INSTITUT UNIVERSITAIRE DE TECHNOLOGIE FV DE BANDJOUN

Support de cours Architecture et maintenance des terminaux mobiles

Dr. JAGHO Brel

CHAPITRE I : INTRODUCTION A LA MAINTENANCE INFORMATIQUE

I. Introduction et contexte d'étude

Dans le cadre de ce cours, la maintenance informatique sera définit comme étant l'ensemble d'actions techniques, administratives, et de management durant le cycle de vie d'un équipement informatique, destinées à le maintenir ou a le rétablir dans un état dans lequel il peut accomplir la fonction requise (*une tache indispensable*). Selon la définition de l'AFNOR, *la* ***maintenance*** vise à maintenir ou à rétablir un équipent informatique dans un état spécifié afin que celui-ci soit en mesure d'assurer un service déterminé. Elle regroupe ainsi les actions ci-après :

- ***Dépannage*** : C'est tout simplement une action de remettre un équipement informatique en état de fonctionner.
- ***Réparation*** : c'est une action de faire disparaitre un dysfonctionnement ou atténuer les conséquences d'une détérioration quelconque d'un équipement informatique.
- ***Réglage*** : c'est une action de mettre au point le fonctionnement d'un équipement informatique. Outre, c'est un enchainement des opérations propres à une fonction ou processus donné.
- ***Révision*** : c'est tout simplement, l'action d'examiner de nouveau, de mettre à jour ou de modifier le fonctionnement d'un équipement informatique.
- ***Contrôle*** : C'est une action de la surveillance soit directement ou soit indirectement du fonctionnement d'un équipement informatique.
- ***Vérification*** : c'est une action de soumettre un équipement informatique à un examen ou à une confrontation avec les faits, des preuves pour tester l'exactitude.

II. Les fonctions de la maintenance

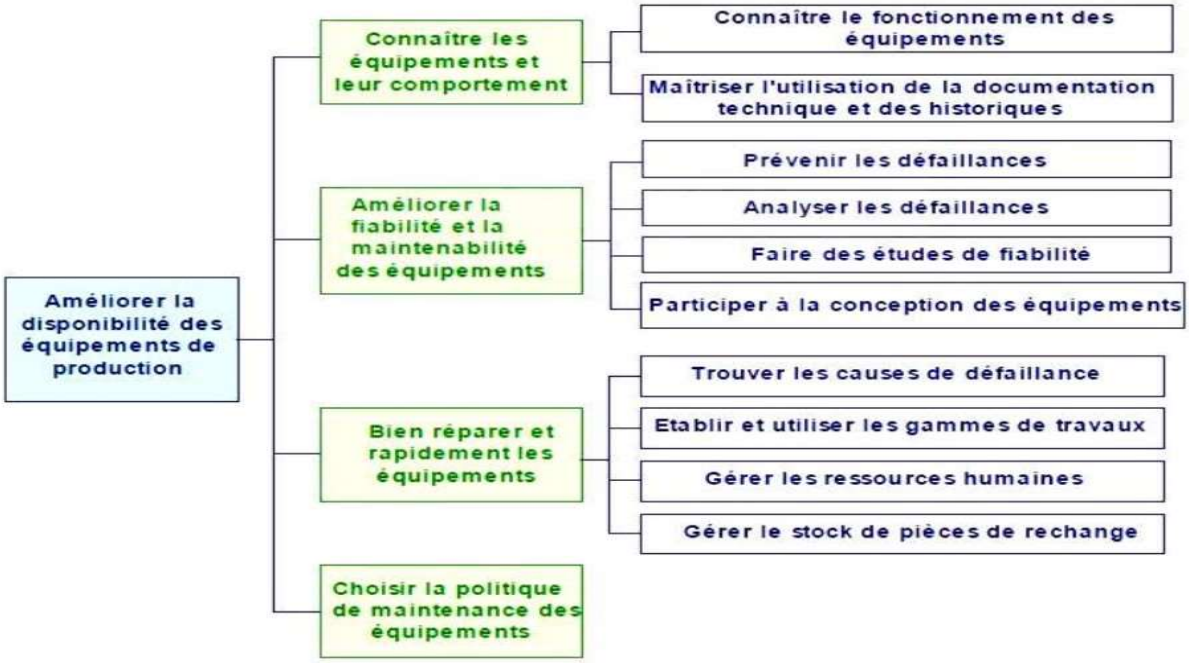
Par définition, « ***une fonction*** » est un ensemble d'Operations concourant au même résultat et exécutées par un organe donné. En informatique, c'est un ensemble d'instructions ou rôles joués par équipement informatique en termes de la production et de la satisfaction d'une tache quelconque. C'est les fonctions les plus usuelles de la maintenance informatique sont :

1- La protection du parc informatique

Un patrimoine représente des investissements importants pour lesquels il faut s'assurer un retour rapide, ce qui passe par une bonne disponibilité avec un

niveau de rendement optimal. Sa maintenance ne se limite plus à sa simple remise en état. Le service maintenance doit à travers cette obligation satisfaire les besoins de la production, ce qui revient à améliorer la disponibilité des équipements informatiques de production et l'interface production maintenance, c'est-à-dire connaitre et appliquer les méthodes et outils pour améliorer la communication ainsi que l'efficience3. Ainsi donc, la protection du parc informatique peut être réalisée en *4* étapes dont :

- ***Connaissance des équipements et leur comportement*** : ici, il est question de bien connaître le fonctionnement des équipements informatiques ; ainsi que Maîtriser l'utilisation de la documentation technique et des historiques.
- ***Amélioration de la fiabilité et la maintenabilité des équipements informatiques*** : ici, il est question de prévenir les défaillances ; Analyser les défaillances ; Faire des études de fiabilité ; et possiblement participer à la configuration de ces équipements.
- ***Bonne réparation des équipements informatiques*** : ici, il est question de trouver les causes de défaillances ; Etablir et utiliser les gammes de travaux ; Gérer les ressources humaines ; Gérer le stock de pièces de rechange.
- ***Choisir la politique de maintenance des équipements informatiques :*** ici, il est question de choisir les stratégies correspondantes au mode de fonctionnement de ces équipements.



Etapes de Protection du parc informatique

2- La satisfaction des besoins de l'exécution

La satisfaction des besoins de l'exécution de l'entreprise peut s'effectuer à plusieurs niveaux notamment : Obtenir le cout global minimal pour les équipements informatiques ; Se mettre en conformité avec la législation sur la sécurité ; Se mettre en conformité avec la législation sur l'environnement ; Participer à la qualité des produits fabriques, Participer à l'amélioration des couts de fabrication, Participer à l'image de marque de l'entreprise.

III. Les conséquences de la non maintenance informatique

Les conséquences de non maintenance informatique peuvent être considérées comme ce qui est produit ou les résultats caractéristiques d'une règle d'inférence applicable sur chaque équipement informatique. De la sorte, les conséquences les plus usuelles peuvent être catégorisées au nombre de trois :

a) La dégradation progressive des fonctions informatiques

La présence d'un esprit prévisionnel dans l'entreprise permet de la protéger des pertes énorme du à l'arrêt de la production et les différentes pénalités qui peuvent en découle.

b) La dégradation du matériel

Tout équipement informatique atteint la fin de sa durée de vie, et quand cela arrive, il lâche et provoque la des dégâts importante dans son usage. Ceci montre que si on attend l'apparition de la défaillance, cela peut entrainer une dégradation importante du matériel et freiner par la même occasion la production.

c) Les accidents graves

Une maintenance mal effectue ou qui ne tient pas compte de la sécurité des ouvriers peut entrainer des accidents graves. En conclusion, la maintenance est un soutient de production de toute entreprise qui lui permet d'atteindre les objectifs : Disponibilité du matériel pour assurer la production; Protège le parc matériel et augmenter sa dure de vie Sécurité.

