicielles et les applications tierce partie.
Ce dernier risque est moins vrai dans les écosystèmes qui définissent l'iPhone et BlackBerry, dans lequel les fournisseurs de matériel et de logiciels sont identiques. Il est plus spécifique à l'écosystème Android, où le rôle de chaque acteur est bien séparé.

Généralement, l'émergence de l'Android comme célèbre dans la majorité des appareils mobiles. Parce qu'il s'agit d'un système d'exploitation ouvert et personnalisable (open source), permet aux acteurs de développement d'applications de bâtir leurs projets principalement dans Java. Un SDK [2](outils de développement) est fourni gratuitement par Google pour les trois systèmes d'exploitation majeurs (Windows, Mac OS X et Linux).

Contrairement au système d'exploitation IOS d'Apple qui est protégé et non accessible pour éviter les preuves, favorisées par les malveillants. Les malwares utilisent une variété de techniques pour attaquer les appareils mobiles, qui sont associés aux attaques dans le système de télécommunication câblé, lorsqu'ils utilisent certaines techniques uniques, mais ils sont

[1] PDA (Personal Digital Assistant) est un ordinateur de poche composé d'un processeur, de mémoire vive, d'un écran tactile et de fonctionnalités réseau dans un boîtier compact d'extrêmement petite taille.

[2] SDK est un ensemble d'outils logiciels destinés aux développeurs, facilitant le développement d'un logiciel sur une plateforme donnée.

différenciés de façon à transporter le trafic. La voie des ondes radio comme exemple dans les réseaux cellulaires (GSM, UMTS, LTE ...), wifi et bluetooth, C'est l'un des problèmes de sécurité des appareils mobiles.

Problématique :

La problématique est :

- La sécurité des voies des ondes radio est-elle encore un problème majeur dans l'établissement d'une communication sécurisée entre les appareils mobiles?
- Envisager une transmission radio qui peut augmenter le potentiel d'attaques sur les appareils mobiles.
- Devoir savoir d'une manière récurrente que la voie hertzienne et la transmission chiffrée de données, garantissent une connexion sûre entre les appareils mobiles.

Objectifs :

Les objectifs sont :

- Un état de l'art de sécurité des appareils mobiles et des problèmes de mobilité et de la couverture du réseau.
- L'étude des mécanismes de communication des appareils Mobiles et les techniques de sécurité.
- Les principaux écarts des attaques sont de définir leurs types et leurs caractéristiques ainsi que les modes de dysfonctionnement résultants de ces attaques sur des appareils mobiles avec des démonstrations.
- Etude comparative et une proposition d'une méthode optimale Pour déterminer une sécurité mobile.

Notre mémoire est organisé en Cinque chapitres :

- Chapitre I : Principe de fonctionnement et architecture des réseaux mobiles.
- Chapitre II : Puces ETSI/GSM : composants matériels et logiciels et mode de fonctionnement.
- Chapitre III : les systèmes des exploitations des appareils mobiles.
- Chapitre IV : attaques aux appareils mobiles.
- Chapitre V : synthèse et conclusion

Etat de L'art :

Le sujet de la sécurité des appareils mobiles est l'un des plus intéressants, ce qui est devenu d'un ensemble de travail, parmi ceux-ci:

Sebastien Josse :[5]

Il se démontre, la pertinence de la cryptographie boîte blanche [3]dans le contexte viral. Il a défini en outre des axes d'amélioration des implémentations boîte blanche de l'AES et du DES. Et que l'étude complète le panorama de la menace virale, concernant en particulier les virus spécialisés dans l'extorsion [YY96, YY04, Gaz08], Une partie de cette étude a été publiée dans les actes de la conférence EICAR [4]2008 [Jos08]. Et aussi, il a étudié les aspects techniques et théoriques liés à la protection et à la rétro-ingénierie logicielle, au regard de la théorie de la complexité et de l'optimisation des programmes.

Futai Zou, Siyu Zhang, Tianqi Wan, Li Pan : [6]

Ils ont montré que l' Android est l'une des plates-formes informatiques mobiles les plus populaires aujourd'hui, son ouverture attire également l'attention d'un grand nombre de développeurs et de chercheurs en sécurité. Plus de cours des dernières années, la plate-forme Android a trouvé une vulnérabilité de privilèges multiples. Il existe également des centaines d'applications contenant un code malveillant.
Ils ont classé une série d'attaques à distance et locales pour les appareils Android Actuellement, selon le Marché officiel et après avoir étudié le mécanisme de sécurité de la plate-forme Android et les menaces de sécurité existantes, tels que le vol de la vie privée, le détournement et les pratiques de communication à distance, etc. Par ailleurs, ont étudiés la détection et le système de code malveillant d'Android .Les méthodes de renforcement et de défense, ils espèrent d'offrir une compréhension globale de la sécurité pour Android Plate-forme.

Joshua Drake: [17]

Expert zimperium zLabs et vice-président de la plate-forme de recherche et d'exploitation, il a découvert plusieurs vulnérabilités critiques dans la bibliothèque Stagefright et les correctifs

[3] la Black Box est un modèle traditionnel, suppose que l'agresseur n'a aucun accès physique à la clé (l'algorithme exécutant le chiffrement ou le déchiffrement), ni à aucun traitement interne, mais peut seulement observer des informations et un comportement externes. Ces informations sont constituées soit par le texte en clair (entrée), soit par le texte chiffré (sortie) du système, en supposant une visibilité nulle des opérations d'exécution du code et de chiffrement dynamique.

[4] EICAR, European Institute for for Computer Antivirus Research, http ://www.eicar.org/.

fournis par Google pour sécuriser Android. Ils ont signalé qu'ils ont fourni ces correctifs aux transporteurs et vendeurs via Zimperium Handset Alliance (ZHA) et que des correctifs ont été appliqués, des années pourraient être nécessaires pour atteindre tous les appareils.

Stagefright est une vulnérabilité critique Android. Il permet aux pirates d'obtenir «médias» ou «privilèges système» sur votre appareil après traitement d'un message MMS entrants, en surfant sur le web une quelconque des 11 vecteurs d'attaque potentiels. Dans de nombreux cas, l'attaque ne nécessite aucune action de l'utilisateur final. Pour aggraver les choses, l'attaquant peut supprimer les MMS avant de l'ouvrir.

Saud Alotaibi , Steven Furnell , and Nathan Clarke :[20]

Grâce à leurs contributions aux systèmes d'authentification transparents pour la sécurité des appareils mobiles. Ils ont considéré que la biométrie physiologique souffre de problèmes tels que la qualité de l'image, ont généralement besoin de matériel supplémentaire et sont consommés l'énergie. Les études ont révélé que la biométrie comportementale peut fonctionner dans une authentification transparente et continue en permettant de construire un profil de comportement de l'utilisateur pendant que l'utilisateur utilise l'appareil, sans nécessité d'actions délibérées de l'utilisateur légitime. Ainsi que l'utilisateur est mobile, le micro-mouvement du périphérique mobile peut affecter les performances de la biométrie basée sur le toucher et provoquer un taux d'erreur élevé. Et aussi, Une approche tactile pourrait être vulnérable aux attaques de shoulder-surfing .[5]

Patrick Gueulle : [21]

Il se déduit que lors de l'authentification de la carte SIM avec l'opérateur, et confirme l'enregistrement du mobile sur le réseau, l'algorithme A3/A8 calcule un résultat dont le nombre de bits est inférieur à celui des deux opérandes qui lui sont soumis. Cela n'a rien d'exceptionnel (l'algorithme « Secure Hash » SHA-1 repose sur ce même principe de génération d'un condensé), mais il en résulte nécessairement qu'un même résultat peut être obtenu à partir de plusieurs couples d'opérandes distincts. Bien entendu, la probabilité est infime d'obtenir les bonnes valeurs de SRES et de Kc à partir d'une clef Ki incorrecte, et quand bien même cela arriverait, cela ne donnerait accès au réseau que pour un temps très court.
On a annoncé qu'une faille appelant un chat un chat et que les universitaires américains faisaient état de graves défauts dans la méthode mathématique utilisée, prouvant ainsi la faisabilité du « clonage » de cartes SIM. Il est édifiant, suggèrent-ils, de solliciter l'algorithme de façon à provoquer des « collisions », c'est-à-dire l'occurrence de couples d'opérandes distincts menant à un résultat identique. Il a été démontré que des calculs relativement simples permettent de découvrir deux octets de la clef Ki (normalement inaccessible en lecture) lors de chaque

[5] En sécurité informatique, regarder par-dessus l'épaule (anglais : Shoulder surfing) est une technique d'ingénierie sociale utilisée pour dérober de l'information à une personne en particulier.il n'y a pas besoin de compétences particulières, uniquement d'agilité et de préparation.

collision. Cela étant, il semblerait que la totalité de la clef puisse être ainsi reconstituée en moins de 200 000 sollicitations d'une carte SIM basée sur l'algorithme COMP128.

Marc Jacob :[15]

en octobre 2009, il a été développé la version 3.0 de "Security BOX Mobile (une gamme de solutions logicielles) ", la sortie du produit est un successeur vise d'améliorer la version 2.8, qui a été déjà apparu en 2008. Arkoon Security BOX Mobile est une solution de sécurité complètement transparente pour l'usager qui occupe toute la fonctionnalité de son terminal mobile avec un niveau de sécurité est plus élevé. Elle assure la confidentialité des données du terminal et des cartes mémoires. La connexion au système d'information est sécurisée et la synchronisation des emails s'effectue dans la plus stricte confidentialité. Parmi les nouveautés apportées, notons en particulier deux aspects qui caractérisent cette nouvelle version.
L'un des aspects est l'authentification forte, se privilégié par une carte cryptographique micro SD. La carte prend en charge l'ensemble des opérations cryptographiques et stocke les clés de l'utilisateur. Elle permet de gérer les ports par exemple le Bluethooth (sauf oreillette), l'IRDA, les clés USB... Cette technologie est certifiée EAL5+ qui est un atout pour renforcer la confiance du produit auprès des grandes entreprises et des administrations.

Le deuxième aspect, est une administration centralisée se forme des mises à jour du logiciel, politique de sécurité et les clés de l'utilisateur sont réalisées à distance avec un système de contrôle d'intégrité. Elle permet de renforcer sa position de fournisseur de solutions de chiffrement de données et supportée par les terminaux basés sur Windows Mobile 6.1 ou supérieur.

fernand lone sang :[16]

Leur objectif se déroule sur l'étude des attaques qui sont extrêmement difficile à détecter par les logiciels classiques afin de proposer des contre-mesures adaptées, basée sur des composants fiables et incontournables. Pour vérifier ce manuscrit, en début, il doit être conçu des malveillants de composants matériels et agissants de la même manière qu'un programme intégrant un cheval de Troie ; afin d'y intégrer des fonctions malveillantes (typiquement une porte dérobée dans son firmware).on a élaboré un modèle d'attaques de différents niveaux d'abstraction d'un système informatique .ce modèle sera l'appliqué à deux approches : une analyse de vulnérabilités traditionnelle ,de proposer des contre-mesures à partir d'une faille de nombreuse preuves de concepts et une analyse de faille par fuzzing sur les bus entrée-sortie reposant sur un outil baptisé IRONHIDE capable de simuler des attaques depuis un composant matériel malveillant .

CHAPITRE I

Principe de fonctionnement et architecture des réseaux mobiles

1 INTRODUCTION :

Les télécommunications sont la transmission de signes, de signaux, de messages, d'écrits, d'images et de sons ou d'intelligence de toute nature par des systèmes de câblage, de radio, d'optique ou d'autres systèmes électromagnétiques. Les télécommunications se produisent lorsque l'échange d'informations entre les participants à la communication inclut l'utilisation de la technologie. Il est transmis électriquement sur des supports physiques, tels que des câbles, ou par rayonnement électromagnétique. De tels chemins de transmission sont souvent divisés en canaux de communication qui offrent les avantages du multiplexage. Le terme est souvent utilisé dans sa forme plurielle, les télécommunications, parce qu'il implique de nombreuses technologies différentes.

Les premiers moyens de communiquer sur une certaine distance comprenaient des signaux visuels, tels que des balises, des signaux de fumée, des télégraphes de sémaphore, des signaux et des héliographes optiques. D'autres exemples de communication pré-moderne à longue distance comprenaient des messages audio tels que des battements de tambour codés, des cornes soufflées par les poumons et des sifflets aigus. Les technologies du 20e et du 21e siècle pour la communication longue distance comprennent généralement les technologies électriques et électromagnétiques, comme le télégraphe, le téléphone et le téléimprimeur, les réseaux, la radio, la transmission par hyperfréquences, la fibre optique et les satellites de communication.

Une révolution dans la communication sans fil a commencé dans la première décennie du 20ème siècle avec les développements pionniers dans les communications de radio par Guglielmo Marconi, qui a gagné le prix Nobel dans la Physique en 1909. D'autres inventeurs et développeurs pionniers notables dans le domaine des télécommunications électriques et électroniques incluent Charles Wheatstone et Samuel Morse (inventeurs du télégraphe), Alexander Graham Bell (inventeur du téléphone), Edwin Armstrong et Lee de Forest (inventeurs de la radio), ainsi que Vladimir K. Zworykin, John Logie Baird et Philo Farnsworth Des inventeurs de la télévision).

2 HISTORIQUE :

A l'origine, les téléphones mobiles ont été installés en permanence dans les véhicules, mais à plus tard les versions comme le soi-disant portatifs, étaient équipées de prise spécifique afin qu'ils pouvaient aussi être transportées et pourraient ainsi être utilisés comme un mobile, portable talkie-walkie. Pendant le début des années 1940, Motorola a développé une radio bidirectionnelle, le talkie-walkie et développé plus tard. Un appareil radio « Poignée-Talkie » à piles (HT) et bidirectionnelle à la taille d'un bras d'homme, pour l'armée américaine.

En effet, le premier télégraphe transatlantique est construit en 1866, pas grand chose à voir avec les téléphones cellulaires, mais une avancée majeure dans la communication néanmoins. Plus tard et précisément en l'année 1921, le service de Police de Detroit, au Michigan commence installation de radios mobiles, fonctionnant autour de 2 MHz, dans leur voiture d'équipe. Ils

rencontrent de nombreux problèmes tels que le surpeuplement sur les canaux et les interférences terrible .ainsi dans les années 1940 les radios mobiles sont capables de fonctionner à 30 à 40 MHz et deviennent beaucoup plus fréquentes entre les services de police et les riches. Plusieurs organisations et entreprises privées commencent à l'aide de ces mêmes radios pour leur profit personnel. Plus tard en 1945, été le premier mobile-radio-téléphone service, est établi à Saint-Louis. Le système est composé de six canaux qui ajoutent au plus 150 MHz. Le projet est approuvé par la FCC, mais suite à l'intervention massive, l'équipement fonctionne à peine.

En 1947, Bell Labs , a proposé que les tours de cellules aux coins de l'hexagone, plutôt que les centres et ont des antennes directionnelles qui pourrait transmettre/recevoir dans 3 directions en 3 cellules adjacentes à six pans creux .Le système fonctionne à des fréquences d'environ 35 à 44 MHz, mais une fois de plus, il y a une quantité massive d'interférence dans le système. AT&T déclare le projet une panne. Dans 1967, chaque téléphone mobile a dû rester dans la zone cellule desservie par une station de base tout au long de l'appel téléphonique. Cela n'a pas fourni de continuité de service téléphonique automatique pour les téléphones mobiles se déplaçant dans plusieurs zones de la cellule. En 1970, E. Amos Joel, Jr., un autre ingénieur de Bell Labs, a inventé un système automatique « appel de procédure de transfert » pour permettre à des téléphones mobiles pour se déplacer dans plusieurs zones de la cellule au cours d'une conversation simple sans perte de conversation.

Enfin, la FCC statue que Western Electric peut fabriquer des produits à usage tant cellulaire et terminal. (Fondamentalement, ils admettent qu'ils ont mis les compagnies de téléphone environ 7 ans de retard) .le téléphone mobile était surtout connu pour son utilisation dans la voiture. Nokias Mobira , sorti en 1982, fut le premier de son genre. Un téléphone de voiture qui pesait presque 10 kilos, Nokias Mobira ressemblait à une grande radio plutôt qu'un phone mobile conventionnel .en 1988 d'entre les années plus importantes dans l'évolution du téléphone portable. L'Association de l'industrie de la technologie cellulaire est créée et contribue à faire de l'industrie dans un empire. Un de ses plus grandes contributions est quand il a aidé à créer la technologie TDMA du téléphone, le téléphone portable plus évolué encore. Elle sera disponible aux tous publics.

3 les Réseaux GSM : (Global System for mobile communications)

3.1 Définition réseau :

C'est une norme développée par l'Institut européen de normes de télécommunications (ETSI) pour décrire les protocoles pour les réseaux cellulaires numériques (2G) deuxième génération utilisés par les téléphones mobiles, d'abord déployés en Finlandes juillet 1991. en 2014, il est devenu la norme mondiale de facto pour les communications mobiles avec plus de 90% des parts de marché, opérant dans plus de 219 pays et territoires. Les réseaux 2G développées comme un remplacement pour les réseaux cellulaires analogiques de première génération (1G), et la norme

GSM a été décrit comme un réseau numérique, commutation de circuit optimisé pour la téléphonie vocale duplex intégral.

