HORS SERIE SPECIAL MOBILE

PIRAT'Z

HACKERS & GAMERS

Juillet - août 2005

LECHATKITU

4 €

Skype sur ton mobile 100% gratos

Comment cloner ta carte SIM en 10 mn

BLUETOOTH : trop pas fiable

Le Mag ki va empeché ton opérateur 2 dormir tranks

La recette maison du déblockage téléphone

DOM: 4.80 euros - BEL: 4.80 euros - CAN: 5.95 $CAD - MAR : 35 MAD

L 13117 - 10 H - F: 4,00 € - RD

GSM PIRATRY

EDITO

Sur les millions de lecteurs de ce fabuleux magazine seule une minuscule, voire même microscopique partie de nos lecteurs lisent les éditos ! Les statistiques sont formelles : sur les 10 993 478 lecteurs du dernier numéro, seules onze personnes l'ont lu.

J'ai donc l'honneur de t'annoncer que tu n'es plus un simple lecteur fondu dans la masse - je te tutoie même désormais - mais l'Élu ! Encore bravo, toi qui non seulement lit notre magazine (ce qui montre déjà une certaine clairvoyance) et qui donc nous voue une adoration sans limites pour lire ces quelques lignes. Je te remercie du fond du coeur, c'est grâce à des gens comme toi, fidèle et fou d'amour, que la puissance de la philosophie Pirat'z dépasse largement celle de Nietzsche.

Mais d'un autre côté, c'est TOI qui devrait nous remercier pour tous ces bijoux que nous t'offrons. Pirat'z, c'est une boucherie, une bombe atomique qui déchire sa maman. Bref comme nous vous le disions, Pirat'z rox !

Je suppose que tu ne lis pas ces lignes pour apprendre des lieux communs, mais plutôt pour savoir pourquoi ce mag ? Eh bien, c'est une excellente question même si la réponse est évidente.! Plutôt que de faire un long discours, je vais vous parler de ma femme - ah non, c'est pas dans le bon mag ça ! Je vais plutôt vous raconter l'anecdote véridique qui nous a poussé à faire ce mag.

J'étais tranquillement assis dans le métro lorsqu'un de mes potes, qui venait d'avoir un D500 (celui de la couv' héhéhé !), lança un scan bluetooth. Et visiblement, un téléphone compatible se trouvait non loin de nous ! Nous effectuâmes immédiatement une demande de connexion. L'histoire aurait très bien pu se terminer là. Mais non ! Sous nos yeux ébahis, notre voisin d'en face sortit sa tête de son journal et son téléphone de sa poche (attention, pas l'inverse), regarda d'un air hagard son téléphone et appuya naturellement sur " ok " avant de remettre et son téléphone et sa tête à leurs endroits initiaux. Inutile de vous dire que nous avions alors accès à toutes ses données : photos, vidéos, SMS, etc.

Les portables sont quelque chose de fabuleux mais hélas aujourd'hui autant vulnérables, il fallait donc y remédier.

Nous allons justement vous parler de toutes ces bidouilles insoupçonnées. Il ne te restera plus, mon cher, qu'à devenir un vrai l33t du portable (et ça en plus, c'est fashion;)

Sommaire

PIRAT'Z HORS SÉRIE SPÉCIAL GSM

Redacteur en chef : ARTYC
Conception graphique : WEEL
Illustrations : LECHATKITU
ISSN en cours
Numero de comission paritaire en cours
Directeur de la publication : O. ANDRE

IMPRIME EN FRANCE

TELECOMS, CHOISIR LA BONNE NORME

Tout au long de ce journal, nous allons parler télécommunications. C'est un sujet extrêmement dur à expérimenter. Il est indispensable, pour bien comprendre tous les mécanismes de ces modes de communication, de passer par la théorie qui vous permettra, plus tard, d'aborder la pratique sans trop de difficultés. Accrochez-vous !

INTRODUCTION

De nos jours, les télécoms tiennent une place importante dans notre vie quotidienne. Avec ce développement, de nouvelles technologies sont apparues en nombre. Cet article va vous éclairer sur les différents choix qui vous sont proposés. L'étude des infrastructures et une présentation des normes vous offriront un grand champ de vision de ce monde des télécoms.

RTC

Le premier type de réseau de télécoms que nous allons voir est le RTC (Réseau Téléphonique Commuté), le téléphone fixe. Ce type de réseau est le plus ancien qui soit encore en fonctionnement actuellement.

ARCHITECTURE

Un réseau de type RTC est composé de trois grandes parties :

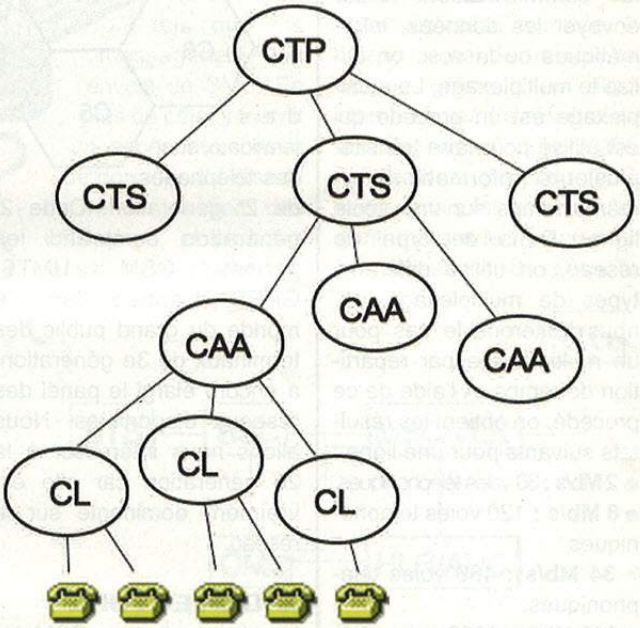
- **Commutation :** elle permet la mise en relation des différents usagers du réseau.
- **Transmission :** elle permet la liaison entre les commutateurs du réseau, on l'appelle aussi réseau de transmission.
- **Distribution :** elle permet aux usagers de se raccorder correctement au plus proche commutateur disponible.

Puis ce réseau de téléphone est composé de trois zones :

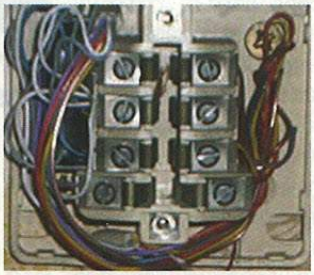
- **ZAA :** Zone à Autonomie d'Acheminement : Cette zone est la plus basse du réseau, elle est composée des commutateurs CAA (Centre de rattachement à Autonomie de d'Acheminement) pour accueillir les utilisateurs. Les utilisateurs sont directement reliés au CAA ou alors un CL (Centre Local) sert d'intermédiaire. La ZAA est un réseau de forme étoilée.
- **ZTS :** Zone de Transite Secondaire : Cette zone fait suite à la ZAA, elle est composée des commutateurs CTS (Commutateur de Transite Secondaire). Elle ne correspond pas directement avec les usagers du réseau. Elle peut servir de lien entre plusieurs CAA lorsque les deux abonnés ne dépendent pas de CAA proches.
- **ZTP :** Zone de Transite Principale : Cette zone est la plus haute, elle est utilisée pour les liaisons longue distance. Elle est composée de commutateurs CTP (Commutateur de Transite Primaire) et CTI. Elle fait la liaison entre les commutateurs CTP et le commutateur CTI.

Pour se connecter aux réseaux internationaux, des commutateurs de transites primaires sont reliés à des commutateurs de transites internationaux.

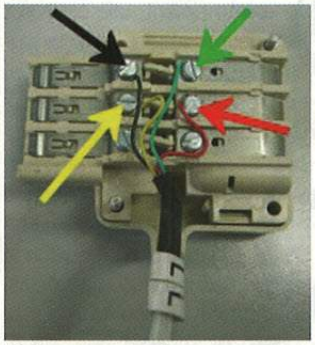
De plus, deux usagers se trouvant dans une même ZAA peuvent se joindre sans passer par le réseau national.



Prise



Prise mural



Prise ouverte

Par exemple, en France, à la fin du XXe siècle, on trouvait 5 ZTP, 39 ZTS, 1000 CAA ainsi que 10 000 CL regroupés dans plus de 400 ZAA. France Telecom essaie depuis des années de réduire le nombre de ZAA pour atteindre, en 2008, un nombre inférieur à 200.

COMMUNICATION

Maintenant que l'architecture des réseaux de type RTC vous est connue, parlons de la communication. Pour envoyer les données, informatiques ou la voix, on utilise le multiplexage. Le multiplexage est un procédé qui est utilisé pour faire transiter plusieurs informations en même temps sur une seule ligne. Dans ce type de réseau, on utilise différents types de multiplexage. Ici, nous traiterons le cas pour un multiplexage par répartition de temps. À l'aide de ce procédé, on obtient les résultats suivants pour une ligne :

- **2 Mb/s :** 30 voies téléphoniques.
- **8 Mb/s :** 120 voies téléphoniques.
- **34 Mb/s :** 480 voies téléphoniques.
- **140 Mb/s :** 1920 voies téléphoniques.
- **565 Mb/s :** 7680 voies téléphoniques.

Depuis peu, la fibre optique remplace petit à petit les anciennes lignes, on utilise alors le multiplexage SDH, pour hiérarchie numérique synchrone.

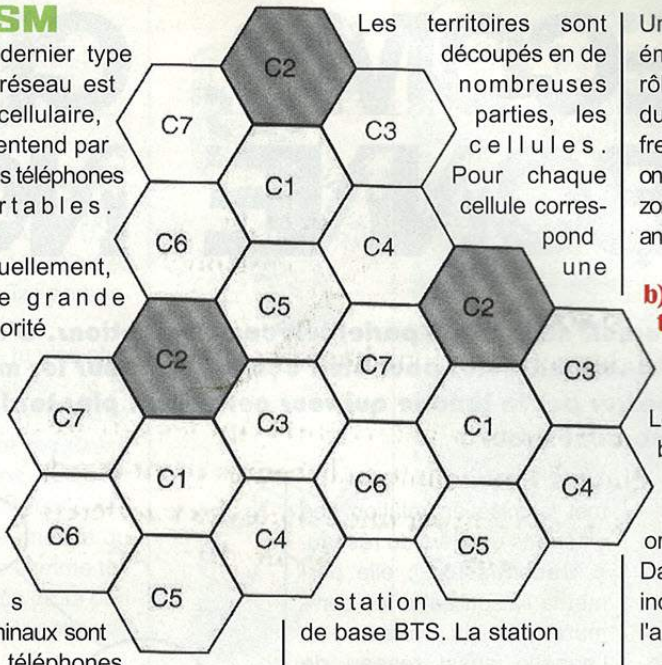
OUVERTURE

Le réseau RTC est encore extrêmement utilisé, il est encore présent dans la plupart des foyers français, cependant son avenir n'est pas certain. L'arrivée du VOIP pour le grand public va peut-être faire disparaître cette technologie d'ici quelques années.

GSM

Le dernier type de réseau est le cellulaire, on entend par là les téléphones portables.

Actuellement, une grande majorité des terminaux sont des téléphones de 2e génération. Cette 2e génération comprend les normes GSM, UMTS, GPRS. L'entrée dans le monde du grand public des terminaux de 3e génération, a encore élargi le panel des réseaux disponibles. Nous allons nous intéresser à la 2e génération car elle est vraiment dominante sur le réseau.



ARCHITECTURE

Un réseau de type GSM est un réseau dit cellulaire, composé de cellules, *(voir schema)*.

Un réseau de type GSM a besoin de six principaux équipements qui vont servir à assurer une couverture radioélectrique du réseau, la communication, l'exploitation et l'interconnexion, à gérer des bases de données, à localiser l'utilisateur. Nous allons voir plus en détail chacun de ces équipements afin de mieux comprendre l'acheminement de nos communications téléphoniques.

a) La station de base BTS (Base Transceiver Station)

Les territoires sont découpés en de nombreuses parties, les cellules. Pour chaque cellule correspond une station de base BTS. La station est utilisée pour fournir des points d'entrées aux communications des utilisateurs. Ce type de station assure une couverture radioélectrique d'une cellule entière. La taille des cellules est très variable selon que l'on est dans une zone urbaine ou rurale (plus la densité de population est grande, plus les cellules sont petites, minimum 200 m, et si la densité de population est très faible la zone couverte par une cellule augmente jusqu'à 30 km). En effet, les stations de base BTS ne peuvent gérer que 8 communications car la technique de multiplexage AMRT a une limite de 8.

On reverra plus tard quels sont les points de sécurité que créent les stations de base BTS.

Une station de base est un émetteur-récepteur, dont le rôle est la modulation, démodulation, multiplexage, chiffrement. Il mesure aussi les ondes reçues des terminaux de sa zone, puis envoie les données à analyser au BSC.

b) Le contrôleur de stations de base BSC (Base Station Controller)

Le contrôleur de station de base sert de connexion entre plusieurs stations de bases, on dit que c'est un organe intelligent du réseau. Dans un sens, le contrôleur indique à une station de base l'arrivée d'un nouvel utilisateur

Antenne BTS

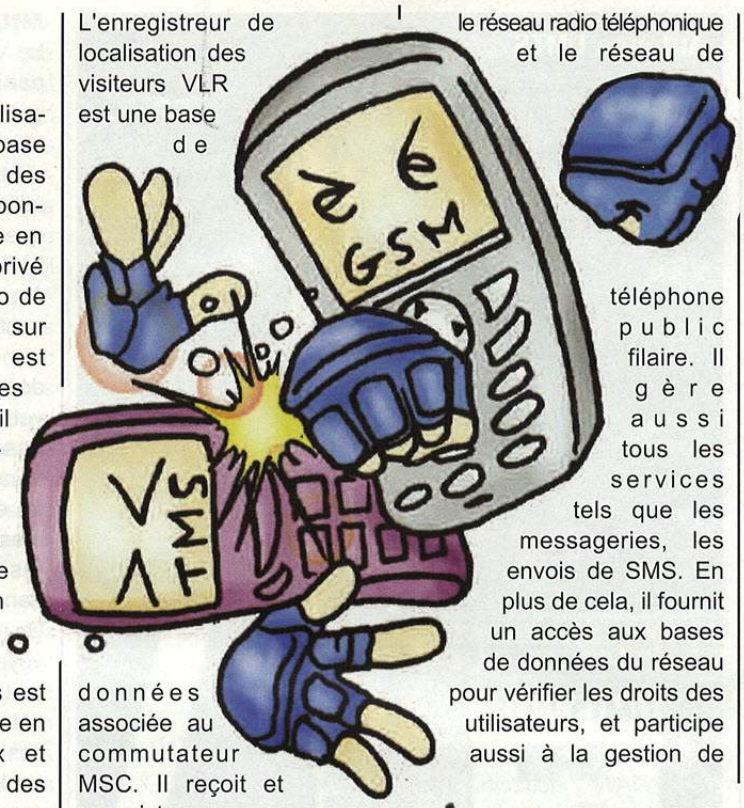
et dans l'autre sens, il indique à la base de données HLR la nouvelle position de l'utilisateur. À chaque fois que l'on s'apprête à changer de cellule, les informations de notre carte SIM sont envoyées à la base de donnée HLR avec notre future station de base. Le contrôleur de stations analyse les données de la BTS, puis donne l'ordre du changement de cellule.

c) L'enregistreur de localisation nominal HLR (Home Location Register)

L'enregistreur de localisation nominale est une base de données stockant des informations sur les abonnés du réseau. Il garde en mémoire le numéro privé de l'usager, son numéro de terminal, son profil, et sur quelle VLR l'usager est actuellement. Selon les fournisseurs d'accès, il peut y avoir un ou plusieurs HLR, cela dépend de l'espace disponible sur les machines ainsi que de leurs performances, en fait de l'investissement du fournisseur. Cette base de données est très importante, elle gère en permanence les lieux et informations principaux des utilisateurs, tels que sa position, l'état de son téléphone (allumé, éteint, en communication...). Le HLR différencie les terminaux (Le téléphone en lui-même) et les utilisateurs (carte SIM), car si un usager met sa carte SIM dans le téléphone d'un autre, il faut bien que ce soit le propriétaire de la carte SIM qui paie et non le propriétaire du téléphone. Le HLR enregistre les principales informations de la carte SIM telles que le numéro privé de l'utilisateur (celui ci est crypté et ne peut être décrypté que par le HLR). La base de données de l'HLR contient toutes les informations sur tous les utilisateurs, leur abonnement, leur temps de communication, leur dernier emplacement. Le HLR est une structure très importante dans un réseau de type GSM, particulièrement pour la sécurité.

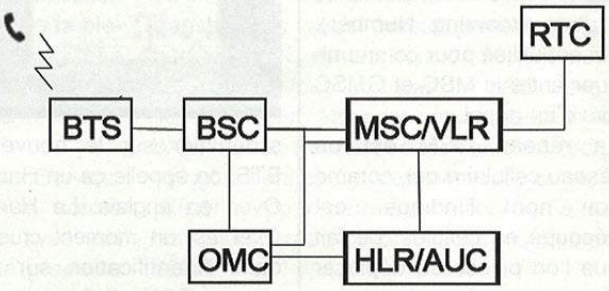
d) L'enregistreur de localisation des visiteurs VLR (Visitor Location Register)

L'enregistreur de localisation des visiteurs VLR est une base de données associée au commutateur MSC. Il reçoit et enregistre en permanence et de manière dynamique tous les déplacements de l'utilisateur. Le VLR stocke uniquement ces informations pour les usagers présents dans sa zone, à la différence du HLR. En général, on a un VLR pour un MSC, mais il est possible d'avoir plusieurs MSC pour un VLR.



e) Le commutateur MSC (Mobile Switching Center)

La principale fonction du commutateur MSC est d'assurer l'interconnexion entre le réseau radio téléphonique et le réseau de téléphone public filaire. Il gère aussi tous les services tels que les messageries, les envois de SMS. En plus de cela, il fournit un accès aux bases de données du réseau pour vérifier les droits des utilisateurs, et participe aussi à la gestion de déplacement des abonnés. C'est l'élément du réseau qui exécute le changement de cellule de l'utilisateur. Il est en permanence en relation avec le VLR.



f) Le centre d'authentification AUC (AUthentication Center)

Le centre d'authentification est aussi une base de données, qui est utilisée pour identifier les utilisateurs et éviter les fraudes. Dans cette base de données, sont enregistrés tous les numéros d'abonnements des utilisateurs ainsi que leurs droits, afin qu'à tout moment l'opérateur connaisse l'état de facturation de n'importe quel utilisateur. En effet, le réseau de téléphone portable est relativement bien protégé par plusieurs sécurités. La première intervient lors de l'allumage de notre terminal, avec l'entrée du code PIN, qui est comparé avec celui enregistré sur la carte SIM. Puis, pour chaque demande de service au réseau, l'utilisateur doit s'identifier au près du AUC en envoyant son numéro d'abonnement. Il est ensuite vérifié avec les droits de l'utilisateur. Cette étape n'est pas aussi simple que l'on peut penser, car il ne faut pas dévoiler le numéro secret de l'usager. Une fois cette vérification terminée, le réseau demande un résultat obtenu grâce à un algorithme secret. Le résultat est ensuite envoyé puis vérifié, du Terminal jusqu'au AUC, sans jamais faire passer l'algorithme sur le réseau pour des questions de sécurité. Toutes ces protections sont indispensables, car dans le système employé par les opérateurs, l'utilisateur ne peut pas contester sa facture, donc les risques de fraudes doivent être minimes.

g) Le centre d'exploitation et de maintenance OMC

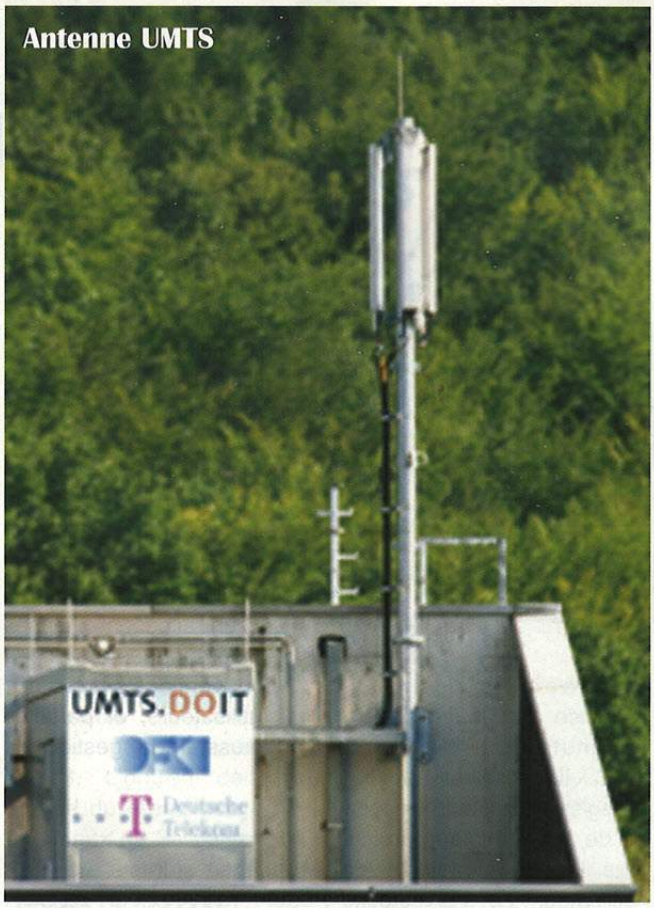
Le centre d'exploitation et de maintenance est la partie du réseau des opérateurs qui gère les problèmes techniques et la gestion administrative. La partie de la gestion administrative est en contact avec la base de donnée HLR, c'est elle qui gère la facturation, les changements d'abonnements...
En ce qui concerne la gestion des problèmes techniques, l'OMC sert à repérer les disfonctionnements dans le réseau, les

mises à jour du logiciel, les problèmes de sécurité et les performances du réseau.