IV. Les niveaux de la maintenance informatique

Un « *niveau de la maintenance* » peut être considéré comme un ensemble des étapes successives de l'analyse hiérarchiquement subordonnées les unes aux autres à partir d'un degré atteint dans une opération définissant les interventions à suivre. La norme NF X 60-010 définit, à titre indicatif, cinq « niveaux de maintenance » :

Niveau 1 : C'est un degré d'opérations qui engagent des travaux des réglages simples qui ne nécessitent pas de démontages ni ouverture de l'équipement informatique pouvant être exploité sur place. C'est par exemple : remise à zéro d'un automate après arrêt d'urgence, changement de consommable.

Niveau 2 : C'est un degré d'opérations qui engagent des travaux de dépannage par échange standard et des opérations mineures de maintenance préventive pouvant être effectué sur place par des techniciens habilite dans un domaine précis. C'est par exemple : un changement d'un relais ou contrôle de fusibles ou encore de réenclenchement de disjoncteur dans une industrie.

Niveau 3 : C'est un degré d'opérations qui engagent des travaux d'identification et diagnostic de pannes, de réparation par échange standard, des réparations mécaniques mineures et maintenance préventive (*par ex. réglage ou réalignement des appareils de mesure*) préventive pouvant être effectué sur place ou dans un atelier de maintenance par des techniciens spécialisés. C'est par exemple : l'identification de l'élément défaillant, recherche de la cause, élimination de la cause, remplacement
Niveau 4 : C'est un degré d'opérations qui engagent des travaux importants de maintenance corrective ou préventive sauf pour de rénovations et reconstructions des réglages des appareils de mesure ou de contrôle des étalons pouvant être effectué dans des ateliers spécialisés avec outillage général, bancs de mesure et documentation par une équipe avec encadrement technique spécialisé. C'est par exemple : intervention sur matériel dont la remise en service est soumise à qualification.
Niveau 5 : C'est un degré d'opérations qui engagent des travaux de rénovations, de reconstructions et des réparations importantes étalons pouvant être effectué dans des usines des constructeurs ou reconstructeurs par des moyens proches de la fabrication. C'est par exemple : mise en conformité selon réglementation d'équipements lourds.

V. Les outils d'aide à la maintenance

De part sa définition, un « outil d'aide a la maintenance » est un instrument ou élément d'une activité permettant ou facilitant un équipement informatique de réaliser une opération déterminée. Dans le cadre de ce cours, on pourra distinguer 2 sortes d'outils d'aide a la maintenance : *les outils matériels et logiciels.*

a) Les outils matériels

Ce sont des instruments électroniques et électriques permettant à un bon mainteneur de réaliser une opération précise afin de maintenir un équipement informatique dans son état habituel. On regroupe sous cette appellation les éléments suivants :

- **Jeu de tournevis :** est un ensemble de différents tournevis utilisés pour l'insertion et le retrait des vis dans les matériaux. Conçu pour visser des vis à petite échelle mais détient une multitude de fonctions secondaires dont la principale est peut être l'ouverture des pots de peinture. Il existe plusieurs types de tournevis adaptés aux différents types de vis : *à tête fendue ou plat, cruciforme, Pozidriv, Torx, Tri-Wing, spéciaux, etc*.

Jeu de tournevis

- **Jeu de pince :** Une pince est un outil servant à saisir des objets fermement et à les courber ou à les presser, par exemple. Elle vous permet également de couper de fines feuilles de métal. Une pince se constitue de deux branches qui sont reliées entre elles par une charnière, qui forme le point d'appui, et ressemble ainsi à une paire de ciseaux. On retrouve des pinces dans la boîte à outils des électriciens, des mécaniciens, des plombiers, des informaticiens et des bricoleurs. Il existe des pinces dites : *tenailles, universelles, multiprise, pince à cintrer, pince à becs, pince à dénuder, pince à œillet, pince à cosse, pince à riveter, pince étau, pince à tubes, etc.*

Jeu de pince

- **Souffleur :** La poussière est l'ennemi numéro 1 de votre ordinateur et dès qu'elle fait son apparition à l'intérieur du boitier, il faut s'en débarrasser au plus vite avant qu'elle ne détériore vos composants. En effet, une poussière très abondante peut ralentir la vitesse de rotation des ventilateurs comme celui du

processeur ou de la carte graphique et abimer vos composants qui ont besoin d'être refroidis en permanence.

Souffleur

- **Bracelet anti-statique :** est un outil électronique qui permet d'annuler les charges statiques dues au corps humain et à l'environnement ambiant. Pour que le système fonctionne, il est nécessaire de vous relier avec un fil électrique protégé par une résistance à la terre de votre installation électrique. Le bracelet est composé de 3 parties : Le bracelet en bande velcro, la résistance de protection, et l'ensemble fiche banane et pince croco

Bracelet anti-statique

- **Le fer à souder :** Un fer improprement appelé « à souder » est un appareil polyvalent puisqu'il peut effectuer différentes tâches comme le soudage, la coupe à chaud, le thermorétractage, le brasage, le ponçage de peintures et la pyrogravure. Ces travaux sont possibles grâce aux 6 accessoires interchangeables dont se dote cet appareil. Bien qu'il soit possible d'utiliser cet appareil à l'extérieur en flamme directe, il faut reconnaître que la tâche est difficile puisque la flamme s'éteint facilement dès que le vent souffle.

Fer à souder

- **L'étain :** est un métal relativement rare à la base de nombreux alliages et sert principalement à la fabrication d'objets.

Etain

- **Multimètre digital ou analogique :** Le multimètre est certainement l'outil le plus précieux pour un technicien. Généralement, on utilise un multimètre pour mesurer une tension, un courant, une résistance et même la continuité. Les derniers modèles de multimètre ont montré qu'ils sont des appareils aux possibilités illimitées : désormais, ils peuvent également indiquer la température, mesurer la capacité et l'inductance, tester la charge des piles ... Ils permettent également de vérifier que des diodes et des transistors sont en bon état. Certains appareils haut de gamme sont équipés de la fonction « True RMS » (« True RMS » = valeur effective précise) qui permet de mesurer précisément des tensions alternatives qui n'ont pas une forme sinusoïdale.

Multimètre digital et analogique

- **Pompe à dessouder :**

Pompe à dessouder

b) Les outils logiciels

Ce sont des utilitaires de diagnostic ou dépannage, il s'agit, en somme, de petits programmes de test contenu dans certains systèmes d'exploitation livrés sur le marché informatique. Ces outils permettent de tester, de réparer ou d'optimiser l'outil informatique. Ainsi, Un bon technicien doit avoir à sa possession les utilitaires suivants : Antivirus, programmes de détection et de réparation des secteurs de mémoires de masse, disquette de démarrage pour les principaux systèmes d'exploitation et, Cd d'installation des systèmes d'exploitation.

CHAPITRE II : TYPOLOGIE DE LA MAINTENANCE INFORMATIQUE

Il existe différents types de maintenance s'agissant des machines, et tout autant en matière de logiciels, déterminés en fonction de leur finalité, de leur résultat et des moyens techniques d'intervention. Par conséquent, l'analyse sera différente selon qu'il s'agira de *hardware* ou de *software*. On distinguera alors 2 grandes catégories de maintenance informatique : *La maintenance matérielle* et, *La maintenance logicielle*.