Cette élargie au fil du temps afin d'inclure les communications de données, tout d'abord par commutation de circuits de transport, puis par transport de données de paquet via GPRS (General Packet Radio Services) et EDGE (Enhanced Data rates for GSM Evolution or EGPRS).Par la suite, le 3GPP mis au point la (troisième génération 3G) UMTS normes suivies de quatrième génération (4G) LTE Advanced normes, qui ne font pas partie de la norme ETSI GSM. « GSM » est une marque détenue par la GSM Association. Il peut aussi désigner le codec voix (initialement) couramment utilisé. [4]

3.2 L'architecture du réseau :

L'architecture du réseau GSM tel que défini dans les spécifications GSM peut être regroupé en quatre domaines principaux (Figure 1.1) :

- La station Mobile (MS)
- Le Sous-système radio (BSS)
- Le sous-système fixe (NSS)
- Le Sous-système de soutien et de fonctionnement (OSS)

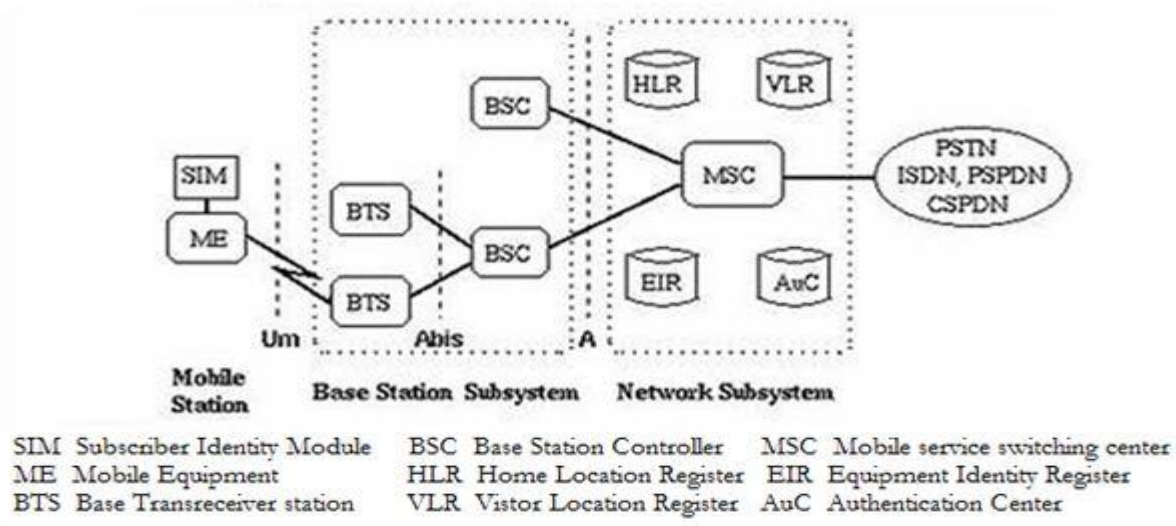

Figure 1.1: les Composants de réseau GSM. [59]

3.2.1 La station mobile (MS) :

La station mobile(MS) est la pièce d'équipement remis à l'utilisateur d'établir les connexions pour transporter les discours et les données afin d'échanger des messages SMS. elle Contient l'équipement terminal(ME) et la carte SIM (Subscriber Identity Module).Chaque pièce d'équipement terminal est identifié de manière unique par un IMEI Nombre (International Mobile Equipment Identity) attribué par le fabricant. [3]

3.2.2 Le Sous-système radio (BSS):

Sous système de radio le BSS garantit une transmission radio du mobile, gère les ressources radio et permettant la mobilité sur mobile. Le sous-système BSS est composé de deux éléments :

3.2.2.1 Le BTS (Base Transceiver Station) :

leurs antennes associées qui transmettent et reçoivent pour communiquer directement avec les mobiles. Le BTS est l'élément qui définit pour chaque cellule. Le BTS communique avec les mobiles et l'interface entre les deux est connu comme l'interface de messagerie unifiée avec ses protocoles associés. [4]

3.2.2.2 Le BSC (Base Station Controller) :

Le BSC constitue la prochaine étape dans le réseau GSM. Le BSS effectue un transcodage des canaux vocaux, l'attribution des canaux radio aux téléphones mobiles, la pagination, la transmission et la réception sur l'interface aérienne et de nombreuses autres tâches liées au réseau radio. [4]

3.2.3 Le sous-système fixe (NSS):

Le NSS est utilisé pour le traitement dans l'établissement de la communication comme des appels ainsi que pour la gestion de l'itinérance et mobilité. Le NSS se compose de commutateurs téléphoniques MSC (Mobile services Switching Center), GMSC (Gateway MSC) et les bases de données HLR (Home Location Register), VLR (Visitor Location Register), AuC (authentification Center) et EIR (Equipment Identity Register). [3]

3.2.3.1 Le MSC (Mobile services Switching Center) :

Le MSC effectue l'interrupteur horaire de division des circuits à 64 kbit/s. Il gère pour établir la communication grâce à la signalisation des messages échangés entre le MS et les entités du NSS. Il transfère les messages texte SMS et exécute la rétrocession lorsque cela est nécessaire. [4]

3.2.3.2 Le GMSC (Gateway MSC) :

Le GMSC est un type particulier de MSC qui mène à l'interface avec la téléphonie fixe PSTN au réseau de téléphonie ou avec un autre PLMN mobile réseau quand cela ne peut pas interroger le HLR. Elle est utilisée pour établir un appel reçu par le MSC auquel est connecté le mobile. [3]

3.2.3.3 Le VLR (Visitor Location Register) :

Le VLR est une base de données qui mémorise les données de l'utilisateur actuel dans la zone géographique couverte par un ou plusieurs MSCs. il contient des informations sélectionnées à partir du HLR qui active les services sélectionnés pour l'abonné individuel à prévoir. Le VLR peut être implémentée comme une entité distincte, mais il est généralement réalisé comme faisant partie intégrante de la MSC, plutôt qu'une entité distincte. De cette façon l'accès est rendu plus rapide et plus pratique. [3]

3.2.3.4 Le HLR (Home Location Register) :

Le HLR est une base de données qui gère les détails de chaque abonné Cette base de données contient toutes les informations administratives sur chaque abonné ainsi que leur dernier emplacement connu. De cette façon, le réseau GSM est en mesure d'acheminer les appels vers la station de base pertinente pour les MS. Lorsqu'un utilisateur bascule sur leur téléphone, le téléphone s'enregistre auprès du réseau et de là, il est possible de déterminer quel BTS il communique avec afin que les appels entrants peuvent être acheminés correctement. Même lorsque le téléphone n'est pas actif (mais allumé) il se réinscrit périodiquement pour s'assurer que le réseau (HLR) est au courant de sa dernière position. Il y a un seul HLR par réseau, bien qu'il peut être distribué à travers différents centres secondaires à pour des raisons opérationnelles. [3]

3.2.3.5 Centre d'authentification (AUC) :

AUC est une base de données protégée qui contient la clé secrète également contenue dans la carte SIM de l'utilisateur. Il est utilisé pour l'authentification et pour chiffrer les communications

pour chaque abonné. Elle est généralement liée à la HLR et tous peuvent être intégrés dans l'appareil-même. [3]

3.2.3.6 Centre EIR (Equipment Identity Register):

L'EIR est une base de données qui contient le numéro IMEI de l'équipement terminal. Il est consulté lorsqu'il y a des demandes de connexion provenant d'un utilisateur. Il peut contenir un blanc liste de tous les numéros de réception partagée par tous les numéros de terminales dans la même série, une liste noire des terminaux volés ou interdits et une liste grise des terminaux qui ont défauts de fonctionnement insuffisants pour justifier une interdiction complète. [3]

3.2.4 Le sous-système de soutien de fonctionnement (OSS):

Le sous-système de soutien OSS ou l'exploitation est un élément au sein de l'architecture du réseau GSM global qui est connecté aux composantes de la NSS et le BSC. Il est utilisé pour contrôler et surveiller l'ensemble du réseau GSM et il est également utilisé pour contrôler la charge de trafic de la BSS. Il est à noter que le nombre de BTS augmente avec la mise à l'échelle de la population d'abonné certaines des tâches de maintenance est transférés de la BTS, ce qui permet des économies dans le coût de possession du système. [4]

4 les Réseaux GPRS : (General Packet Radio Service)

4.1 Définition réseau :

GPRS est l'abréviation anglaise de (General Packet Radio Service), il se présente un service basé sur les paquets de données mobiles sur le système mondial de communications mobiles (GSM), des systèmes de communication cellulaire 3G et 2G. C'est une technologie commutation de paquets à ciel ouvert non vocales, à grande vitesse et utile destinée aux réseaux GSM.
GPRS peut être utilisé pour activer les connexions selon des protocoles Internet qui prennent en charge une grande variété d'entreprises, ainsi que des applications commerciales, Il permet l'envoi et la réception de grandes quantités de données à travers des réseaux de téléphonie mobile. Avant d'envoyer les données, il est divisé en paquets individuels et déplacé à travers le réseau central et de la radio. Les données sont ensuite remontées à fin du destinataire. [3]

4.2 Présentation de l'infrastructure d'un réseau GPRS :

Tout d'abord, un réseau GPRS est un réseau IP. Le réseau est ainsi constitué de Routeurs IP. L'introduction de la mobilité s'exige également la précision de Deux nouvelles entités :

- Le nœud de service - le SGSN.
- Le nœud de passerelle - le GGSN.

Une troisième entité - le BG joue un rôle supplémentaire de sécurité.

Le réseau GPRS ajoute un certain nombre de "modules" sur le réseau GSM sans changer le réseau existant. Ainsi sont gardés tous les Architectures modules GSM, nous verrons également quelques modules GSM sera utilisé pour le fonctionnement du réseau GPRS. [4]

4.3 Les équipements GSM utilisés dans le réseau GPRS :

Le réseau GPRS prend en charge son architecture sur les éléments du réseau GSM

- Le BTS et le BSC peuvent couvrir un territoire national pour localiser les terminaux
- Le MSC le VLR peut fournir et gérer les problèmes Abonnés itinérants sur les réseaux GSM et GPRS.
- le GMSC permet une communication interne au réseau par l'envoi des messages courts destinés au terminal GPRS.
- Le HLR pour gérer les questions liées à la localisation des Individus (en mode GPRS, fournir une carte de la ville où L'Abonné).
- L'EIR pour gérer les problèmes liés au terminal cible

Le réseau GPRS dépend entièrement du bon fonctionnement de L'infrastructure du réseau GSM. Le réseau GSM est en effet une base Pour la mise en œuvre du réseau GPRS. [4]

4.4 L'architecture du réseau GPRS :

L'introduction du service GPRS n'est pas une grande mise à jour sur l'infrastructure du réseau GSM existant. L'impact apparait essentiellement sur l'ajoute de nouvelles entités du réseau [4] (Figure 1.2) :

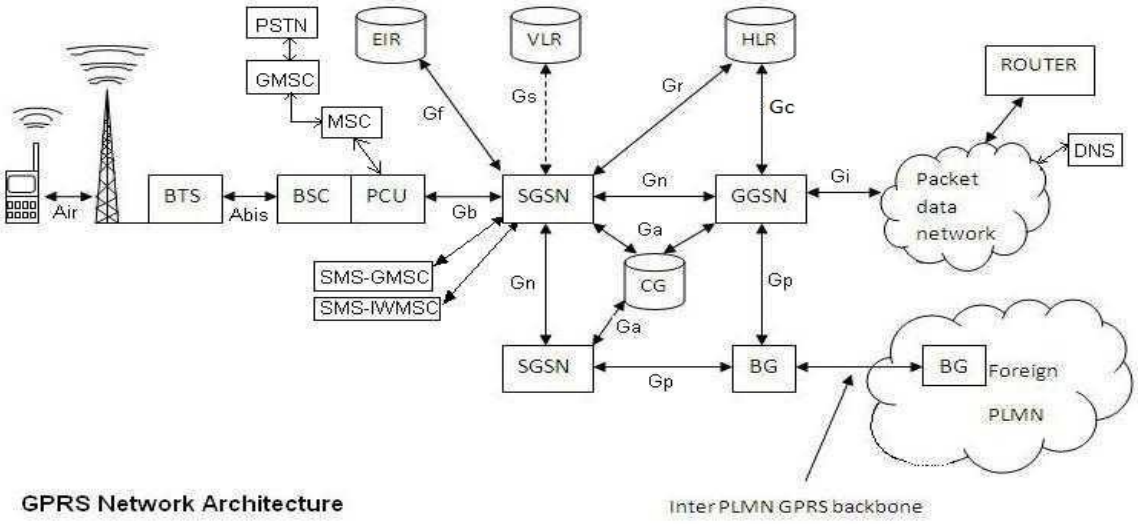

Figure 1.2: l'architecture de réseau GPRS.[60]

4.4.1 Le nœud de service (SGSN) :

L'élément SGSN ou portion GPRS Support Nœud du réseau GPRS, il fournit une gamme de services pour les mobiles :

- Paquet de routage et de transfert
- Gestion de la mobilité
- Pose/dépose
- Gestion de la liaison logique
- Authentification
- Chargement des données

4.4.2 Le nœud de passerelle (GGSN) :

Le GGSN, passerelle GPRS Support Nœud, est l'une des entités plus importante au sein de l'architecture du réseau GPRS.

Le GGSN organise l'interfonctionnement entre le réseau GPRS et les réseaux de commutation par paquets externes auxquelles les mobiles peuvent être Connectés. Il peut s'agir des réseaux Internet .

Le GGSN peut être considéré comme une combinaison de la passerelle, routeur et pare-feu qu'il cache le réseau interne vers l'extérieur. En fonctionnement, Lorsque le GGSN reçoit des données, adressées à un utilisateur spécifique, Il vérifie si l'utilisateur est actif, puis transmettre les données. Dans la direction Opposée, les données de paquet du mobile sont acheminées vers le réseau de la bonne destination par le GGSN. [4]

4.4.3 Le module PCU :

PCU ou l'unité de contrôle de paquet est un routeur matériel qui est ajouté à la BSC. Il différencie les données destinées à la norme GSM réseau (données à commutation de circuits) et les données destinées au réseau GPRS
PCU lui.même peut être une entité physique, ou plus souvent de nos jours il est incorporé dans le contrôleur de station de base, BSC, ainsi économiser les coûts de matériel supplémentaire. [3]

4.4.4 Le module BG :

Une fonction de passerelle frontière met.fin à l'interface de Gp pour un PLMN (Public Land Mobile Network). Cette fonction est généralement un routeur de bordure soutenant le BGP (Border Gateway Protocol) et les protocoles de sécurté comme IPSec (Sécurité IP). [4]

4.4.5 Le mobile GPRS :

Trois classes de mobile sont définies en fonction de leur capacité à en même temps utilisées le réseau GSM et le réseau GPRS :

- un mobile de classe A peut utiliser simultanément les services offerts par le GPRS et Réseaux GSM
- un mobile de classe B peut utiliser séquentiellement les services offerts par le GSM ou Réseaux GPRS
- un mobile de classe C peut utiliser les services offerts par le réseau GPRS ou le réseau GSM. Elle est différente du mobile de classe B dans le sens où ce n'est pas ont un mode veille qui analyse les deux types de réseau.

5 UMTS : (Universal Mobile Telecommunications System)

5.1 Définition réseau :

L'UMTS, abréviation d'Universal Mobile Télécommunications System, est un réseau 3G standard utilisé dans une grande partie du monde comme une mise à niveau vers les réseaux mobiles GSM existants. UMTS utilise WCDMA, une technologie qui partage beaucoup avec les réseaux CDMA utilisées dans le monde entier, même si ce n'est pas compatible avec eux. Niveau de base des réseaux UMTS sont généralement capables d'une vitesse de liaison descendante aussi rapide que 384 kbit/s.

5.2 Présentation de l'infrastructure d'un réseau UMTS:

Le réseau UMTS se combine avec les réseaux existants GSM et GPRS. ces derniers fournissent des fonctionnalités respectives de voix et Informations ; Le réseau UMTS fournit ensuite les fonctionnalités multimédia. [18]

5.3 La Technologie WCDMA :

C'est le premier projet de partenariat de troisième génération à accès multiple (3GPP) à large bande .les réseaux de la Division du Code (WCDMA) ont été lancés en 2002. à la fin de 2005, il était de 100 réseaux WCDMA ouverts et un total de plus.de 150 opérateurs avec licences d'exploitation de fréquences WCDMA.

Actuellement, les réseaux WCDMA sont déployé en bande UMTS. la technologie WCDMA fournit certains avantages, elle visant l'exploitation d'une plus grande part du trafic voix et données, elle améliore également la voix de base. la capacité de voix offerte est très élevée en raison du contrôle de l'interférence des mécanismes.

WCDMA permet simultanée voix et données, qui permettent par exemple la navigation ou par courriel lors de conférence vocale ou vidéo partage en temps réel , pendant la voix appelle. [18]

5.4 L'architecture du réseau:

L'architecture de réseau UMTS peut être divisée en trois éléments principaux (Figure 1.3) :

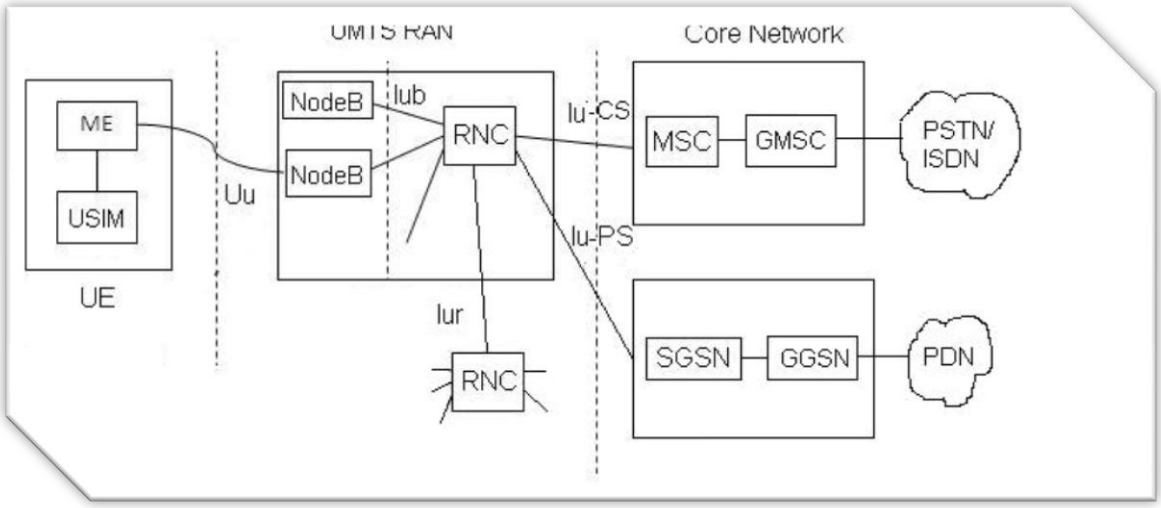

Figure 1.3: l'architecture de réseau UMTS.[61]

5.4.1 Équipement utilisateur (UE):

L'équipement utilisateur ou UE est le nom donné à ce qui composé de l'équipement mobile (ME) correspondant au combiné téléphonique (appareil mobile) et à la carte USIM. [8]

5.4.1.1 l'équipement mobile (ME) :

Les technologies des télécommunications et de l'informatique sont se rapprochent en intégrant les systèmes d'exploitation et des applications (navigateur web par exemple) sur les terminaux UMTS (les stations mobiles) ces derniers utilisera les réseaux GSM/GPRS/UMTS.[8]

5.4.1.2 La carte USIM :

La carte USIM en 3G est l'équivalent de la carte SIM en 2G, elle assure la sécurité du terminal et la confidentialité des communications. Elle se compose des algorithmes de chiffrement à clé publique sont utilisés. [8]

5.4.2 Le sous-système radio (RNS):

Le sous-système radio RNS (Radio Network Subsystem) ou Le réseau d'accès UTRAN se compose de deux composantes principales :

5.4.2.1 Contrôleur de réseau radio (RNC) :

Cet élément de l'UTRAN contrôle les ressources radio des Node B qui sont branchés dessus, c'est-à-dire les ressources radio dans son domaine. le RNC s'engage à la gestion des ressources

radio et certaines des fonctions de gestion de la mobilité, mais pas tous. C'est également le point auquel le cryptage / décryptage est effectué afin de protéger les données de l'utilisateur contre les écoutes. [8]

5.4.2.2 Node B :

Le node B est le terme utilisé au sein de l'UMTS pour désigner l'émetteur/récepteur de station de base. Cette partie de l'UTRAN contient l'émetteur et le récepteur pour communiquer entre eux au sein de la cellule. Il participe avec le RNC en rôle de la gestion des ressources. [8]

5.4.3 Le sous-système réseau (UMTS Core Network):

L'architecture de sous-système réseau 3G UMTS est une migration de ceux utilisés pour le GSM avec d'autres éléments superposés pour activer la fonctionnalité supplémentaire exigée par l'UMTS. [8]

6 CONCLUSION

Les architectures des réseaux de télécommunications cellulaires GSM, GPRS et UMTS sont complémentaires. Cependant, les éléments qui composent leurs architectures sont différents. L'architecture GSM est le nœud d'autres architectures cellulaires qui sont auteur de ce noyau et l'exploites. Elle est le plus utilisée dans le monde et initialement plus classique, c'est la voie des ondes radio de voix. L'évolution de l'architecture des réseaux cellulaires précédentes se tenir à besoins de transfert de voix, des données et multimédias, à partir des réseaux GSM, GPRS et UTMS respectivement.