COMMUNICATION

Pour communiquer sur un réseau de type GSM, il faut être identifié sur le réseau, plus précisément sur le BTS. Dans un réseau de type GSM, l'usager est identifié à l'aide d'un numéro unique, le MSISDN. Sur le réseau, il est identifié par un autre numéro unique et secret, l'IMSI. Ce chiffre privé est le pilier de la sécurité de l'authentification du GSM, c'est pourquoi il doit voyager le moins possible sur le réseau. Pour y remédier, une fois l'usager identifié, il communique avec un numéro temporaire qui lui a été attribué, le TMSI. Enfin un dernier identifiant est le MSRN (Mobile Station Roaming Number), qui est utilisé pour communiquer entre le MSC et GMSC lors d'un appel.

Le réseau GSM est un réseau cellulaire qui, comme son nom l'indique, est découpé en cellules. Le fait que l'on puisse se déplacer librement, même lors d'un appel, pose problème. On est en effet identifié, mais dans une cellule. Une cellule étant entouré par six autres, comment prévoir ce changement ? Votre terminal émet des ondes jusqu'à la BTS de sa cellule, mais en fonction de son éloignement de celle-ci, la réception varie. Le terminal, lorsqu'il s'approche d'une bordure de cellule, émet jusqu'à au moins un autre BTS, le réseau calcule donc approximativement le déplacement de l'usager. Une fois la route sélectionnée et validée par le réseau, il faut opérer le changement de cellule et donc



Antenne UMTS

s'identifier sur le nouveau BTS, on appelle ça un Hand-Over, en anglais. Le Hand-Over est un moment crucial dans l'identification sur un réseau GSM. Il faut savoir que la cellule dans laquelle on se trouve et le changement de cellule sont vraiment importants. Votre terminal communique en permanence avec la BTS, toute les 60Ms, pour savoir où vous êtes et adapter la puissance du signal émis par votre terminal. Plus vous êtes loin, plus vous devez émettre fort, et plus vous consommez de batterie. La plus grande autonomie des batteries est un désir de tous, pour une meilleure économie aussi. La puissance d'émission dépend au carré, de la distance qui sépare votre mobile de la BTS.

Pour émettre un appel, un abonné du réseau GSM compose le numéro de son correspondant, sa demande arrive à la BTS de sa cellule. Elle traverse le BSC pour aboutir dans le commutateur du réseau, où l'abonné est d'abord authentifié puis son droit d'usage vérifié. Le commutateur MSC transmet alors l'appel au réseau public et demande au contrôleur BSC de réserver un canal pour la future communication. Lorsque l'abonné demandé décroche son téléphone, la communication est établie.

VOIP

VOIP, Voice over Internet Protocol, un sigle que l'on retrouve de plus en plus souvent dans les médias, journaux, internet et télévisés. Mais qu'est-ce qui se cache derrière ce protocole ?

Dans le passé et encore actuellement pour la majorité d'entre vous, lorsque vous téléphoniez avec votre téléphone fixe, vous utilisiez un réseau de type RTC. Maintenant, pour certains, il est possible de passer par un autre type de réseau, en l'occurrence le VOIP.

ARCHITECTURE

Le VOIP est un réseau bien particulier car il utilise en grande partie un réseau déjà existant et très connu, celui d'internet. En effet, ce réseau utilise votre ligne téléphonique physiquement, comme l'ADSL, par exemple.

Alors que vos appels passant par le RTC doivent suivre des lignes de téléphone depuis chez vous jusqu'à votre interlocuteur, le VOIP passe par internet pour transférer les données. C'est un énorme avantage en termes d'économie puisque le réseau est déjà implanté dans le monde entier.

De plus, le VOIP permet d'envoyer des fax et d'appeler tout en étant connecté à internet, mais aussi de consulter ses mails, tout ça sur une seule ligne. Un problème va cependant se poser.

Là où le téléchargement ou la navigation sur des sites internet tolère des ralentissements, une communication vocale ne permet pas de ralentissements ou de coupure. La qualité de connexion va alors poser problème. Voyons comment se déroule un appel sur un réseau VOIP.

COMMUNICATION

Dans un premier temps, les opérations se déroulent sur votre PC uniquement. L'ordinateur doit numériser, puisque quand vous parlez ce n'est pas du numérique, puis encoder les données, et enfin les compresser. Tout cela prend un certain temps en fonction de la qualité des composants de l'ordinateur. De plus, la compression ne peut se faire " à la volée ", il faut donc couper l'enregistrement, puis compresser le fichier et le découper en paquets pour l'envoi sur internet. La dernière variable est votre bande passante disponible pour envoyer les paquets.

On vient de voir tous les facteurs qui peuvent causer des soucis lors d'appels passant par le VOIP. Seulement un dernier point reste à voir, les envois de paquets par internet. En effet, l'envoi de paquets par internet ne garantit pas 100 % d'envoi réussi, des paquets se perdent ou n'arrivent pas dans l'ordre envoyé. On doit donc attendre les possibles paquets retardataires, ce qui entraîne un blanc dans la discussion. Les opérateurs ont admis qu'en dessous de 20 % de pertes, une conversation reste audible.

Le matériel nécessaire pour utiliser le VOIP est différent selon qu'on est dans une entreprise ou que l'on est un particulier. Nous prendrons le cas des particuliers. Les terminaux de téléphonie VOIP ne sont actuellement pas en vente, on doit alors faire avec ce qu'on a : un ordinateur. Un ordinateur composé d'une carte son, d'un micro, d'enceintes et d'une connexion internet, fera l'affaire. Vous pourrez appeler de votre ordinateur vers des numéros de téléphone du monde entier pour le même prix. Cependant, un frein à cette technologie est l'absence d'annuaire. Votre ordinateur ne possède pas de numéro de téléphone donc l'appel ne peut se faire que dans un seul sens. Pour le moment, aucune solution n'a été trouvée pour remédier à ce problème excepté l'utilisation de Skype (article dédié à Skype dans ce numéro).

Ce type de réseau peut être utilisé dans de nombreuses configurations, en local, dans une entreprise, ou non. Un appel VOIP peut être émis par un PC vers un autre PC, par un PC vers un téléphone ou même par un téléphone vers un téléphone. Dans le dernier cas, on peut opter soit pour un SoftPhone qui se branche sur le PC, soit pour un IpPhone qui est un téléphone indépendant. Désormais, de nombreux fournisseurs d'accès à internet offrent la possibilité de connecter à leur modem un téléphone qui passera par VOIP. De plus, l'arrivée de cette technologie a permis de résoudre certains problèmes que rencontrait France Telecom. Par exemple, avant, lorsque vous étiez en ligne sur internet, vous étiez injoignable. Avec le VOIP lorsqu'on vous contacte, le service @llo de France Telecom vous permet de recevoir un message sur internet vous précisant que l'on cherche à vous joindre. Ce service @llo fut le premier à mettre en relation un appel téléphonique et un ordinateur.

Antenne UMTS

Mais c'est quoi ces trucs dont tout le monde parle ?

LA 2G

Le GSM (Global System Communication for Mobile) est la norme actuelle de la plupart de vos portables (2G). Elle a été créée début des années 1990. Les SMS utilise ce protocole de communication d'une vitesse faible de 9,6 kbits/s.

Le GRPS (General Packet Radio Service) est une version améliorée de la norme GSM. Il est donc compatible avec cet ancien réseau. Le GRPS est la première technologie qui permet l'accès à Internet. Il est surnommé 2.5G car on parle d'étape transitoire aux portables de 3e génération. Sa vitesse est de 171,2 kbits/s.

Le petit dernier avant les 3G est l'EDGE (Enhanced Date rate for GSM Evolution) ou encore le 2,75G. Toujours basé sur ces ancêtres, il développe une vitesse de 384 kbit/s.

Famille des 3G

Les téléphones de 3e génération, avec l'UMTS (Universal Mobile Telecommunication Services), permettent des débits supérieurs à 1 Mbit/s. Grâce à ce débit, comme vous avez dû le voir aux informations, la visiophonie, l'échange de données de taille importante est maintenant possible. L'UMTS ne risque pas d'éclater le marché étant donné que son débit réel se rapproche du GRPS et de l'EDGE et que les coûts des infrastructures sont énormes.

2°) Le WAP et i-mode

Beaucoup d'utilisateurs pensent accéder à Internet grâce au WAP ou par i-mode, ce qui est totalement faux ! Tout d'abord, le WAP et l'i-mode utilisent les normes de transmission vues précédemment, telles que le GRPS ou les normes supérieures. Le GSM ne possède pas un débit assez suffisant pour atteindre du contenu Web dans de bonnes conditions. Ces deux technologies sont en fait des méthodes de simplification pour permettre d'accéder à du contenu Internet. Voyons ça un peu plus en détail.

Vous êtes un peu curieux sur l'avenir, il ne vous reste plus qu'à faire un peu de recherche sur le HSDPA (vous allez baver).

LE WAP

Le WAP standardise la communication entre un terminal mobile (téléphones portables, PDA, etc.) et une passerelle garantissant l'accès à Internet. Chaque terminal mobile devra être équipé d'un client WAP. Le langage utilisé sera un dérivé du HTML, le WML (Wireless Markup Language) incluant un langage de script nommé WMLScript. Il y a énormément de choses à apprendre sur le WAP, on vous conseille donc d'aller visiter :

http://www.wapforum.org/.

L'i-mode

L'i-mode est basé sur le même principe, mais il est beaucoup plus souple étant donné qu'il utilise le HTML. Cela ne veut pas dire qu'il est plus compétent que le WAP, au contraire, son langage le laisse peu évolutif et donc moins puissant.

COMMENT DEBL SON TELEPH

On ne peut plus faire cents mètres sans voir un magasin de portables. Il y en a partout ! Certes, nous sommes de plus en plus accros à cet outil mais que lisons-nous sur les vitrines ? "Deblocage." En effet ce business commence à être des plus lucratifs. Eh bien ! Nous allons voir, dans la pratique, comment ça se passe et vous pourrez même le faire vous même...

INTRO

Lorsque vous achetez un téléphone portable avec ou sans abonnement, il est dans 95 % des cas bloqué par l'opérateur, ceci dans le but de vous empêcher de l'utiliser avec un opérateur concurrent. Mais pourquoi ? Les opérateurs ont sans doute tout simplement peu d'intérêts à vous laisser utiliser leurs téléphones portables chez la concurrence...

Le déblocage d'un téléphone a donc pour effet d'enlever la restriction sur un opérateur et d'accepter toutes les cartes SIM du monde.

Cependant, vous pouvez à tout moment débloquer votre téléphone portable et ce tout à fait légalement ! Pour ce faire, il existe deux manières : soit par code, soit par câble avec un logiciel de déblocage spécifique. Ces logiciels ou codes sont fournis par les revendeurs de téléphones qui les vendent aux magasins de déblocage à des sommes astronomiques...

Nous allons voir, tout au long de ce dossier, les deux différentes manières de débloquer votre téléphone portable.

I) Déblocage par code

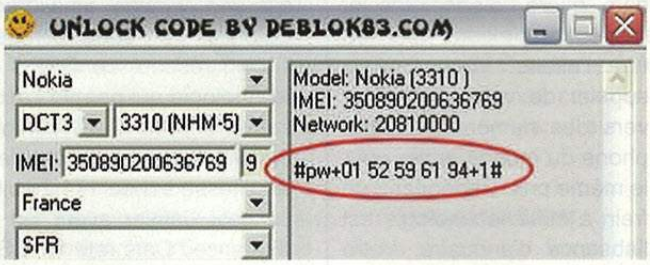
Cette démarche est simple est ne nécessite aucune connaissance ! (Et n'annule pas votre garantie, contrairement à la méthode par câble, ce qui reste un avantage non négligeable.) Cette méthode est donc vraiment celle qui est recommandée...

Le déblocage par code, comme son nom l'indique, nécessite un code (on ne s'en serait pas douté) d'une longueur variable allant de 4 à 15 caractères. Selon les modèles, ce code n'est connu que par l'opérateur qui bloque le téléphone.

Cela dit, pour certains modèles comme les Nokia , LG, Nec... (la liste exhaustive est consultable sur : http://www.deblok83.com/forum/viewtopic.php?id=7) il est possible de calculer le code de déblocage grâce à des logiciels (calculateurs) disponibles sur le Net en renseignant l'imei (International Mobile Equipment Identity, qui est un numéro composé généralement de 15chiffres qui identifie de façon unique votre téléphone), le modèle et l'opérateur qui bloque votre mobile. Vous pouvez l'obtenir en saisissant le code *#06# sur le clavier de votre GSM. Il est également inscrit sur l'étiquette se trouvant sous la batterie.

Pour mieux comprendre le fonctionnement, voici un exemple concret :

Dans ce cas, je veux débloquer un Nokia 3310 (un bestseller). Donc je récupère l'imei de mon 3310 soit en regardant derrière la batterie, soit en tapant *#06# sur le clavier. Je saisis l'opérateur qui bloque mon 3310, dans notre exemple c'est SFR, puis je valide. J'obtiens le code suivant : #pw+01 52 59 61 94+1#



Selon la marque des téléphones, il existe une méthode bien spécifique pour rentrer ce code (voir sur cette page le guide de déblocage : http://www.deblok83.com/guidedeblocage.html). Dans notre exemple, c'est à dire pour les Nokia, il suffit de procéder ainsi :

1) allumez le téléphone sans la carte SIM,

2) saisissez les codes suivants (pour obtenir le p w et le + il faut appuyer plusieurs fois sur la touche *) : #pw+01 52 59 61 94+1#

3) un message de type " restriction off " va s'afficher indiquant que votre Nokia est débloqué.

Sur quelques téléphones, comme certains Samsung, on peut débloquer l'appareil non pas par code calculé grâce à un logiciel mais plutôt en recourant à des codes universels. C'est-à-dire que les codes sont identiques pour les mêmes modèles.

À titre d'exemple, je vais vous indiquer quelques codes permettant de débloquer ces Samsung.

- **Pour débloquer les Samsung E700,E710, X100, X600, S500**

1) - Allumez votre téléphone sans carte SIM

2) - Tapez sur le clavier du téléphone : *2767*688#

3) - Voilà votre téléphone déverrouillé.

- **Pour débloquer les Samsung V200, S100, S300**

OQUER
IONE PORTABLE

1) - Allumez votre téléphone sans carte SIM
2) - Tapez les codes suivants sur votre clavier :
*2767*63342#
*2767*3855#
*2767*2878#
*2767*927#
*2767*7822573738#
3) - Votre téléphone est déverrouillé.

- **Pour débloquer les Samsung A800 et A300**

1) - Allumez votre téléphone sans carte SIM
2) - Tapez sur le clavier le code *2767*637#
3) - Votre téléphone est déverrouillé.
Ce code ne déverrouille pas toutes les versions !

Sachez que ces astuces sont tirées du site
DEBLOK83.com
rubrique Astuces et codes, accessibles directement depuis cette url : http://www.deblok83.com/astuces.html.

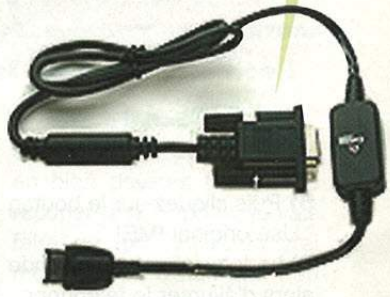
Les téléphones pour lesquels on peut calculer le code de déblocage et ceux dont il existe des codes universels ne sont pas nombreux, seuls 10 % des téléphones existant sur le marché sont déblocables de cette manière.
Pour avoir les codes de déblocage de ces téléphones, il y a deux solutions. La première consiste à les demander à l'opérateur : il vous réclamera en moyenne entre 70 et 180 euros si cela fait moins de 6 mois que vous possédez l'appareil, par contre au delà de 6 mois l'opérateur est obligé de vous le communiquer gratuitement. L'autre solution est de passer par un site qui peut vous l'avoir pour un prix plus que raisonnable. Par exemple le site www.deblok83.com s'engage à vous fournir le code de déblocage de votre mobile pour la somme de 13 euros (11 euros si vous êtes membre) et ceci dans un délai maximum de 48 h.
Pour ceux qui aiment mettre leurs mains dans le cambouis et qui maîtrisent assez bien l'informatique (ça ne devrait pas vous poser de problème en tant que lecteur de Pirat'z averti), il y a la possibilité de débloquer les téléphones portables par câble, avec un logiciel de déblocage spécifique.

II) Déblocage par câble

Le déblocage par câble nécessite de prendre quelques précautions. Dans un premier cas, les manipulations par câble annulent la garantie de votre téléphone (ça peut être embêtant). De plus, en cas de fausse manipulation, le téléphone peut se voir endommagé, voire complètement inutilisable... C'est donc à vos risques et périls.
Tout d'abord, le choix du câble est très important ! Il faut utiliser un câble unlock correspondant à votre portable, que vous pourrez acheter soit sur Internet (www.gsm3000.com par exemple), chez les magasins spécialisés ou bien sur Ebay qui fourmille de matériel en tout genre à des prix défiant toute concurrence...
Une fois le bon câble en main, il vous faut le logiciel de déblocage adéquat pour votre téléphone. Il existe des centaines de logiciels qui débloquent les téléphones, chacun d'eux débloquant un certain modèle (téléchargeables sur : www.deblok83.com/logiciels.html).
Les méthodes diffèrent plus ou moins selon les logiciels utilisés, mais le principe est toujours le même.

À titre d'exemple, nous allons débloquer un Siemens SL55 :

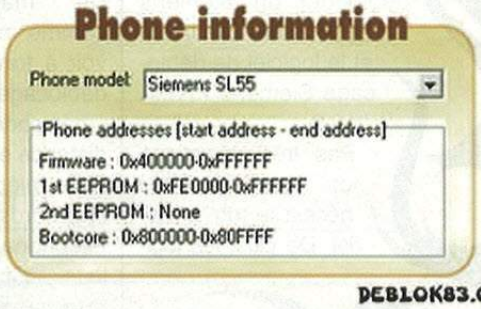
Voici le câble nécessaire au déblocage :

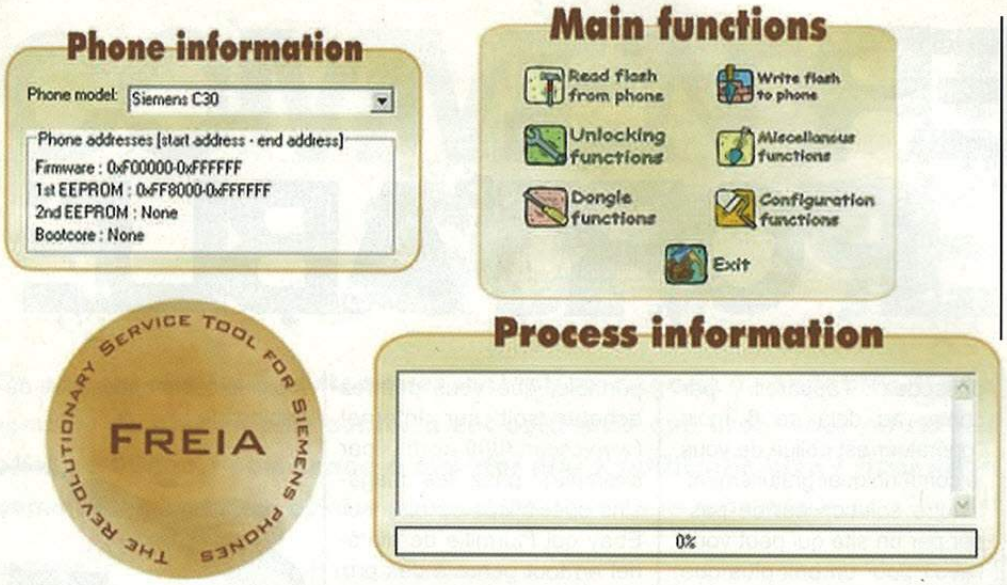


Le logiciel qui sera utilisé dans notre exemple pour débloquer les Siemens SL55 est Siemens Freia v10.0 (téléchargeable depuis : deblok83.com/logiciels-siemens.html).