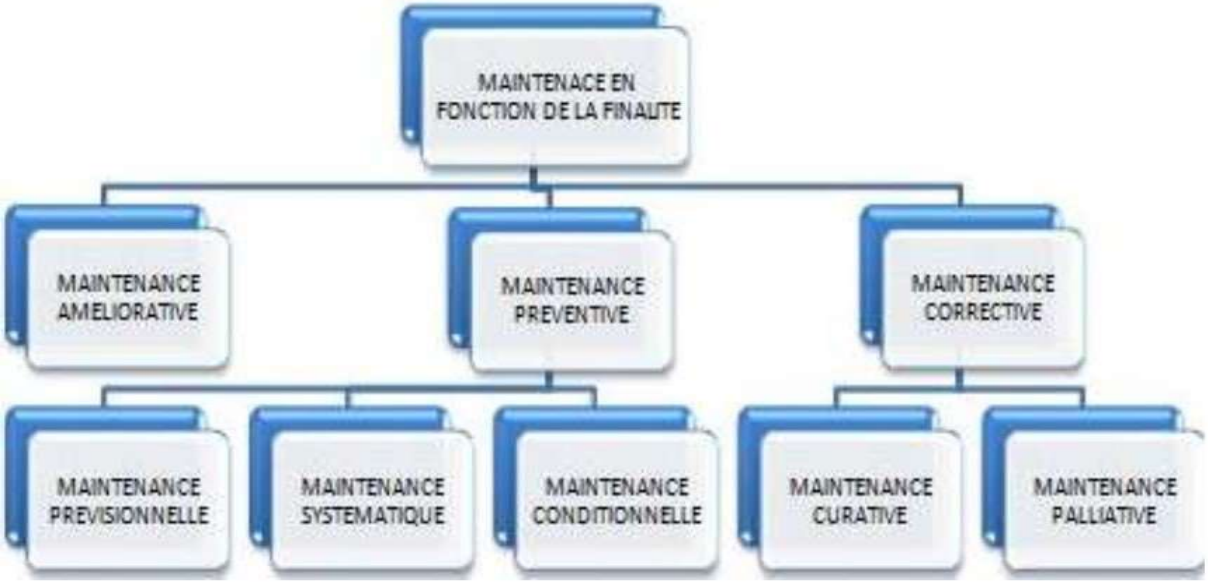
I- La maintenance matérielle

*La **maintenance matérielle*** vise à rétablir physiquement les composants matériaux d'un équipent informatique dans un état spécifié pour un service déterminé. En conséquence, La maintenance matérielle doit être envisagée, selon :

- La maintenance en fonction de la finalité
- La maintenance en fonction du résultat
- La maintenance en fonction des moyens techniques d'intervention

1- La maintenance en fonction de la finalité

La classification en fonction de la finalité est celle qui résulte d'une cause finale, c'est-a-dire qui a un caractère de ce qui tend a un but. Ici, On distingue trois grandes catégories : ***la maintenance préventive, la maintenance corrective*** et ***la maintenance méliorative*** sachant que les trois catégories de maintenance peuvent être prévues au sein du même contrat.



Organigramme de la Maintenance en fonction de la finalité

- *La maintenance préventive* consiste à empêcher tout incident technique au moyen de la prévention, autrement dit, elle est une maintenance effectuée avant la détection d'une défaillance d'un outil informatique, à des intervalles prédéterminés ou selon des critères prescrits conformément aux instructions du fabricant (*suite à l'analyse de l'évolution surveillée de paramètres significatifs*) et destinée à réduire la probabilité de défaillance d'une entité. Ce type de maintenance comprend ***la maintenance systématique***, *la* ***maintenance conditionnelle*** *et la* ***maintenance prévisionnelle.***

- *La maintenance corrective*, aussi appelée « *maintenance curative* » consiste à intervenir une fois que le problème technique est survenu, afin d'y remédier et de supprimer les causes d'un dysfonctionnement. Autrement dit, c'est une maintenance effectuée après la détection d'une défaillance et destinée à remettre un outil informatique dans un état lui permettant d'accomplir efficacement une fonction très bien précise.

- ***La maintenance méliorative*** est un ensemble des mesures techniques, administratives et de gestion, destinées à améliorer la sureté de fonctionnement d'un équipement informatique sans changer sa fonction requise. C'est ainsi que l'amélioration se rapporte à des modifications de la conception d'origine dans le but *d'augmenter la durée de vie des composants*, *de les standardiser*, *de réduire la consommation d'énergie*, *d'améliorer la maintenabilité*, etc

2- La maintenance en fonction du résultat

La maintenance en fonction du résultat, est celle qui résulte d'une conséquence d'un acte ou d'un phénomène directement lié à l'utilisation des équipements informatiques. Lorsque la maintenance se définit en fonction de son résultat, il est question de l' « ***unités d'usage :*** *c'est quantifier le nombre de fois où le bien à maintenir est utilisé par son détenteur* » de l'outil informatique, en termes ***de disponibilité***, ***d'état de référence*** et de ***durabilité résiduelle ou potentielle d'utilisation***:

- ***la disponibilité***, consiste à évaluer le temps pendant lequel un matériel ou un système informatique est rendu indisponible, en raison d'une opération de maintenance. Autrement dit, le temps de réponse à une demande d'intervention. Dans tous les cas, la durée d'indisponibilité ne saurait dépasser un certain seuil appelé « ***seuil de tolérance***».
- ***l'état de référence,*** se définit par les particularités que l'équipement informatique à maintenir doit avoir tout au long du contrat. Il ne s'agit pas de l'état d'origine, sinon d'un état proche : est toléré un certain écart par rapport à celui-ci, sachant qu'il ne doit pas être trop élevé.
- Enfin, ***la durabilité résiduelle ou potentielle d'utilisation*** évalue l'état d'un équipement informatique à l'expiration du contrat de maintenance. Bien entendu, seront pris en compte les critères d'obsolescence, de performance, d'actualité et de nouveauté car, le domaine informatique évolue vite, et le marché regorge d'innovations techniques qui n'attendent pas. Un matériel peut donc devenir rapidement dépassé, ce qui s'ajoute à son usure naturelle. C'est pourquoi, il est important de savoir s'il a encore de la valeur à un instant *t* ainsi qu'un quelconque avenir, et s'il lui reste quelques performances. Cela permettra à son utilisateur de déterminer s'il lui est possible de le céder à un tiers ou s'il est nécessaire de le remplacer par d'autres matériels plus récents et plus sophistiqués.

3- La maintenance en fonction des moyens techniques d'intervention

De plus en plus, les opérations de maintenance sont effectuées à distance et de manière automatisée, l'utilisateur se contentant d'appliquer les instructions du mainteneur. Il s'agit des hypothèses où les incidents sont de faible gravité et où un novice peut s'en sortir en suivant les consignes données. Ici, il sera davantage question d'assistance par téléphone ou par mail permettant de recevoir des conseils à la moindre difficulté.

Pour les opérations de maintenance plus complexes, le contrat peut prévoir le déplacement du mainteneur au domicile de son cocontractant, sachant que cela dépendra de la taille du matériel concerné. S'il s'agit de tout un système informatique lourd et complexe, il sera souhaitable de ne pas le déplacer pour éviter de l'endommager davantage. À côté de cela, des procédures automatiques d'alertes permettront, au mainteneur, d'intervenir lui-même, directement, dès lors qu'il aura détecté la réunion de conditions susceptibles d'entraîner une panne.

Enfin, notons qu'il existe *des* ***logiciels de gestion de maintenance assistée par ordinateur (GMAO)***, spécialement conçus pour assister les services de

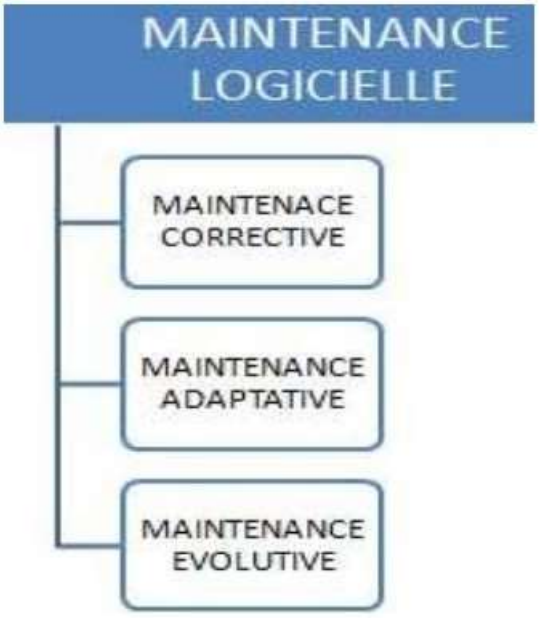
maintenance dans leurs activités, y compris en matière de logiciels. Il s'agit de véritables outils d'accompagnement, très utiles, mais qui demandent un réel investissement de la part du prestataire mainteneur. Les GMAO gèrent les opérations de maintenance et leur historique, le budget qui y est consacré, le planning et la préparation des interventions, la gestion du stock des pièces de rechange susceptibles de remplacer les pièces défectueuses, les fiches d'intervention et de suivi des machines, les modes opératoires…

Ils définissent également l'aide au diagnostic, analysent les causes des pannes et des défaillances antérieurement décelées, et déterminent leurs risques de survenance afin de s'en prémunir… En résumé, ils renforcent l'efficacité de la maintenance, ou du moins la rendent efficace si elle ne l'est pas.