Ultérieurement, l'évolution en domaine des télécommunications se résulte à une nouvelle norme, c'est Long-Term Evolution (LTE). LTE à permettre la communication sans fil haute vitesse pour appareils mobiles et terminaux de données, basée sur les technologies GSM / EDGE et UMTS / HSPA.

L'architecture des réseaux cellulaires vise à fournir différents services et applications à l'utilisateur déterminé par son terminal mobile, l'appareil mobile peut intégrer une carte à puce qui est devenue l'interface de pertinence des réseaux cellulaires.

CHAPITRE II

Puce ETSI/GSM : composants matériels et logiciels et mode de fonctionnement

1 Introduction :

L'importance d'utilisation de la carte à puce dans différents domaines soutenu au principe de l'intégration facile dans les appareils de la téléphonie et portable, les cartes de paiement et de crédit, ainsi que des pièces d'identité. Elle se constitué d'une technologie plus complexe, permet de l'évolution de nouvelles applications. en France précisément dans les années 1970, été déposés les premiers brevets de la carte à mémoire ou à processeur.

En fait, elle offre un ensemble de délégations soutiennent aux techniques cryptographiques qui permets d'identifier le porteur et d'effectuer des fonctions sécurisées comme la surveillance des télécommunications et des faits bancaires, contrôle des déplacements. Mais elle représente une clé d'authentification, toutes les informations sont enregistrées sur une puce de quelques millimètres carrés. [7]

Les systèmes électroniques modernes (systèmes embarquées), s'appropriés les ordinateurs personnels, assistants numériques personnels, téléphones mobiles et, routeurs de réseau qui sont utilisés les Puces Sim. aujourd'hui beaucoup de recherches intéressent à faire le point sur cette technologie, leurs applications, leurs sécurités et tentent de découvrir comment le marché a évolué ….

2 Historique :

Un ensemble des brevets qui sont concernés de développer de carte de crédit, qui se composent d'une unité électronique intégrée, elle a été apparu presque à l'année 1967 et s'a commencé à être publiées. L'évolution de ces inventions peut les réduire dans le tableau au dessous.[1]

Nom inventeur	Brevet, Pays et année
Pomeroy	Aux Etats-Unis en l'année 1967
Jules Ellingboe	Un système de paiement électronique sur une carte de crédit à contacts. Aux Etats-Unis en 1970
John Halpern	stylo électronique sécurisé de paiement.. Aux Etats-Unis en 1972
Kunitaka Arimura	méthode d'authentification dynamique. Au Japon en 1970
Jurgen Dethloff	En Allemagne (1977)
Roland Moreno	France (1974)
Michel Ugon	France (1977)
Louis Guillou	France (1979)

Tableau 1: évolution des inventions de carte de crédit

L'invention de Roland Moreno , est une carte à logique branchée et n'était pas programmable, se compose d'une mémoire intégrée. Ultérieurement, Michel Ugon avait révélé la résolution du problème chez l'inventeur CII-Honeywell Bull – se récolte que l'intégration d'un microprocesseur peut donner la mieux fonctionnalité à la carte, et assurer la sécurité a l'intermédiaire d'algorithmes

cryptographiques. Aussitôt, a été apparu le premier brevet est baptisée CP8, comme une carte intelligente. Ainsi en 1981, né le premier calculateur monolithique pour la carte à puce, appeléeSPOM Pour la raison de sécurité. [1]

3 Définition de la Carte Sim, modèles, leurs caractéristiques et leurs standards ETSI /GSM :

3.1 Définition :

La carte SIM, est l'acronyme de (Subscriber Identity Module). Une notion a été apparu en 1988, en général est une puce contient un microcontrôleur et une mémoire. Ce puce soutien d'un appareil numérique pour enregistrer les informations spécifiques à l'abonné d'un réseau mobile.

La carte SIM inclut les différentes informations concernant l'abonné et leur téléphone mobile, ces données permettent de réaliser les fonctions suivantes :

- l'authentification et l'identification d'un abonné.
- l'intégrité et la confidentialité des données.
- sécurisation des accès aux fichiers. [2]

3.2 Les modèles de La Carte Sim :

le tableau au dessous, se démontre les différents modèles de la SIM.

Caractéristiques / Modèle	longueur	largeur	épaisseur	Norme de référence
La carte Sim complète	de 85,6 mm	54 mm	0,76 mm	ISO/CEI 7810:2003, ID-1
Mini Sim/ normale	25 mm	15 mm	0,76 mm	ISO/CEI 7810:2003, ID-000
micro Sim	15 mm	12 mm	0,76 mm	ETSI TS 102 221
nano Sim	12,3 mm	8,8 mm	0,67 mm	ETSI TS 102 221
carte Sim embarquée	6 mm	5 mm	< 1mm	JEDEC Design Guide 4.8, SON-8

Tableau 2: Les modèles de la Carte Sim

3.3 Caractéristiques physiques d'une carte SIM :

la carte SIM a été constitué En début des années 90 , d'un CPU de 8 bits pour la taille de ses registres, RAM de taille 128 octets et la ROM de 7 Ko ,ainsi l' EEPROM de 3 Ko .Ces caractéristiques ont été évoluée issue des besoins des individus et leurs appréciations .

Plate-forme à puce	UniverSIM® M2M Zaniah 64 SMD	SkySIM® M2M Argo SMD	SkySIM® M2M Argo Plug
Mémoire client	64KB	64KB	64KB
ROM	384KB	-	-
EEPROM	64KB	320KB	320KB
RAM	8KB	8KB	8KB
COPRCESSEUR CRYPTO	1024 BIT	-	-
écart de température	-25°C TO 85°C	-40°C TO 105°C	-40°C TO 105°C
Gamme de tension	1.8/ 3 / 5V	1.8/ 3 / 5V	1.8/ 3V

Tableau 3: les caractéristiques physiques de différentes cartes SIM (G&D)et leurs types

G&D6 a proposé la plate-forme SIM "SkySIM®" pour le marché Java Card ™. La flexibilité de la carte SIM, où que se localise le mobile, permet aux opérateurs de réseau de l'adapter et à mineur coût à leurs besoins.

En particulier, G & D offre des avantages contrariant à la chaleur et au froid, ainsi que la ténacité à l'eau et aux vibrations, où les environnements incommodes tels que les véhicules. En plus des fonctions SIM 3GPP, SkySIM® et SkySIM® CX basées sur Java signifient que des fonctions logicielles mises à jour peuvent également être utilisées. Pour cela, des cartes SIM flexibles et très robustes sont recherchées.

[6] Giesecke & Devrient est un groupe technologique international vise de développer, produire et de distribuer des produits et solutions de paiement qui assurent les communications et la gestion des données personnelles.

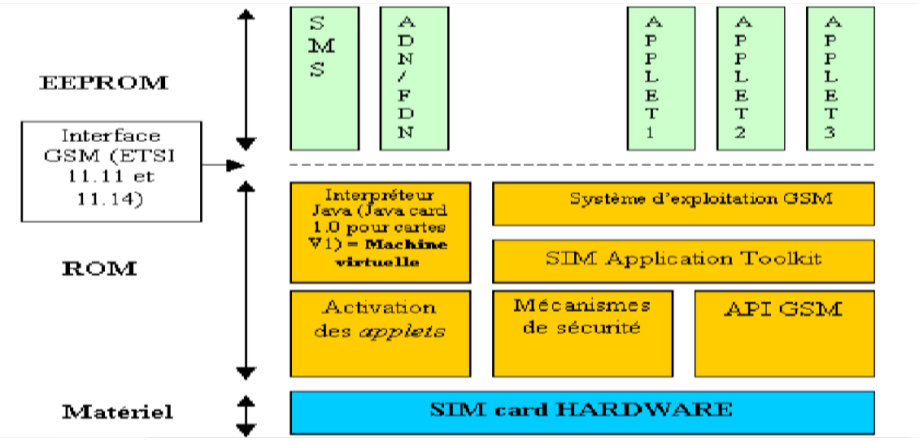

Figure 2.1: la structure de la carte SIM. [9]

- SMS : Service de Messages courts.
- ADN : Numéro abrégé de numérotation.
- FDN: Numéros de numérotation fixes.
- APPLET ; Est un programme Java qui s'exécute dans un logiciel de navigation compatible avec Java ou dans la Visionneuse d'applet JDK.
  API GSM : En tant que développeur de logiciels pour les plates-formes mobiles, vous pouvez être intéressé par l'intégration des fonctions de téléphonie dans votre application.

3.4 Les standards ETSI /GSM :

Un standard (une norme) est un produit dépend de ses spécifications, qui sont énoncées dans une référence. Il exige les moyens et les critères selon lesquels la conformité peut être vérifiée.

L'ETSI, l'Institut européen des normes est tributaire des télécommunications, afin de produire des normes qui s'appliquent à l'échelle mondiale et qui sont associées aux technologies de l'information et de la communication, détient les technologies fixes, mobiles, radiophoniques, convergentes, diffusées et Internet. ETSI a été désigné normes pour le fameux système de téléphonie cellulaire GSM. [2] [9]
le tableau suivant présenter les déférantes normes :

La norme	Description
GSM 11.11	définit les types de la carte SIM qui sont utilisé par la 2° génération des téléphones mobiles.
GSM 11.14	Une carte SIM Tool Kit devient contrôler un téléphone mobile ; accéder a son clavier et à son écran. Elle peut également envoyer et recevoir des messages SMS.
GSM 3.48	Mécanismes de sécurité dédiés à STK[7]
GSM 3.19	API java pour les cartes SIM.
3 GPP TS 51.011 (ETSI GSM 11.11).	Gestion des Fichiers et Authentification
3 GPP TS 51.014 (ETSI GSM11.14).	SIM Toolkit Applet Management
3 GPP TS 43.019.	SIM API for Java Card

Tableau 4: Les standards ETSI /GSM

4 Le système d'exploitation et de fichiers de la carte SIM :

4.1 Le système d'exploitation de la carte SIM:

Le système d'exploitation d'une carte SIM se réside en mémoire ROM, où il est pré-enregistré en usine, sous une forme non altérable, et pour éventuellement certaines de ses fonctions modifiables dans l'EEPROM. Il est également important que ces systèmes d'exploitation se conforment à des standards en ce qui concerne leur mode de communication. Notamment la norme ISO 7816-4 (specifics organization, security and command for interchange), a été rédigée pour cet usage en définissant la structure des commandes-réponses. Elle définit également une structure pour les données et les applications ainsi qu'une architecture pour la sécurité. Ainsi ces systèmes d'exploitation sont responsables de : [2]

[7] Le SIM Application Toolkit se compose d'un ensemble de commandes programmées dans la carte SIM qui définit comment la carte SIM doit interagir directement avec le monde extérieur et déclenche des commandes indépendamment du combiné et du réseau.

- La gestion de la mémoire (ROM, RAM, EEPROM)
- La gestion de fichiers .
- Le contrôle d'exécution de code .
- Le chargement, le lancement et la gestion des applications .
- La transmission de données .
- L'exécution et la gestion des algorithmes de cryptographie.

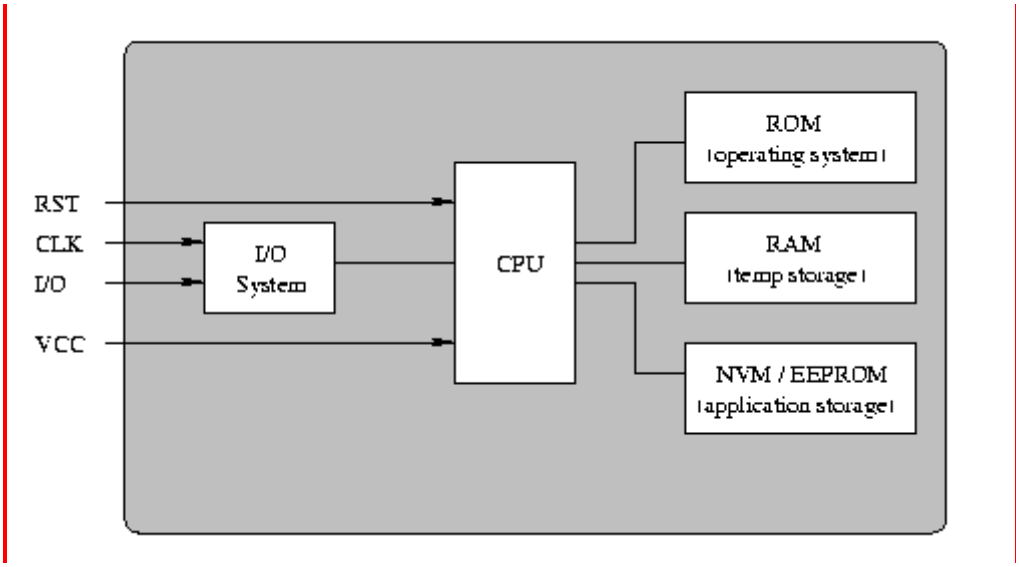

Figure 2.2: Éléments de l'architecture des cartes à puce. [52]

La sélection de la plate-forme de cartes SIM appropriée est pour l'opérateur de téléphonie mobile un premier pas important dans la définition de sa stratégie de service. Les plates-formes ne doivent plus seulement répondre aux exigences des réseaux GSM et 3G. De nouvelles fonctions s'y sont ajoutées, comme par exemple la communication en champ proche (NFC[8]), la technologie LTE[9], les cartes SIM multi-mégaoctets ou le Smart Card Web Server (SCWS).

4.2 Le système de fichiers de la carte SIM:

Une arborescence de répertoires est créée dans la mémoire EEPROM. Le répertoire racine s'appelle le MS, pour Master File et contient des sous-répertoires DF, pour Dedicated File (contenant eux-mêmes des sous-répertoires ou fichiers), et des fichiers EF, pour Elementary File

[8] La NFC, ou Near Field Communication (Communication dans un champ proche),est une technologie simple et intuitive qui vous permet d'utiliser votre téléphone portable à des fins innovantes. L'Open Handset Alliance est un consortium de plusieurs entreprises dont le but est de développer des normes ouvertes pour les appareils de téléphonie mobile.

[9] LTE (LONG TERM EVOLUTION) est une norme de télécommunication se définie par le consortium international de télécommunications 3GPP.

(ne contenant pas de sous répertoires). Ces répertoires et fichiers seront remplis lors de l'étape de personnalisation, où l'opérateur attribue à la carte SIM la clé d'authentification Ki et l'identification de l'abonné (IMSI) qui sont enregistrés dans les répertoires MF/EFiccid et MF/DFgsm/Efimsi respectivement.[2]

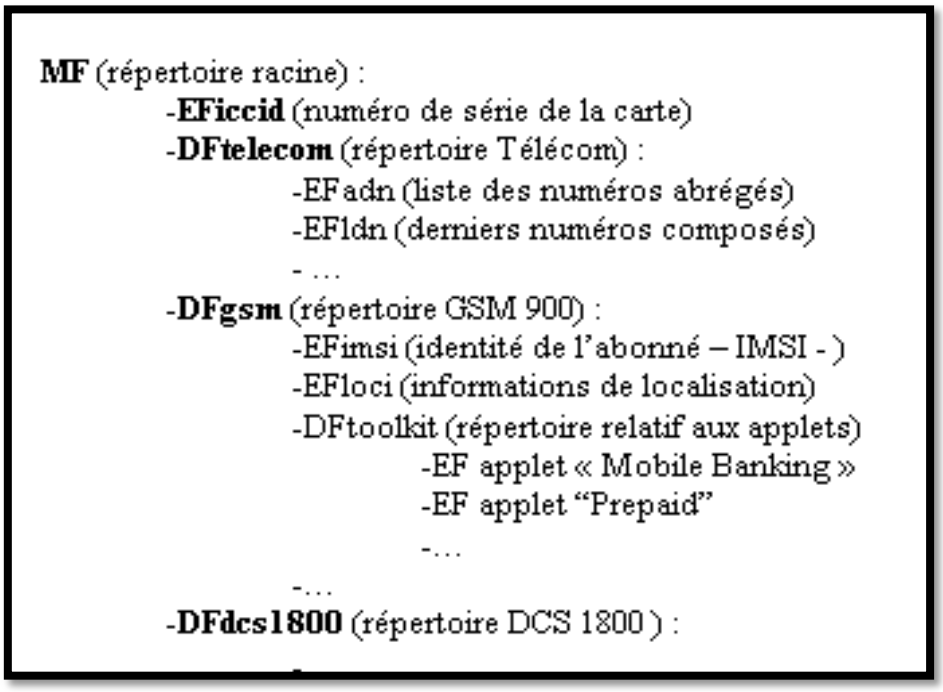

Figure 2.3: Les répertoires/fichiers de la SIM. [63]

Le répertoire GSM se compose de divers fichiers :

- Le fichier EFIMSI (6F07) contient le paramètre IMSI.
- Le fichier EFLOCI (6F 7E) contient principalement les paramètres : TMSI, LAI.
- Le fichier EFLP (Langage préférence).
- EFKc (Ciphering key Kc) contient la clé Kc et le numéro de séquence de la clé.
- EFSST (SIM service table) : la liste des services disponibles dans la carte.
- Service n°1 : CHV1 disable function.
- Service n°2 : Abbreviated Dialling Numbers (ADN).
- Service n°3 : Fixed Dialling Numbers (FDN).
- Service n°4 : Short Message Storage (SMS).
- etc.
- EFACM (Accumulated call meter): contient le nombre total d'unités pour l'appel courant et les appels précédents.
- EFMSISDN (MSISDN): contient le numéro de l'abonné MSISDN.