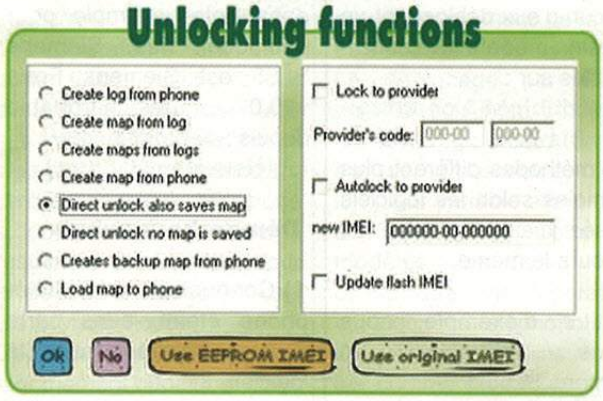
Démarche à suivre

1) Connectez votre téléphone éteint, sans carte SIM, au câble, puis lancez le logiciel.
2) Sélectionnez le modèle de votre portable, dans notre exemple le SL55.
(voir image page 14)
3) Une fois votre modèle sélectionné, cliquez sur le bouton " Unlocking fonctions ".
4) Après avoir cliqué sur ce bouton, sélectionnez " Direct unlock also saves map ".





5) Puis cliquez sur le bouton " Use original IMEI ".
6) Le logiciel vous demande alors d'allumer le téléphone.



7) Cliquez brièvement sur le bouton " ON " de votre téléphone.
8) Voilà, votre téléphone est maintenant débloqué.

Voilà en ce qui concerne la manipulation pour débloquer un Siemens SL55 avec un câble et le logiciel de déblocage Siemens FREIA v10.0.

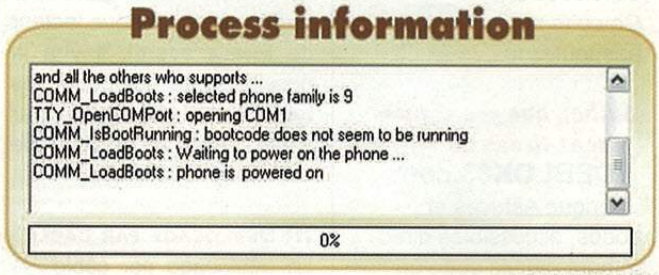
Pas très compliqué en général mais nécessite du matériel. De plus, les logiciels de déblocage sont de moins en moins gratuits. En effet, les téléphones sont de plus en plus compliqués à débloquer. Par conséquent, les développeurs de logiciels mettent du temps à trouver les solutions de déblocage et font donc payer la licence du logiciel.

CONCLUSION

De manière générale, comme nous avons pu le voir à travers ce dossier, le déblocage peut se faire :
- par code, rapide, fiable, à distance et sans danger pour votre téléphone mais payant (13 euros) si c'est pas un téléphone mentionné dans la liste consultable sur http://www.deblok83.com/forum/viewtopic.php?id=7
- ou par câble, mais cela nécessite du matériel software (logiciels qui sont payants pour certains types de téléphones) et du matériel hardware (câbles et connectiques).

Pour plus d'informations concernant le déblocage ou la téléphonie en général, n'hésitez pas à venir poser vos questions sur le forum de deblok83 accessible depuis cette url : http://www.deblok83.com/forum/ ou en m'envoyant un mail à : webmaster@deblok83.com

Il existe d'autres sites où vous pourrez trouver des logiciels et codes gratuitement. Je vous invite également à aller faire un tour sur le site : http://www.gsmactua.com.



Liste non exhaustive des codes pour Samsung :

- Samsung A300 : *2767*637#
- Samsung A400 : *2767*637#
- Samsung A800 : *2767*637#
- Samsung E500 : *2767*688#
- Samsung E700 : *2767*688#
- In newer phones : #*7337#
- Samsung P400 : *2767*3855#
- Samsung S100 : *2767*7822573738#
- Samsung S300 : *2767*7822573738#
- Samsung S500 : *2767*3855#
- Samsung SGH600 : *2767*3855# ; *2767*2878#
- Samsung SGH2100 : *2767*3855# ; *2767*2878#
- Samsung V200 : *2767*7822573738#

Vous retrouverez pleins de codes et astuces sur **www.deblock83.com** et **www.gsmactua.com**

LA FIN DES OPERATEURS TELEPHONIQUES

Skype, tout pour téléphoner gratuitement

À l'heure où les opérateurs rivalisent d'imagination pour conquérir de nouveaux clients, Skype commence à pointer le bout de son nez avec une offre tout à fait alléchante puisqu'elle permet de téléphoner gratuitement d'ordinateur à ordinateur en passant par la Voip. Ce sujet est bien plus qu'épuisé. Mais Skype, ce n'est pas seulement ça ! Nous allons voir que grâce à lui nous pouvons aussi téléphoner de notre portable, et ce gratuitement ou à des prix défiant toute concurrence !

Les concepteurs de Kazaa, Niklas Zennström et Janus Friis, révolutionnent à nouveau le monde du peer to peer avec la mise à disposition de la téléphonie gratuite pour tous. Skype est un nouvel outil de communication entre ordinateurs en passant par Internet. Vous branchez votre micro à votre ordinateur, et vous vous connectez au réseau des millions d'utilisateurs dans le monde qui utilisent déjà ce service. Le principe est que vous gérez une liste de contacts, et pouvez appeler ceux qui sont connectés. La qualité des conversations est à l'heure actuelle très bonne et vous pouvez gérer des conférences avec plusieurs utilisateurs, mettre en absence des appels, avoir un répondeur... Il est de plus possible de téléphoner sur des mobiles ou des téléphones fixes. C'est payant mais le prix défie toute concurrence. Enfin, vous pouvez même obtenir un numéro de téléphone associé à votre Skype, qui permettra à vos contacts de vous joindre via des téléphones fixes sur un numéro qui vous est unique.

Dorénavant, il est possible d'utiliser Skype sur votre portable ou PDA. Plus besoin de s'embêter avec l'utilisation d'un ordinateur et d'un micro, très compliqué à brancher (n'hésitez pas à vous reporter à l'article dédié à ce sujet :p) Vous pouvez l'installez sur votre Pocket PC et l'utiliser comme si vous téléphoniez avec votre mobile, mais gratuitement, avec vos contacts Skype.

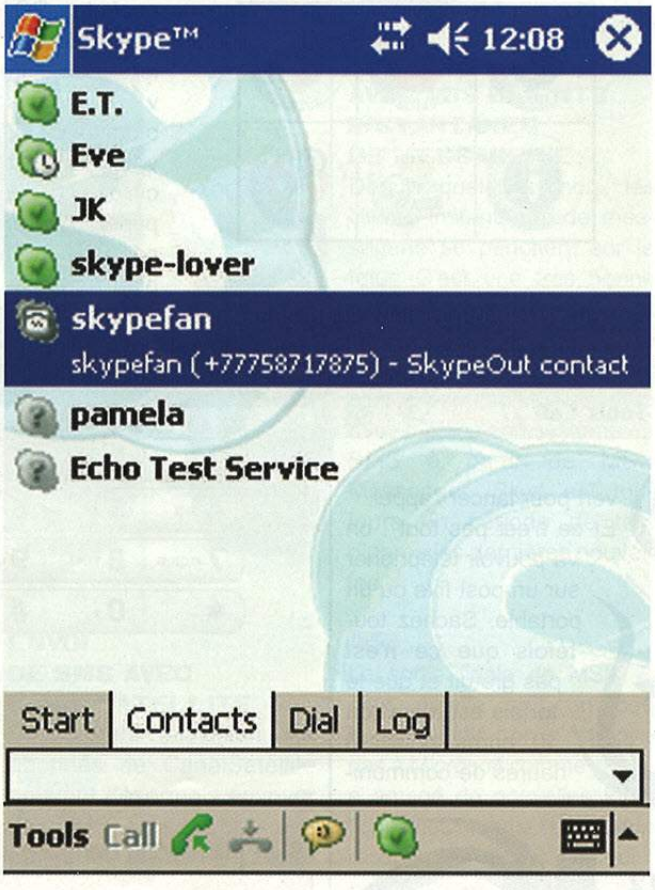
Pour l'installer, vous avez besoin d'un pocket PC doté d'une version de Windows Mobile 2003. Ne vous laissez pas impressionner par le côté difficile de cette installation, ce n'est pas si terrible que ça. Vous devez également posséder une connexion haut débit (du type wireless) ce qui est de nos jours très simple à trouver même dans rue avec la croissance des hotspots que l'on trouve désormais partout. En revanche on ne peut pas utiliser le gprs car il n'est pas assez puissant. Skype pour Pocket_PC est écrit en JAVA, vous avez deux versions possibles qui vous permettent de l'installer de deux manières différentes :

- Une synchronisation avec votre PC Windows à l'aide d'Active Sync (la version très compliquée...).
- Soit vous téléchargez une version préinstallée.

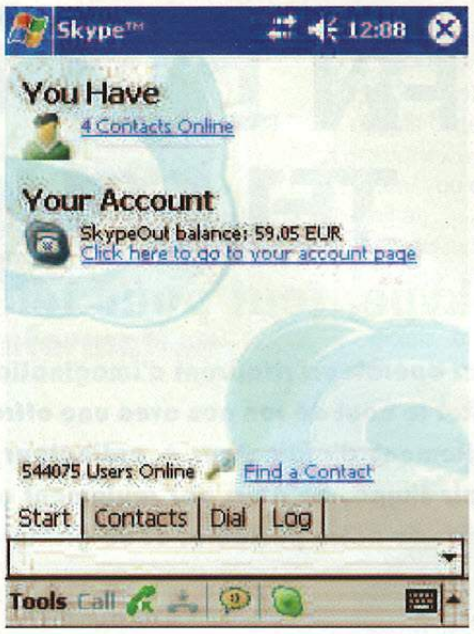
Vous trouverez tout ça sur **http://www.skype.com/products/skype/pocketpc/.** Prenez la deuxième version proposée, **http://www.skype.com/go/getskype-pocketpc-cab**

Exécutez le programme téléchargé et cliquez sur "ok", rentrez ensuite vos login et mot de passe, ou créez un compte. Si vous aviez déjà un compte et des contacts, eh bien devinez ! Vous les récupérez :) Trop fort, je vais faire de mon PDA un vrai mobile. Ouf, c'était pas trop dur jusqu'ici... Allez, on continue :

Eh bien maintenant, vous pouvez gérer votre compte, comme sur votre ordinateur ! Ouvrez votre liste de contacts :

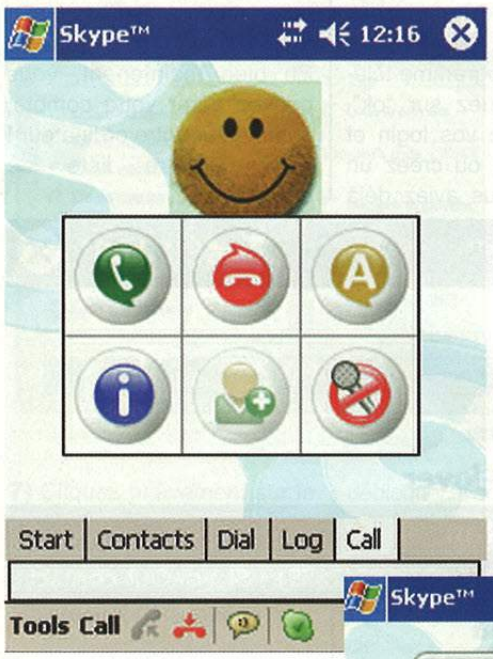


cation dans une dizaine de pays; les prix quand vous appelez des portables ou sur des zones non couvertes. Allez sur **https://secure.skype.com/store/buy/skypeout.html** où vous aurez à donner vos login et mot de passe pour acheter du crédit. Avec ça, vous vous assurez de longues heures de communication pas chères.

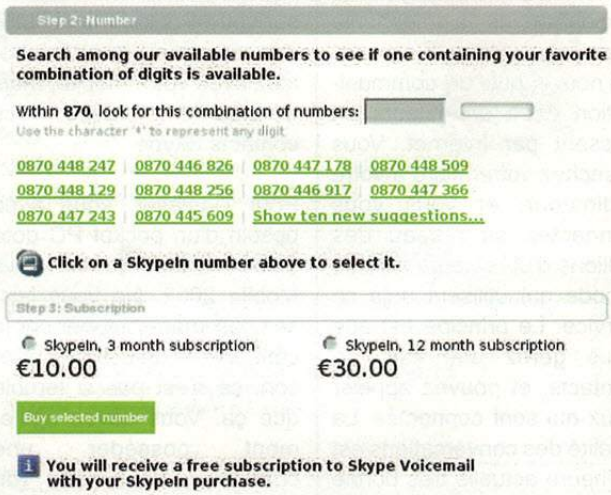


téléphone qui deviendra le vôtre. Ainsi, si vous êtes susceptible d'être contacté dans plusieurs pays ou ne voulez tout simplement pas donner d'argent à France Telecom pour une ligne téléphonique, vous serez toujours joignable.

et appuyez sur la touche représentée par le téléphone

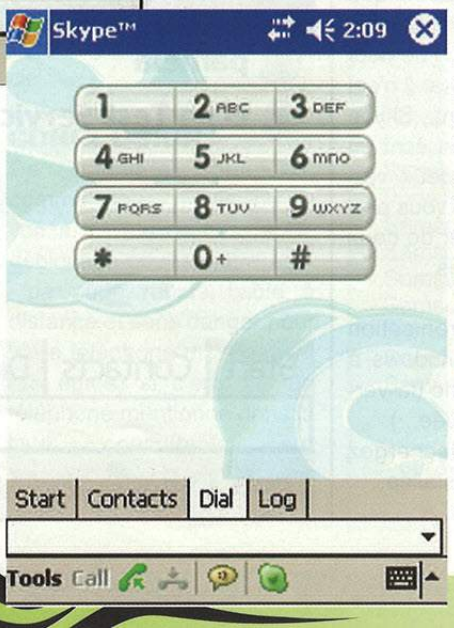


Vous pouvez appeler des numéros fixes en utilisant le dialpad : De plus, Skype s'intègre totalement à votre pocket PC. Avant d'appeler quelqu'un via vos contacts, vous pourrez choisir de passer l'appel par Skype ou bien normalement. Vous



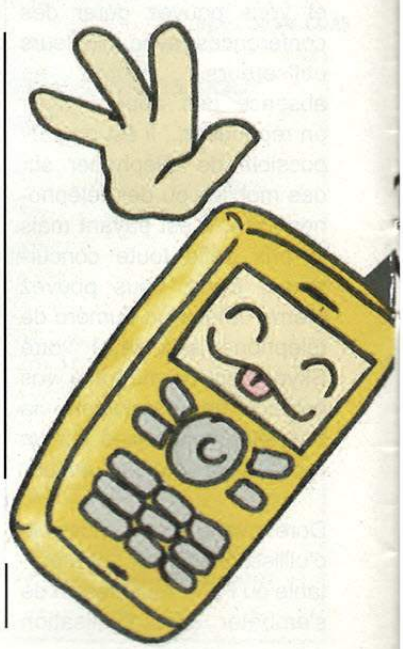
pouvez donc les appeler avec votre forfait, ou gratuitement via Internet.

Enfin vous pouvez acheter un numéro de téléphone, sur lequel vos correspondants vous appeleront. Allez dans la section suivante sur le site après vous être identifié : **https://secure.skype.com/store/buy/skypeout.html**. L'état de votre compte s'affichera dans la section start. Vous pouvez sélectionner un numéro de



vert pour lancer l'appel.

Et ce n'est pas tout : on va pouvoir téléphoner sur un post fixe ou un portable. Sachez toutefois que ce n'est pas gratuit et que le forfais est d'environ 10 euros pour 10 heures de communi-



LES SMS ENVAHISSENT LE MONDE

Les SMS et autres types de messages sont devenus une véritable drogue dans la vie de milliers de propriétaires de téléphones portables. Des centaines de milliards de SMS se sont déjà échangés, et ça ne fait que de s'amplifier. Ces personnes utilisent ces technologies pour communiquer avec leurs ami(e)s, participer à des émissions de télévision, recevoir des informations, payer des services ou même faire des dons. Bref, les SMS sont partout et sont désormais indispensables.

DES PETITES DEFINITIONS

De nouvelles technologies comme les normes de transmission sans fil (GSM, GPRS, EDGE, UMTS) donnent de nouveaux pouvoirs aux SMS. On voit donc ces SMS, également appelés textos, se développer et former de nouveaux types de messages : les EMS et SMS. Rappelons tout d'abord de quoi il s'agit.

SMS

Pour commencer, un SMS - de l'acronyme « Short Message Service » - est un petit message court de 160 caractères. Or un texto possède une capacité de 140 octets. Ça ne paraît pas un peu louche tout ça ? Sur les portables, on code chaque caractère avec 7 bits et non avec 8 bits comme sur un ordinateur, on peut donc caser 160 caractères dans 140 octets. Les SMS utilisent la norme de transmission GSM ; il ne peut être envoyé que du texte.

EMS

L'EMS (Enhanced Message Service) est une évolution de SMS qui permet d'envoyer des messages longs (255 SMS théoriques), des images, des animations

et des sons simples. Il est donc compatible sur les téléphones portables utilisant la norme GSM. Seule la vitesse de cette norme reste un handicap, ce qui ne facilite pas son développement.

MMS

Le MMS (Multimedia Messaging Services) est le summum de la messagerie mobile. Il n'a pas de limite puisqu'ilcombine la simplicité d'un SMS avec les fonctions de l'email. Le MMS supporte un grand nombre de fichiers multimédias, que ce soit de la mise en page de texte, de la vidéo, de l'audio, des animations ou encore des données. Tout est permis ! Le MMS fonctionne avec le Wap et des normes de transmission supérieures au GSM, c'est-à-dire le GPRS, l'EDGE ou l'UMTS (se référer aux premiers articles sur les réseaux).

DICTER SES SMS MAGIQUE

Il est maintenant possible de dicter ses SMS avec les nouveaux téléphones Samsung. Malheureusement, ces téléphones (le P207 et l'A800) ne sont pas encore en vente en Europe, mais rassurez-vous, ça va finir par arriver. Cette technologie risque de révolutionner toutes ces années de frappe au clavier même si elle n'est cependant pas totalement fiable pour l'instant. L'outil utilisé pour la reconnaissance vocale se nomme QuickPhrase de l'entreprise VoiceSignal Technologies. Cette fonction est baptisée Speed To Text. Maintenant, il ne vous reste plus qu'à imaginer un temps réduit et une facilité supplémentaire pour envoyer un SMS, qui ne vous abîmera désormais plus les doigts. Vive la technologie !
Un bijoux ? Non, le P207 de Samsung

ENVOI DE SMS AVEC CANALSATELLITE

Depuis leur télévision, les abonnés de CanalSatellite peuvent désormais envoyer des SMS qui sont bien évidemment (hélas ?!) facturés. Le programme utilisé pour permettre ce système se prénomme RegieLine 2.0 appuyé de « back-office » pour permettre le renvoi vers les opérateurs. Équipé de votre télécommande, allez sur le canal 241 et vous disposerez d'un clavier virtuel pour remplir le numéro du destinataire et du message. Il y a aussi les smileys, des messages prédéfinis et le dictionnaire SMS.