À côté du GMAO, un logiciel dit *de* ***système expert*** pourra intervenir. Son rôle est d'aider un technicien durant une intervention de maintenance. Il offre un diagnostic rapide, une réparation aisée, et se fonde sur une base de données répertoriant les causes, les effets et les moyens de réparation. Mais, cette base ne recense pas toutes les défaillances existantes et nécessitera d'être continuellement enrichie : ce qui s'avérera très lourd au final.

II- La maintenance logicielle

La ***maintenance logicielle*** vise à rétablir effectivement les composants logiciels (systèmes informatiques) d'un équipent informatique dans un état spécifié pour un service déterminé. La maintenance logicielle se subdivise en trois types : *la* ***maintenance corrective****, la* ***maintenance adaptative*** *et la* ***maintenance évolutive*** *:*



- **La maintenance corrective :** consiste à corriger les défauts de fonctionnement ou les non-conformités d'un logiciel.
- **La maintenance adaptative :** consiste à adapter l'application sans changer la fonctionnalité du logiciel afin que celle-ci continue de fonctionner sur des versions plus récentes des logiciels de base, voire à faire migrer l'application sur de nouveaux logiciels de base.
- **La maintenance évolutive :** consiste à modifier progressivement l'application logicielle en l'enrichissant de fonctions ou de modules supplémentaires, ou en remplaçant une fonction existante par une autre, voire en proposant une approche différente.

Lorsque l'on acquiert un logiciel dans le commerce, une **licence d'utilisation** donnant droit à son titulaire à une maintenance comprenant les corrections, les améliorations et les mises à jour est concédée par la même occasion. Seules sont comprises les améliorations nécessaires au fonctionnement du logiciel et dépassant le cadre des simples mises à jour. En effet, inclure des améliorations plus conséquentes reviendrait à acquérir la dernière version éditée du logiciel visé, voire un logiciel distinct, équivalent et commercialisé par un autre éditeur. Cela aurait des conséquences sur le marché du logiciel. Dès lors, la maintenance logicielle exclut les améliorations de performances.

CHAPITRE III : ARCHITECTURE INTERNE DES TERMINAUX MOBILES

Un **appareil mobile** (traduction littérale du terme anglophone « *mobile device* ») est un appareil informatique portatif utilisable de manière autonome lors d'un déplacement. Les appareils mobiles sont de petite taille — certains peuvent être mis dans les poches. Ils sont typiquement dérivés des téléphones mobiles, et permettent d'accéder au Web, de lire du courrier électronique, de prendre des photos, de jouer à des jeux vidéo, d'écouter de la musique, de regarder des clips vidéo ou bien de télécharger des applications. Ils peuvent également comporter un calendrier ou un carnet d'adresses.

La plupart des appareils mobiles n'ont pas de disque dur et les programmes sont enregistrés sur des mémoires internes ou des cartes. Ils fonctionnent sur batterie, ont un écran de petite taille, un clavier dépouillé, et peu de puissance de calcul. Ils sont typiquement d'usage personnel Il est souvent possible de les relier à un ordinateur. Certains appareils mobiles peuvent être connectés à Internet et ils peuvent alors servir à envoyer des courriels, accéder au Web et aux messageries instantanées.

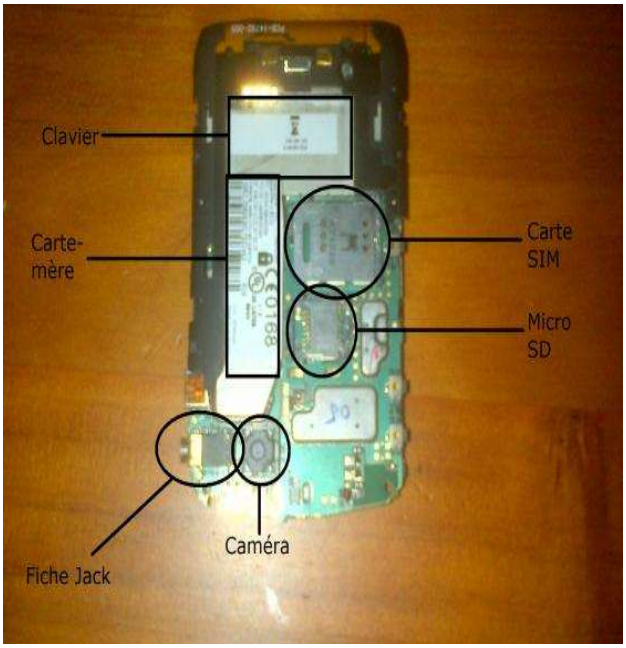
I- Structure et composants internes des terminaux mobiles

Les terminaux mobiles sont composés de plusieurs éléments matériels tels que :

- **Le processeur** : C'est le cerveau du terminal, il traite toutes les informations et exécute les tâches demandées. Les processeurs des terminau mobiles sont généralement conçus pour être économe en énergie tout en offrant des performances suffisantes pour les applications courantes telles que les navigations sur le web, la lecture de vidéos et l'exécution des jeux.
- **La mémoire vive (RAM)** : elle permet au processeur de stocker temporairement les données nécessaires au fonctionnement des applications. Elle permet a l'appareil de fonctionner rapidement et efficacement. Plus la mémoire vive est grande, plus l'appareil peut exécuter de taches simultanément sans ralentir. Cependant, la mémoire vive est limitée et ne peut pas stocker des données de manière permanente. Lorsque l'appareil est éteint, toutes les données stockées dans la mémoire vive sont effacées. Les fabricants de téléphones mobiles proposent des appareils avec différentes capacités de mémoire vive pour répondre aux besoins des utilisateurs.

- **La mémoire interne** : elle sert à stocker les applications, les fichiers, les photos, etc. c'est une mémoire permanente. Elle permet a l'appareil de conserver des informations même lorsqu'il est éteint. Plus la mémoire est grande, plus l'utilisateur peut stocker de données sur son appareil. Cependant, cette mémoire interne est également limitée et peut être remplie rapidement si l'utilisateur ne supprime pas régulièrement les fichiers inutiles. Les fabricants de téléphone mobiles proposent des appareils avec différentes capacités de mémoire interne pour répondre aux besoins des utilisateurs.
- **L'écran** : interface visuelle qui permet à l'utilisation de voir et d'interagir avec le contenu de l'appareil. Il affiche les informations ainsi que les commandes et les options pour naviguer dans les applications, les menus et permet l'interaction avec l'utilisateur. Les écrans des téléphones mobiles peuvent être de différentes tailles et résolutions, offrant des expériences visuelles plus ou moins agréables selon les préférences de l'utilisateur. Certains écrans sont également équipes de technologies avancées permettant a l'utilisateur d'interagir avec l'écran sans toucher physiquement l'appareil.
- **La batterie** : C'est l'élément qui fournit l'énergie nécessaire pour faire fonctionner l'appareil. Elle est généralement rechargeable et peut être amovible ou intégrée a l'appareil. La durée de vie de la batterie dépend de plusieurs facteurs, tels que la taille de l'écran, puissance du processeur, l'utilisation des applications et la qualité du réseau. Les fabricants proposent souvent des fonctionnalités pour optimiser la durée de vie de la batterie, telles que le mode économie d'énergie ou la gestion des applications en arrière-plan. Les utilisateurs peuvent également prendre des mesures pour prolonger la durée de vie de leur batterie, comme réduire la luminosité de l'écran ou désactiver les connexions sans fil lorsque celles-ci ne sont pas nécessaires.
- **La carte mère** : c'est la carte sur laquelle on retrouve tous les éléments interne d'un terminal mobile. C'est la pièce maitresse de l'appareil. La carte mère est responsable de la communication entre tous les composants du téléphone, tels que le processeur, la mémoire, la batterie et les capteurs. La carte mère contient également les connecteurs pour les ports de chargement, les cartes SIM et les carte mémoire. Elle est généralement fabriquée à partir d'un matériau durable et résistant, tel que le plastique renforcé de fibre de verre. Les fabricants de téléphones mobiles conçoivent souvent des cartes