4.3 Etude d'une carte UICC : [10]

La carte de circuit intégré universel (UICC) est la carte à puce utilisée dans les terminaux mobiles dans les réseaux GSM et UMTS. L'UICC assure l'intégrité et la sécurité de toutes sortes de données personnelles, et elle détient généralement quelques centaines de kilo-octets. Avec l'avènement de plus de services, l'espace de stockage devra être plus grand. L'UICC est la carte physique et les cartes SIM / USIM / ISIM 2G sont des applications sur la carte UICC. L'IMS SIM détient les données fournies par l'opérateur IMS, généralement le même opérateur qui fournirait des services USIM qui permettraient de camper sur le réseau 3G ou LTE.
Identité utilisateur privée: identifie l'utilisateur uniquement avec l'opérateur IMS et est utilisé lorsque l'utilisateur s'inscrit dans le réseau IMS. Ceci est utilisé par l'opérateur pour vérifier l'abonnement et les services auxquels l'utilisateur peut se prévaloir.
Identité utilisateur publique: un utilisateur peut avoir plusieurs identités publiques pouvant être utilisées pour différents services. Pour bénéficier d'un service particulier, l'utilisateur doit s'inscrire auprès de l'identité publique particulière autorisée pour ce service.
Clés de sécurité: les clés de sécurité sont utilisées pour l'authentification sur le réseau IMS.Nom du domaine du réseau domestique: c'est le nom du point d'entrée que l'utilisateur utilise pour s'inscrire. Cela garantit qu'une demande d'utilisateur soit envoyée au réseau domestique.
Référence de règle d'accès: Ceci est utilisé pour stocker des informations sur le numéro d'identification personnel qui doit être vérifié pour accéder à une application particulière Adresse de P-CSCF: s'il n'est pas possible de trouver dynamiquement la fonction de contrôle de session d'appel de proxy, cette adresse est utile Données administratives: certaines de ces informations pourraient être spécifiques à l'opérateur. [10]

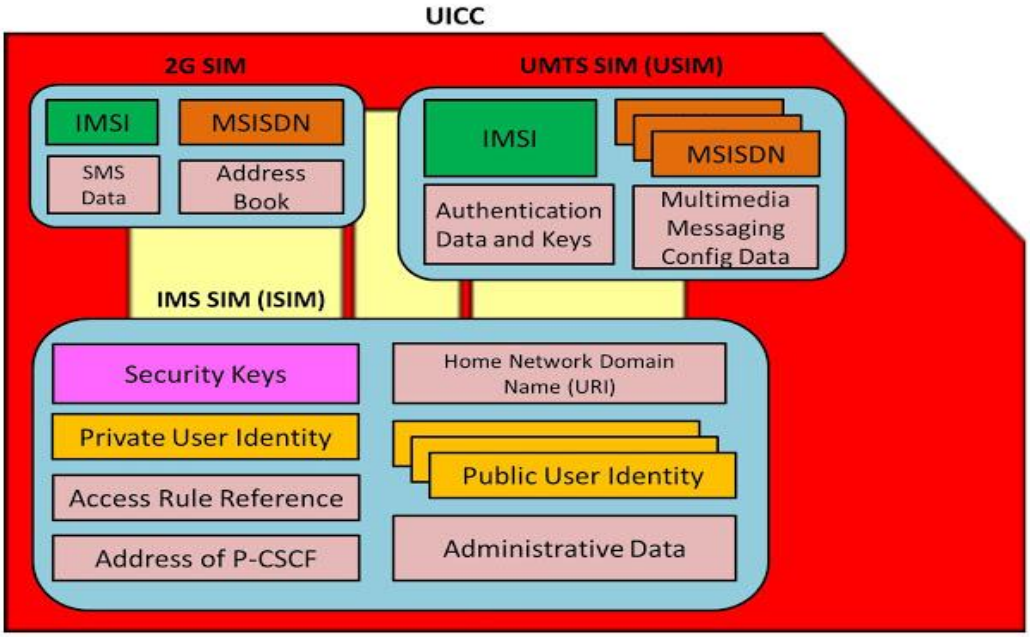

Figure 2.4 : les différents composants logiciels de la carte UICC.[58]

5 Numérotations liées à la mobilité :

L'abonné en réseau GSM se définit par plusieurs adresses comme des identités.

5.1 Identité unique de l'abonné (IMSI) : .[11] .[12]

En anglais (International Mobile Subscriber Identity), est un identificateur international suit le plan d'identification E.212 de l'IUT, en forme d'un code qui est enregistré dans la carte SIM, ce code dépend uniquement d'un abonné qui possède un abonnement mobile auprès d'un opérateur, il vise d'identifier celle-ci via les réseaux mobiles. Cette identité soutient un appareil numérique pour l'adressage spécifique d'une station mobile et approuvé la facturation correcte d'un abonné mobile

L ' IMSI n'est pas employé de la part d'abonné mobile, n'est exploité que par le réseau GSM et aussi qui ne change pas avec le temps. Se varie exceptionnellement dans les cas de perte ou de renouvellement de carte SIM, habituellement afin d'éviter l'interception par un intrus, il doit être le transporté rarement que réalisable sur l'interface radio au but de confidentialité ainsi en cas d'absence de TMSI, l'IMSI soutien en conséquence au réseau à prospecter l'utilisateur.

L'IMSI est chiffré sur 15 bits et regroupe trois parties :

- MCC (Mobile country Code) : permet de connaitre l'indicatif du pays domicile de l'abonné mobile (208 pour la France comme exemple).
- MNC (Mobile network code) : permet de connaitre l'indicatif du PLMN nominal de l'abonné mobile.
- MSIN (Mobile Subscriber Identification number) : permet de connaitre le numéro de l'abonné mobile à l'intérieur du réseau GSM.

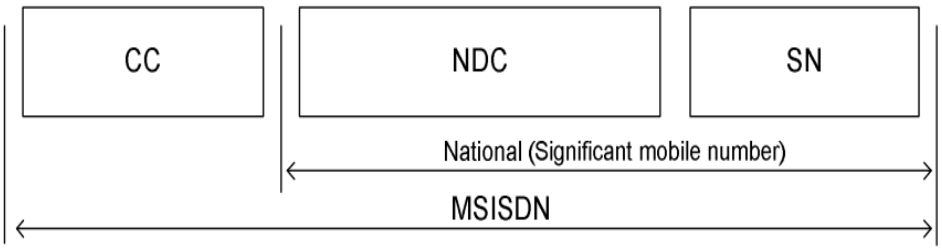

Figure 2.5: Composition de l'IMSI. [12]

5.2 Numéro de téléphone de l'abonné (MSISDN) : .[11] .[12]

En anglais (Mobile Subscriber Integrated Services digital Network Number), vise de déterminer le numéro de réseau numérique à intégration de services de l'abonné mobile. Tous simplement, c'est le numéro de téléphone unique qui a dédié à la carte SIM d'un téléphone mobile et a connu à l'extérieur du réseau GSM, pour identifier un abonné mobile aussi bien que l'IMSI, au but de transmission des appels. Le MSISDN se dépend de l'IMSI d'un abonné, à partir de la table du HLR. il est analogue au plan de numérotation téléphonique international E.164, se regroupe les champs suivant :

- code pays ou Country code (CC) : désigne l'indicatif du pays de l'abonné ou souscrit son abonnement (ex ; 237 pour le Cameroun, 228 pour le togo),
- National (Significant) mobile Number : désigne le numéro national du mobile composé du National Destination code (NDC) indiquant le PLMN particulier dans le pays et du subscriber Number (SN) approuvé librement par l'opérateur.

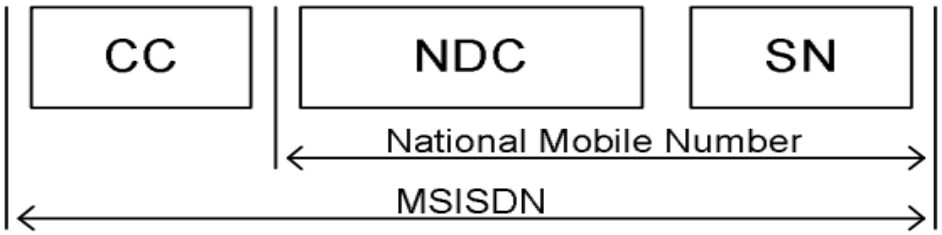

Figure 2.6: Structure du MSISDN. [12]

– champ CC : code pays du VLR courant du mobile,
– champ NDC : code du PLMN du VLR courant du mobile, –numéro d'abonné.

Le MSISDN joue le même rôle de l'IMSI, qui autorise à un PLMN de savoir le HLR de l'abonné à partir des premiers chiffres du champ SN. L' existence des champs CC et NDC vise aussi de l'utiliser également à désignation globale dans le SCCP au but du routage des messages entre PLMN usuel et le HLR nominal de l'abonné.

5.3 Identité de l'équipement mobile (IMEI) :[13][12] [11]

L'IMEI en anglais (International Mobile Equipment Identity), qui désigne l'identité de l'équipement mobile au territoire mondial, et s'a attribué d'un numéro ordinaire et unique, permet d'identifier les stations mobiles au réseau GSM, WCDMA et IDEN, ainsi que certains stations satellitaires. Il s'imprime généralement à l'intérieur du téléphone.
Peut être utilisé le numéro IMEI spécifiquement que l'IMSI et le MSISDN comme un moyen d'interception, qui est codé sur au plus 15 chiffres :

- TAC (Type Approval Code) : une partie est codé sur 8 chiffres permet de designer le constructeur (exemple; 01124500 pour Apple, 35151304 pour nokia). ..
- FAC (Final Assembly Code) : une partie est codé sur 2 chiffres qui désigne l'usine de fabrication,
- Serial Number (SNR) : numéro code sur 6 chiffres absolument réservé au constructeur.

-Spare (accorder) : un chiffre réservé pour l'instant.

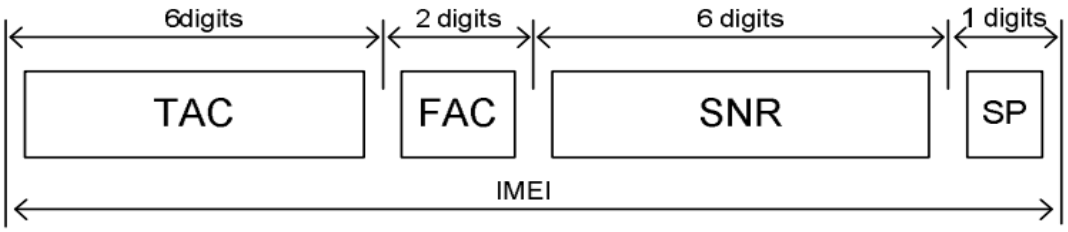

Figure 2.7: Structure de l'IMEI. [12]

5.4 identité temporaire d'abonné mobile (TMSI) : .[11] .

C'est le code qui est couramment transporte entre le téléphone mobile et le réseau. Il a attribué à l'abonné d'une manière temporaire et d'une façon locale, le VLR alloue un numéro temporaire unique à chaque mobile se localisant dans sa zone de couverture , ce numéro est appelé TMSI (Temporary Mobile Subscriber Identity). Le VLR est capable de corréler l'IMSI d'un mobile et son identité temporaire courante (TMSI). Le TMSI est conjoint sur la partie MS-MSC/VLR. inversement, le HLR qui ne le reconnaisse pas.
Il se fonctionne afin d'identifier le mobile en cas d'appelé ou appelant lors d'une communication, et doit être le changé a chaque variation de VLR aux raisons de sécurité .mais beaucoup de mobiles dépendants de VLR distincts peuvent avoir le même TMSI, celle-ci est permet de réduire la taille des messages d'appel a partir de sa structure qui est codée sur 4 octets, et est optionnelle par l'operateur.

5.5 MSRN (Mobile Station Roaming Number): .[12]

Le MSRN vise de router des appels entrants instantanément du commutateur passerelle (GMSC) vers le commutateur courant (MSC) de la station mobile. Il est apporte par le VLR conjoint du mobile de manière provisoire et uniquement en cours d' établissement d'un appel vers la station mobile .le MSRN suivant le format E.164 , a la même structure que le MSISDN (le MSRN peut être conforme au MSISDN dans certains cas) . Elle appropriée a un numéro du MSC dans lequel se trouve l'abonné. Cet adressage est intègre au réseau national et il est accessible par le réseau fixe.

6 CONCLUSION

L'évolution de la carte SIM ce qui a été présenté comme une application sur la nouvelle carte à puce UICC, pour assurer l'intégrité et la sécurité de toutes sortes de données personnelles et elle est utilisé pour offrir des services importants dans nos jours tels que les services Web, jeux, messagerie, commerce mobile. Cette dernière conduit à l'augmentation et à la popularité croissante des réseaux mobiles, ainsi que des appareils mobiles.

Les appareils mobiles ont des caractéristiques spéciales qui sont différenciées des autres appareils. Ces spécificités telles que la limitation d'énergie, la faible puissance de traitement, la mémoire limitée ... Puis; Toutes les applications orientées vers ces appareils doivent se conformer à ces contraintes et limitations et conviennent au système d'exploitation installé précédemment sur ces appareils mobiles.

L'utilisation des systèmes d'exploitation mobiles augmente les niveaux de sécurité de l'appareil mobile , qui sera le sujet de notre prochain chapitre.

CHAPITRE III

Le système d'exploitation des appareils mobiles

1 introduction :

Aujourd'hui les appareils mobiles sont des outils de productivité que nous utilisons pour planifier des projets de construction sur site, enregistrer des données patients lors d'une consultation, prennent des commandes donnent des présentations, envoyez des messages/courriels, appels téléphoniques, prennent des photos, naviguer dans nos voitures et tellement plus. Il va de soi, alors, que ces dispositifs sont de plus en plus ancré dans l'environnement de travail quotidien.

Réellement, il nous s'exige à permettre l'accès des appareils mobiles à certaines de nos informations plus sensibles — travailler les e-mails, documents budgétaires, information sur les ressources humaines, des plans d'affaires. Le nombre de choses que nous consommons par mobile est en plein essor. En vertu de la façon dont nos habitudes de travail ont changé et l'exhaustivité des données accessibles sur ces appareils. Les gents professionnels de la sécurité, ils ont maintenant reconnaissent que les périphériques mobiles sont un vecteur prescrit pour l'attaque. En fait, 67 % ont déclaré que leur organisation a probablement subi une violation de données par le biais de mobile. Les attaques par phishing, attaques usurpées de Wi-Fi, applications malveillantes, etc. sont les coupables probables.

2. Les différentes systèmes d'exploitation des appareils mobiles :

Le système d'exploitation mobile se définit comme un assortiment de programmes qui sont liés entre eux, afin de la corrélation entre les ressources matérielles de l'appareil et ses applications logicielles. Il garantit le démarrage et le bon fonctionnement de l'appareil mobile et les différents aspects de la sécurité.

Aujourd'hui, il rang plusieurs systèmes d'exploitation grâce à la compétition , comme :

2.1 iOS :

2.1.1 définition :

Le système d'exploitation mobile iOS (anciennement iPhone OS), est dévoilé en 2007 pour l'iPhone, iOS a été étendu pour prendre en charge d'autres périphériques Apple tels que iPod Touch (septembre 2007) et iPad (janvier 2010). Il est dérivé de OS X dont il partage les fondations (le kernel hybride XNU basé sur le micro-noyau Mach, les services Unix et Cocoa, etc.). iOS comporte quatre couches d'abstraction, similaires à celles de Mac OSX : une couche « Core OS », une couche « Core Services », une couche « Media » et une couche « Cocoa ». [14]

L'iOS n'avait aucun nom officiel avant la publication du kit de développement iPhone (SDK) le 6 mars 2008. Le SDK disponible pour macOS, propose les outils nécessaires à la création d'une application pouvant tourner sous iOS, son téléchargement et son utilisation sont gratuits. De surcroît, le portail App Store, dédié à l'exposition de toutes les applications développées pour ce système d'exploitation, est souvent présenté comme un modèle économique couronné de succès.[22]

2.1.2 Les technologies de Sécurité :

IOS utilise de nombreuses fonctionnalités de sécurité dans le matériel et les logiciels :

- Démarrage sécurisé :

Avant de démarrer complètement dans iOS, il existe un code de bas niveau qui s'exécute à partir de la ROM de démarrage. Sa tâche est de vérifier que le démarreur de niveau bas est signé par la clé publique de la racine Apple Root avant de l'exécuter. Ce processus consiste à s'assurer qu'aucun logiciel malveillant ou autrement non autorisé ne peut être exécuté sur un périphérique iOS. Une fois que le démarreur de bas niveau termine ses tâches, il exécute le chargeur de démarrage de niveau supérieur, appelé iBoot.
iBoot va alors charger le noyau iOS ainsi que le reste du système d'exploitation. [22]

- Enclave sécurisé :

Est un coprocesseur trouvé dans les périphériques iOS qui contiennent Touch ID. Il a son propre processus de démarrage sécurisé pour s'assurer qu'il est complètement sécurisé. L'Enclave sécurisé de chaque périphérique possède une ID unique qui lui est donnée lors de sa création et ne peut pas être modifiée. L'Enclave sécurisé contient également un compteur anti-replay pour empêcher les attaques de force brut.
Les périphériques iOS peuvent avoir un code d'accès utilisé pour débloquer le périphérique, modifier les paramètres du système et chiffrer le contenu de l'appareil. Jusqu'à récemment, il s'agissait généralement de quatre chiffres à long terme. Les mots de passe à six chiffres sont désormais par défaut sur iOS avec l'option de revenir à quatre ou d'utiliser un code d'accès alphanumérique.[22][25]

- Touch ID :

Touch ID est un scanner d'empreintes digitales incorporé dans le bouton d'accueil et peut être utilisé pour débloquer le périphérique, effectuer des achats et se connecter à d'autres fonctions. Lorsqu'il est utilisé, Touch ID enregistre temporairement les données d'empreinte digitale dans la mémoire chiffrée dans l'Enclave sécurisé, comme décrit ci-dessus. Il n'y a aucun moyen pour le

processeur principal du périphérique ou toute autre partie du système d'accéder aux données d'empreintes digitales brutes obtenues à partir du capteur Touch ID. [22][23]

- Randomisation de la disposition de l'espace d'adresse :

L'approche de localisation d'espace d'adresse (ASLR) est une technique de bas niveau pour empêcher les attaques de corruption de mémoire telles que les débordements de tampon. Cela implique de placer des données dans des emplacements sélectionnés au hasard dans la mémoire afin de rendre plus difficile la prévision de moyens de corrompre le système et de créer des exploits. L'ASLR rend les bogues d'applications plus susceptibles de bloquer l'application que d'écraser silencieusement la mémoire, que le comportement soit accidentel ou malveillant.[24]

- Mémoire non exécutable:

IOS utilise la fonction Exécute Never (XN) de l'architecture ARM. Cela permet à certaines parties de la mémoire d'être marquées comme non exécutables, en fonction d'ASLR pour éviter les attaques de débordement de tampon.[22]

- Sécurité de l'application et de l'internet :[25][22]

Il existe un ensemble très étendu de contrôles de confidentialité contenus dans iOS avec des options pour contrôler la capacité des applications d'accéder à une grande variété d'autorisations telles que la caméra, les contacts, l'actualisation de l'application arrière, les données cellulaires et l'accès à d'autres données et services. La plupart du code dans iOS, y compris les applications tierces, s'exécutent en tant qu'utilisateur "mobile" qui n'a pas de privilèges root.