LES SMS AVEC VOS CLIENTS INSTANTANES DE MESSAGERIE

Depuis quelques mois, les clients instantanés de messagerie se penchent sur le futur. C'est une très bonne nouvelle pour l'avenir étant donné que le monde évolue et que les besoins seront plus présents. MSN a déjà mis en place son système de SMS à partir de MSN Messenger, Skye est toujours en période de test d'après les dernières nouvelles.

MSN

La sortie finale de MSN 7, bien qu'elle soit un peu buguée (ndlr : on n'échappe pas à Microsoft comme ça...), a amené de nouvelles fonctionnalités comme l'envoi et la réception de SMS. Hé oui !

Les betas testeurs ont bien travaillé. Une personne dans la rue peut désormais communiquer avec vous sur MSN par l'intermédiaire de son téléphone portable. Ne vous réjouissez pas trop vite, il faut acheter des packs de SMS par MSN avant de pouvoir mettre en place le système, mais le prix du SMS reste quasiment le même que celui d'un opérateur classique (3,99 euros pour 25 SMS, 6,99 euros pour 50 SMS et 19,99 euros pour 150 SMS).

SKYPE

Skype prépare une nouvelle version beta pour ce même système mais la société prévoit de ne pas passer par des opérateurs et donc de proposer des SMS à des prix défiant toute concurrence. On attend de voir ça avec impatience.

COMMUNIQUER PAR MSN ET PAR EMAIL EN SMS

MSN Mobile est une sorte de passerelle entre votre téléphone portable et les services Hotmail ou Messenger. Ce service n'est malheureusement disponible que pour les abonnés à Bouygues Telecom. Pour en bénéficier, il vous faut un téléphone portable pouvant recevoir des SMS, un abonnement grand public Bouygues Telecom de 2 heures minimum, un ordinateur connecté à Internet et un compte MSN Hotmail. Si vous n'avez pas de compte, rendez-vous sur : http://www.hotmail.com/ pour souscrire. Remplissez ensuite le formulaire d'inscription sur : http://mobile.msn.com/ puis vous devriez recevoir un SMS de la part de Bouygues Telecom comprenant les tarifs du service (1 SMS envoyé à 0,15 euros, 1 SMS reçu à 0,20 euros). Répondez à ce SMS avec le message « OK » et vous recevrez un code de confirmation pour valider votre inscription.

MSN Mobile Hotmail

Votre téléphone est maintenant prêt. Nous allons pouvoir passer aux petites configurations nécessaires. Toujours sur : http//mobile.msn.com, connectez vous puis cliquez sur « Éditer vos filtres MSN Hotmail ». Pourquoi utiliser des filtres ? Tout simplement car vous n'allez pas payer tous les mails que vous allez recevoir, il faut donc choisir des mots clef comme un nom, une adresse email, l'objet du message. Vous pouvez également choisir de recevoir les messages des personnes figurant uniquement dans votre liste de contacts. Ou pour les riches, vous pouvez tout recevoir. Ce service utilise les mêmes règles de filtrage contre les courriers indésirables que Hotmail.

MSN Mobile Messenger

Continuer à chatter avec vos ami(e)s 24h/24 où que vous soyez par SMS, ce n'est pas miraculeux ? Ce système est un coup de main à prendre. On a dû mettre en place un système de commandes pour afficher la liste de contacts, récupérer des informations sur un contact, etc. En obtenant la liste des contacts en envoyant un SMS, un numéro sera attribué à chaque personne en ligne. Dès que vous aurez le numéro de Bob, il suffira de commencer votre message par son identifiant.

Sachez qu'il existe d'autres entreprises offrant les mêmes services pour l'envoi et la réception de mail par SMS, comme Orange qui permet de recevoir, bien sûr gratuitement et directement sur son mobile, l'expéditeur et le sujet d'un mail. Cette technologie se développe de plus en plus, notamment avec l'arrivée du blackberry, véritable ordinateur mobile, ou autre pocket PC.

FAIRE DES RECHERCHES SUR GOOGLE PAR SMS

L'année dernière en 2004, Google a lancé un nouveau service du nom de Google SMS permettant d'envoyer des requêtes sur le moteur de recherche via SMS. Les réponses des recherches ne sont pas des pages web mais uniquement du texte. Vous n'avez donc pas besoin d'avoir un téléphone portable avec un client Internet. Pour l'instant, ce service n'est disponible qu'aux États-Unis et en Grande-Bretagne. Prenez patience, visitez de temps en temps http://www.google.com/sms/

ETRE INFORME PAR SMS

Il existe énormément de services proposant de vous informer par SMS. Par exemple, il est possible de rester informé du départ ou de l'arrivée d'un vol pour Mexico grâce au service AéroSMS.

SNCF a mis en place le même système pour savoir si un train est à l'heure, en retard ou supprimé. Les opérateurs français comme Bouygues Telecom proposent aussi des services d'information par SMS sur le sport ou tout autre thème. Il existe des villes proposant les informations municipales par SMS, parfois gratuites comme pour les communes en Sud-Mayenne grâce à C1Plus.com. Un autre exemple, vous pouvez recevoir un bulletin météo chaque jour par Météo France. En allant encore plus loin, il existe un système de commande par SMS pour contrôler l'alarme de votre voiture (verrouillage, déblocage, etc.).
Les perspectives sont nombreuses, que nous réserve l'avenir sur un monde de SMS ?

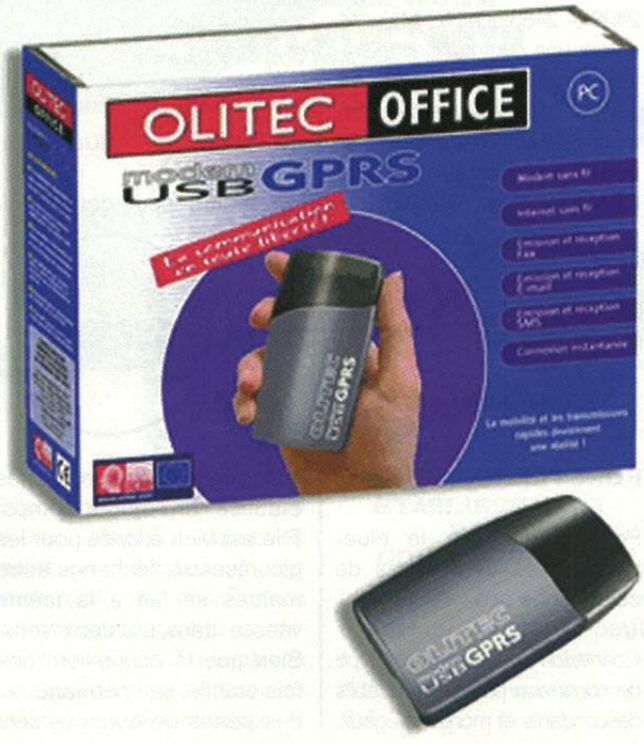
TEXTO GRATUIT OU SUPERCHERIE

En ce qui concerne les SMS, on peut en envoyer sur des sites proposant des envois gratuits mais vous serez toujours limité en nombre ou par d'autres choses comme de la publicité ou des inscriptions obligatoires. Voici une liste de sites permettant d'envoyer des SMS gratuits :

http://sfr.annyway.net/mms?req=SFR.viewCreateMMSForm : 3 MMS par jour
http://textoweb.services.sfr.fr/SFR_TextoWeb_Lot3_V4/ : 10 SMS pour les clients SFR
http://www.orange.fr/0/visiteur/PV?PS=EXTWEB2SMS : 1 SMS par jour pour les clients Orange
http://www.smseverywhere.com/send.htm : SMS vers Canada et US illimités
http://www.smsgratuit.com/ : 2 SMS gratuits à l'inscription
http://www.radins.com : 2 SMS par jour
http://www.ileoo.net/ : 2 SMS par mois
Voilà de quoi faire quelques économies non négligeables. Pour information, il existe d'autres méthodes pour envoyer des SMS gratuitement mais ça, c'est à vous de les trouver ;))

UTILISER UN MODEM GSM GRPS POUR ENVOYER SES SMS

Vous avez sûrement dû déjà entendre parler du fait qu'il est possible de se connecter à Internet en utilisant son téléphone portable, mais vous ne savez pas comment. Les téléphones récents, c'est-à-dire les mobiles aux normes GPRS et supérieures, sont équipés de modems internes. On retrouve donc des modems intégrés correspondant aux différentes normes (GRPS / EDGE / UMTS). Ces modems restent pauvres au niveau des fonctionnalités mais il existe des solutions matérielles complètes externes. Avec des modems cellulaires (GPRS, EDGE, UMTS) en PCMCIA ou externes en USB munis d'une antenne radio et de la carte SIM de votre opérateur qu'il faudra placer dans le modem, on peut désormais parler de solutions professionnelles. Equipez-vous de votre ordinateur portable et du modem cellulaire (+ SIM et antenne) et vous serez apte à recevoir ou à envoyer vos messages (SMS, fax et e-mails) et à profiter de tous les services qu'offre Internet à n'importe quel endroit où que vous soyez. Ceci peut-être très avantageux pour une personne amenée à voyager beaucoup.



PCMCIA

Après avoir installé les pilotes de votre carte PCMCIA, il suffit d'installer le logiciel fourni avec le matériel ou de créer une connexion basique par modem. Sachez que le débit varie en fonction de la qualité de votre modem (tri-bande, etc.) et de l'antenne radio intégrée à votre modem PCMCIA.

C'est, disons entre parenthèses, la petite nouveauté qui occupe la même place qu'un paquet de clopes (avis aux fumeurs). Nous allons prendre l'exemple du modem GPRS d'Olitec. Il se connecte en USB et est auto-alimenté.
(photo *ci-dessus*)

Conclusion : La mobilité n'a plus de limites !

XeLory

COMMENT SE PRO
D'UNE ATTA

Mon téléphone est bluetooth, mon ordinateur portable est bluetooth, ma toute nouvelle voiture supporte le bluetooth, mais qu'est-ce que c'est que ce bluetooth ? le bluetooth est présent dans de plus en plus de domaines, mais n'est pas connu du grand public. Pourtant cette norme de communication sans fil pose énormément de problèmes de sécurité, et d'intégrité. Dans cet article, nous allons voir comment fonctionne cette norme ainsi que les problèmes de sécurité rencontrés.

PRESENTATION

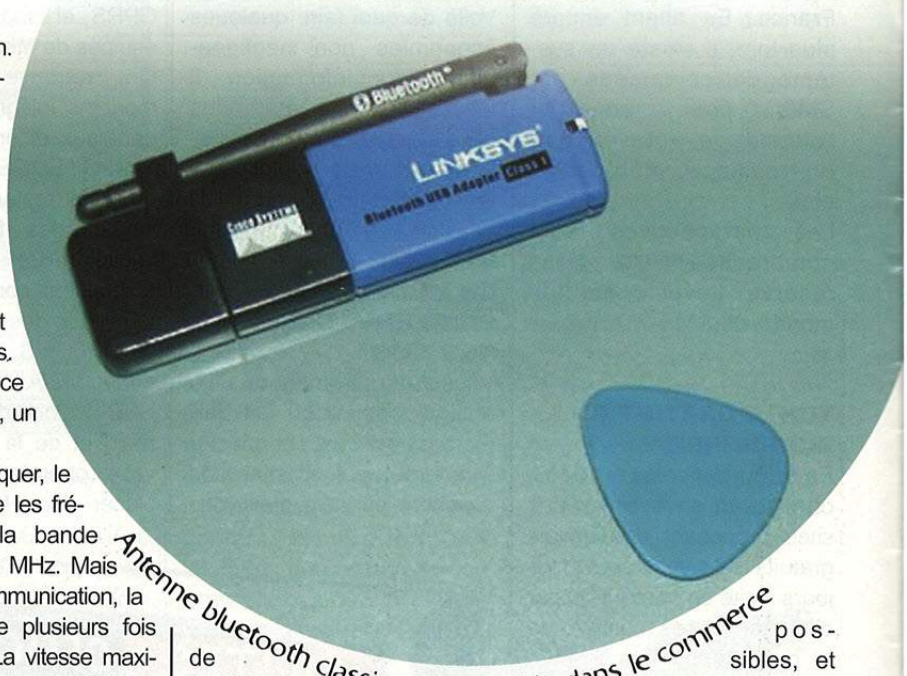
Le bluetooth est né du regroupement des fabricants Ericsson, qui est l'initiateur de ce projet, d'IBM, d'Intel, de Nokia et de Toshiba. Le bluetooth a été créé afin de mettre en relation de nombreux périphériques sans fil.

Actuellement, plus de 3000 marques font partie du Bluetooth Special Interest Group, dont Microsoft, 3 Com, Motorola. L'expansion et la réussite du bluetooth ont permis de voir ses compétences s'accroître. Ce type de connexion est maintenant, non seulement dans l'informatique, mais dans la téléphonie, l'automobile et presque tous les systèmes possédant de l'informatique embarquée.

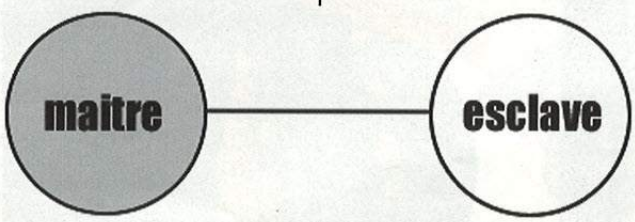
NORME ET FONCTIONNALITE

Le bluetooth est cependant limité à 8 connexions simultanées, à partir du même composant. La communication établie, est du type maître-esclave. Un maître peut avoir un ou plusieurs esclaves. Deux esclaves peuvent communiquer entre eux seulement en passant par leur maître commun. Pour augmenter le nombre de périphériques connectés ensemble, on peut alors relier plusieurs maîtres, qui partageront leurs esclaves. On appelle ce type de réseau, un picoréseau.

Pour communiquer, le bluetooth utilise les fréquences de la bande 2400 – 2483,5 MHz. Mais durant une communication, la fréquence varie plusieurs fois par seconde. La vitesse maximale de transfert est 1Mb/s ce qui est peu mais suffisant pour l'usage qui lui est réservé.



Antenne bluetooth classique disponible dans le commerce



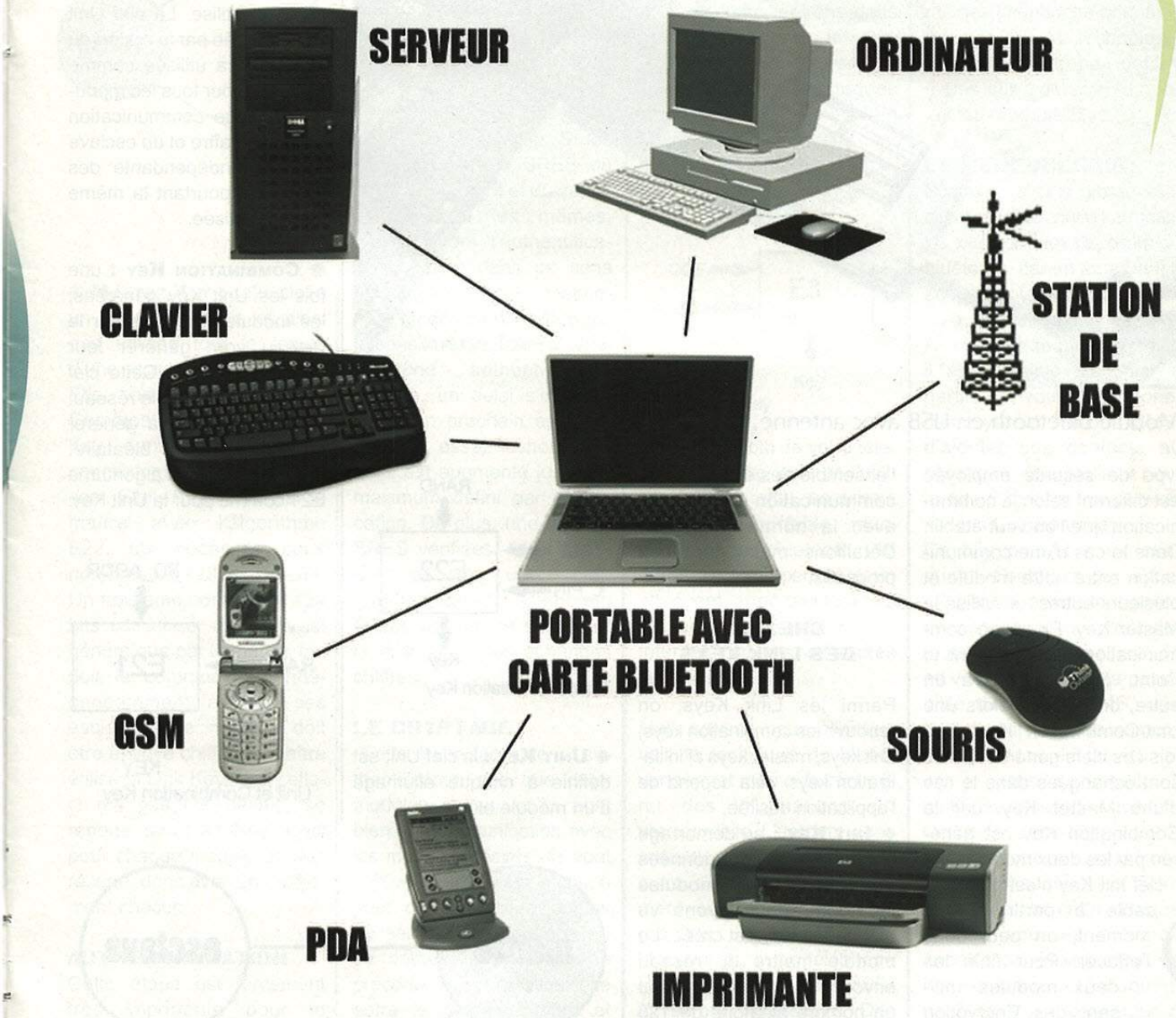
FONCTIONNEMENT

Pour fonctionner, le bluetooth utilise deux types de connexions :

Connexion synchrone : ce type de connexion permet des débits descendants et montants égaux, de 432Kb/s permanent.

Un maître peut donc avoir trois connexions synchrones établies en même temps. Elle est bien adaptée pour les picoréseaux, l'échange entre maîtres se fait à la même vitesse dans les deux sens. Bien que la connexion, une fois établie, soit permanente, des pertes de données sont possibles, et dues à des erreurs de décodage. Dans le cas d'une erreur, le maître ou l'esclave ayant reçu le paquet erroné renvoie à son maître un paquet indiquant l'erreur. Puis le maître envoie le paquet de nouveau. Cette protection contre les erreurs d'envoi est efficace, mais incompatible avec des connexions faisant transporter la voix. En effet, si lors de votre conversation, un paquet est mal envoyé, votre interlocuteur recevra votre phrase coupée. Puis dans la phrase suivante, il recevra la syllabe ou le mot manquant.