mères personnalisées pour leurs appareils, afin d'optimiser les performances et la compatibilité avec les autres composants du téléphone. En cas de problème avec la carte mère, il est souvent nécessaire de remplacer l'ensemble du téléphone ou de le faire réparer par un professionnel.



II- Environnement logiciel des terminaux mobiles

1) Les systèmes d'exploitation

Le système d'exploitation (OS) est le logiciel qui gère tous les composants matériels et logiciels du terminal. Il permet également d'installer et d'exécuter des applications. Les principaux OS utilisés sur les terminaux mobiles sont :

a) Google Android

Google Android est le système d'exploitation le plus populaire au monde. Il est principalement utilisé sur les tablettes et les smartphones. Il fonctionne également sur des appareils fabriqués par d'autres fabricants. Les utilisateurs ont accès à de nombreuses applications mobiles disponibles sur le Google Play Store.

Google Android comprend un système d'exploitation basé sur le noyau Linux, une interface graphique, un navigateur web et des applications pour l'utilisateur final qui peuvent être téléchargées. Bien que les premières démonstrations d'Android aient présenté un smartphone générique QWERTY et un grand écran VGA, le système d'exploitation a été écrit pour fonctionner sur des combinés relativement bon marché avec des claviers numériques conventionnels.

Cet OS a été publié sous la licence open source Apache v2, ce qui permet de développer de nombreuses variantes du système d'exploitation pour d'autres appareils, tels que les consoles de jeu et les appareils photo numériques. Android est basé sur des logiciels libres, mais la plupart des appareils Android sont préinstallés avec une suite de logiciels propriétaires, tels que Google Maps, YouTube, Google Chrome et Gmail.

Caractéristiques :

- L'interface utilisateur par défaut d'Android repose sur des manipulations directes telles que le tapotement, le glissement et le pincement pour déclencher des actions
- Lorsqu'un utilisateur démarre un appareil, Android OS affiche l'écran d'accueil, qui est le principal centre de navigation des appareils Android et qui est composé de widgets et d'icônes d'applications
- Les applications peuvent ajouter des widgets qui affichent principalement des informations
- Le applications sont au format APK (*Android Package Kit* ou *Android Application Package*)
- L'utilisateur peut installer de nouvelles applications à partir de Google Play ou via des sources inconnues
- Android OS comprend également des fonctions permettant d'économiser la batterie. Le système d'exploitation suspend les applications qui ne sont pas utilisées afin d'économiser la batterie et l'utilisation du processeur
- Android comprend des fonctions de gestion de la mémoire qui ferment automatiquement les processus inactifs stockés dans sa mémoire
- Le système d'exploitation Android est hautement personnalisable, ce qui permet de créer une interface utilisateur simple et conviviale.
- Android prend en charge la connectivité 3G, 4G, 5G, Bluetooth, CDMA, GSM, Hotspot, NFC, UBB, VOLTE, VPN et WiFi
- Ce système d'exploitation peut exécuter plusieurs services et applications en arrière-plan
- Android prend en charge de nombreuses langues, notamment le chinois, le néerlandais, l'anglais, le français, l'allemand, l'hindi, le japonais et le russe

b) IoS

iOS est le système d'exploitation mobile d'Apple qui équipe l'iPhone et l'iPod Touch. Jusqu'en 2019, il était également le système d'exploitation utilisé par l'iPad (dont nous parlerons prochainement).

Apple iOS utilise une interface multi-touch dans laquelle des gestes simples permettent de faire fonctionner les appareils compatibles, comme faire glisser son doigt sur l'écran pour passer à la page suivante ou pincer ses doigts pour effectuer un

zoom arrière. Des millions d'applications iOS peuvent être téléchargées dans l'App Store d'Apple, le magasin d'applications le plus populaire de tous les appareils mobiles.

Vous bénéficiez bien entendu de l'ensemble des applications Apple ainsi que le support complet de leurs produits.
Les produits Apple tels que les iPhones, les iPads, les Apple TV, les Apple Watches et les ordinateurs Mac sont étroitement intégrés à iCloud, iMessage, FaceTime et d'autres services internes.

Caractéristiques :

- Interface utilisateur fluide et ultra-rapide
- L'écran d'accueil, rendu par SpringBoard, affiche les icônes des applications et un menu fixe en bas où les utilisateurs peuvent épingler les applications qu'ils utilisent le plus fréquemment
- Diverses fonctions d'accessibilité sont disponibles sur le logiciel pour aider les utilisateurs souffrant d'un handicap visuel et/ou auditif
- Siri est un Assistant personnel intelligent, intégré à l'iPhone en 2011
- Support complet des produits et matériels Apple
- La principale plate-forme matérielle est l'architecture ARM

c) Ububtu Touch

Canonical, l'éditeur de la distribution Linux Ubuntu, a décidé d'étendre son territoire avec son système d'exploitation mobile open source, Ubuntu Touch.
Pour cela, Canonical s'est associé à certains fabricants d'appareils pour lancer l'Ubuntu Phone.
Le fabricant espagnol BQ est devenu le fabricant du premier appareil fonctionnant avec Ubuntu Touch en février 2015. Il a été rapidement suivi par le fabricant chinois Meizu. Ces premiers appareils étaient destinés aux développeurs, et c'est la raison pour laquelle j'ai déconseillé l'achat du BQ Ubuntu Phone à l'époque.

Deux ans et quelques téléphones basés sur Ubuntu plus tard, Canonical a finalement décidé d'abandonner son système d'exploitation mobile. Cependant, UBports tente toujours de maintenir Ubuntu Touch en vie.

Grâce aux efforts d'UBports, Ubuntu Touch reçoit quelques mises à jour. Il y a une poignée d'appareils qui sont supportés par Ubuntu Touch. Vous pouvez consulter la liste ici.

Ubuntu Touch est censé ressembler à Ubuntu sur un smartphone. Si vous avez utilisé Ubuntu sur votre PC, un smartphone contenant le même système n'est peut-être pas une mauvaise idée. Pour ceux qui n'ont jamais essayé Ubuntu, cette alternative

Android pourrait être une expérience rafraîchissante. Ce système d'exploitation est livré avec des applications de base préinstallées telles que le composeur, le calendrier et le navigateur internet. Ubuntu Touch est également connecté à l'OpenStore de Linux.

Ubuntu Touch n'est pas exclusif à une marque particulière. UT prend en charge plusieurs smartphones et tablettes. Le Fairphone 2 et le OnePlus One sont des exemples d'appareils utilisant ce système d'exploitation.

Caractéristiques :

- Fabriqué par une marque connue
- Connecté à l'Open Store Linux
- Totalement indépendant de Google et des services Android
- Prend en charge les smartphones et les tablettes

d) Sailfish OS

Sailfish OS est une continuation du système d'exploitation abandonné MeeGo, lui-même basé sur Maemo et Moblin. Il est maintenant développé par la finlandaise Jolla, fondée par des anciens de Nokia.