Le cadre de sécurité du transport d'applications exige que les serveurs utilisent au moins TLS 1.2. Cependant, les développeurs sont libres de remplacer ce cadre et d'utiliser leurs propres méthodes de communication sur les réseaux. Lorsque le Wi-Fi est activé, iOS utilise une adresse MAC aléatoire pour que les périphériques ne puissent être suivis que par quelqu'un qui renifle le trafic sans fil.

- Authentification à deux facteurs :

L'authentification à deux facteurs est une option dans iOS pour s'assurer que même si une personne non autorisée connaît une combinaison d'identifiant et de mot de passe Apple, elle ne peut pas accéder au compte. Cela fonctionne en exigeant non seulement l'identifiant et le mot de passe Apple, mais aussi un code de vérification qui est envoyé à un périphérique déjà connu pour être approuvé. [25][22]

2.2. Windows Phone :

2.2.1 définition :

A été lancé en novembre 2010 avec Windows Phone 7, par Microsoft, il succède Windows Mobile en étant plus orienté vers un grand public. Il est basé sur un noyau Windows CE. C'est le futur Windows 8 qui est annoncé comme pouvant équiper des tablettes à sa sortie. Windows Phone 8.1 est la dernière version publique du système d'exploitation, lancée à la fabrication le 14 avril 2014. Windows Phone a été remplacé par Windows 10 Mobile en 2015; Il met l'accent sur une plus grande intégration et une unification avec son homologue PC, y compris un nouvel écosystème d'application unifiée, ainsi qu'un élargissement de son champ d'application pour inclure des tablettes de petite taille.
Microsoft propose ses Windows Phone Developer Tools pour le développement des applications . Ce package, gratuit, comprend : Visual Studio 2010 Express, la version légère casino online et gratuite de Visual Studio 2010. Un émulateur Windows Phone Expression Blend, pour la création des écrans. [26][27]

2.2.2. Les technologies de sécurité en Windows 10 Mobile :

le système d'exploitation Windows 10 , utilise les technologies de sécurité pour protéger l'usager contre les menaces de sécurité connues et émergentes dans le spectre des vecteurs d'attaque. Ces technologies comprennent:

- Windows Hello : Les fonctions améliorées d'identité et de contrôle d'accès garantissent que seuls les utilisateurs autorisés peuvent accéder aux données et aux ressources de l'entreprise. Windows Hello simplifie le déploiement et l'utilisation de l'authentification multifactorielle (MFA), offrant des méthodes d'authentification par code PIN, compagnon et biométrie.

- Windows Information Protection : La séparation automatique des données permet de partager les informations d'entreprise avec les données personnelles et les applications.

- Résistance aux logiciels malveillants : Les protections multi-couches intégrées au matériel de l'appareil, aux processus de démarrage et à la plate-forme d'application contribuent à réduire la menace de malware qui peut compromettre les dispositifs d'employés.[28]

2.3. BlackBerry OS :

2.3.1 définition :

BlackBerry OS est un système d'exploitation mobile exclusif développé par le fabriquant canadien RIM (Research In Motion).il se limite pour sa ligne BlackBerry de périphériques portables, pour smartphones et PDA. Le système d'exploitation fournit un multitâche et prend en charge les périphériques d'entrée spécialisés qui ont été adoptés par BlackBerry pour être utilisés dans ses ordinateurs de poche, en particulier le trackwheel, le trackball ,et plus récemment, le trackpad et l'écran tactile

La plate-forme BlackBerry est peut-être mieux connue pour son support natif pour les courriels d'entreprise, via Java Micro Edition MIDP 1.0 et, plus récemment, un sous-ensemble de MIDP 2.0, qui permet une activation et une synchronisation sans fil complète avec Microsoft Exchange, Lotus Domino ou Novell GroupWise , Le calendrier, les tâches, les notes et les contacts,lorsqu'ils sont utilisés avec BlackBerry Enterprise Server. Le système d'exploitation prend également en charge WAP 1.2. .[29]

Les mises à jour du système d'exploitation peuvent être automatiquement disponibles auprès des opérateurs sans fil qui prennent en charge le BlackBerry (BlackBerry) via le service de chargement du logiciel aérien (OTASL).

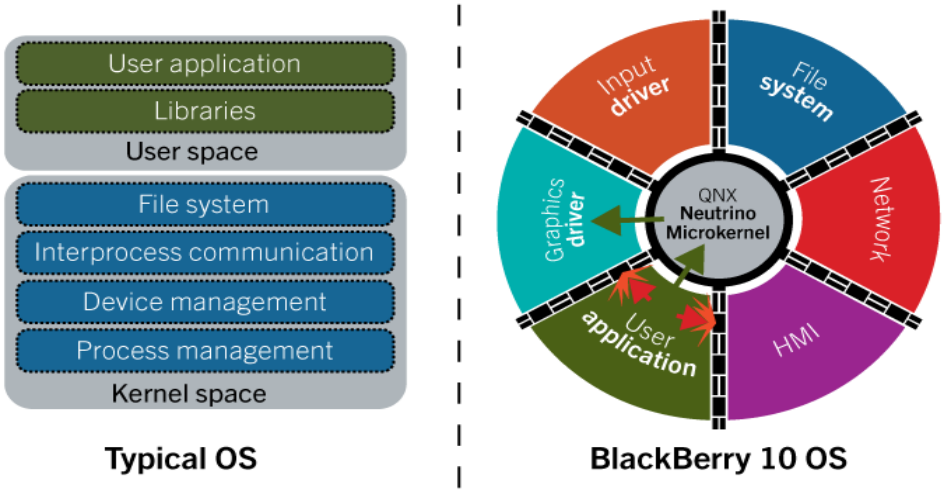

Figure 3.1: diagramme de BlackBerry 10 OS. [30]

2.3.2. Sécurité de la plate-forme BlackBerry 10 OS :

Diverses mesures sont utilisées à la sécurité mobile, pour protéger le matériel et le système d'exploitation BlackBerry 10 et établir la racine de la confiance. Les processus de cryptage et d'authentification BlackBerry utilisent la racine de la confiance pour créer des clés de cryptage et de signature qui protègent vos applications et vos données.[30]

Le BlackBerry 10 OS est inviolable, résilient et sécurisé. Son noyau effectue les actions clés suivantes pour protéger l'appareil :
- Quand il commence, il effectue un test d'intégrité. Si le test d'intégrité détecte des dommages au noyau, le périphérique ne démarre pas.
- Si un processus cesse de répondre, il isole un processus dans son espace utilisateur et redémarre le processus sans affecter négativement d'autres processus.
- Il utilise un partitionnement adaptatif pour empêcher les applications d'interférer ou de lire la mémoire utilisée par une autre application.
- Il valide les demandes de ressources et contrôle comment les applications accèdent aux fonctionnalités du périphérique, telles que l'accès à la caméra, aux contacts et aux informations d'identification du périphérique.[31]

2.4. Symbian OS :

2.4.1 définition :

Nokia créa Le système d'exploitation mobile nommé Symbian OS en 1998 en compagnie de Panasonic, Psion, Ericsson et Motorola. Nokia fut ensuite le principal utilisateur de Symbian pendant de nombreuses années pour équiper ses téléphones mobiles et smartphone, et racheta tous les droits du consortium Symbian Ltd en 2008.
Aujourd'hui, la plateforme pour téléphones mobiles Symbian succède à Symbian OS et Nokia Series 60, en unifiant ces deux composantes système. Auparavant, Symbian OS nécessitait une surcouche pour présenter une IHM aux utilisateurs. Le framework Series 60 de Nokia était alors un de ceux couramment utilisés dans ce but, en compagnie d'UIQ et Java ME. [32]

2.4.2. Les Malwares qui sont menacés l'OS Symbian: [33]

Symbian OS est soumis à une variété de virus dont le plus connu est Cabir. Habituellement, ils se transmettent par téléphone au téléphone par Bluetooth. Jusqu'à présent, aucun n'a profité de défauts dans le système d'exploitation Symbian, mais ils ont tous demandé à l'utilisateur s'il souhaitait installer le logiciel, avec des avertissements quelque peu importants qu'il ne peut y avoir confiance, bien que certains s'appuient sur l'ingénierie sociale, Souvent sous la forme de messages qui viennent avec le logiciel malveillant, ce qui signifie être un utilitaire, un jeu ou une autre application pour Symbian.

CardTrap est un virus qui est disponible sur différents types de smartphone qui a pour objectif de désactiver le système et les applications tierces. Il fonctionne en remplaçant le fichier qui est utilisé au démarrage du smartphone et celui de chaque application nécessaire à leur démarrage pour empêcher leurs exécutions. Il existe différentes variantes de ce virus dont Cardtrap.A pour

les appareils du type SymbOS. Il infecte également la carte mémoire avec les logiciels malveillants capables d'infecter Windows.

FlexiSpy est une application qui peut être considérée comme un cheval de Troie basée sur Symbian. Le programme envoie toutes les informations reçues et envoyées par le smartphone à un serveur FlexiSpy. Il a été créé à l'origine pour protéger les enfants et espionner les conjoints adultères. C'est pour cette deuxième partie (espionnage) qu'il peut être considéré comme un cheval de Troie.

Drever.A est un trojan de fichier SIS malveillant qui essaie de désactiver le démarrage automatique des applications Simworks et Kaspersky Symbian Anti-Virus.
Locknut.B est un trojan de fichier SIS malveillant qui prétend être un patch pour les téléphones mobiles Symbian S60. Lorsqu'il est installé, il bloque un composant de service système critique. Cela empêchera toute application d'être lancée dans le téléphone.
Mabir.A est essentiellement Cabir avec une fonctionnalité MMS ajoutée. Les deux sont écrits par le même auteur, et le code partage de nombreuses similitudes. Il se propage à l'aide de Bluetooth via la même routine que les premières variantes de Cabir. Au fur et à mesure que Mabir.A s'active, il recherchera le premier téléphone qu'il trouve et commence à envoyer des copies de lui-même sur ce téléphone.

Fontal.A est un trojan de fichier SIS qui installe un fichier corrompu qui provoque l'échec du téléphone lors du redémarrage. Si l'utilisateur essaie de redémarrer le téléphone infecté, il sera bloqué en permanence sur le redémarrage et ne pourra pas être utilisé sans désinfecter, c'est-à-dire l'utilisation de la combinaison de touches de reformatage qui permet au téléphone de perdre toutes les données. Étant un cheval de Troie, Frontal ne peut pas se propager seul - la manière la plus probable pour l'utilisateur d'être infecté serait d'acquérir le fichier à partir de sources non fiables, puis de l'installer sur le téléphone, par inadvertance ou autrement.

Une nouvelle forme de menace de logiciels malveillants pour Symbian OS sous la forme de «firmware cuisiné» a été démontrée lors de la conférence internationale Malware, MalCon, décembre 2010, par le pirate indien Atul Alex.

2.4.3 L'ignorance de la sécurité de la plate-forme:

Les périphériques Symbian OS 9.x peuvent être piratés pour supprimer la sécurité de la plate-forme introduite dans OS 9.1 en avant, permettant aux utilisateurs d'exécuter un code non signé. Cela permet de modifier les fichiers système et d'accéder aux zones précédemment verrouillées du système d'exploitation. Le hack a été critiqué par Nokia pour augmenter potentiellement la menace posée par les virus mobiles car un code non signé peut être exécuté.[33]

2.5 Android :

2.5.1 Définition :

Le système d'exploitation mobile Android ,est développé par l'Open Handset Aliance. Il a été annoncé en 2007 et en 2008, il est devenu une plateforme en code source ouverte. L'Android est basé sur le noyau Linux et utilise la plateforme java pour ses applications.
En termes d'application, Android a intégré plusieurs services de Google pour accéder rapidement aux services d'internet comme Gmail, YouTube, Google Talk, Google Calendar et Google Maps.
Android est un système d'exploitation puissant et moderne, caractérisé par la simplicité et la flexibilité; Cela signifie que le système est développé avec une simple langue java, et il s'adapte à de nombreuses structures différentes.
En outre, l'Android est open source; Ainsi, il donne aux développeurs la possibilité d'améliorer les applications. Le noyau Linux offre une excellente mémoire, gestion des processus, modèle de sécurité, support de bibliothèque partagée ... etc. Le SDK de l'Android offre complètement les API, avec un accès facile pour le développeur.

Une API (interface de programmation), est un ensemble de règles à suivre pour pouvoir interagir avec d'autres applications. Dans le cas de Google API, il permet notamment de communiquer avec Google Maps.[39] [40]

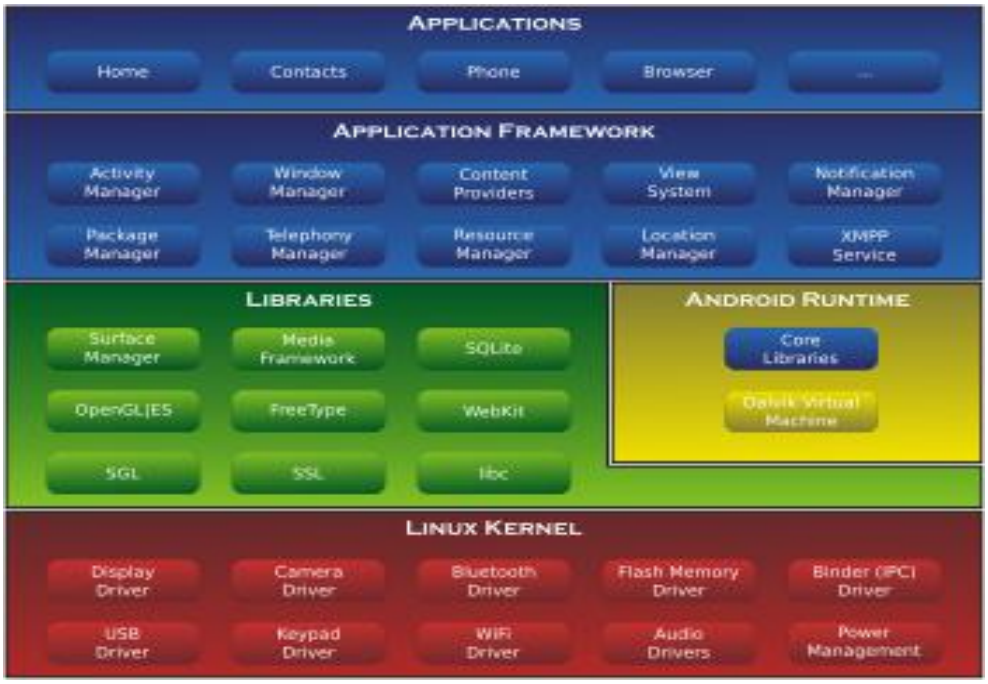

Figure 3.2: diagramme d'architecture du système d'exploitation Android**.** [40]

2.5.2 Sécurité et confidentialité :

- Caractéristiques techniques de sécurité :

Les applications Android sont exécutées dans un bac à sable, une zone isolée du système qui n'a pas accès au reste des ressources du système, à moins que les autorisations d'accès ne soient explicitement accordées par l'utilisateur lorsque l'application est installée.

Depuis février 2012, Google a utilisé son scanner de logiciels malveillants, Google affirme de surveiller et d'analyser les applications disponibles dans Google Play Store. Une fonctionnalité "Vérifier les applications" a été introduite en novembre 2012, dans le cadre de la version du système d'exploitation Android 4.2 "Jelly Bean", pour analyser toutes les applications, tant de Google Play que de sources tierces, pour des comportements malveillants. À l'origine, seulement pendant l'installation, Verify Apps a reçu une mise à jour en 2014 pour "constamment" analyser les applications et, en 2017, la fonctionnalité a été rendue visible par les utilisateurs dans un menu dans Paramètres.[40]
Avant d'installer une application, Google Play Store affiche une liste des exigences auxquelles une application doit fonctionner.

- Menaces de sécurité communes :

La recherche de la société de sécurité Trend Micro répertorie l' abus de service premium comme le type le plus courant de logiciels malveillants d'Android, où les messages texte sont envoyés à partir de téléphones infectés à des numéros de téléphone à taux élevé sans le consentement ni même la connaissance de l'utilisateur. D'autres logiciels malveillants affichent des publicités indésirables et intrusives sur l'appareil ou envoient des informations personnelles à des tiers non autorisés. Les menaces de sécurité sur Android augmentent de façon exponentielle; Cependant, les ingénieurs de Google ont fait valoir que la menace de malware et de virus sur Android est exagérée par les entreprises de sécurité pour des raisons commerciales, et ont accusé l'industrie de la sécurité de jouer avec crainte de vendre des logiciels de protection antivirus aux utilisateurs. Google soutient que les logiciels malveillants dangereux sont en fait extrêmement rares et un sondage réalisé par F-Secure a montré que seulement 0,5% des logiciels malveillants d'Android signalés étaient issus du magasin Google Play. [40]

3. Conclusion

Les réseaux mobiles et la sécurité sont considérés comme le contraire par de nombreux utilisateurs. Il est difficile de croire en la sécurité mobile lorsqu'on a une telle accessibilité évidente à un support sans fil. . Les réseaux mobiles héritent du problème de sécurité en raison de la présence de support sans fil sans oublier les caractéristiques physiques des unités mobiles telles que les ressources limitées en énergie et en traitement.

Cependant, la communauté académique et industrielle de la recherche a mis au point des mécanismes et des protocoles de sécurité pour perpétuer ce mariage entre les réseaux mobiles et la sécurité.

En dépit de la diversité de ces mécanismes de sécurité, ils ne sont pas tous applicables dans les réseaux mobiles en raison des contraintes de ces derniers. Nous avons donc besoin de concevoir des mécanismes de sécurité spécifiques aux réseaux mobiles, tout en respectant ces propres caractéristiques.