TEGER
CK DU BLUETOOTH



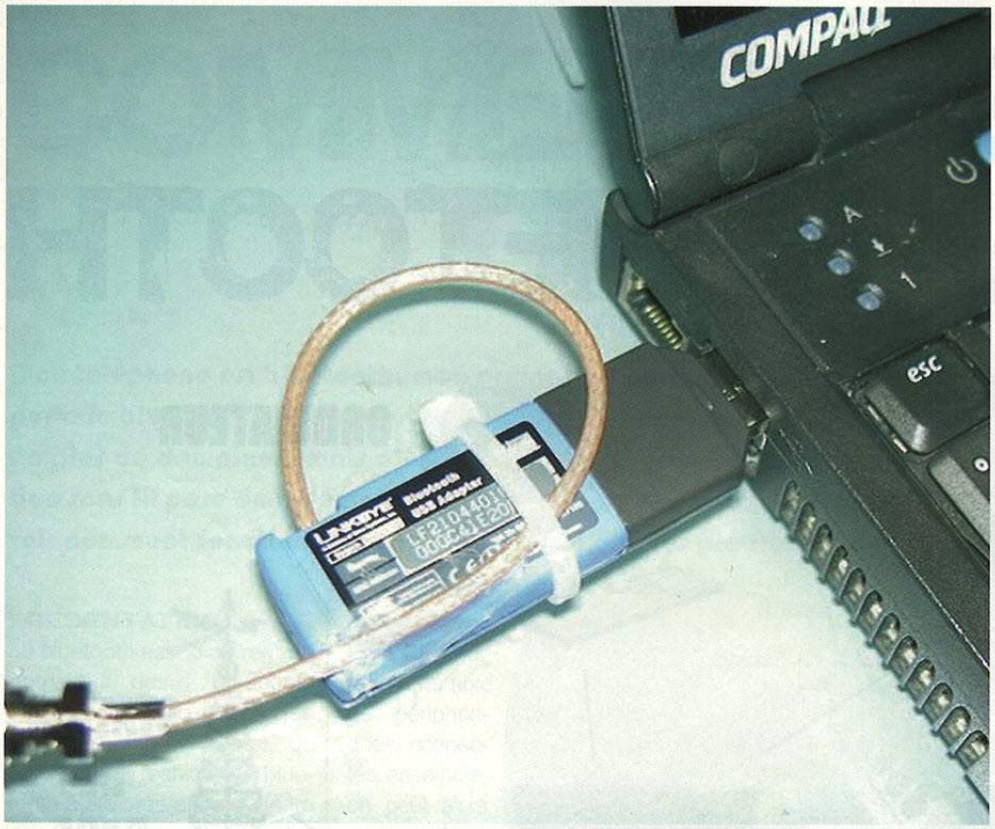
CONNEXION ASYNCHRONE : cette connexion asynchrone permet des débits de 721 kb/s dans un sens et 57kb/s dans l'autre sens. Elle est utilisée principalement pour la navigation internet où l'on sait que la réception est souvent plus importante que l'envoi. De même, pour une connexion entre un ordinateur et une imprimante, le choix d'une connexion asynchrone est parfaitement adapté. La plupart du temps, l'imprimante reçoit les informations de l'ordinateur.

ETABLISSEMENT DE LA COMMUNICATION

L'établissement d'une connexion bluetooth peut s'effectuer de différentes manières au niveau sécurité.

ETAPES DE SECURITE

Dès lors que deux modules veulent entrer en contact, la sécurité du réseau doit s'établir. En premier lieu une Init Key est générée, puis une Link Key. Pour la suite, le



Module bluetooth en USB avec antenne, le must du pirate.

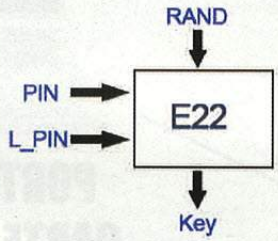
type de sécurité employée est différent selon la communication que l'on veut établir. Dans le cas d'une communication entre notre module et plusieurs autres, on utilise la Master Key. Pour une communication de type Point to Point, d'un module à un autre, on utilisera alors une Unit/Combination Key. Une fois ces clefs générées, elles sont échangées dans le cas d'une Master Key, car la Combination Key est générée par les deux modules. La clef Init Key n'est plus utilisable à partir de ce moment, on peut donc l'effacer. Pour finir, les deux modules utilisent des Encryption Key qui leur permettront de coder les données envoyées.

Nous venons de voir succinctement comment se déroulait l'ensemble des étapes d'une communication sécurisée avec la norme Bluetooth. Détaillons maintenant ces procédés.

CREATION DES LINK KEYS

Parmi les Link Keys, on retrouve les combination keys, unit keys, master keys et initialization keys, cela dépend de l'application désirée.

● **Init Key :** au démarrage d'un échange de données entre plusieurs modules bluetooth, nous avons vu qu'une Init Key est créée. Le module maître du réseau envoie en clair sur le réseau un nombre aléatoire de 128 bits, RAND, à l'autre module. Puis, à l'aide des codes pin et de leur longueur, chaque module utilise l'algorithme E22 pour calculer avec sa Key Init de 128bits. Une fois l'Init Key transmise à l'autre module, elle peut être effacée du module.

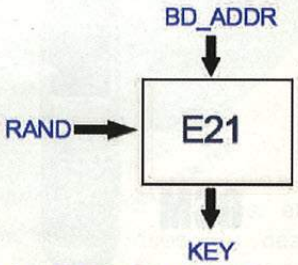


Master et Initiation Key

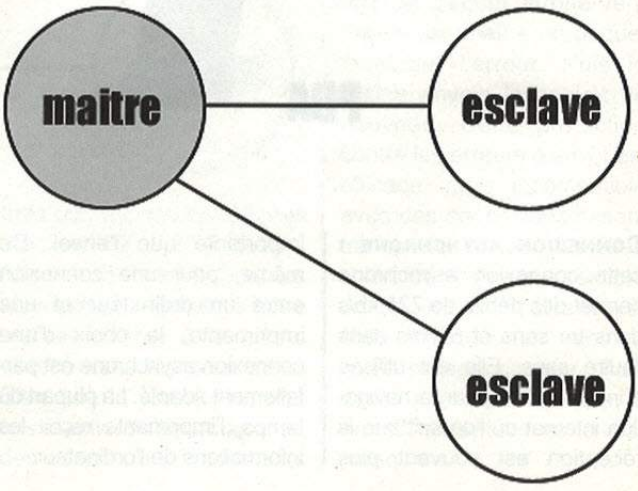
● **Unit Key :** la clef Unit est définie à chaque allumage d'un module bluetooth.

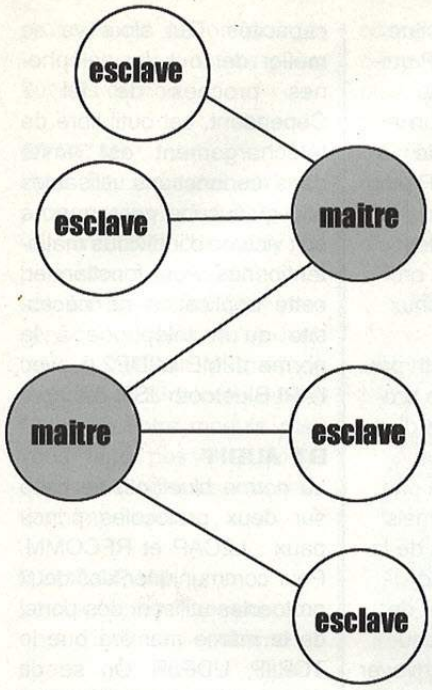
Elle est donc unique, et stockée dans la mémoire interne du module. Elle est générée à partir de l'algorithme E21, qui nécessite deux paramètres. Un nombre aléatoire de 128bits, et la BD_ADDR de 128 bits aussi, généreront l'Unit Key de 128bits. L'utilisation de l'Unit Key dépend de la nature du module *(maître ou esclave)* que l'on utilise. La clef Unit Key générée par le maître du réseau sera utilisée comme Link Key pour tous les modules. Chaque communication entre un maître et un esclave est bien indépendante des autres, et pourtant la même clef est utilisée.

● **Combination Key :** une fois les Unit Key générées, les modules présents sur le réseau vont générer leur Combination key. Cette clef ne voyage pas sur le réseau. Chaque module va générer un nombre RAND aléatoire, puis à l'aide de l'algorithme E21 comme pour la Unit Key.



Unit et Combination Key





● **Master Key :** cette clef a un but bien précis et n'est pas utilisée tout le temps d'une connexion bluetooth. Elle sert à remplacer la Combination Key et l'Unit Key dans le cas d'une connexion de type broadcast. Elle est générée par le maître avec l'algorithme E22, qui nécessite deux nombres de 128bits chacun. Un troisième nombre de 128 bits est utilisé, mais il n'est généré que par le maître, qui doit le communiquer indépendamment à tous ses esclaves. Ce nombre doit être envoyé chiffré, le maître utilise la Link Key, et si celle-ci n'a pas été définie, se reporte sur l'Init Key. Ceci pour chaque module de son réseau, donc avec un chiffrement chacun.

AUTHENTIFICATION

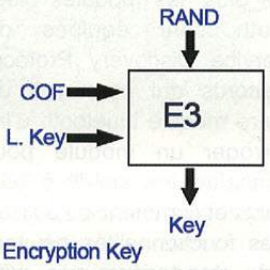
Cette étape est forcément très importante pour le réseau puisqu'elle confirme qu'un module fait bien partie dudit réseau et que celui-ci pourra communiquer. Cette authentification se déroule dans les deux sens, c'est-à-dire que le maître doit identifier l'esclave et inversement. Pour cela, le module qui doit s'authentifier auprès de l'autre reçoit du vérifieur un nombre aléatoire, envoyé en clair sur le réseau. Puis les deux modules génèrent, à partir de l'algorithme E1, un nombre SRES. L'algorithme E1 utilise un nombre aléatoire, une Link Key et une adresse BD_ADDR du module qui doit s'authentifier. Si les nombres SRES du vérifiant et du vérifié sont les mêmes, alors l'authentification dans ce sens est réussie. Il faut maintenant qu'elle se déroule dans le sens inverse. Par sécurité, si une authentification échoue, un délai s'instaure avant un prochain essai. À chaque essai échoué, le délai est augmenté jusqu'au maximum défini par l'application. De plus, une fois les SRES vérifiées, l'algorithme E1 génère une clef, l'Authenticated Ciphering Offset, qui pourra servir par la suite pour des échanges chiffrés.

LE CRYPTAGE

Cette étape fait suite à l'authentification dès que deux modules savent qu'ils sont bien en communication avec les modules désirés. Ils vont chiffrer leur communication pour des raisons évidentes de sécurité. Cette étape ne se déroule pas comme la précédente. Ici, la différence entre le module maître et esclave est importante. L'algorithme utilisé est l'E3, qui nécessite un nombre aléatoire RAND généré par le maître, l'adresse BD_ADDR du maître, l'horloge du maître (clock) et la COF qui provient de l'authentification, plus précisément de l'ACO. Cette clef de cryptage est générée à chaque demande de chiffrement.

Le chiffrement est mis à jour pour chaque paquet de données envoyé sur le réseau, grâce à l'horloge du maître.

Maintenant que vous savez comment fonctionne un réseau de module bluetooth, et sa sécurité, entrons dans le vif du sujet avec les problèmes de sécurité rencontrés. Toutes ces attaques sont très simples à mettre en ?uvre. C'est pourquoi il faut systématiquement désacti-



ver le bluetooth de votre téléphone lorsque vous ne l'utilisez pas. En effet, un simple ordinateur portable muni d'une carte bluetooth (15 euros en usb) permet à un attaquant, armé des logiciels d'attaque disponibles sur internet, de mener toutes celles-ci...

Mais comme nous allons le voir, la technique du bloooover permet même de récupérer des informations sur votre mobile bluetooth sans ordinateur portable, juste avec un téléphone totalement anodin. Seul un programme en JAVA, blooover.jar, et un téléphone supportant MIDP 2.0 et JSR-82 seront nécessaires. Des programmes comme BTClass ou le scanner redfang d'@Stake vous seront bien utiles. Ces programmes sont libres de droits et disponibles sur internet.

LE BLUE JACKING

Le bluejacking est une technique qui permet à n'importe qui se trouvant dans la zone couverte par une liaison bluetooth d'envoyer des messages aux autres terminaux inclus dans la zone. Pour éviter ce type de problème, il faut configurer votre terminal bluetooth sur " non détectable ". Le problème vient ici du fait que la majorité des téléphones portables équipés de la technologie bluetooth sont, par défaut, réglés sur " détectable ", ce qui les rend faillibles.

LE BLUEBUGGING

Sûrement la plus grosse attaque disponible contre les modules téléphoniques disposant du bluetooth, car un attaquant a accès à votre téléphone ainsi qu'à toutes les commandes AT de votre terminal. En fait, il est possible d'appeler à partir de votre téléphone, d'envoyer et lire des SMS, d'ajouter des contacts au répertoire, et le meilleur pour la fin, d'écouter les conversations téléphoniques.
Ce bug permet à un attaquant d'entamer un appel téléphonique vers le numéro de son choix, ou d'écouter toutes les conversations de sa victime. De plus, la possibilité d'envoi de SMS, permet de connaître le numéro de téléphone de la victime, car je vous le rappelle, il n'est pas nécessaire que l'attaquant connaisse votre numéro pour que vous vous fassiez attaquer. Une autre possibilité de cette attaque est de voir les numéros appelés par la victime et de les remplacer. L'attaquant peut aussi se connecter à internet via le téléphone piraté, puis envoyer de façon anonyme toutes sortes de mails ou de programmes, voire de virus.
Cependant l'attaquant est confronté a une contrainte physique. Le bluetooth utilise en effet la classe d'énergie 2,

ce qui fait qu'un réseau bluetooth ne s'étend que sur une dizaine de mètres.
Pourtant, en août 2004, une équipe a réussi à utiliser un réseau bluetooth et à exploiter des failles sur une longue distance. À 1700 m de la cible, avec du matériel très sommaire, composé d'un ordinateur portable, d'un dongle usb bluetooth modifié, d'une petite antenne portative et bien sûr d'un téléphone bluetooth.

LE BLUESNARFFING

Cette attaque découverte en 2003 est probablement la plus connue des failles bluetooth. Elle permet à un attaquant de se connecter de manière invisible sur un réseau bluetooth, et de s'octroyer les droits nécessaires pour récupérer de nombreuses informations d'un mobile. Pour utiliser cette faille, l'attaquant se sert de la couche OBEX et du profil OPP. Ce profil est activé par défaut sur de nombreux téléphones afin de faciliter les échanges avec d'autres types de modules bluetooth. Grâce à OBEX, l'attaquant peut utiliser les commandes Connect, Disconnect, Put, Get, Abort & SetPath sur le module de la victime et ainsi lire et récupérer des fichiers dont l'attaquant connaît le nom et l'emplacement. Le problème est que ces fichiers ont des emplacements définis et connus. Les exemples ci-dessous ne sont valides que pour les téléphones Ericsson et ne montrent que les fichiers qui sont utilisables avec les commandes PUT et GET, soit les plus dangereuses dans ce cas d'accès aux fichiers.

BLUEPRINTING

Le but de cette technique est de pouvoir récupérer un maximum d'informations sur le matériel utilisé par les usagers. En effet, elle permet de récupérer l'équivalent de l'adresse MAC de nos cartes réseaux. Cette adresse est composée de 6 bytes, les trois premiers correspondent au fabricant. Pour les trois bytes suivants, les rangées ne sont pas encore totalement connues, ce qui ne permet pas de connaître précisément tous les modèles, cependant le scanner créé par @stake, redfang, fonctionne bien.
De plus, les modules bluetooth sont équipés du Service Discovery Protocol Records qui permet à un autre module bluetooth d'interroger un module pour connaître les services présents et comment les utiliser. Ces fonctionnalités peuvent être répertoriées puis utilisées pour reconnaître le type de matériel employé.

BLUESMACK

Cette faille correspond au DoS de nos PC. Elle consiste à envoyer énormément de requêtes à un seul module. Dans le cas du bluetooth, la faille se situe dans la couche L2CAP qui permet à un module de demander un écho à un autre. Le principe est le même que pour l'ICMP ping sur les ordinateurs. On peut aussi pinger un module bluetooth à partir d'un ordinateur portable sous linux avec la couche Bluez (Official Linux Bluetooth protocol stack), et avec le programme l2ping. Le but d'un DoS dans le cadre d'un réseau bluetooth n'est pas de saturer ce réseau mais d'épuiser les batteries de la cible. En effet, le grand nombre de requêtes et de réponses demande beaucoup d'énergie pour envoyer en permanence ces informations.

BLOOOVER

La majorité des gens pense que pour attaquer un module bluetooth, il faut être dans la courte portée du réseau bluetooth avec son ordinateur portable, ce qui peut paraître suspect en extérieur. Seulement, une application JAVA a été développée pour fonctionner sur les téléphones de type bluetooth, afin d'avoir les mêmes capacités. Qui alors va se méfier de tous les téléphones proches de lui ? Cependant, cet outil libre de téléchargement est limité dans les fonctions utilisables afin qu'aucune personne ne soit victime d'individus malintentionnés. Pour fonctionner, cette application ne nécessite qu'un téléphone à la norme J2ME MIDP2.0 avec l'API Bluetooth JSR-82.

BT AUDIT

La norme bluetooth se base sur deux protocoles principaux : L2CAP et RFCOMM. Pour communiquer, ces deux protocoles utilisent des ports, de la même manière que le TCP/IP, UDP/IP. On se dit tout de suite, si j'ai des ports, j'ai des services associés, donc je peux scanner. En effet, les équivalents des ports du L2CAP sont numérotés de 1 à 65 535 en ne tenant compte que des nombres impairs et les ports du RFCOMM de 1 à 30. Ces " ports " dans la couche L2CAP sont appelés PSMs (Protocol Service Multiplexers).
Deux scanners de ports existent déjà, un pour chaque protocole, PSM_SCAN et RFCOMM_SCAN. Ces deux

telecom/devinfo.txt	Information hardware	GET
telecom/rtc.txt	The Real Time Clock	GET/PUT
telecom/pb.vcf	Level 2 access (Access)	GET/PUT
telecom/pb/luid/.vcf	Add new entry	PUT
telecom/pb/0.vcf	Own business card	GET/PUT
telecom/pb/###.vcf	Level 3 static index access	GET/PUT
telecom/pb/luid/*.vcf	Level 4 unique index access	GET/PUT
telecom/pb/info.log	Supported properties and memory info	GET
telecom/pb/luid/###.log	Change log	GET
telecom/pb/luid/cc.log	Change counter	GET
telecom/cal.vcs	Calendar Level 2 access	GET/PUT
telecom/cal/luid/.vcs	Add new entry	PUT
telecom/cal/###.vcs	Level 3 static index access	GET/PUT
Telecom/cal/luid/*.vcs	Level 4 unique index access	GET/PUT
Telecom/cal/info.log	Supported properties and memory info	GET
Telecom/cal/luid/###.log	Change log	GET
Telecom/cal/luid/cc.log	Change counter	GET

L'attaquant sait donc où aller et quoi récupérer.

programmes ne font que lister et donner l'état de ports, ouverts ou non.

BTSCAN

Pour ne pas attaquer son propre materiel il fallait trouver une methode pour ne pas s'auto-bluesnarfer. La solution est de se faire passer pour quelque chose d'autre. Le BTscan permet de modifier la Bluetooth device Class de votre module pour vous faire passer pour ce que vous désirez : ordinateur, imprimante, ...

BLUESPAM

Le bluespam, comme son nom l'indique, concerne le spam de module Spam. Nous n'aborderons pas ici le sujet du spam massif, mais du spam, pour le défi technique de quelques modules. Le bluespam recherche tous les modules bluetooth joignables dans sa zone d'une dizaine de mettre, et essaie d'envoyer un message. Si un module du réseau supporte l'OBEX, alors il recevra ce message. On peut en plus avec un Palm définir ce que l'on souhaite envoyer, un fichier par exemple. On peut aussi s'en servir comme défense en Spam Back, si quelqu'un vous envoie un message par ce moyen, vous lui renvoyez immédiatement un message par le même moyen.

BLUESNARF ++

Cette attaque est relativement récente. Ce n'est qu'une variante améliorée du bluesnarf. Elle utilise toujours la commande GET à cause de l'OBEX, et l'utilise pour mettre un serveur OBEX FTP. De cette manière, l'attaquant peut voir tous les fichiers. La commande " ls " indique les fichiers présents dans le répertoire en cours, ce qui évite de trouver la doc sur chacun des modules pour connaître les noms et emplacements des fichiers. De plus, avec ce serveur, l'attaquant a tous les droits : d'écriture, de lecture, d'exécution et, le plus dangereux, d'effacement dans le cas d'une carte mémoire.

HELLO MOTO

Cette attaque, comme son nom l'indique, a été découverte sur un téléphone de la marque Motorola. Dans les téléphones Motorola équipés du bluetooth, une faille permet d'accéder aussi aux commandes AT du téléphone. L'attaquant démarre une communication avec OBEX en faisant croire qu'il va envoyer une Vcard, c'est-à-dire de synchroniser HotSync, son module bluetooth, avec un autre pour envoyer carte de visite et agenda. Puis l'attaquant coupe l'envoi de Vcard, mais la victime, elle, le considère comme étant un module sûr. Alors l'attaquant peut envoyer ce qu'il veut à la victime.

L'INTEGRITE

Les modules bluetooth dans leurs communications, en particulier la réception de paquets, ne vérifient pas l'intégrité des paquets et donc leur provenance. On peut donc utiliser une attaque de type " man in the middle ". Cela permet de recevoir les informations d'un module, de les enregistrer si l'on veut les modifier, puis de continuer leur envoi vers le module cible.