Sailfish OS est un autre système d'exploitation basé sur Linux.
Il dispose déjà d'un ensemble de fonctionnalités complète. Bien qu'il soit totalement indépendant d'Android, Sailfish est toujours compatible avec ce système d'exploitation via la une bibliothèque logicielle libre Hybris.
Cela signifie que vous pouvez utiliser des applications Android sur des téléphones équipés de Sailfish. La dernière version de Sailfish OS est connue sous le nom de Sailfish X, qui fonctionne sur les appareils Sony Xperia X. Actuellement, de nombreux téléphones phares de Sony sont compatibles avec ce système d'exploitation mobile. Pour être exact, le système d'exploitation est disponible pour les Sony Xperia 10, Xperia 10 PlusRead More Reviews, Xperia XA2, Xperia XRead More Reviews, et Gemini PDA.

Malheureusement, Sailfish OS n'est pas open source et la version gratuite est une version d'essai limitée dans le temps. La plupart des téléphones habituels compatibles avec Linux fonctionnent avec Sailfish OS, bien que le développement se concentre sur les appareils Sony Xperia X, Sony Xperia 10 et Gemini PDA.

La version complète de Sailfish X coûtera environ 50 dollars et n'est disponible que dans l'Union européenne, en Norvège et en Suisse.

Caractéristiques :

- Tire ses origines de Nokia et du système d'exploitation MeeGo
- N'est pas totalement open source
- Entièrement indépendant d'Android, mais peut toujours prendre en charge le système d'exploitation en question
- Actuellement en version 3.0, la dernière mise à jour ayant été diffusée récemment
- Livré avec Sailfish Browser est le navigateur web par défaut basé sur Gecko
- Développé en C et utilisent l'API Qt sur Wayland

e) MIUI

MIUI est le système d'exploitation du fabriquant de smartphone Xiaomi.
C'est un fork créé par la société Xiaomi en 2010, basé sur le projet AOSP (Android Open Source Project). Actuellement, cette alternative à Android en est déjà à sa 12e version. La première version, MIUI 1, était basée sur Android 2.1 et a été publiée en août 2010. Comme ce système d'exploitation est basé sur Android, ses caractéristiques sont très proches de celles du système d'exploitation principal. MIUI possède l'une des interfaces utilisateur les plus fluides au monde aujourd'hui. Il dispose également d'une version du mode Ultra Battery Saver de Samsung et du Dark Mode. Le multitâche et le tiroir d'applications sont également présents sur ces téléphones.

MIUI est actuellement une exclusivité de Xiaomi. MIUI 12, la dernière version de ce système, prend en charge la série Xiaomi Mi, qui compte trois smartphones. Elle prend également en charge deux appareils de la série Xiaomi Redmi K.

Caractéristiques :

- Exclusivité des appareils Xiaomi
- Système d'interface utilisateur basé sur Android
- Téléchargement d'applications à partir du Play Store

f) Sirin OS

Fondée en 2013 par l'entrepreneur israélien Moshe Hogeg, Sirin Labs a été conçue pour les crypto-monnaies. La première version de Sirin OS, a été publié en 2018.

Sirin OS est actuellement exclusif à la seule marque de smartphone de Sirin Labs, FINNEYRead More Reviews. FINNEY est le premier smartphone blockchain au monde, ce qui en fait l'unité parfaite pour héberger Sirin OS. Cette combinaison est certainement quelque chose que les traders devraient considérer comme une alternative aux téléphones Android.

Enfin Sirin est toujours connecté à Android via le magasin d'applications, car ce système d'exploitation vieux de deux ans n'a pas encore son propre magasin d'applications.

Caractéristiques :

- Prise en charge d'un seul appareil (FINNEY par Sirin Labs)
- Spécialement conçu pour être suffisamment sécurisé pour stocker des crypto-monnaies
- Possède son propre système de jetons (SIRIN Token)
- Idéal pour les traders de crypto-monnaies

2) Les applications

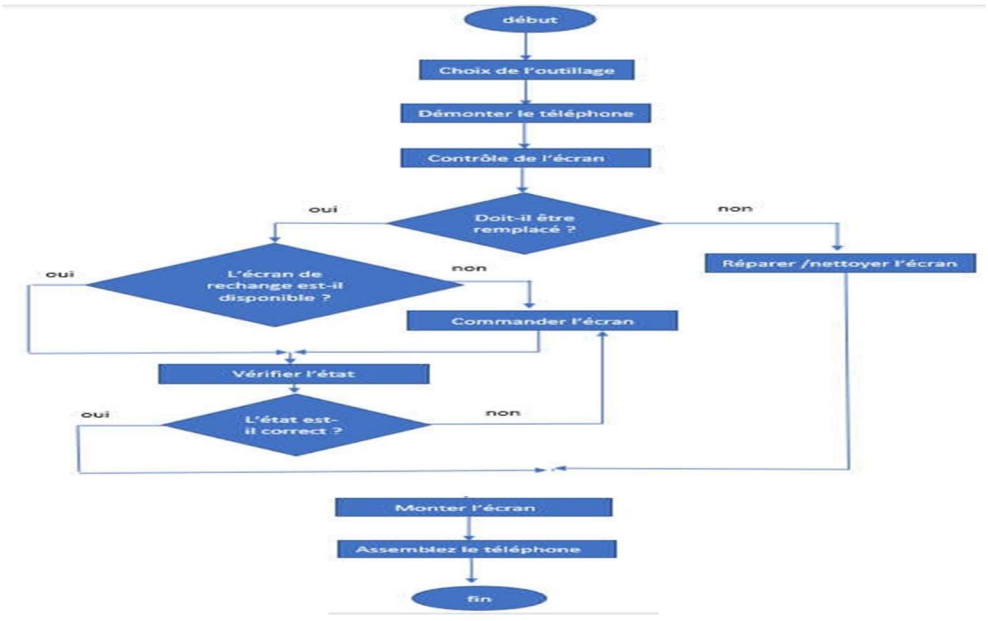
Les applications sont des programmes informatiques qui permettent d'effectuer des tâches spécifiques telles que la communication, la navigation, la productivité, les jeux, etc. Elles sont développées pour fonctionner sur un OS spécifique et sont disponibles sur les magasins d'applications. Nous pouvons télécharger ces applications via : Apple store pour les systèmes IOS, google Play store et Android market pour le téléchargement des applications pour Android.

CHAPITRE IV : MAINTENANCE CURATIVE ET QUELQUES TECHNIQUES DE REPARATION

La **maintenance corrective curative**, en abrégé la **maintenance curative**[1], est une subdivision de la maintenance corrective, par opposition à ce qu'on appelle la « maintenance corrective palliative », c'est-à-dire le dépannage (ou réparation provisoire). Cette distinction est inconnue chez les auteurs de langue anglaise. Pour ceux-ci, la maintenance curative est synonyme de maintenance corrective (ou correctrice) et s'oppose à la maintenance préventive (angl. *preventive maintenance* ou *preventative maintenance*).

I- Flow-chart de diagnostic

Les flow charts ou organigrammes étaient à l'origine utilisés par les ingénieurs industriels pour structurer les processus de travail tels que la fabrication a la chaine de montage. Aujourd'hui, les organigrammes sont utilisés à diverses fins dans les domaines de la fabrication, le l'architecture, de l'ingénierie, des affaires, de la technologie, de l'éducation, des sciences, de la médecine, du gouvernement, de l'administration et de nombreuses autres disciplines. Le flow chart parfois appelé organigramme des tâches ou logigramme est un diagramme qui aide les individus à visualiser un processus en étapes discrètes organisées dans la séquence d'événements. Il montre les étapes sous forme de boîtes de différents types, et leur ordre en reliant les boîtes avec des flèches. Les organigrammes sont utilisés pour analyser, concevoir, documenter et résoudre un problème précis. Le flow chart permet de représenter des processus ou des workflow (flux de travaux). Ci-dessous un exemple de flow-chart pour le changement d'écran d'un téléphone



II- Déblocage des terminaux mobiles

Il est assez régulier d'être en possession d'un terminal mobile qu'il faille « débloquer ». Ci-dessous quelques définitions techniques adaptées au contexte de certaines situations et quelques solutions pour chaque cas de figure.

a) Définitions

- Le code PIN (Personal Identification Number), c'est le code d'entrée (le mot de passe en quelque sorte...) de votre carte SIM. Il est demandé normalement à chaque démarrage ou redémarrage du téléphone.