CHAPITRE IV

attaques aux appareils mobiles

1 Introduction :

Tout appareil mobile connecté à un réseau informatique est potentiellement vulnérable à une attaque.
Une attaque peut exploiter une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur internet des attaques ont lieu en permanence, à raison de diverses attaques visent a chaque machine connectée.
Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

2. Les attaques en réseau mobile :

Les attaques en réseaux mobiles aujourd'hui sont si nombreuses qu'il serait illusoire de prétendre les décrire tous. Cependant, il est possible d'élaborer une typologie des faiblesses de sécurité afin de mieux comprendre ces attaques, qui ont la caractéristique commune d'exploiter les faiblesses de sécurité.
Les attaques sur les réseaux mobiles peuvent être classées dans les catégories suivantes:

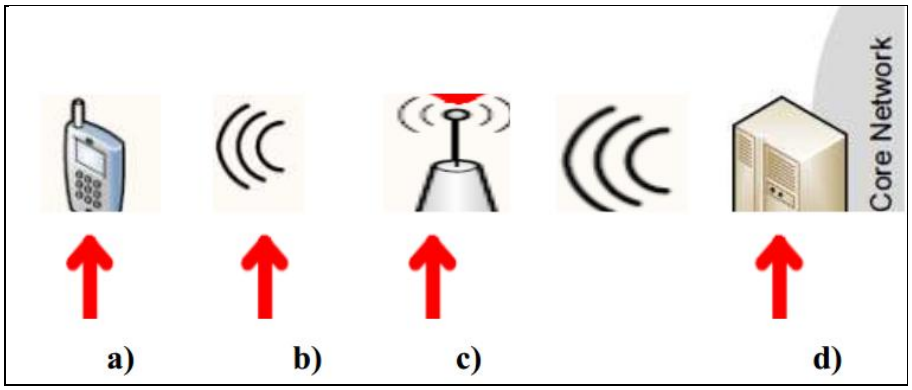

Figure 4.1: Les attaques en réseaux mobiles

a) appareil mobile. b) Attaques sur l'interface radio.
c) Attaque sur les points d'accès. d) Attaques sur le réseau cœur.

2.1 Les attaques sur les appareils mobiles :

Les unités mobiles sont exposées à des attaques que les ordinateurs. La sécurité des unités mobiles est plus complexe que la sécurité des ordinateurs à cause de leurs propres caractéristiques. L'unité mobile peut exposer à plusieurs risques comme.

2.1.1 Attaques par déni de service :

Ils ont pour but de rendre un service ou un appareil inutilisable pour son utilisateur, en le rendant indisponible. Les problèmes des attaques DoS contre les appareils mobiles sont imputables principalement à leur forte connectivité et fonctionnalités réduites. Par exemple, une attaque DoS courante consiste à envoyer une grande quantité de trafic à une unité connectée au réseau. Alors qu'un attaquant a besoin de beaucoup de ressources pour attaquer un ordinateur normal ou un serveur, un appareil mobile, par le fait de sa capacité de traitement limitée, peut être plus facilement rendu inutilisable par l'envoi massif de trafic depuis l'attaquant. [42]
Le Déni de service (DoS) sur VoIP s'appuie d'un ensemble des requêtes qui sont lancés « flooding SIP », « TCP syn » ou « UDP », (par exemple, demandes d'enregistrement et d'appels...) visent de saturation des services VoIP. L'utilisation de ce genre d'attaques notamment, se cible les serveurs, les passerelles, les proxys ou encore les téléphones IP qui voient leurs ressources, sont rapidement saturées par ces requêtes dont l'objectif est de perturber, voire mettre hors service le système ciblé. Une autre attaque également répandue consiste à envoyer des commandes « BYE » au téléphone afin de mettre fin à la conversation en cours... [44]

2.1.2 Virus :

Les virus, vers et chevaux de Troie, sont des menaces pour les appareils mobiles, de la même manière qu'ils le sont pour les ordinateurs. Les vers peuvent avoir un coût s'ils se répandent en utilisant un service pour lequel l'utilisateur est facturé, comme le MMS par exemple. Dans ce cas, un vers s'envoyant lui-même à des centaines d'unités mobiles peut causer un dommage substantiel au propriétaire de l'appareil infecté. D'autre type de virus peut facilement outre passer les mécanismes de sécurité configurés seulement pour détecter des attaques externes.
Les virus peuvent aussi placer un cheval de Troie sur l'appareil, permettant le vol des données ou l'enregistrement des activités d'un utilisateur, en envoyant périodiquement des rapports.
Un virus a été découvert en mars 2005 sous le nom CommWarrior, est plus discret avec sa version CommWarrior.Q qui se diffuse de trois façons, à savoir les ondes radio Bluetooth, les cartes mémoire, mais aussi, notamment, via les messages MMS (Multimedia Messaging Service). Ses récoltes apprises sont des périphériques exécutant le système d'exploitation SymbianOS dans la version 8.1 et antérieures. [43]
Autres virus nommé Geinimi, est un logiciel malveillant à s'attaquer à la plateforme Android et pareillement, la première véritable instance de botnet mobile. il s'appuie sur un serveur distant

qui lui envoie des commandes comme l'installation ou la suppression de certains logiciels sur le smartphone.

2.1.3 L'usurpation de l'identité :

L'usurpation de l'identité (en anglais, Shoping ou Impersonation), dans ce type d'attaques, l'attaquant essaie de prendre l'identité d'un autre nœud mobile afin de pouvoir recevoir ses messages ou d'avoir des privilèges qui ne lui sont pas accordés. [45]
Un attaquant peut usurper l'identité d'usager, partir de copie les données de sa carte SIM et se faire passer pour lui. Ceci pose des problèmes de sécurité dans des pays où les appareils mobiles permettent de faire des commandes, de consulter ses comptes ou encore servir de carte d'identité.

2.2. Attaques sur l'interface radio :

L'interface radio par leur nature plus vulnérable aux attaques que l'interface filaire.
Le support de transmission étant partagé. Quiconque se trouvant dans la zone de couverture du réseau peut en intercepter le trafic ou même reconfigurer le réseau à sa guise. De plus, si une personne malveillante est assez bien équipée, cette dernière n'a pas besoin d'être située dans la zone de couverture. Il lui suffit d'utiliser une antenne avec ou même sans l'aide d'un amplificateur pour accéder au réseau.
Il existe un grand nombre d'attaques différentes qui influencent la connectivité d'une cible.

2.2.1. Attaque par interposition (Man In The Middle Attack) :

Un attaquant peut se reposer entre une unité mobile et un point d'accès et intercepter les messages entre eux. C'est une attaque dangereuse qui touche la confidentialité et l'intégrité des informations, elle est désigné aussi écoute clandestine des transmissions sans fil pour objectif d'extraire des informations confidentielles.[46]
Les attaques sur l'interface radio par interposition peuvent être :
Passive : l'attaquant écoute seulement les communications entre le dispositif mobile et la station de base pour extraire des informations confidentielles comme les noms d'utilisateurs et mots de passe présente dans toutes les communications sans fil.
Active : en plus de l'écoute, l'attaquant injecte ou modifie les données transmisses.
C'est à cette époque d'ailleurs que l'on rencontre Zitmo. Ce virus est la première extension mobile connue de ZeuS, un cheval de Troie bancaire pour PC très virulent. Zitmo intercepte les SMS expédiés par les banques aux clients pour détourner les opérations bancaires en ligne.

Comme exemple, un smartphone compromis peut enregistrer les conversations de l'utilisateur avec d'autres personnes et les transmettre. Ceci provoque des problèmes de confidentialité pour les utilisateurs et de sécurité pour les industries.

2.2.2. Attaque par l'épuisement du medium :

le canal de transmission hertzien se restreinte d'une bande passante. Il s'épuise d'un ensemble des trames massives qui sont envoyés en même temps.par exemple un nœud peut très bien saturer le médium en émettant des trames de contrôle ou de données et empêcher ainsi les autres nœuds de communiquer.

2.3. Attaque sur les points d'accès :

2.3.1. Dénie de service :

Un attaquant peut acheter un équipement de station de base BTS et l'installe. Le terminal mobile se reliera au BTS attaquants, s'il a les caractéristiques de l'opérateur et un meilleur signal que la vraie station de base.
La fausse station de base se pose entre les unités mobiles et la station de base d'origine et intercepte les communications sans être découvert. [47]
L'attaquant pourrait envoyer un signal "occupé" à l'unité mobile chaque fois qu'il demande un service. Aussi, il est possible que le BTS réponde à une demande de service par un message interdisant la station mobile d'accéder au canal dans un temps spécifique. Cette attaque peut être considérée comme déni de service puisqu'elle dénie les utilisateurs légitimes d'employer le réseau.

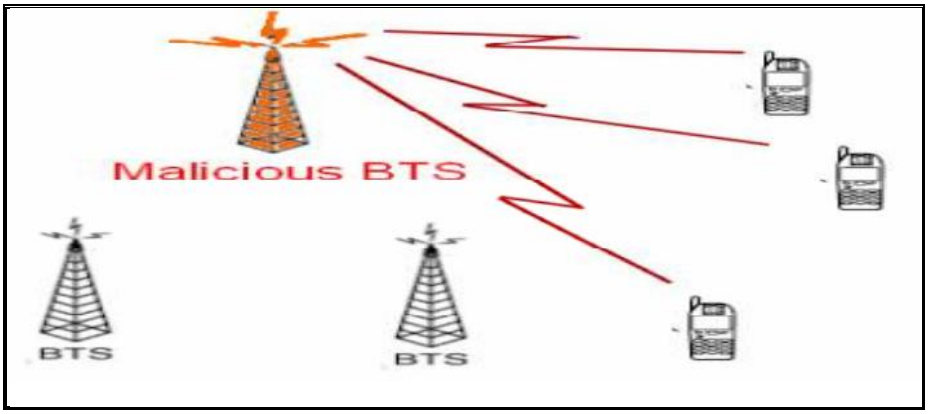

Figure 4.2: Attaque sur les BTS.[47]

Un pirate qu'utilise la méthode du `jumeau diabolique' met en place un identifiant (SSID) pour reproduire un point d'accès (AP) d'une entreprise, comme exemple. Puis le pirate perturbe le point d'accès légitime en le déconnectant, en lui envoyant un déni de service ou en créant suffisamment d'interférences radio autour de l'AP, avec par exemple un objet en métal, pour interrompre et empêcher toute communication avec des ordinateurs voisins ou tout autre moyen

de communication. Les utilisateurs connectés à l'AP légitime, perdent leur connexion et se reconnectent sur le `jumeau diabolique' permettant ainsi au pirate d'intercepter tout le trafic.

2.3.2. Détournement d'une session :

Un utilisateur malveillant peut détourner une session déjà établie, et peut agir en tant que station de base légitime.
Attaque par « relecture » ou « Détournement d'enregistrement » de sessions autorisées obtenues grâce à une analyse de trame par un « sniffer » sur le réseau ou par interception de trafic. Cette attaque se déroule au niveau du protocole SIP, elle utilise la commande « Register » qui sert à localiser un utilisateur par rapport à son adresse IP. Le pirate peut alors rejouer ces sessions de « register » valide en modifiant uniquement l'adresse IP de destination en sa faveur…Cette attaque est due au fait que le protocole SIP transite une partie des informations en clair, il est donc possible de mettre en place du SIPS qui intègre des mécanismes d'authentification et assure l'intégrité des données. [48]

2.4. Attaques sur le réseau cœur[10] :

Le réseau cœur est considéré la base des réseaux de mobiles. Il représente la base des fonctionnalités des unités mobiles, comme la fonctionnalité téléphonique ou de suivi d'emails. Donc, une attaque réussie sur le cœur réseau peut bloquer totalement le réseau de mobile.

2.4.1. Dénie de service distribué :

Le but principal d'une attaque de type dénie de service distribué DdoS est de rendre un serveur public incapable de fournir des services aux utilisateurs légitimes. Une station de base peut être une cible typique d'une telle attaque de DdoS. Come les virus informatique ne concernent pas seulement les ordinateurs, ils touchent même les réseaux informatiques comme les réseaux de mobiles, donc ils sont considérés le moyen principale pour réaliser ce type d'attaque.
Un attaquant équipé par des virus peut envoie des paquets de commande à tout les nœuds de réseau pour demander des services de réseau cœur. Avec la limitation des capacités de traitement des requêtes des demandes ; la cible sera immédiatement bloqué et par conséquence le réseau sera bloqué. [42]
Quand le réseau cœur stocke des informations vitales pour la sécurité comme les mots de passe des utilisateurs, les clés,….. , on distingue d'autre forme d'attaque comme :

[10] Core de réseau, est la partie centrale d'un réseau de télécommunications qui fournit différents services aux clients connectés par le réseau d'accès. L'une des principales fonctions consiste à acheminer les appels téléphoniques dans le RTPC.

2.4.2. l'attaque par force brute :

Généralement les mots de passe de la plupart des logiciels sont stockés cryptés dans un fichier. Pour obtenir un mot de passe, il suffit de récupérer ce fichier et de lancer un logiciel de brute force craking. Ce procédé consiste à tester de façon exhaustive toutes les combinaisons possibles de caractères (alphanumériques + symboles), de manière à trouver au mois un mot de passe valide. Cette attaque se base sur le fait que n'importe quel mot de passe est crackable. Ce n'est qu'une histoire de temps. Mais la puissance des machines double tous les deux ans. On parle de plus en plus de processeurs 1,2 GHz… de plus, les crackers n'hésitent pas à fabriquer des cartes électroniques de cracking, ce qui améliore en conséquence la rapidité de la machine, donc les chances de trouver un mot de passe valide. En générale, cette méthode est empruntée lorsque la méthode du dictionary cracking a échoué. [49]

3. Types d'attaques aux appareils mobiles :

3.1. Attaques basées sur les moyens de communication :

3.1.1. Attaque basée sur les SMS et MMS :

Les failles dans le gestionnaire des SMS et des MMS sont ciblées par certaines attaques.
Il est possible en envoyant un SMS mal-formé de bloquer le téléphone à redémarrer. Lorsqu'un utilisateur du modèle Nokia entre une adresse mail supérieure à 32 caractères cela mène au dysfonctionnement complet du gestionnaire de messagerie qui est mis hors-service. Cette attaque est nommée "curse of silence". La norme impose que la taille maximale d'une adresse mail fixée a 32 caractères.[51]

Le virus CommWarrior exploit le carnet d'adresses et envoie des messages MMS incluant un fichier infecté aux destinataires.

3.1.2. Attaques basées sur les réseaux de communication :

- Attaques sur les réseaux GSM :

L'attaquant peut tenter à casser le chiffrement du réseau mobile. Le chiffrement des réseaux GSM fait partie de la famille des algorithmes A511. Ce dernier étant une version plus faible. Il a

[11] A5/1 est un algorithme de chiffrement par flot utilisé dans le cadre des communications GSM. Il produit une suite pseudo-aléatoire avec laquelle on effectue un XOR avec les données. Une autre variante existe, la A5/2. On trouve aussi le terme de A5/3 (KASUMI), bien que ce dernier ne soit pas un algorithme de chiffrement par flot mais

été prouvé qu'il était possible de casser cet algorithme de chiffrement. En juillet 2007, le 3GPP a décidé d'interdire l'usage de la version A5/2. [50]

- Attaques sur les réseaux Wifi :

L'attaquant tente de trouver des informations confidentielles à partir d'écoute des communications Wifi . Cette information sécrète peut être une clé privée ou publique de l'expéditeur ou du destinataire ou des données sécrétées.
Au départ les réseaux sans fils étaient sécurisés par des clés WEP 12, ces clés sont des chiffrements courts et faibles qui sont adoptés des failles. ils se constituent essentiellement des algorithmes de vérification d'intégrité et d'authentification qui sont très facilement contournables et l'algorithme de chiffrement RC4 ,se présente des clés faibles et l'espace disponible pour les IV est trop petit.
La taille des clés est courte de 40 bits (5 caractères en code ascii !!!) ou 104 bits et/ou trop simples , qui sont partagées sur tous les clients connectés, et d'un format de chiffrement statiques. et simple à les Casser par attaque dictionnaire.[51]

Actuellement, le protocole de sécurité WPA à protéger les réseaux sans fil.
La clé WPA est une "clé pré-partagée". Le chiffrement peut être vulnérable si la longueur de la clé partagée qu'est choisi par l'usager, est courte. Par exemple, les utilisateurs d'appareils mobiles ont tendance à définir des clés courtes qui ne contiennent que des nombres. L'attaquant réussisse une attaque par force brute. Si l'attaquant arrive à casser la clé d'identification, il lui sera possible d'attaquer tout le réseau.

- Principe des attaques sur le Bluetooth :

Les appareils mobiles, leurs problèmes de sécurité sont liés au Bluetooth. Soit que la fonction Bluetooth est activée par défaut sur le terminal, ou via d'une commande manuelle s'exécute par l'usager en cas de la demande d'une autre interface Bluetooth. Cette connexion externe permet de manipuler des messages SMS ou MMS par un cheval de Troie ou un mini d'application .ils sont installés sur le terminal à l'insu de l'utilisateur qui permettra d'autoriser automatiquement toutes nouvelles connexions Bluetooth d'autres mobiles ou d'ordinateurs portables.[51]

Les logiciels malveillants utilisent des vulnérabilités tous simplement parce que les services non enregistrés ne nécessitent aucune authentification. Par exemple ; Cabir est un ver qui se propage via la connexion Bluetooth. Le ver recherche les appareils à proximité, avec le Bluetooth en mode découverte et s'envoie vers le périphérique cible. La transmission doit être acceptée par le destinataire ; l'utilisateur doit accepter le fichier entrant et installer le programme. C'est seulement après l'installation que le ver infect l'appareil.[50]

---

de bloc. L'algorithme A5 utilise une clé de 64 bits mais son implémentation dans le GSM n'utilise que 54 bits effectifs (10 bits sont mis à zéro).

[12] Le WEP (Wired Equivalent Privacy) est le protocole de chiffrement par défaut introduit dans la 1ère norme 802.11 datant de 1999. il permet de sécuriser les réseaux sans file wifi,

3.2. Attaques basées sur les failles des applications logicielles :

Certaines attaques sont basées sur des vulnérabilités de l'OS ou des applications embarquées.

3.2.1. Failles du navigateur Web :[51][52]

L'attaquant utilise le navigateur Web sur les appareils mobiles pour les cibles. Les navigateurs Web mobiles sont issus de moteurs de liaison HTTP et de rendu du HTML, tels que WebKit 13ou Gecko.
Par exemple, l'exploit des failles du navigateur Web mobile pour déverrouiller l'iPhone avec le firmware 1.1.1 . Autre exemple, Il y avait une faille basée sur le dépassement de tampon de la pile dans une bibliothèque utilisée par le navigateur Web .