ATTAQUE ALGEBRIQUE

Une attaque de type mathématique est aussi envisageable pour casser la Key Stream Generator, soit la clef utilisée pour chiffrer les communications.

CODE PIN

Le code pin est très important dans une communication sécurisée entre des modules bluetooth, puisque c'est à partir de ce code que l'algorithme E22 va générer la clef d'initialisation. En effet, pour générer cette clef, seul le code PIN est inconnu, puisque le reste des informations voyage dans les airs sans aucun chiffrement. La longueur des codes pin étant majoritairement de 4 chiffres, cela donne 10 000 possibilités, ce qui est très faible pour un chiffrement. De plus, on sait parfaitement qu'un grand nombre de gens laisse le code pin par défaut, 0000.

UNIT KEY

Dans une communication entre deux modules bluetooth, une link key est utilisée comme seule information cachée, pour le chiffrement et l'authentification sur le réseau. Prenons l'exemple où le module X communique avec le module Y et qu'ils utilisent la Link Key du module X. Un troisième module Z entre dans le réseau et utilise donc la clef du module X. À partir de ce moment, le module Z peut être authentifié aussi sur le module Y, ou même écouter ce module en faisant quelques calculs pour trouver l'encryption key.

CONCLUSION

On vient donc de voir que les modules bluetooth souffrent d'un grand manque de sécurité. Ces failles ne sont pas tant dues à la norme bluetooth qu'à l'implantation de cette norme avec le matériel. La norme bluetooth est par exemple, parfaitement préparée pour communiquer dans un lieu public puisque les ondes changent de fréquence plusieurs fois par seconde.

Cependant, les applications pour communiquer dans les lieux publics sont de plus en plus nombreuses, et les failles aussi.

Snoop_Psykoman

CLONAGE DE L

Le clonage de cartes SIM est un domaine dont on entend souvent parler, sans pour autant savoir de quoi il s'agit réellement. Le réseau GSM est loin d'être bien sécurisé, vous le verrez tout au long de cet article et a fortiori dans ce numéro spécial. Nous reviendrons donc dans un premier temps sur l'architecture GSM indispensable à la compréhension de cet article. Puis nous verrons plus en détail les méthodes d'identification d'un portable et comment jouer de ces faiblesses pour pouvoir faire des clones de cartes SIM...

I RETOUR SUR L ARCHITECTURE RESEAU GSM

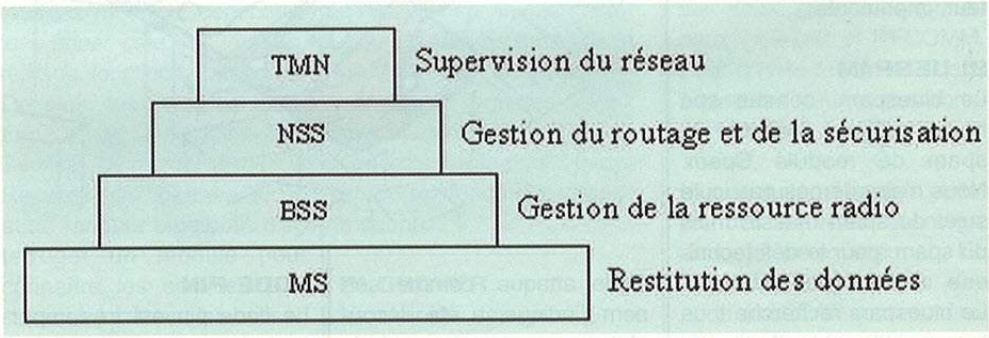
La structure du réseau GSM peu être assimilée à une pyramide à quatre étages.
En partant de la base, nous avons :

- Le Mobile Segment (MS) : Il s'agit de l'ensemble des téléphones mobiles et autres appareils pouvant se connecter au réseau GSM.
- Le Base Station Subsystem (BSS) : Correspond aux dispositifs du réseau chargés de gérer les ressources radios ainsi que d'assurer les transmissions des données par ondes radios.

Ce segment regroupe :

- les BTS (Base Transceiver Station), ensemble d'émetteurs récepteurs chargés de faire l'interface entre les structures fixes du réseau et les stations mobiles (tels les portables...). Elles s'occupent de tout ce qui est modulation, démodulation, correction des erreurs de signaux et autres fonctions plus pointues.

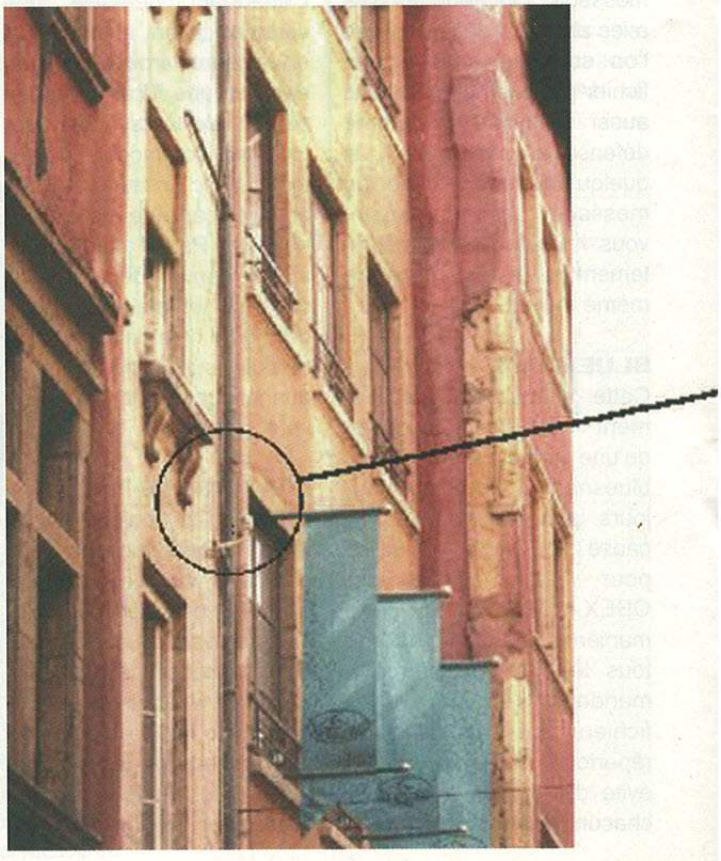
Il existe plusieurs types de BTS (rayonnantes, ciblées, micro BTS) souvent aidées dans leur tâche par des amplificateurs de signaux. Celles-ci font désormais parti de notre paysage urbain.



- Le BSC (Base Station Controller) correspondant au " cerveau " du BSS. Il peut avoir sous son contrôle une centaine de BTS. Il a pour tâche l'allocation des canaux, la régulation de la puissance d'émission des mobiles et des BTS, le changement de canal d'un mobile, voire d'une BTS si nécessaire.

Il va faire l'interface entre le BSS et le Network SubSystem (NSS), étage supérieur de notre pyramide.

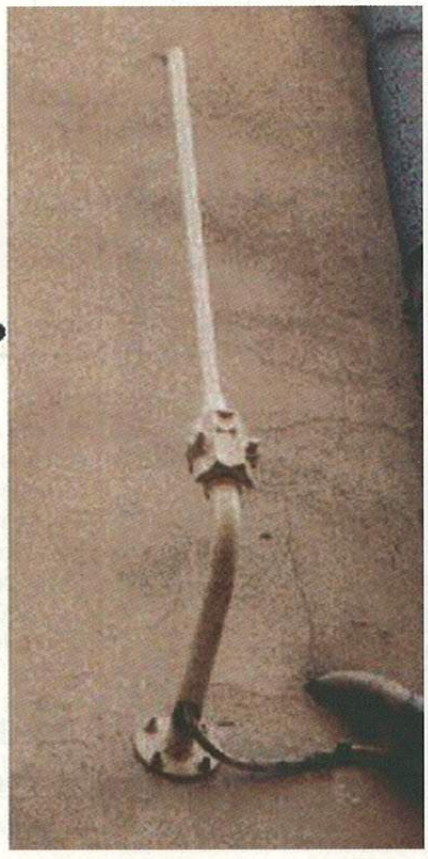
- Le Network SubSystem (NSS) : Ce segment comprend l'ensemble des structures indispensables à l'établissement des communications au sein du réseau ainsi qu'à la gestion de la mobilité des stations. Il gère ainsi les fonctions de routage et d'interconnexion.



LA CARTE SIM

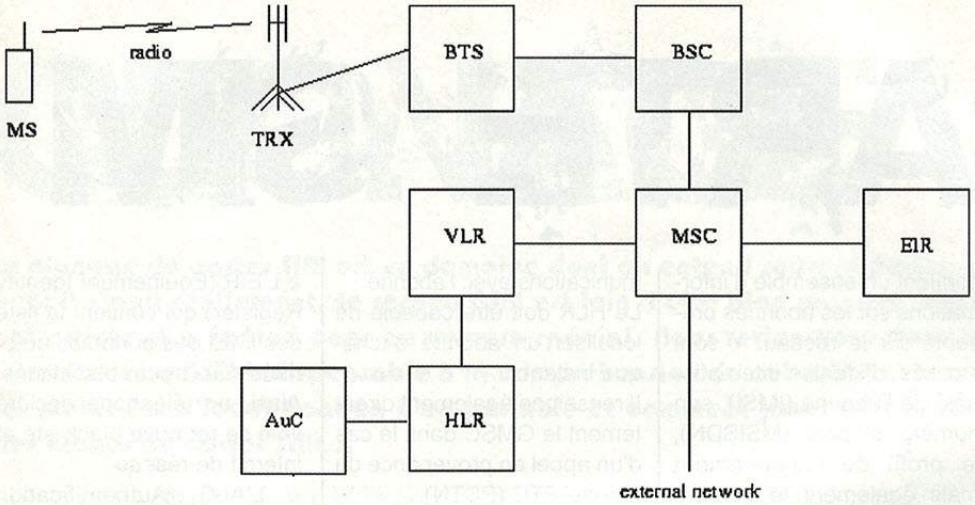
Ce segment regroupe :

- Les MSC (Mobiles-services Switching Center) / GMSC (Gateway Mobiles-services Switching Center) : Ils ont le rôle de commutateurs et assurent le routage vers un autre MSC lors d'un appel de mobile à mobile ou assurent l'interconnexion avec le réseau PSTN (Public Switched Telephone Network) (Réseau Téléphonique Commuté " RTC " en français), auquel cas le routage s'effectue vers un GMSC. Il s'occupe également de l'acheminement des SMS.
- Le HLR (Home Location Register) : Il s'agit de la base de données gérant les abonnés d'un opérateur. Il peut être assimilé à la mémoire centrale du réseau et contient un ensemble d'informations sur les abonnés présents sur le réseau. Y sont stockés : l'identité internationale de l'abonné (IMSI), son numéro d'appel (MSISDN), le profil de l'abonnement mais également le numéro du VLR où est enregistré l'abonné, et d'autres informations relatives à l'identification et au chiffrement des communications (RAND, SRES, Kc).
Le HLR a aussi pour tâche de fournir aux VLR des informations relatives à l'abonné, de se mettre à jour avec les informations récupérées au niveau des VLR (tel le changement de localisation), et la récupération, au niveau de l'AuC, des données nécessaires au chiffrement des communications avec l'abonné.
Le HLR doit être capable de localiser un abonné à chaque instant.
Il renseigne également directement le GMSC dans le cas d'un appel en provenance du réseau RTC (PSTN).
- Les VLR (Visitor Location Register) : On peut les comparer à des mémoires temporaires. Un VLR s'interface entre le HLR et un MSC et est relié à l'AuC et à d'autres VLR.
Il contient les mêmes informations que celles contenues dans le HLR sur les abonnés actifs (ou en veille) se situant dans sa zone de couverture, à la différence que l'IMSI est remplacé par le TMSI (Temporary Mobile Subscriber Identity) afin d'éviter que l'IMSI soit envoyé sur les ondes et ainsi garantir plus de confidentialité pour l'abonné (ce numéro lui étant propre). Le stockage d'informations au niveau du VLR désengorge le HLR en lui évitant une multitude de requêtes. Alors que le HLR renseigne le GMSC lors d'un appel provenant du réseau RTC, le VLR quant à lui donne au MSC les informations nécessaires à l'établissement d'un appel en provenance d'un mobile. Il va également servir à mettre à jour le HLR sur la localisation de ses abonnés.
- Le Telecommunication Management Network (TMN) : Il s'agit d'un réseau de management en interface avec le réseau GSM proprement dit. Il permet ainsi d'effectuer des opérations de maintenance, de supervision mais également regroupe des fonctions de sécurisation. On y retrouve ainsi :
- L'EIR (Equipement Identity Register) qui contient la liste des IMEI des portables autorisés ou alors blacklistés. Ainsi, un téléphone déclaré volé se retrouve blacklisté et interdit de réseau.
- L'AuC (Authentification Center) a en mémoire une copie de la Ki contenue également dans la carte SIM du mobile. Cette clé permet, grâce à différents algorithmes (que nous aborderons dans une seconde partie), l'authentification du mobile ainsi que le cryptage des données envoyées sur le réseau. Il limite ainsi tout accès frauduleux au réseau.
- Les OMC (Operations and Maintenance Center), qui assurent des fonctions de configuration et de contrôle à distance. Il peut ainsi administrer le trafic au niveau du BSS mais aussi au niveau des MSC/GMSC.
- Le NMC (Network Management Centre) qui assure des fonctions de supervision du réseau, *(voir schéma page 22)*.

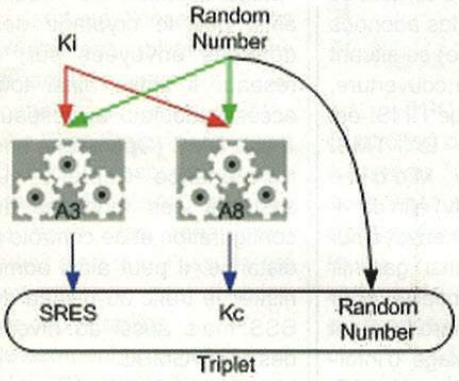


II IDENTIFICATION D'UN MOBILE SUR LE RESEAU GSM

Pour éviter tout accès non autorisé au réseau GSM ainsi que pour plus de confidentialité, la sécurité des communications repose sur deux paramètres : l'IMSI (identifiant propre à l'abonné) et la Ki. Cette dernière est une clé de 128 Bits, renfermée dans la carte SIM et dont L'AuC détient une copie. Cette clé sert à générer, grâce à l'algorithme Comp128, SRES (Signed RESponse) de 32 bits et Kc clé de 64 Bits deux



séquences indispensables respectivement à l'identification et à l'encryptage des données transmises par ondes (seule partie cryptée du réseau).

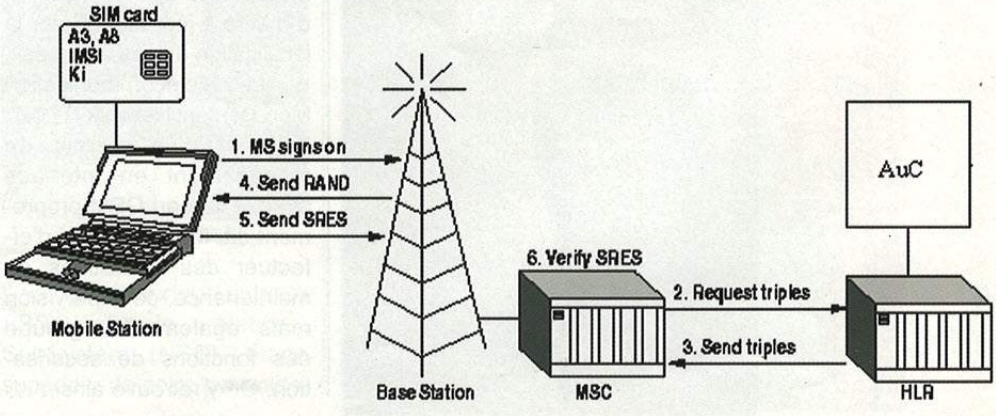


Lorsqu'un mobile procède à son identification, celui-ci envoie au MSC/VLR son IMSI, qui lui attribue alors un TMSI permettant d'augmenter la confidentialité de l'abonné et ainsi éviter au maximum que ce dernier puisse être tracé par des entités non autorisées, l'IMSI étant propre à un utilisateur contrairement au TMSI qui lui est temporaire.

Parallèlement à cela, le MSC envoie au HLR une requête pour obtenir un triplet contenant RAND, SRES et Kc.

Le HLR, après les avoir obtenus par l'AuC, renvoie cinq triplets au MSC, lui évitant ainsi d'avoir à effectuer la demande à chaque identifications du mobile. Le MSC renvoie alors le RAND d'un des triplets au mobile. Celui-ci génère, avec l'algorithme Comp128 de la SIM, en utilisant le RAND venant de lui être envoyé et la Ki de sa SIM, le SRES qu'il renvoie à son tour au MSC. Le SRES calculé par le réseau et celui calculé par le mobile sont alors comparés. S'ils sont identiques, alors l'identification est validée et le mobile a accès au réseau, sans quoi il n'est pas accepté.

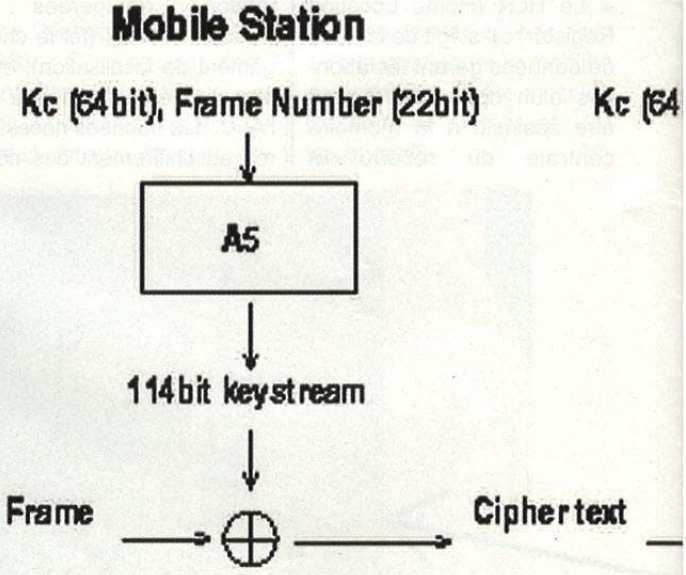
La Ki et le RAND permettent également de générer grâce à l'algorithme Comp128 la Kc qui sera utilisée pour encrypter toutes les données transmises par ondes, telle la parole, en utilisant l'algorithme A5.



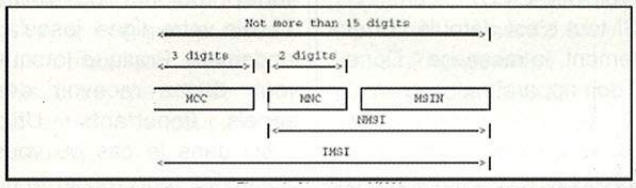
III CLONAGE DE LA CARTE SIM

Avant de passer à la pratique, (désolé pour les impatients, mais comme disait l'autre : "sans maîtrise, la puissant n'est rien"), encore quelques lignes de théorie.
Comme nous l'avons vu dans la partie précédente, l'identification d'un mobile repose sur l'IMSI et la Ki. Ainsi, il suffirait d'extraire ces deux identifiants et de les implanter dans une carte vierge pour obtenir un clone.

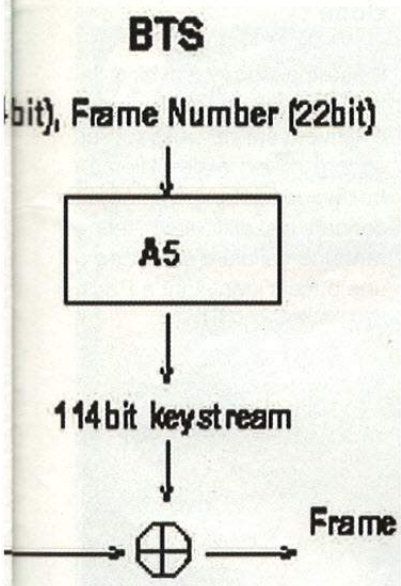
L'extraction de l'IMSI ne pose aucun problème, elle est accessible en lecture et peu être récupérée avec un lecteur de carte.
L'IMSI peut être découpée en trois partie : le Mobile Country Code (MCC), qui



identifie le pays (208 pour la France), le Mobile Network Code (MNC), qui identifie l'opérateur (10 pour SFR) et enfin le MSIN, qui est propre à l'abonné et l'identifie chez l'opérateur. L'association MNC+MSIN forme le National Mobile Subscriber Identity (NMSI) et identifie l'abonné dans le pays.