- Le code PUK (PIN Unlock Key), c'est le code demandé pour déverrouiller la carte SIM en cas de trois mauvais codes PIN saisis, il ne peut vous être fourni que par votre opérateur.

- Le code de restriction, aussi appelé code opérateur, code NCK Network Control Key ou code réseau vous permet de débloquer votre téléphone pour l'utiliser avec n'importe quelle carte SIM des différents opérateurs.

- IMEI: International Mobile Equipment Identity, littéralement en français « identité internationale d'équipement mobile ») est un numéro qui permet d'identifier de manière unique chacun des terminaux de téléphonie mobile (ME) GSM ou UMTS.

Ce numéro permet à l'opérateur du réseau d'identifier le mobile appelant et ainsi de l'autoriser ou non à se connecter. Il permet ainsi l'établissement des appels d'urgence sans SIM pour certains pays (par exemple le numéro d'urgence européen 112 en Europe). Son rôle le plus connu est de pouvoir bloquer un mobile volé (grey list, black list) auprès de l'ensemble des opérateurs ayant souscrit à la base de données IMEI.

*#06# saisi au clavier de votre téléphone vous permet d'obtenir votre code IMEI.

- Le code de sécurité est propre au téléphone. Activé par le propriétaire du mobile, il est demandé pour éviter qu'une autre personne puisse se servir de l'appareil (en cas de vol par exemple...). Ce code est entièrement modifiable.

❖ Simlockage

- Ce qu'on appelle le déblocage, le déverrouillage ou le désimlockage d'un téléphone mobile, c'est le fait de déprogrammer la

carte électronique interne d'un téléphone pour lui permettre de fonctionner avec n'importe quelle autre carte SIM.

- Les téléphones sont vendus bloqués car ils sont sponsorisés par votre opérateur (il paye une grosse partie du prix du téléphone). En contrepartie, l'utilisation du téléphone sur un autre réseau est limitée. Ceci pour des raisons économiques évidentes : l'opérateur a investi dans le téléphone et il est donc normal que vous dépensiez votre argent sur son réseau. Légalement, on ne peut vous interdire de débloquer votre mobile, mais il faut bien sûr que vous en soyez le propriétaire. Le prix peut varier aussi selon la valeur du téléphone !

Si vous demandez à votre opérateur de débloquer votre mobile, il doit vous fournir le code de déblocage selon des modalités précisées dans votre contrat. Si votre opérateur se charge de l'opération, le principe du déverrouillage vous est envoyé (message SMS par exemple) ou effectué directement en ligne (généralement une combinaison de touches à taper sur le clavier de votre mobile...code à entrer...etc).

Vous pouvez aussi le faire faire par une société indépendante qui peut alors désimlocker votre appareil pour un prix modique, mais attention ! Dans ce cas-là, vous perdez la garantie, et de mauvaises manipulations peuvent entraîner des dommages irréversibles !

❖ Dé-Simlockage

Vous êtes l'heureux propriétaire d'un iPhone, d'un Samsung Galaxy ou encore d'un Sony Speria, mais vous ne pouvez pas l'utiliser avec un autre opérateur que celui qui vous l'a vendu ?

Le désimlockage, appelé aussi déblocage ou déverrouillage, d'un téléphone consiste à casser le verrou mis en place par un opérateur afin de le rendre compatible avec l'ensemble des fournisseurs mobiles. Cette action est indispensable si vous avez acquis un téléphone bloqué chez un opérateur de téléphonie tel que Orange, SFR ou Bouygues Telecom. Cette pratique est réglementée par la loi.

Comment effectuer le désimlocage d'un portable ?

Il y a différentes techniques de déblocage selon le modèle, la marque, le pays d'origine et l'opérateur du téléphone toutefois les démarches restent les mêmes.

De plus, la durée de l'opération peut varier de quelques minutes ou heures à quelques jours. Le déblocage sur internet sera de manière générale plus rapide.

- En passant par l'opérateur d'origine

En exprimant votre souhait de débloquer votre téléphone auprès de l'opérateur de téléphonie mobile vous ayant fournis le terminal, celui-ci est dans l'obligation de satisfaire à votre requête. Il convient alors de contacter le service client adapté et de lui fournir les informations nécessaires. Il est généralement question de communiquer le nom et prénom du titulaire du mobile, la référence du contrat et le numéro téléphonique, une adresse email, la marque et modèle du téléphone, ainsi que le code IMEI.

Une fois votre demande pris en compte, l'opérateur de réseau mobile vous recontactera pour vous fournir toutes les informations nécessaires pour débloquer le téléphone : code de déverrouillage propre à votre mobile ainsi que la procédure à suivre.

Il existe plusieurs autres moyens de désimlocker votre mobile. Je vous invite à faire d'autres recherches complémentaires sur Internet.

Le déblocage des terminaux mobiles est une thématique assez vaste qui peut aller jusqu'à constituer tout un domaine de formation. Aussi, de façon générale, les différents trucs et astuces sont contenus sur Internet avec d'autres découvertes qui ne peuvent être connus qu'en pratiquant au quotidien.

CHAPITRE V : SECURITE ET PROTECTION DES APPAREILS MOBILES

Les téléphones mobiles intelligents (smartphones), les tablettes et les terminaux mobiles informatiques sont devenus des instruments pratiques du quotidien, tant pour un usage personnel que professionnel. Leurs capacités ne cessent de croître et les fonctionnalités qu'ils offrent s'apparentent, voire dépassent parfois, celles des ordinateurs. Ils contiennent tout autant et plus d'informations sensibles ou permettent d'y accéder. Ils sont plus faciles à perdre ou à se faire voler. Ces appareils mobiles sont, malgré tout, généralement bien moins sécurisés que les ordinateurs par leurs propriétaires.

I- Bonnes pratiques à adopter pour la sécurité des appareils mobiles

1- Mise en place des codes d'accès

Qu'il s'agisse du code de déverrouillage ou du code PIN, ces protections complémentaires empêcheront une personne malintentionnée de pouvoir se servir facilement de votre appareil si vous en perdez le contrôle (perte, vol, abandon) et donc d'accéder à vos informations. Bien entendu, vos codes d'accès doivent être suffisamment difficiles à deviner (évitez 0000 ou 1234, par exemple). Activez également le verrouillage automatique de votre appareil afin que le code d'accès soit demandé au bout de quelques minutes si vous laissez votre appareil sans surveillance.

2- Chiffrage des données de l'appareil

En cas de perte ou de vol, seul le chiffrement des données contenues dans votre appareil vous assurera qu'une personne malintentionnée ne pourra pas contourner les codes d'accès et accéder quand même à vos informations. Tous les appareils récents proposent cette option qu'il suffit d'activer dans les paramètres et qui est quasi transparente à l'utilisation. Si vous utilisez une carte d'extension mémoire pour stocker vos informations, vérifiez qu'elle est également chiffrée.

3- Application des mises à jour de sécurité

Qu'il s'agisse du système d'exploitation (Android, iOS) ou des applications qui sont sur votre appareil, installez sans tarder les mises à jour dès qu'elles sont proposées car elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations.

4- **Faire des sauvegardes**

Votre appareil mobile contient généralement des informations que vous n'avez nulle part ailleurs, comme votre répertoire de contacts, vos messages, vos photos… Pensez à le sauvegarder régulièrement car vous pourriez tout perdre en cas de casse, de perte ou de vol.