Une faille était due à un module de bibliothèque obsolète et vulnérable, sur le navigateur web mobile d'Android . Elle a été découverte en octobre 2008. Cette vulnérabilité issue du système de sandboxing qui limitait les effets de cette faille pour le processus de navigateur Web mobile sur Android OS. Tous les attaques classiques liés au Web comme; Le phishing, les sites Web malveillants sont pertinents pour les appareils mobiles.

La grande différence est que les appareils mobiles ne possèdent pas encore d'antivirus puissant ,selon L'étude de la société de sécurité allemande Fraunhofer AISEC, qui a été examiné les logiciels antivirus d'Avast, AVG, Bitdefender, ESET, F-Secure, Kaspersky, Lookout, Intel Security (anciennement McAfee), Norton, Sophos et Trend Micro, a révélé que "les applications antivirus testées ne le font pas Fournir une protection contre les logiciels malveillants personnalisés ou les attaques ciblées ", et que" les applications antivirus testées n'ont pas non plus été en mesure de détecter les logiciels malveillants complètement inconnus à ce jour ..

3.2.2. Failles du système :

Les Attaques graves sont venues de l'élimination des fonctions de protection qui nécessitent un changement du système d'exploitation lui-même, afin d'utiliser les firmwares et des certificats de signature malicieuse.

Théoriquement l'appareil mobile présente un avantage par rapport aux disques durs car les fichiers OS sont en firmware, et ne peuvent pas être modifiés par des logiciels malveillants. Mais dans certains systèmes d'exploitation, il était possible de contourner ceci: dans Symbian OS, il était possible d'écraser le fichier avec un fichier du même nom.

13 WebKit est une bibliothèque logicielle libre permettant aux développeurs d'intégrer facilement un moteur de rendu de pages Web dans leurs logiciels. Elle est disponible sous licence BSD et GNU LGPL. Originellement réservée au système d'exploitation Mac OS X (à partir de la version 10.3 Panther), elle a été portée vers Linux et Windows. Ainsi le portage de WebKit pour les environnements GTK+ et Qt se nomment respectivement WebKitGTK+ et QtWebKit.

La sécurité du firmware Symbian de nokia est basée sur un fichier de configuration SWIPolicy central. Par exemple, il était possible, en 2008, de manipuler un firmware Nokia avant que celui-ci n'ait été installé, en fait, dans certaines versions téléchargeables, ce fichier était lisible par l'homme, il était donc possible de modifier et de modifier l'image du firmware, ceci a été résolu Par une mise à jour de Nokia. Précédemment, les vulnérabilités ont été apparues dans l'exécution de machines virtuelles de certains appareils.

En fait, lorsque le système d'exploitation Android est intégré dans la majorité des appareils mobiles et les plus exploités. Cependant, plusieurs des failles ont été émergés au niveau de ce système. Une faille dénommée « Exploid », bien connue par administrateurs Linux, est référé par le code CVE-2009-1185. Rage Against The Cage, une faille due au problème de la fonction du processus adb lorsque RLIMIT NPROC a été atteint et une faille qui permet de modifier la valeur de la constante globale (normalement en lecture seule) ro.secure , surnom « Killing In The Name Of « .ainsi le bug qui se constitue d'une erreur d'implémentation de /dev/ashmem . Cette constante, définie à la compilation du système, indique au processus adb s'il doit s'exécuter sous l'identité root.

En effet, il est virtuellement possible d'écrire dans le répertoire /system (au travers de la commande adb remount à l'intérieur du terminal).un certain nombre de téléphones modernes disposent d'une protection contre le reflashage intempestif de la partition système d'android. Cette protection est souvent liée à l'utilisation d'un composant mémoire capable de vérifier une signature cryptographique (par exemple un composant eMMC).

En plus, la haute gravité soutenue des bugs sur le système Android .ils permettent à l'attaquant de les exploits afin de commander et de contrôler les périphériques infectés, à l'insu de l'utilisateur. Par exemple, Stagefright est le groupe de bogues logiciels qui affectent les versions 2.2 ("Froyo") et plus récent du système d'exploitation Android, permettant à un attaquant d'effectuer des opérations arbitraires sur le périphérique de la victime par l'exécution de code à distance et l'escalade de privilèges. D'autre exemple, un bug touchant environ 60 % des terminaux tournant sous Android a récemment été découvert. La faille exploite le composant WebView des systèmes utilisant les versions antérieures à 4.4 (Kitkat).

3.2.3. Failles logicielles :

les vulnérabilités d'implémentation logicielle sont faciles à identifier dans le système Android en cas de l'utilisation massive de code Open Source .il se concerne de mener les alertes de sécurité des principaux projets ! Lorsqu'ils sont disponibles, ce qui n'est pas assurément le cas pour le noyau Linux...
Les vecteurs principaux (en termes de nombre de lignes de code et d'exposition) sont le système Linux et le navigateur Web (et particulièrement le moteur WebKit, commun avec Safari).

Il ne faut pas oublier non plus qu'Android intègre Flash Player... et se situe avec les mêmes failles. comme exemple ces failles permettent au attaquant de connecter au port série virtuel d'une

application vulnérable, afin de prendre le contrôle total de l'appareil. [52]

4. Exemples des attaques aux appareils mobiles :

4.1. Aircrack-ng :

4.1.1. Définition :

Aircrack-ng est une suite complète d'outils pour évaluer la sécurité du réseau Wifi. Il se concentre sur différents domaines de la sécurité Wifi:
Surveillance: capture et exportation de données par paquets pour les fichiers texte pour un traitement ultérieur par des outils tiers.
Test: Vérification des cartes Wifi et des capacités du pilote (capture et injection).
Cracking: WEP[14] et WPA[15] PSK[16] (WPA 1 et WPA2) .[53][54]

Tous les outils sont une ligne de commande qui permet des scripts lourds. Beaucoup de GUI[17] ont profité de cette fonctionnalité. Il fonctionne principalement Linux, mais aussi Windows, OS X, FreeBSD, OpenBSD, NetBSD, ainsi que Solaris et même eComStation2.
Cependant, ce logiciel peut permettre à un cracker d'entrer sans autorisation sur un réseau informatique, ce que de nombreux pays répriment comme un délit.

4.1.2. Principe de fonctionnement :

Ces paramètres, sont les adoptés dans tous les exemples :
00:13:10:1F:9A:72 est l'adresse MAC du point d'accès (BSSID) sur le canal 1, avec le SSID hakin9demoet.
00:09:5B:EB:C5:2B est l'adresse MAC du client sans fil (utilisant le WEP ou WPA-PSK

[14] Le WEP (Wired Equivalent Privacy) est le protocole de chiffrement par défaut introduit dans la 1ère norme 802.11 datant de 1999. Il est basé sur l'algorithme de chiffrement RC4 avec une clé secrète de 40 ou 104 bits combinée à un vecteur d'initialisation (Initialisation Vector – IV) de 24 bits afin de chiffrer un message en clair M et sa somme de contrôle (checksum) – l'ICV (Integrity Check Value). Le message chiffré est alors déterminé en utilisant la formule suivante : C= [M|| ICV(M)] + [RC4(K|| IV)].

[15] Wifi Protected Access (WPA et WPA2) est un mécanisme pour sécuriser les réseaux sans-fil de type Wifi. Il a été créé au début des années 2000 en réponse aux nombreuses et sévères faiblesses que des chercheurs ont trouvées dans le mécanisme précédent, le WEP.

[16]Le phase-shift keying (ou PSK, soit « modulation par changement de phase1 ») désigne une famille de formes de modulations numériques qui ont toutes pour principe de véhiculer de l'information binaire via la phase d'un signal de référence (porteuse), et exclusivement par ce biais.

[17] Graphic Utilizator Interface(GUI) : une interface permet à l'utilisateur de l'adapte, puisque elle est visuelle et graphique.

suivant les cas). La plupart des commandes nécessitent les privilèges root[18]. [55]

En début, il doit être activé le mode moniteur sur les cartes sans fil ,pour capturer tous le trafic (voir le **Listing 1**).

Listing 1. Activation du mode moniteur

```
# airmon.sh  start  ath0
Interface          Chipset          Driver
ath0               Atheros          madwifi (monitor mode enabled)
```

La deuxième étape consiste de découvrir les réseaux sans fil environnants, à partir de scannage des 14 canaux qui sont utilisés par les réseaux Wifi (voir le **Listing 2**). [55]

Listing 2. Découverte des réseaux et des clients Wifi environnants

```
# airodump  ath0  wep-crk  0
                    BSSID              PWR  Beacons  # Data  CH  MB  ENC          ESSID
00:13:00:13:10:1F:9A:72                 62    305          16     1    48  WEP  hakin9demo
                    BSSID                STATION          PWR     Packets          ESSID
      00:13:00:13:10:1F:9A:72      00:0C:F1:19:77:5C      56       1          hakin9demo
```

À partir du résultat du **Listing 2**, il peut de déduire :
Un point d'accès avec le BSSID 00:13:10:1F:9A:72 utilise le protocole WEP sur le canal 1 avec le SSID hakin9demo.
Un client identifié par la MAC 00:0C:F1:19:77:5C est associé et authentifié sur ce réseau sans fil.

La capture doit être réalisée sur le canal adéquat pour éviter de perdre des paquets lors du passage sur les autres canaux.

[18] Dans les systèmes de fichiers informatiques, la racine des répertoires ou dossiers (appelé aussi la racine d'un disque) est la base des répertoires dans la hiérarchie. Il peut être imagé par un tronc d'un arbre, c'est-à-dire le point de départ de toutes les branches (de tous les répertoires/dossiers).

L'étape à suite, il est possible de lancer l'injection de trafic avec aireplay en utilisant les informations précédemment découvertes. L'injection commencera dès qu'une requête ARP correspondant au BSSID attaqué sera capturée sur le réseau sans fil :

```
# aireplay -3 \
-b 00:13:10:1F:9A:72 \
-h 00:0C:F1:19:77:5C \
-x 600 ath0
(...)
Read 980 packets
(Got 16 ARP requests),
Sent 570 packets...
```

En fin, il est utilisé l'aircrack pour casser la clé WEP. Il est possible de lancer cette étape sur le fichier pcap a lors que airodump capture toujours le trafic (voir les résultats d'aircrack sur la Figure 1) :

```
# aircrack -x -0 wep-crk.cap [55]
```

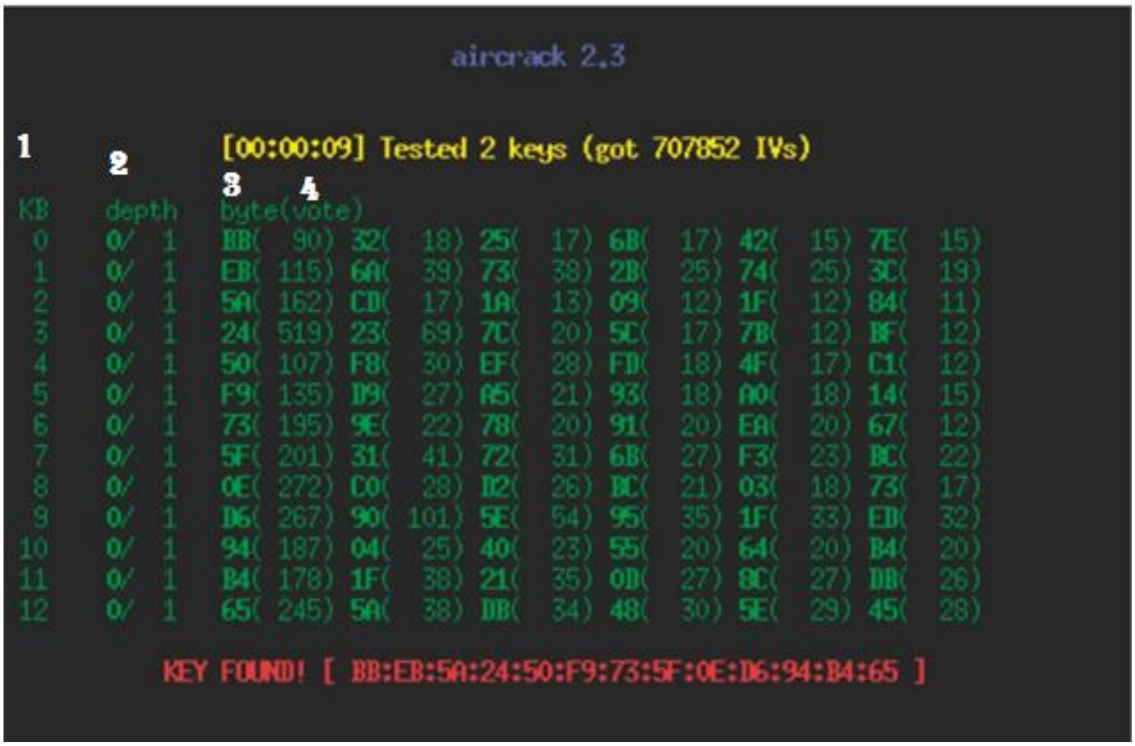

Figure 4.3: Capture d'écran des processus Aircrack-ng.

1. L'Octet de la clé.
2. Profondeur de recherche de la clé actuelle.
3. les vecteurs d'initialisation fuités en Octet.
4. Évaluation indiquant que l'information est correcte. [55]

En utilisant une série de tests statistiques appelés les attaques FMS [19]et Korek[20], les votes sont accumulés pour les clés probables pour chaque octet clé de la clé WEP secrète. Différentes attaques ont un nombre différent de votes associés à eux car la probabilité de chaque attaque donnant la bonne réponse varie mathématiquement. Plus il y a d'accumulation de valeur de clé potentielle particulière, plus il est probable qu'elle soit correcte. Pour chaque octet de touche, l'écran affiche la clé secrète probable et le nombre de votes accumulés jusqu'à présent. Inutile de dire que la clé secrète avec le plus grand nombre de votes est probablement correcte mais n'est pas garantie. Aircrack-ng testera ensuite la clé pour la confirmer. [53]

À la fin, tout est simplement une mathématique "simple" et une force brute21!

4.1.3. La description :

Aircrack-ng peut récupérer la clé WEP une fois que suffisamment de paquets cryptés ont été capturés avec airodump-ng. Cette partie de la suite aircrack-ng détermine la clé WEP en utilisant la méthode simple de cassage de clé WEP.
L'attaque pratique contre le WEP s'appuie sur une suite d'outils composée de 3 principaux binaires étant utilisé successivement pour retrouver la clé :

- airodump : permet de découvrir les réseaux WEP environnants,
- aireplay : permet d'injecter artificiellement du trafic,
- aircrack : récupérateur de clé WEP utilisant les IVs uniques collectés préalablement.

L'injection de trafic utilisant aireplay n'est supportée que sur une certain nombre de puce Wifi, le support pour l'injection en mode moniteur nécessite la dernière version des pilotes

[19] "Les cryptoanalystes Fluhrer, Mantin et Shamir (FMS) ont découvert des faiblesses inhérentes à l'algorithme RC4 de programmation des clés. Or l'algorithme RC4 utilisé par WEP se sert d'un vecteur d'"initialisation de 24 bits et ne renouvelle pas les clés de cryptage de manière dynamique. Fluhrer, Mantin et Shamir ont pu montrer que ces faiblesses pouvaient avoir des applications pratiques dans le décryptage des trames 802.11 qui utilisent WEP. Cette attaque se concentre sur une classe élargie de vecteurs d'"initialisation faibles qui peuvent être générés par RC4 et met en évidence les méthodes qui permettent de « casser » la clé en utilisant certaines formes récurrentes des vecteurs d'"initialisation.
[20] les attaques de Korek se basent toutes sur la même technique. L'idée est d'exploiter le biais de Roos dans le KSA de RC4, et de le combiner à d'autres vulnérabilités du PRGA. Le premier type d'attaque a pour but d'envoyer une certaine valeur contenant un octet de la clé secrète (par exemple K[3]) directement sur le premier ou le deuxième octet du keystream. Il s'agit de la généralisation des attaques FMS. Le deuxième type d'attaque est d'agir indirectement sur la valeur du premier octet du keystream. Un dernier type d'attaque vote négativement pour des valeurs d'octets de la clé secrète. Par exemple, certaines valeurs ne sont pas possibles. Ces votes négatifs aident à améliorer le recouvrement de la clé secrète.
[21] L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.

modifiés, car il est possible d'injecter et de capturer simultanément le trafic ,en utilisant une seule carte sans fil. [54] [55]

Le rôle de l'attaquant est d'engendrer du trafic vise de capturer des IVs uniques transmis entre le point d'accès et un client normal. Certaines données chiffrées sont facilement détectables car elles ont des longueurs fixes, des adresses destinations fixes, etc. C'est le cas par exemple des requêtes ARP22. Ces requêtes ARP peuvent être rejouées afin de générer des réponses ARP d'un client légitime, ces messages étant chiffrés avec de nouveaux IVs.[48]

4.2. Stagefright :

4.2.1. Définition :

Stagefright est une vulnérabilité critique pour Android. Il permet à un attaquant d'effectuer des opérations arbitraires sur le dispositif de la victime par l'exécution de code à distance et une élévation de privilèges. après avoir traité un message MMS entrant en naviguant sur le Web. Dans de nombreux cas, l'attaque ne nécessite aucune action de l'utilisateur final. Pour aggraver les choses, l'attaquant peut supprimer le MMS avant de l'ouvrir. [56]

4.2.2. Description :

Les chercheurs en sécurité démontrent des vulnérabilités avec une preuve de concept qui envoie des messages MMS spécialement conçus au dispositif victime et, dans la plupart des cas, ne nécessite aucune action de l'utilisateur final lors de la réception des messages pour réussir. L'utilisateur n'a rien à voir avec "accepter" le bug - il se passe dans l'arrière-plan. Le numéro de téléphone est la seule information cible. [56]

Le vecteur d'attaque sous-jacent exploite certaines vulnérabilités de débordement d'entier dans le composant de noyau applications appelé « Stagefright », qui est une bibliothèque de logiciels complexes mis en œuvre principalement en C ++ dans le cadre du Android Open Source Project (PSBA) et utilisé comme moteur de back-end pour jouer différents formats multimédias tels que les fichiers Mp4.

Les bugs découverts ont été fournis avec plusieurs identificateurs de vulnérabilité et d'exposition communes, qui sont collectivement appelés le bug Stagefright.

[22] Le protocole ARP (Address Resolution Protocol– RFC826) est utilisé pour faire la correspondance entre des adresses IP sur 32 bits et l'adresse Ethernet sur 48 bits (les réseaux Wifi utilisent aussi le protocole Ethernet).