La récupération de la Ki quant à elle s'avère être beaucoup moins aisée. En effet, la Ki est interdite en lecture et n'est transmise à aucun moment. Néanmoins, l'algorithme Comp128 fut mis à mal par David Wagner



et Ian Goldberg, qui remarquèrent que sous certaines conditions il était possible de récupérer des informations sur la Ki. Ainsi en procédant à une méthode visant à faire générer à la carte SIM des milliers de SRES et Kc, il était possible, après cryptanalyse, de déduire la Ki. Ceci prend néanmoins quelques heures (variable en fonction du matériel utilisé).
Note : Il s'agit de la version 1 de Comp128. Sur les cartes actuelles, on rencontre une version renforcée de Comp128 limitant les requêtes envoyées ou alors la nouvelle version de Comp128 : Comp128v.2.

Passons maintenant aux travaux pratiques :p

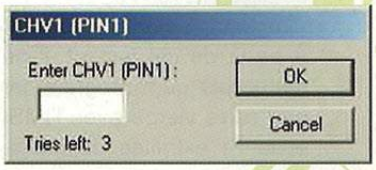
- Extraction IMSI et Ki

Dans un premier temps, nous allons procéder à l'extraction de l'IMSI et la Ki.
Pour cela nous devons disposer d'un programmateur de carte à puce, de la puce dont on souhaite réaliser le clone, d'un logiciel d'extraction et, bien entendu, d'un PC.
Pour notre démonstration, le logiciel d'extraction choisi sera SimScan V2.01 pour sa simplicité et par goût personnel, mais il faut savoir qu'il existe désormais une multitude de softs de la sorte et autres packs d'extraction.

1/ Branchez votre programmateur à votre PC.
Note : SimScan ne prend en charge que les programmateurs connectés sur le port COM, et ne fonctionne pas sur les cartes possédant l'algorithme Comp128v.2. À vous de trouver d'autres versions de softs qui réalisent cela.

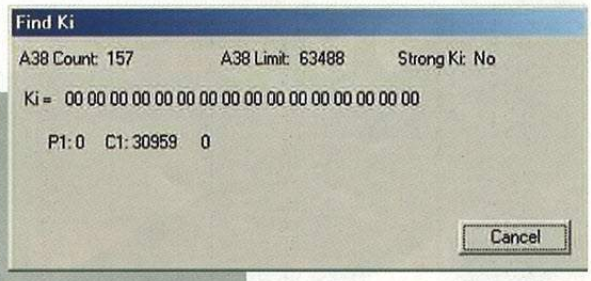
2/ Insérez votre carte dans le programmateur et lancez SimScan.
L'interface suivante apparaît alors.

Vérifiez que votre carte est bien reconnue en cliquant sur TEST, ceci devrait vous

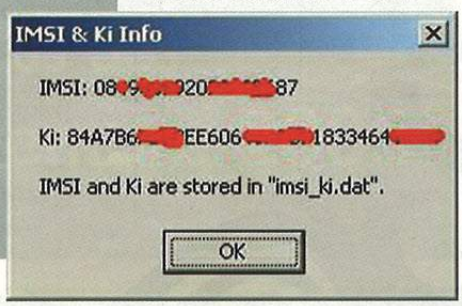


renvoyer l'ATR de votre carte.
Cochez la case A38 Limit et laissez Strong Ki décochée.
Cliquez alors sur " Find Ki ", entrez votre code PIN.

L'interface suivante apparaît. Elle vous permet de suivre l'état de l'extraction de la Ki.



Note : Si, après 60000 requêtes (A38 count), aucune paire de la Ki n'a été découverte, stoppez et relancez en cochant " Strong Ki ".
Si tout se passe correctement, la fenêtre suivante devrait apparaître résumant les paramètres extraits de la SIM.



Je vous conseille de lire la documentation accompagnant ce logiciel pour plus de détails.

À partir de cet instant, il ne reste plus qu'à programmer une carte vierge avec l'IMSI et la Ki extraites de l'originale.

● Programmation du clone

Possédant la Ki et l'IMSI, nous allons alors programmer notre clone.

Nous avons besoin d'une carte vierge (types Goldwaffer, Silver), des fichiers permettant d'émuler le fonctionnement d'une carte SIM (Algorithme, etc.), de SimScan et d'un téléphone GSM.

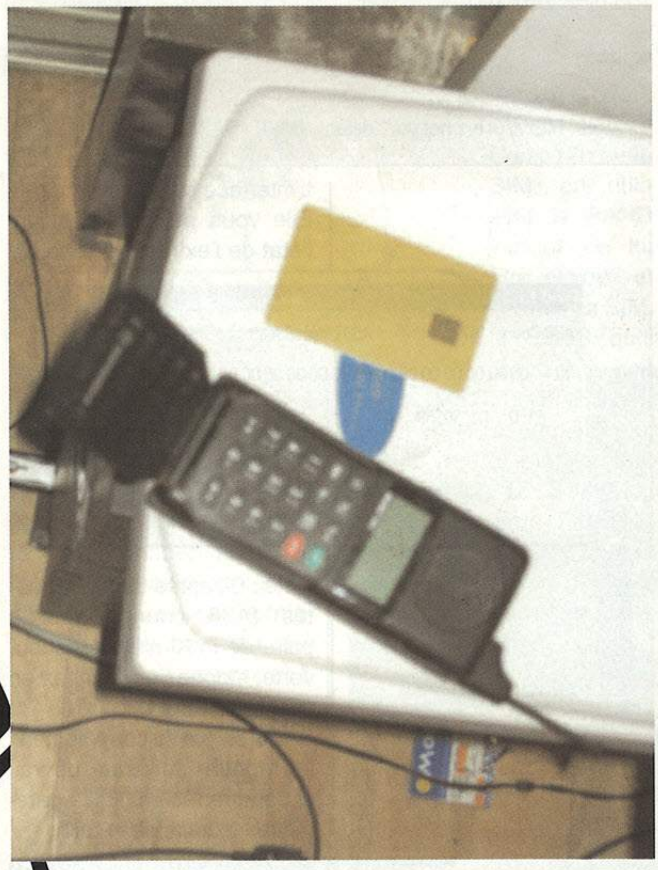
Ici, nous utiliserons une Goldwaffer.

1/ Commencez par programmer, à l'aide d'un soft tel Icprog, le PIC et l'EEPROM de la Gold avec les fichiers reproduisant le fonctionnement des algorithmes Comp128, A3 et le fonctionnement d'une carte SIM.

2/ Procédons maintenant à l'ajout de la Ki et de l'IMSI.

Lancez à nouveau SimScan et cliquez sur le bouton " WR Ki & IMSI ".

Une fenêtre apparaît reprenant les résultats de l'extraction.



Vérifiez qu'ils sont corrects puis cliquez sur " Write ".

On vous demande alors d'entrer un code PIN approprié permettant de définir la position dans la carte de votre clone. Il est en effet possible d'en stocker jusqu'à 8 pour les fichiers de notre démonstration (à condition de posséder une carte d'une capacité suffisante).

Nous nous contenterons d'une seule :p

Note : Il vous sera possible de trouver sur Internet des programmes permettant d'en stocker jusqu'à 10 et plus (voir SIM-EMU).

Si tout s'est déroulé correctement, le message " Done ! " doit apparaître.

3/ Test de notre clone.

Introduisez votre carte fraîchement programmée dans un téléphone GSM, mettez sous tension, entrez votre code PIN et là, Bingo !, vous possédez un double de votre SIM.

Par flemme de découper ma Gold, j'ai utilisé une antiquité me permettant de la mettre en entier. Pratique les vieilleries ;)

IV QUELQUES EXPLICATIONS

Certains peuvent se demander où est l'intérêt de réaliser un clone de sa propre carte.

En voici quelques uns :

Pour les personnes possédant plusieurs comptes, possibilité leur est offerte de les stocker tous sur la même puce sans avoir à trimbaler autant de téléphones ou de puces qui risqueraient d'être perdues.

Il vous est également possible d'utiliser votre clone comme sauvegarde de dépannage. Dans le cas où vous oublieriez votre téléphone au bureau, vous auriez toujours possibilité d'avoir votre ligne jusqu'au lendemain. Pratique lorsque vous devez recevoir des appels importants. Utile aussi dans le cas où vous bloqueriez par mégarde le code PIN de votre puce.

Nous venons donc de voir qu'il y a de nombreux intérêts à posséder un clone de sa puce.

Récapitulation sur ce qu'il est possible, ou pas, de faire avec son clone :

Il est impossible d'avoir à la fois son clone et l'original d'activés sur le réseau, et encore moins à des kilomètre l'un de l'autre. L'opérateur connaît les distances séparant une cellule d'une autre ; une puce s'identifiant à Paris puis à Marseille à quelque minute d'intervalle paraîtrait suspecte.

La dernière puce s'étant manifestée sur le réseau récupère la ligne. Ainsi, si un appel est effectué vers son

numéro, c'est la dernière identifiée qui le réceptionnera et non pas les deux qui se mettent à sonner. Il en est de même pour les SMS.
Pour récupérer la ligne, une simple tentative d'appel, rallumage du portable ou autre manipulation visant à se connecter suffit.
Chez certains opérateurs, le fait de voir deux puce en même temps sur le réseau suffit à blacklister le numéro. (Mes tests chez SFR n'ont pas entraîné la coupure de ma ligne).
Quant à ceux qui pensaient pouvoir mettre leur ligne sur écoute, le clone n'est pas la solution car une seule puce peu s'y trouver.

Sur ce, amusez-vous bien ;)

THUG

Sources :

http://www.issadvisor.com/columns/GSMSecurity/GSMSecurity.htm
http://www.mpirical.com/companion/mpirical_companion.html
http://www.willassen.no/msl/diplom.html
http://users.net.yu/~dejan/ << SimScan et fichier pour programmer PIC et EEPROM
http://www.tele-servizi.com/Janus/motpages.html
http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-9900/a5/Netsec/netsec.html
http://www.hds.utc.fr/~ducourth/TX/CEL/CEL-gsm.html

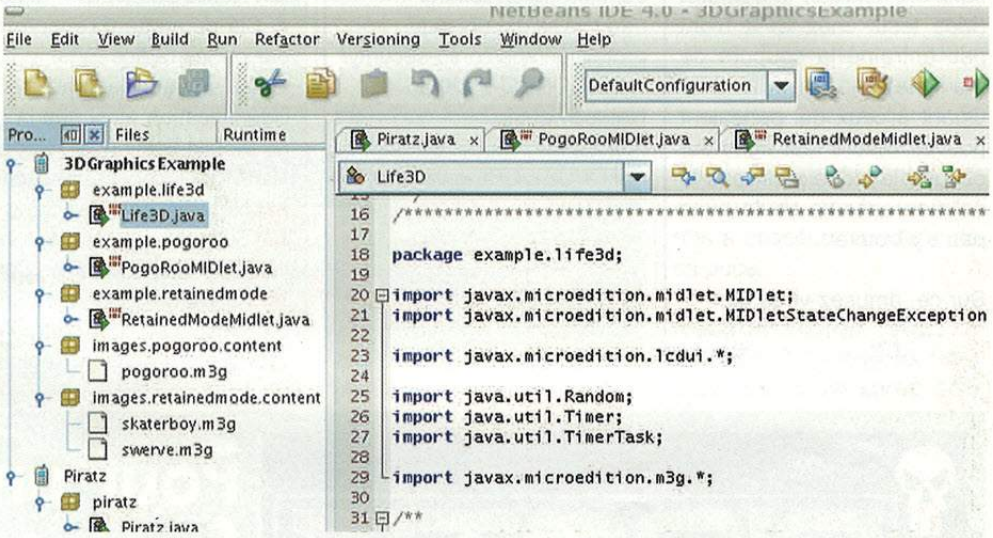
Glossaire :

A3 Algorithme d'authentification du mobile
A5 Algorithme de chiffrageutilisé pour crypter les données transmises
A8 Algorithme permettant la generation de la clef privée
Kc pour la voix
AuC Authentication Center. Centre contenant les algo A3 A8, RAND, Ki, SRES
BSC Base Station Controller.
BSS Base Station Subsystem : regroupe BTS et BSC
BTS Base Transceiver Station
COMP128 Algo regroupant A3 et A8
GSM Global System for Mobile
HLR Home Location Register
Kc Clé permettant l'encryptage des données transmises par ondes radios
Ki Clé secrète de la puce. C'est sur elle que repose l'identification ainsi que la génération de la Kc
MS Mobile Station, le téléphone
MSC Mobile services Switching Center
NSS Network and Switching Subsystem
SIM Subscriber Identity Module. Carte du téléphone contenant IMSI, Ki, et les algorithmes Comp128 (A3+A8) et A5
SRES Signed RESponse. Générée par A3 en réponse a un RAND pour permettre l'identification
VLR Visitor Location Register

PROGRAMME TON

Aujourd'hui, nous possédons quasiment tous un téléphone portable équipé des dernières technologies (bluetooth, gprs, appareil photo, etc.) incluant une machine virtuel java.
Le but de cet article est de vous présenter les fondements de la programmation sur mobile en se basant sur un exemple de jeu extrêment simple permettant de bien comprendre les mécanismes mis en œuvre dans ce genre de programmes.

PLAN



INTRODUCTION

Il est possible de développer des applications pour mobiles à différents niveaux, suivant le modèle de téléphone que vous utiliserez mais surtout par rapport au système d'exploitation qui lui est intégré. Pour commencer, vous devez savoir quel type de programme vous souhaitez réaliser ; le choix de la technologie à employer dépendra certainement de votre application. Le moyen le plus simple pour débuter est d'utiliser le langage java car la quasi totalité des téléphones intègrent une machine virtuelle pour lancer des applications écrites en java. C'est ce que nous utiliserons dans cet article.

L'avantage du java est la portabilité. Dans le plupart des cas, votre application pourra être utilisée sur l'ensemble des téléphones ou autres systèmes compatibles J2ME. Vos programmes ne seront pas portables seulement si vous utilisez des API spécifiques à votre modèle de téléphone car les constructeurs fournissent parfois des SDK (software development kit) personalisés que vous pourrez vous procurer sur leurs sites respectifs .

Aujourd'hui, la plupart des constructeurs intègrent le système d'exploitation symbian à leurs produits (on peut citer par exemple Nokia et Sony Ericsson) . Ce système est très bien documenté, il existe déjà un grand nombre d'ouvrages qui lui sont consacrés et les différentes API sont assez simples à maîtriser. De plus, ce système d'exploitation offre la possibilité d'utiliser d'autres langages de programmation tels que le c++ ou le visual basic, ce qui permet de contrôler chacun des éléments du téléphone (infrarouge, réseau, appareil photo, etc.). Pour en savoir plus à ce sujet, il vous suffit de vous rendre dans la section Developper de http://symbian.com/, vous y trouverez toute la documentation nécessaire.

Les possibilités de développement ne se limitent qu'à votre imagination et des applications très puissantes ont vu le jour, bien qu'elles ne soient pas toujours légitimes. Il faut donc rester prudent lorsque vous recevez de nouvelles applications car le contrôle que l'on obtient sur le téléphone peut également vous nuire... En effet, depuis l'apparition du vers Carib, les éditeurs antivirus découvrent régulièrement de nouveaux codes malveillants affectant les gsm. Il est néanmoins possible d'installer un antivirus sur son téléphone. Pour cela, vous devrez vous rendre sur le site http://f-secure.com/ et suivre les instructions d'installation pour utiliser une version d'évaluation de leurs produits.

Maintenant que nous avons quelques connaissances théoriques, nous allons pouvoir commencer la partie vraiment intéressante de l'article en créant nous mêmes un petit jeu en java. Une chose importante à savoir est que vous n'êtes pas

TELEPHONE !

obligé d'avoir un téléphone de dernière génération pour essayer les codes fournis avec l'article. Vous pouvez d'ailleurs tester les codes sans aucun téléphone car Sun fournit un émulateur avec le J2ME.

UN PEU DE PRATIQUE
L'environnement de développement

Avant de commencer à écrire du code, il y a un élément que nous devons impérativement installer : un sdk (software development kit). La méthode la plus simple est de récuperer le J2ME sur le site de Sun mais vous pouvez également récuperer les sdk fournis par le constructeur de votre gsm. Ensuite, il est préférable d'installer un environnement de développement intégré afin de faciliter les étapes de compilation et d'avoir une meilleure productivité. Je vous conseille d'installer netbeans et son module netbeans mobility pour tester vos applications, c'est un programme très puissant et simple d'utilisation que vous devriez prendre en main rapidement. Netbeans a été développé en java, ce qui le rend accessible pour les systèmes Windows, Linux et Solaris.

D'autres applications propriétaires existent telles que eclipse ou Sun java studio mobility qui est basé sur netbeans. Le mieux est de tous les tester afin de voir avec lequel vous êtes le plus à l'aise. Il y aura toujours certains puristes qui préféreront utiliser un simple éditeur de texte tel que vi mais pour du java, je vous conseille VRAIMENT d'installer un IDE ;) .

Plus d'infos sur java

Il y a quelques années, pour développer en java sur des systèmes embarqués, on utilisait les API comprises dans le CDLC (Connected Device Limited Configuration). Mais cela restait assez limité. De nouvelles spécifications sont apparues, puis en 2002, le jcp a sorti la seconde version du MIDP (Mobile Information Device Profile) qui amène beaucoup de nouveautés et facilite grandement l'écriture du code. Tous les derniers téléphones intègrent une machine virtuelle compatible avec ce standard. Il y a régulièrement de nouvelles couches de fonctions ajoutées pour compléter les API traditionnelles on les appels des JSR (java spécification Requests). Vous pouvez retrouver toutes ces spécifications sur : http://jcp.org/en/jsr/all.

Le code des applications pour mobiles ressemble fortement à celui d'un programme java classique, il y a seulement quelques points à ne pas oublier. Chaque programme doit dériver de la classe MIDlet et doit contenir les points d'entrées startApp(), pauseApp() et destroyApp() en remplacement de main(). Les codes pour gsm sont appelés midlet pour faire référence à l'utilisation du MIDP, les midlets sont donc similaires aux applets mais au lieu de les lancer sur un navigateur on les lance sur son mobile ;)

Pour créer des gui, on peut utiliser soit des API de haut niveau si l'on n'a pas besoin de modifier les paramètres standarts des éléments, soit une API de bas niveau qui nous permettra de placer précisement les objets et modifier leur apparence (couleurs, fontes du texte , etc.). Par exemple, pour créer des jeux, on préférera utiliser les API de bas niveau afin d'en contrôler chaque élément.

Au début de chacun de nos codes, il faudra impérativement inclure les librairies qui nous donneront respectivement accès aux fonctions permettant l'intéraction avec le mobile et celles permettant de créer des interfaces graphiques :

```
import javax.microedition.midlet.*;
import javax.microedition.lcdui.*;
```

Dans vos premiers programmes, vous utiliserez certainement les classes de bases donnant accès aux éléments classiques d'une interface graphique.

Les programmes pour mobiles sont composés de deux fichiers. Le premier est un .jar contenant la liste des classes de l'application. Le second fichier comprend une extension en .jad, c'est une sorte de descriptif de l'application qui indique la taille du programme, l'emplacement du fichier de classes et quelques autres options de configuration. En supposant que vous utilisez un IDE, je ne vais pas m'attarder sur les options de compilation et d'exécution car la tâche est automatisée avec ces environnements de développement.