5- **Utilisation d'une solution de sécurité contre les virus et autres attaques**

De nombreuses solutions de sécurité existent pour aider à se protéger des différentes attaques que peuvent subir les appareils mobiles au même titre que les ordinateurs de bureau comme les virus, les rançongiciels (ransomware), l'hameçonnage (phishing)… Des cybercriminels se spécialisent dans les attaques d'appareils mobiles qu'ils savent souvent bien moins sécurisés que les ordinateurs de bureau. Il est donc important d'avoir un bon niveau de protection et de s'équiper d'un produit spécialisé.

6- **Installation des applications que depuis des sites ou magasins officiels**

Seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées. Méfiez-vous des sites « parallèles », qui ne contrôlent pas les applications qu'ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal: elles sont généralement piégées. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application. Au moindre doute, n'installez pas l'application et choisissez-en une autre.

7- **Contrôle des autorisations des applications**

Vérifiez également les autorisations que vous donnez à vos applications lors de leur première installation, mais aussi après leurs mises à jour car leurs autorisations peuvent évoluer. Certaines applications demandent parfois des droits très importants sur vos informations et qui peuvent être « surprenants ». Par exemple, un simple jeu de cartes « gratuit » qui vous demanderait l'autorisation d'accéder à votre répertoire, vos mots de passe, vos messages, votre position GPS ou encore votre appareil photo est évidemment suspect. Au moindre doute, n'installez pas l'application et choisissez en une autre.

8- **Ne pas laisser l'appareil sans surveillance**

Une personne malintentionnée pourrait profiter de votre manque de vigilance pour accéder à vos informations ou piéger votre appareil. Pour ces mêmes raisons, il est fortement déconseillé de laisser un tiers se servir de votre appareil mobile (pour passer

un appel par exemple) sans que vous ne puissiez contrôler physiquement l'utilisation réelle qu'il en fait.

9- **Eviter les réseaux publics wi-fi inconnus**

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire… afin d'en faire un usage délictueux. D'une manière générale, désactivez toutes les connexions sans fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC…) car elles sont autant de portes d'entrée ouvertes sur votre appareil. De plus, elles épuisent votre batterie inutile- ment.

10- **Ne pas stocker des informations confidentielles sans protection**

Ne notez jamais d'informations secrètes comme vos mots de passe ou vos codes bancaires dans votre répertoire de contacts, votre messagerie ou un fichier non chiffré sur votre appareil mobile. Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer. En outre, certaines applications que vous avez installées peuvent aussi accéder et récupérer ces informations dont vous perdriez alors le contrôle. Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.

II- LES LOGICIELS MALVEILLANTS ET LES METHODES D'INFILTRATION

1) Les logiciels malveillants

Les cybercriminels utilisent de nombreux types de logiciels malveillants, ou malwares, pour mener à bien leurs activités. Un ***logiciel malveillant*** est un code qui peut être utilisé pour voler des données, contourner les contrôles d'accès ou endommager ou compromettre un système. Savoir quels sont les différents types et comment ils se propagent est essentiel pour les contenir et les éliminer.
➢ **SPYWARE :** conçus pour vous suivre et vous espionner, les logiciels espions surveillent votre activité en ligne et peuvent enregistrer chaque touche sur laquelle vous appuyer sur votre clavier, ainsi que capturer presque toutes vos données, y compris des informations personnelles.
➢ **Adware :** les logicielles publicitaires sont souvent installées avec certaines versions de logiciels et sont conçus pour diffuser automatiquement des publicités à un utilisateur, le plus souvent sur un navigateur web. Il est courant que les logiciels publicitaires accompagnent les logiciels espions.
➢ **Porte Arrière :** ce type de logiciel malveillant est utilisé pour obtenir un accès non autorisé en contournant les procédures d'authentification

normales pour accéder à un système. Par conséquent, les pirates peuvent accéder à distance aux ressources d'une application et émettre des commandes système à distance. Une porte dérobée fonctionne en arrièreplan et est difficile à détecter.

➢ **Logiciels de rançon (Ransomware) :** ce logiciel malveillant est conçu pour retenir un système informatique ou données qu'il contient en captivité jusqu'à ce qu'un paiement soit effectué. Les rançongiciels fonctionnent généralement en cryptant vos données afin que vous ne puissiez pas y accéder.

➢ **Logiciels effrayants :** il s'agit d'un logiciel malveillant qui utilise des tactiques d'effarouchement pour vous inciter à effectuer une action spécifique. Les Scarewares consistent principalement en des fenêtres de style système d'exploitation qui s'affichent pour vous avertir que votre système est à risque et doit exécuter u n programme spécifique pour qu'il revienne à un fonctionnement normal.

➢ **Rootkit :** ce logiciel malveillant est conçu pour modifier le système d'exploitation afin de créer une porte dérobée, que les attaquants peuvent ensuite utiliser pour accéder à votre ordinateur à distance.

➢ **Virus :** c'est un type de programme informatique qui, lorsqu'il est exécuté, se réplique et s'attache à d'autres fichiers exécutables, comme un document, en insérant son propre code.

➢ **Cheval de Troie :** ce malware effectue des opérations malveillantes en masquant sa véritable intention. Les chevaux de Troie exploitent vos privilèges d'utilisateur et se trouvent le plus souvent dans des fichiers images, audios, ou des jeux. Contrairement aux virus, ils ne s'autorépliquent pas, mais agissent comme un leurre pour dissimuler des logiciels malveillants aux utilisateurs peu méfiants.

➢ **Vers :** il s'agit d'un type de malware qui se réplique pour se propager d'un ordinateur à un autre. Contrairement aux virus, qui nécessitent un programme hôte pour s'exécuter, les vers s'exécutent d'eux même. Les vers partagent des modèles similaires : ils exploitent les vulnérabilités du système, ils ont un moyen de se propager et ils contiennent tous un code malveillant pou endommager les systèmes ou les réseaux informatiques.

2) Les méthodes d'infiltration

➢ Ingénierie sociale
➢ Déni de Service
➢ Dos Distribué
➢ Réseau de zombies

➢ Attaques sur le chemin
➢ Empoisonnement du référencement
➢ Craquage du mot de passe Wi-Fi
➢ Attaques par mots de passe

3) Hackers et acteurs des ménaces

Comme le montre la figure, les termes white hat hacker, black hat hacker et grey hat hacker sont souvent utilisés pour décrire les pirates.
❖ Les ***hackers chapeau blanc*** sont des hackers éthiques qui utilisent leurs compétences en programmation à des fins bonnes, éthiques et légales. Ils peuvent effectuer des tests de pénétration du réseau dans le but de compromettre les réseaux et les systèmes en utilisant leur connaissance des systèmes de sécurité informatique pour découvrir les vulnérabilités du

réseau. Les vulnérabilités de sécurité sont signalées aux développeurs et au personnel de sécurité qui tentent de corriger la vulnérabilité avant qu'elle ne puisse être exploitée. Certaines organisations attribuent des prix ou des primes aux pirates informatiques lorsqu'ils fournissent des informations permettant d'identifier les vulnérabilités.

❖ Les ***hackers chapeau gris*** sont des individus qui commettent des crimes et font des choses sans doute contraires à l'éthique, mais pas pour leur profit personnel ou pour causer des dommages. Un exemple serait quelqu'un qui compromet un réseau sans autorisation, puis divulgue publiquement la vulnérabilité. Les hackers chapeau gris peuvent divulguer une vulnérabilité à l'organisation affectée après avoir compromis leur réseau. Cela permet à l'organisation de résoudre le problème.

❖ Les ***hackers black hat*** sont des criminels contraires à l'éthique qui violent la sécurité des ordinateurs et des réseaux à des fins personnelles ou pour des raisons malveillantes, telles que l'attaque de réseaux. Les hackers black hat exploitent les vulnérabilités pour compromettre les systèmes informatiques et réseau.