4.2.3. Exemple :

L'attaquant peut préparer un MMS contenant à la fois le code d'un malware et une séquence d'instructions destinées notamment à supprimer le message. Il l'envoie à sa victime, la bibliothèque Stagefright de l'appareil, lorsqu'elle est appelée, est pris en charge, le contenu qu'est déjà repéré .elle commence à traiter le message, alors que la victime n'a pas besoin de réveiller son téléphone et d'aller lire le MMS, puisque le travail se fait en amont et ne trouve pas le moindre signe d'activité suspecte lorsqu'il se réveille. C'est évidemment le danger, aucune action n'est nécessaire.[56]
Si un code particulier est intégré dans un cliché, Stagefright se charge de le lire et de le traiter, ouvrant alors la voie à un malware. Un autre scénario possible est la visite d'une page web spécialement conçue puisque la bibliothèque est appelée par d'autres applications pour lire les photos, vidéos, etc. Cela est donc loin de concerner seulement les outils de messageries.

4.3. GinMaster :

4.3.1. Définition :

Android / GinMaster.A-0 est un logiciel malveillant qui envoie les messages SMS, reçus à un serveur distant.
Il Raccorde le périphérique infecté et Envoie des informations sensibles à un serveur distant .il permet de télécharger et d'installer l'application sans aucune préoccupation de l'utilisateur.

Ce malware exige que l'utilisateur l'installe intentionnellement sur le périphérique. Comme toujours, les utilisateurs ne doivent jamais installer de logiciel inconnu ou non. Ceci est particulièrement vrai pour les logiciels illégaux, tels que les applications craquées- ils sont un vecteur préféré pour les infections malveillantes. [41]

4.3.2. Caractéristiques du virus :

Android / GinMaster.A est distribué dans une application de paquetage trojan qui dispose d'un service malveillant qui pourrait arracher le périphérique pour obtenir des privilèges d'administration, installer des applications sans préoccupation de l'utilisateur et publier des informations sensibles.

Une fois l'application lancée, l'URL suivante est acceptée, affichant des informations sensibles (numéro de téléphone, IMEI, type de réseau, informations sur les périphériques, application de package, version Android).
Https: // client. [Censuré] .com / rapport / firstèrun.do
Ensuite, un service accède constamment à cette URL pour recevoir des commandes.

Android / GinMaster.A crée une base de données sqlite pour stocker les paquets installés dans le système et télécharger ces informations sur un serveur distant.
Certains paquetages d' Android/GinMaster incluent Voldbrk pour créer une racine de périphérique et obtenir des privilèges de racine afin d'installer de nouveaux paquets en silence et selon les paramètres reçus du serveur C & C. [41]

4.4. Cabir :

4.4.1. Définition :

est un ver de l'ordinateur apparu en 2004, conçu pour infecter les téléphones mobiles exploitant le système d'exploitation Symbian. Parmi le premier ver de l'ordinateur qui peut infecter les téléphones mobiles. Lorsqu'un téléphone est infecté par Cabir, le message "Caribe" apparaît sur l'écran du téléphone et apparaît chaque fois que le téléphone est allumé. Les signaux sans fil Bluetooth ont soutenu le ver à mesure que la tente s'étend à d'autres téléphones de la zone.[57]

4.4.2. Principe de fonctionnement :

Le ver peut attaquer et répliquer sur les téléphones équipés de Bluetooth. Le ver essaie de se soumettre à tous les périphériques compatibles Bluetooth qui prennent en charge le "Object Push Profile", qui peuvent également être des téléphones non Symbian, des ordinateurs de bureau ou même des imprimantes. Le ver se propage comme un fichier .sis installé dans le répertoire Apps. Cabir ne se propage pas si l'utilisateur n'accepte pas le transfert de fichier ou n'est pas d'accord avec l'installation, bien que certains téléphones plus anciens continuent à afficher des fenêtres contextuelles, car Cabir s'est réinvesti, rendant l'interface utilisateur inutilisable jusqu'à ce que oui soit cliqué.[57]

Alors que le ver est considéré comme inoffensif car il se réplique mais n'effectue aucune autre activité, cela entraînera une réduction de la durée de vie de la batterie sur les appareils portables en raison de la numérisation constante d'autres appareils compatibles Bluetooth.il se propage aussi via le MMS à partir de sa version Mabir.A.

4.5. phishing :

Dans une attaque par phishing (ou hameçonnage), l'application est malveillante et charges une application cible frauduleux.
Généralement les applications mobiles inclure des boutons de partage et de paiement social. Une malicieuse application pouvait inclure de la même façon de « Partager sur Facebook » ou « Mise à niveau de cette application » boutons. En cliquant sur un des boutons devrait diriger l'utilisateur vers un écran qui usurpe l'application cible. L'écran de phishing pourrait demander pouvoirs de mot de passe ou le paiement de l'utilisateur, permettant l'application malveillante pour voler les données. Le phishing demande serait alors charger l'application réelle. Si l'utilisateur n'est pas une

session existante avec l'application réelle, puis l'application réelle demande à l'utilisateur d'entrer son mot de passe. Cela ressemble à comportement de l'application normale après une Tentative de connexion a échoué, donc l'utilisateur peut naturellement suppose qu'elle avait mal orthographié son mot de passe.[58]

5. Conclusion :

La sécurité est le principal problème dans les réseaux mobiles et en particulier les appareils mobiles, qu'ils ont associés à un ensemble de contraintes. Une des vulnérabilités a conduit une entité à utiliser les ressources d'un autre nœud et de garder les ressources propres. Ce type, il crée le problème dans leur environnement, ou il utilise plusieurs aspects de falsifications.

particulièrement , il est clair que le protocole de chiffrement WEP ne garantie pas une sécurité suffisante pour les réseaux sans fil Wifi, il ne peut qu'être utilisé en complémentarité . Le WPA représente une solution sécurisée pour les équipements supportant une mise à jour mais ne pouvant passer au WPA2 mais ce dernier représente une solution plus pérenne et sera à l'avenir le standard en terme de sécurité des réseaux sans fils Wifi.

Il existe de nombreux moyens classiques qui garantissent la sécurité mobile. Procédez comme suit pour éviter les défauts de sécurité. Doit avoir un programme antivirus certifié par un autoritaire, activer le pare-feu et le système d'exploitation doit être mis à jour régulièrement. Ainsi, un programme ou un outil signé par une tierce partie de certification, pour détecter les bogues, est destiné à les faire déclarer comme une procédure de correction.

CHAPITRE V

synthèse et conclusion

1 Introduction:

Aujourd'hui, avec de multiples moyens et des réseaux de communication mobiles, il est nécessaire de mieux sécuriser les appareils mobiles contre les logiciels malveillants, qui sont des fonctionnalités violées et comprennent les effets négatifs sur les applications incluses et les dommages physiques. Pour éviter les effets de menaces qui ont été traitées avec plus de détails dans les axes précédents, il doit être les définis à partir de leurs caractéristiques devenant un exemple de chaque scénario montré séparément.

Il existe un certain nombre de méthodes pour protéger les systèmes d'informations tels que la méthode de protection contre les attaques d'entrée et de sortie. Cette méthode repose sur un laboratoire expérimental qui présente des caractéristiques élevées et est très précis pour effectuer différents processus expérimentaux, tels que l'injection de données dans la carte réseau de type Ethernet et l'étude de la réception du cadre. Est-ce très coûteux et plus cher?. [34]

L'antivirus statique est différencié entre les fichiers système, qui sont des fichiers réguliers ou des logiciels malveillants. Selon le script de fichier, certaines fois contiennent des instructions de suppression ou le lancement de plusieurs processus. [35] Et cela à partir d'une base de données existante sur le programme comme moyen de prise de décision. Pour l'antivirus d'analyse comportementale (heuristique), supposé être un programme pour déterminer s'il s'agit d'un virus. L'analyse comportementale des SI est portée par les entreprises les plus à la pointe : Q1 Labs RSA (EMC), Symantec, etc . Les éditeurs travaillent sur l'analyse comportementale des systèmes afin de détecter la présence de virus inconnus. Sans réussite jusqu'à présent. Les antivirus basés sur des signatures virales sont dépassés. . [36]

L'analyse de comportement est basée sur des modèles comportementaux du système, déduits de la spécification , ou des dossiers de conception ,des codes sources .cette analyse met en jeu des simulations de son comportement ,modélisées à partir de graphes, d'automates à états finis , de tables de décision ,de réseaux de pétri..ect. [34]

En fait, la combinaison de types de programmes malveillants et de toutes les informations qui sont étroitement liées à la mesure de les définir et de les distinguer, pour les utilisations comme une table de décision de diverses utilisations, elle est applicable à une base des modèles de comportement du système, déduits de la spécification. Cela repose sur une comparaison entre les logiciels malveillants en fonction de leurs événements et les techniques de fonctionnements. Ainsi conclure la protection optimale des appareils mobiles, est scientifiquement.

2 Tableau comparatif des attaques :

Tous les types d'attaques découvertes dans divers chapitres, résumés dans le tableau ci-dessous, ont été collectés en fonction d'attaques de supports ou d'attaques d'applications. En particulier, les attaques de supports ont été regroupées dans les différentes classes. (SMS/MMS, réseau, bluetooth, SDCard).

manière d'attaque / Type d'attaque	Attaques supports				Attaques applications
	SMS/MMS	Réseau	BlueTooth	SDCard	
Curse of silence.	Envoi adresse mail trop grande.	/	/		dysfonctionnement complet du gestionnaire de messagerie.
CommWarrior	Envoi fishier infecté	/	Envoi fishier infecté	Envoi fishier infecté	/
DoS /DDoS	/	envoi des paquets passifs et de commandes	/	/	saturation des services
Nmap	/	détection des ports.	/	/	détection des ports.

Wireshark	/	analyseur de protocoles réseau et applicatif.	/	/	analyseur de protocoles réseau et applicatif.
Cain & Abel	/	sniffing	/	/	récupération de mot de passe.
GinMaster	Envoi des informations sensibles.	/	/	S'injecte dans les fichiers.	/
Cabir /Mabir.A	envoi des copies de lui même.	/	Envoi des copies de lui-même.	/	
Stagefright	l'exécution de codes arbitraires à distance.	/	/	/	
Geinimi	/	Recevons des commandes et envoi des informations sensibles.	/	/	/
FlexiSpy	/	envoi les informations reçues	/	/	/

GM Bot	Interception et envoi de données. sensibles.	/	/	/	/
airCrack	/	/	/	/	Craquage des clés d'authentification wifi (wep et wpa-psk (wpa1et wpa2)).
CardTrap	/	/	/	Infecte SDcard	
Drever.A	/	/	/	/	désactivation le démarrage automatique de l'antivirus.
Locknut.B	/	/	/	/	empêche toute application d'être lancée.
Fontal.A	/	/	/	/	formatage de l'appareil.
FairPlay MITM	/	/	/	/	diffusion des logiciels malveillants.
sniffer	/	/	/	/	Interception de trafics.
force brute cracking	/	/	/	/	Craquage des mots de passe.
John The Ripper.	/	/	/	/	la casse de mots de passe.
Burp Suite	/	/	/	/	l'audit des applications web.

Tableau 5: tableau comparatif des attaques

3 Conclusion :

L'évolution permanente des technologies nous contraint à adapter des outils et des méthodes d'analyse informatique. Le volume des éléments numériques présents sur un appareil mobile est beaucoup moins important, ce qui facilite leur analyse. En outre, ces données numériques appartiennent normalement à un seul utilisateur-le propriétaire-ce qui rend leur opération plus pertinente et moins sujette à l'interprétation.

Nous avons fait un tour d'horizon sur les principales modes d'attaques et de vulnérabilités actuelles. Comme nous l'avons vu tout type de programme peut être vulnérable (des buffers overflow ont été trouvés dans php) et par conséquent cet aspect de la sécurité n'est pas à négliger.

En raison de l'absence de ces normes de laboratoire expérimental appliquées comme un moyen de preuve et de transparence. Et les dispositifs de simulation. Nous avons collecté les données dans un tableau comparatif en fonction du type d'attaque et de leur mode de fonctionnement. En effectuant une étude comparative pour déterminer la méthode optimale pour la sécurité mobile.

Le tableau précédent, on le considère comme un outil de décision pour l'intégrer dans une nouvelle méthode analytique de sécurisation à la forme d'une base de données. Nous observons des nouvelles méthodes d'analyse virales, comme des tendances, plus efficace. Mais l'un des méthodes n'est pas réussi à la découverte d'une nouvelle faille ou programme suspect en temps réel ou proactive.

La collection de données n'est pas suffisante. Il est nécessaire de les investir dans des outils qui permettent d'extraire des nouvelles informations et des sens implicites à partir de ces données, et capables de trouver les indicateurs critiques d'une potentielle compromission : ces aiguilles dans la botte de foin.

Finalement et malheureusement, le manque du temps et le thème s'accroit, plus en plus avec une complexité multiple car il est très pompeux, mais nous récoltons au tableau de décision de différents types d'attaques. Nous conserverons cette culture qui sera alimentée par une autre méthode de sécurité dans un futur travail.

Bibliographie :

[1] Louis Goubin « carte à puce » 2005
[2] http://www.etsi.org/standards/
[3] André Perez /mobile network architecture /ISTE LTD 2012.
[4] thèse : Master Pro télécommunication Planification et ingénierie des réseaux de télécoms / UNIVERSITY OF YAOUNDE I/cameroune.
[5] Sebastien Josse /Analyse et détection dynamique de codes viraux dans un contexte cryptographique et application à l'évaluation de logiciels antivirus 2009.
[6] Futai Zou, Siyu Zhang, Tianqi Wan, Li Pan /a survey of android mobile platform security / china 2013.
[7] David B Everett. /Smart Card Tutorial - Part 1 First Published in September 1992
[8]site : http://www.radio-electronics.com/info/cellulartelecomms/umts/umts-wcdma-network-architecture.php.
[9] Samia Bouzefrane les cartes SIM/USIM laboratoire CEDRIC CNAM./2008
[10] MROUEH Lina et LABAKY Elie /Etude des procédures d'enregistrement et d'établissement de session en IMS / 2006.
[11] Payan LP R&T RSFS Téléphonie Mobile Frédéric - Département R&T IUT Nice Côte d'Azur.
[12] M. Veeraraghavan /GSM Mobility Management Fall, Polytechnic,University NewYork 2001
[13] GSM : Global System for Mobile Communications Gestion de la mobilité et Contrôle d'appel EFORT Copyright EFORT 2008.
[14]. http://www.lemagit.fr/definition/iOS.
[15] https://www.globalsecuritymag.fr/_Marc-Jacob_.html.
[16] fernand lone sang/la méthode de protection des systèmes informatique contre les attaques par entrée –sortie /2012.
[17] https://play.google.com/store/apps/details?id=com.zimperium.stagefrightdetector&hl=fr
[18] https://www.tutorialspoint.com/umts/umts_wcdma_technology.htm
[19] Nicolas Ruff_EADS /Sécurité du système Android / Innovation Works 2011.
[20] Saud Alotaibi ,Steven Furnell, and Nathan Clarke /Transparent Authentication Systems for Mobile Device Security
[21] http://www.acbm.com/pirates/num_10/securite-telephones-portables-gsm.html
[22] https://Apple.com.
[23] http://www.iphon.fr/post/comment-eviter-erreur-touch-id-iphone-5s.
[24] https://support.apple.com/fr-ma/HT203015.
[25] Présentation technique de la sécurité iOS | 2016 Apple Inc.
[26] http://www.lemagit.fr/recherche/question?q=Windows_Phone.+
[27] https://www.tutorialspoint.com/umts/umts_wcdma_technology.htm
[28]https://technet.microsoft.com/frfr/library/mt674915(v=vs.85).aspx#s_curit__de_plateforme_d_application.
[29] https://global.blackberry.com/en/index.
[30] https://www.slideshare.net/BlackBerry/black-berry-10securityoverview.
[31] https://help.blackberry.com/en/blackberry-security-overview/latest/blackberry-security-overview/awi1402929620791.html.

[32] https://www.computerhope.com/jargon/s/symbian-os.htm.
[33] http://allaboutsymbian.com/
[34] fernand lone sang/la méthode de protection des systèmes informatique contre les attaques par entrée –sortie /2012.
[35] https://support.kaspersky.com/fr/4436..
[36] https://www.itrust.fr/blog/lanalyse-comportementale-comme-reponse-a-la-complexite/.
[37] https://www.computerhope.com/jargon/s/symbian-os.htm.
[38] http://allaboutsymbian.com/
[39] https://www.computerhope.com/jargon/a/android.htm.
[40] http://www.memoireonline.com/03/12/5548/Rapport-de-stage-sur-le-projet-Locate-my-car-google-map-android.html.
[41] https://home.mcafee.com/virusinfo/virusprofile.aspx?key=1574798#.
[42] Comprendre et anticiper les attaques DDoS : Document réalisé par l'ANSSI (Agence nationale de la sécurité des systèmes d'information ; France), en collaboration avec d'autre sociétés de télécommunications.
[43]http://www.zdnet.fr/actualites/commwarrior-le-premier-virus-qui-se-propage-par-mms-39210950.htm.
[43] Michel Riguidel /La sécurité des réseaux et des systèmes/ 2006-2007
[44] Mr Florent Nolot./Emmanuel NGASSA .
[45] brice augustin et romain /le guen usurpation d'identite sur ethernet.
[46] Ali Davanian – Amit Kumar Gupta – Jan Helge Wolf./Man in the Middle Attacks Network Security Lab – University of Trento – 2016-.
[47] C. Pham Université de Pau et des Pays de l'Adour Département Informatique.
[48] http://www.materiel-informatique.be/ssid.php.
[49] http://www.futura-sciences.com/tech/definitions/informatique-force-brute-1830./
[50]http://motilia.com/-/network-attacks-an-overview.
[51] Romain Raboin /La sécurité des smartphones .
[52] Guillaume HARRY /Failles de sécurité des applications Web/ 2012 .
[53]https://www.aircrack-ng.org/doku.php?id=aircrack-ng.
[54] http://www.info24android.com/la-difference-entre-wep-wpa-wpa2-et-wi-fi-mots-de-passe/
[55] Guillaume Lehembre /Sécurité Wifi – WEP, WPA et WPA2 ;.
[56]https://play.google.com/store/apps/details?id=com.lookout.stagefrightdetector&rdid=com.lookout.stagefrightdetector.
[57] http://www.technewsworld.com/story/34542.html.
[58] https://www.sierre-energie.ch/services-industriels/est-ce-phishing-259.html.
[59] http://www.memoireonline.com/07/08/1383/m_u-m-t-s8.html.
[60] http://www.rfwireless-world.com/Tutorials/gprs-tutorial.html
[61] http://www.rfwireless-world.com/Tutorials/UMTS-Network-Architecture.html
[62]http://people.cs.uchicago.edu/~dinoj/smartcard/arch-1.html.
[63]http://jaaayyy.chez.com/html/Radiomobiles/stage/CarteSIM.html.
[64] https://www.slideshare.net/eXplanoTech/an-introduction-to-voice-and-sms-in-lte-networks-70681388.