Avant de nous lancer dans l'écriture complexe d'un jeu, il est préférable de construire un programme de base afin de mieux se rendre compte de ce que représente un midlet. Voilà donc le code permettant d'afficher un texte sur votre téléphone

```
/*
 * Hello.java : Voilà notre programme de base
 * qui affiche simplement un texte à l'écran.
 * On peut difficilement faire une application
 * plus simple :p
 */
package hello;
import javax.microedition.midlet.*;
import javax.microedition.lcdui.*;

public class Hello extends MIDlet implements
CommandListener {

    private Command QuitME;
    private Display disp;

    public Hello() {
        disp = Display.getDisplay(this);
        QuitME = new Command("Quitter",
                             Command.EXIT, 1);
    }

  /**
   * Point de départ de l'application, on initialise les éléments à afficher puis on se prépare à réagir à certains évènements.
   */
    public void startApp() {
        String notreTexte =
            "Hello World from piratez ! ;-)\n";
        TextBox t = new TextBox("HELLO", notreTexte,
                                100, 0);

        t.addCommand(QuitME);
        t.addCommand(new Command("Commande 2",
                                 Command.SCREEN, 10));
        t.addCommand(new Command("Commande 3",
                                 Command.SCREEN, 10));
        t.setCommandListener(this);
        disp.setCurrent(t);
    }

    public void pauseApp() {
    }

    public void destroyApp(boolean unconditional) {
    }

    /* Cette méthode permet d'intercepter les évènements tels que les clics sur les boutons. Par exemple, on intercepte ici nous mettons fin à l'application lors d'une action sur lebouton quitter. */
    public void
    commandAction(Command c, Displayable s) {

        /*
         * On met fin à l'application seulement si l'utilisateur a cliqué sur Quitter.
         */
        if (c == QuitME) {
            try{
                destroyApp(false);
                notifyDestroyed();
            } catch(Exception e){}
        }
    }
}
```

Maintenant que nous avons vu une application de base, il reste à voir à quoi ressemble le fameux fichier de configuration indispensable au fonctionnement de notre application. Pour notre exemple, ce fichier s'appelera Hello.jad et tient sur quelques lignes :

```
MIDlet-1: Hello, , hello.Hello
MIDlet-Jar-Size: 1552
MIDlet-Jar-URL: Hello.jar
MIDlet-Name: Un premier midlet
MIDlet-Vendor: PiratÆz
MIDlet-Version: 1.0
MicroEdition-Configuration: CLDC-1.1
MicroEdition-Profile: MIDP-2.0
```

NOTRE JEU EATHAT

Le jeu que nous allons créer est extrêment simple. C'est un packman qui doit manger le plus de blackhats et de whithats possible afin de gagner un maximum de points ;)
Pour utiliser le code qui suit, il vous faudra placer les fichiers dans un dossier appelé eatHat. Maintenant que tout est dit, nous pouvons enfin passer au code. Notre jeu est composé de trois images et six fichiers dont voici le code :

—> EatHat.java :

```
package eatHat;
import javax.microedition.midlet.*;
import javax.microedition.lcdui.*;
import javax.microedition.lcdui.game.*;

public class EatHat
   extends MIDlet implements CommandListener {

    private Command quitTheGame =
       new Command("Quitter", Command.EXIT, 0);
    private GameArea game;

    public void startApp() {

        game =
           new GameArea(Display.getDisplay(this),
                        "default");
        game.start();
        game.addCommand(quitTheGame);
        game.setCommandListener(this);
    }

    public void pauseApp() {
    }
```

```
    public void destroyApp(boolean unconditional) {
    }

    public void commandAction(Command c, Displayable d){
        if(c == quitTheGame) {
            destroyApp(false);
            notifyDestroyed();
        }
    }
}
```

—> GameArea.java

```
package eatHat;
import java.io.*;
import javax.microedition.lcdui.*;
import javax.microedition.lcdui.game.*;


public class GameArea extends GameCanvas
  implements Runnable {
    /* *** */
    int score;
    private Display disp;
    private PackManager packmanager;
    private LayerManager layermanager;
    boolean continueTheGame;
    String s;
    /* *** */


    public GameArea(Display d, String tmp) {
        super(true);
        disp = d;
        s = tmp;
        score = 0;
    }

    void start(){
        disp.setCurrent(this);
        continueTheGame = true;
        Thread t = new Thread(this);
        t.start();
    }

    public void paint(Graphics g){
        try {
            if(packmanager == null) {
                packmanager = new PackManager(g);
                packmanager.paint(g, score);
            }
        } catch(Exception ex){}
    }

  public void run(){
        Graphics g = getGraphics();
        while(continueTheGame){
            keycheck();
            score = packmanager.collision(score);
            if( score == 80) {
                continueTheGame = false;
            }
            try {
                paint(g);
                packmanager.paint(g, score);
                flushGraphics();
            } catch(Exception e){}
        }
    }

    void keycheck(){
        int keyState = getKeyStates();
        if ((keyState & LEFT_PRESSED) != 0) {
            packmanager.left();
        }
        else if ((keyState & RIGHT_PRESSED) != 0) {
            packmanager.right();
        }
        else if( (keyState & UP_PRESSED) != 0) {
            packmanager.up();
        }
        else if( (keyState & DOWN_PRESSED) != 0){
            packmanager.down();
        }
    }
}
```

—> PackManager.java

```
package eatHat;
import javax.microedition.lcdui.*;
import javax.microedition.lcdui.game.*;
import java.io.*;

public class PackManager extends LayerManager {
    Packman packman;
    Whitehat[] wh;
    Blackhat bh;
    int score;
    private int SCREEN_X;
    private int SCREEN_Y;
    private int SCREEN_WIDTH;
    private int SCREEN_HEIGHT;

  /** Creates a new instance of PackManager */
    public PackManager(Graphics g) {
        SCREEN_X = g.getClipX();
        SCREEN_Y = g.getClipY();
        SCREEN_WIDTH = g.getClipWidth();
        SCREEN_HEIGHT = g.getClipHeight();
    }

    public void paint(Graphics g, int score)
     throws Exception {
            Image pack_img =
               Image.createImage("/eatHat/packman.png");
            Image wh_img =
               Image.createImage("/eatHat/whitehat.png");
            Image bh_img =
               Image.createImage("/eatHat/blackhat.png");
            g.setColor(0xffffffff);
            g.fillRect(SCREEN_X, SCREEN_Y,
                       SCREEN_WIDTH, SCREEN_HEIGHT);
```

```
        Font font = g.getFont();
        int fontHeight = font.getHeight();
        int fontWidth =
            font.stringWidth("Ton score: "+ score);
        g.setColor(0x00000000);
        g.drawString("Ton score: "+ score,
                     (SCREEN_WIDTH - fontWidth),
                     (SCREEN_HEIGHT - fontHeight),
                     g.TOP|g.LEFT);

        if(packman == null) {
          packman = new Packman(pack_img, 30,30);
          packman.setPosition(134,78);
          append(packman);
        }
        if(wh == null) {
          wh = new Whitehat[3];
          wh[0] = new Whitehat(wh_img, 22,22);
          wh[0].setPosition(50,50);
          wh[1] = new Whitehat(wh_img, 22,22);
          wh[1].setPosition(200,0);
          wh[2] = new Whitehat(wh_img, 22,22);
          wh[2].setPosition(200,190);
          append(wh[0]);
          append(wh[1]);
          append(wh[2]);
        }
        if(bh == null) {
          bh = new Blackhat(bh_img, 18,18);
          append(bh);
        }
        if(score == 80) {
          fontWidth = font.stringWidth(
                      "Bravo tu as gagne !");
          g.drawString("Bravo tu as gagne ! ",
                       50, 50, g.TOP|g.LEFT);
        }
        paint(g,SCREEN_X,SCREEN_Y);
    }

int collision(int score){
    // gestion de la transparence dans le second
      paramètre de collidesWith()
    if( packman.collidesWith(wh[0], true) ) {
        wh[0].setVisible(false);
        score += 10;
    } else if( packman.collidesWith(wh[1], true) ) {
        wh[1].setVisible(false);
        score += 10;
    } else if( packman.collidesWith(wh[2], true)
                                        ) {
        wh[2].setVisible(false);
        score += 10;
    } else if( packman.collidesWith(bh, true) ) {
        score += 50;
        bh.setVisible(false);
    }
    return score;
                }
```

```
    void right() {
        packman.setTransform(0); // TRANS_NONE
        packman.move(1,0); packman.nextFrame();
    }
    void left() {
        packman.setTransform(0);
        packman.setTransform(2); // TRANS_MIRROR
        packman.move(-1,0); packman.nextFrame();
    }

    void up() {
        packman.setTransform(0);
        packman.setTransform(7); // TRANS_ROT_90
        packman.move(0,-1); packman.nextFrame();
    }
    void down() {
        packman.setTransform(0);
        packman.setTransform(5); // TRANS_ROT_270
        packman.move(0,1); packman.nextFrame();
    }
}
```

—> Packman.java :

```
package eatHat;
import javax.microedition.lcdui.*;
import javax.microedition.lcdui.game.*;

public class Packman extends Sprite {
    /* Création d'une nouvelle instance de Packman */
    public Packman(Image image,
                   int frameWidth, int frameHeight) {
        super(image, frameWidth, frameHeight);
    }
}
```

—> Whitehat.java :

```
package eatHat;
import javax.microedition.lcdui.*;
import javax.microedition.lcdui.game.*;

public class Whitehat extends Sprite {
  /* Création d une nouvelle instance de Whitehat */
   public Whitehat(Image image,
                   int frameWidth, int frameHeight) {
        super(image, frameWidth, frameHeight);
   }
}
```

—> Blackhat.java :

```
package eatHat;
import javax.microedition.lcdui.*;
import javax.microedition.lcdui.game.*;

public class Blackhat extends Sprite {
    /* Création d'une nouvelle instance de Blackhat */
    public Blackhat(Image image,
                    int frameWidth, int frameHeight) {
        super(image, frameWidth, frameHeight);
    }
}
```

Les images que nous utilisons doivent avoir une taille bien précise, sinon le jeu ne fonctionnera pas. En effet, chaque image est découpée en frames de taille identique. Par exemple, pour packman.png, l'image est composée de deux frames, chacune faisant 30 x 30 pixels :

Le fichier jad allant avec le jeu doit ressembler à ça :

```
MIDlet-1: EatHat, ,
        eatHat.EatHat
MIDlet-Jar-Size: 8185
MIDlet-Jar-URL: Piratz.jar
MIDlet-Name: eatHat
MIDlet-Vendor: Piratz
MIDlet-Version: 1.0
MicroEdition-Configuration:
        CLDC-1.1
MicroEdition-Profile:
        MIDP-2.0
```

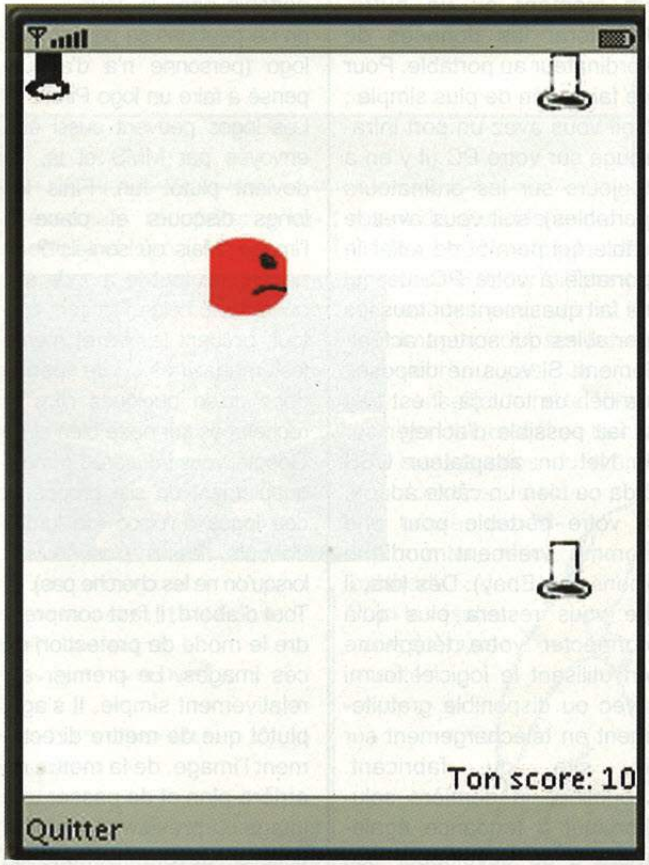
Une fois que vous aurez compilé le code, vous obtiendrez un jeu qui ressemble au screenshot ci-contre.

Comme je vous le disais, le jeu est très simple et il y a beaucoup de choses que l'on pourrait ajouter pour le rendre plus attrayant. Pour vous entraîner, voilà quelques pistes de développement que vous pourriez ajouter à ce jeu :

- gestion de la taille de l'écran, c'est-à-dire empêcher le pacman de sortir de celui-ci.
- randomizer la position des white/blackhats.

ajouter un gestionnaire permettant de mettre le jeu en pause.

- ajouter de nouveaux éléments au décor pour faire une sorte de labyrinthe.
- et tout ce qui vous passe par la tête ... ;-)



CONCLUSION

Voilà qui met fin à cet article. Nous avons vu qu'il est assez simple, avec quelques bases en programmation java, d'ajouter de nouvelles fonctionnalités à son téléphone. Nous ne pouvons évidemment pas décrire chacune des facettes du J2ME mais vous devriez pouvoir continuer de les explorer sans trop de problèmes.
Cependant il peut être intéressant de développer toute la partie réseau liée au téléphone ou d'analyser le fonctionnement d'un virus s'attaquant aux mobiles. Alors espérons que ces sujets seront traités dans de futurs articles. Votre mobile peut devenir une véritable télécommande pour PC ou une console de jeux, c'est donc à vous de créer ces programmes qui vous faciliteront la vie ;) .

REFERENCES

Total Java : livre de Steven Holzner (Eyrolles).
http://java.sun.com/ : vous y trouverez le J2ME ainsi que tout ce dont vous aurez besoin pour vous lancer dans le langage java (tutoriaux, spécifications, codes sources, etc.).

http://www.symbian.com/ : site officiel de systèmes d'exploitation symbian.
http://jcp.org/en/jsr/all : liste de toutes les JSR (Java Specification Request).
http://www.microjava.com/ : excellent site regroupant plusieurs tutoriaux pour se perfectionner.
http://www.f-secure.com/: pour vous tenir informé face aux alertes antivirales sur mobiles, cette société propose également des solutions antivirus pour les mobiles.
http://www.netbeans.org/ : environnement de développement idéal pour programmer en java.
http://eclipseme.org/docs/installation.html: un autre IDE assez simple d'utilisation avec toutes les étapes détaillées pour commencer dans de bonnes conditions.

CUSTOMISER SON
OU L'ART D'AVOIR UN PC

L'achat de logos et de sonneries est devenu un business très lucratif. On ne peut plus lire un magazine ou naviguer sur Internet sans voir apparaitre des pages entières consacrées à l'achat de ces gif ou mid à des prix déroutants. Cependant, la customisation de téléphones portables permet de rendre un petit peu plus fun cet objet dont on ne peut plus se passer. Pirat'z, défenseur des consommateurs et de vos portes monnaie, va vous montrer comment faire pour avoir le portable le plus branché sans débourser le moindre cent, ou presque.

INTRO

Les derniers téléphones s'arrachent à des prix fous (minimum 200 euros). Alors pourquoi ne pas vendre leurs accessoires à des prix tout aussi exorbitants ? C'est sur ce concept simple que les industriels ont tout d'abord commencé à vendre des coques pour téléphones portables coûtant pratiquement le prix du téléphone (et j'exagère à peine). Puis est venu le temps des logos et sonneries sur Nokia. Bien qu'alors très limité, ce marché à littéralement explosé avec l'apparition des écrans couleur et des sonneries polyphoniques.

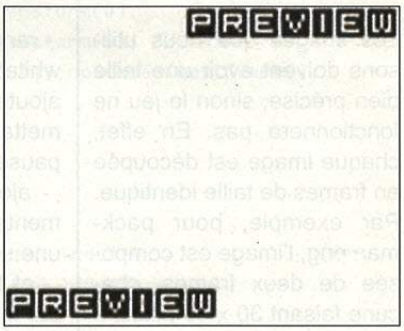
En tant que lecteur de Pirat'z avisé, le fait de payer pour avoir des logos ou des sonneries devrait vous scandaliser ! Heureusement vous lisez Pirat'z et vous allez voir que sur Internet, il suffit en réalité de se servir !

LE CONCEPT

Venant de recevoir mon tout dernier portable (ça faisait 7 ans que j'avais mon 3210) je décide donc, comme tout geek qui se respecte, de le customiser. Manque de pot pour moi, en allant chercher les tout derniers logos et sonneries sur le Net, je me rends compte qu'ils coûtent des fortunes ! Eh bien non, je ne payerai pas pour des images ! Le combat est lancé !

LE MATOS

Comme vous l'avez sans doute compris, il va falloir, à un moment ou un autre, transférer les données de l'ordinateur au portable. Pour ce faire, rien de plus simple : Soit vous avez un port infrarouge sur votre PC (il y en a toujours sur les ordinateurs portables), soit vous avez le câble qui permet de relier le portable à votre PC, ce qui se fait quasiment sur tous les portables qui sortent actuellement. Si vous ne disposez de rien de tout ça, il est tout à fait possible d'acheter sur le Net un adaptateur USB Irda ou bien un câble adapté à votre portable pour une somme vraiment modique (pensez à Ebay). Dès lors, il ne vous restera plus qu'à connecter votre téléphone en utilisant le logiciel fourni avec ou disponible gratuitement en téléchargement sur le site du fabricant. J'oubliais, la dernière solution qui à tendance également à se développer ces derniers temps est le bluetooth si vous disposez d'un mobile compatible. Le transfert de fichiers est en général très simple ; un drag and drop suffit. Nous n'allons donc pas détailler cette phase qui varie selon le modèle et la marque du téléphone. Allez, passons aux choses sérieuses !



LES LOGOS

Eh oui, pour avoir un portable dans le coup, on ne peut pas se passer d'un logo (personne n'a d'ailleurs pensé à faire un logo Pirat'z) ! Les logos peuvent aussi être envoyés par MMS et là, ça devient plutôt fun. Finis les longs discours et place à l'image. Mais où sont-ils ? Je pense que tout le monde sait où ils sont, hélas : ils sont partout, polluent le Net et même les magazines... Je pense donc qu'en quelques clics et recherches sur notre bien aimé Google, vous trouverez immanquablement un site proposant des logos à foison (on tombe d'ailleurs dessus plus souvent lorsqu'on ne les cherche pas).

Tout d'abord, il faut comprendre le mode de protection de ces images. Le premier est relativement simple. Il s'agit, plutôt que de mettre directement l'image, de la mettre en arrière-plan et de passer une image " preview " comme celle-ci, devant. Comme ça on ne peut plus cliquer et télécharger l'image.

La seconde méthode de protection consiste à mettre tous les logos sur des serveurs distants afin d'empêcher l'aspiration du site en entier. Cette protection, tout comme l'autre, n'est pas efficace mais nous fait perdre pas mal de temps pendant l'aspiration du site.

Maintenant, place à la technique ! ou plutôt les techniques ! Les sites n'étant pas tous les mêmes, il s'agira de toujours ruser et innover.

Commençons pas un exemple concret. Nous allons récupérer les logos d'un site

Après un bref coup d'?il, je décide de prendre un logo de pirate ! Mais comment faire ? Eh bien, voici la méthode qui marche à tous les coups ! Certes il faudra parfois faire quelques modifications, mais le principe reste le même. Bien sûr, on utilisera Firefox comme navigateur.

J'ouvre donc la page pour télécharger le logo et là, un pop-up s'ouvre avec mon logo défiguré par un preview. Comment faire ? Eh bien

PORTABLE,
RTABLE UNIQUE GRATOS

c'est très simple ! Nous allons déjà afficher la source de la page. Le clic droit est bloqué mais ceci ne nous pose pas de problème car un CTRL+U affichera quand même la source. Ne nous reste qu'à retrouver l'image dans celle-ci :

```
<tr><td align="center"
valign="middle"
background="http://serveur.du.site.net/t_15/120x160/
040209_skull.gif" style="border:1px solid
#000000;"><img src="img/preview.gif" width="120"
height="160"
style="filter:Alpha(opacity='40');"></td></tr>
<tr><td class="table" align="center>
```

On se rend bien compte ici que l'image n'était pas récupérable par un clic droit normal car elle était en fond d'écran. Cependant, avec la source, on la retrouve sans problème. Nous pouvons désormais récupérer n'importe quel logo.

Une méthode encore plus simple existe. C'est celle de l'aspiration. Eh oui, cette méthode est simple mais extrêmement bourrin (même pas peur) ! Nous allons donc installer n'importe quel aspirateur de site et le lancer sur l'URL cible. Une fois lancé, il faudra tester différentes options pour voir si les images sont sur le serveur ou pas. Je vous conseille de ne télécharger que ce qui se trouve sur les sites du même domaine. Je vous laisse expérimenter cette méthode dont voici le résultat après quelques minutes...

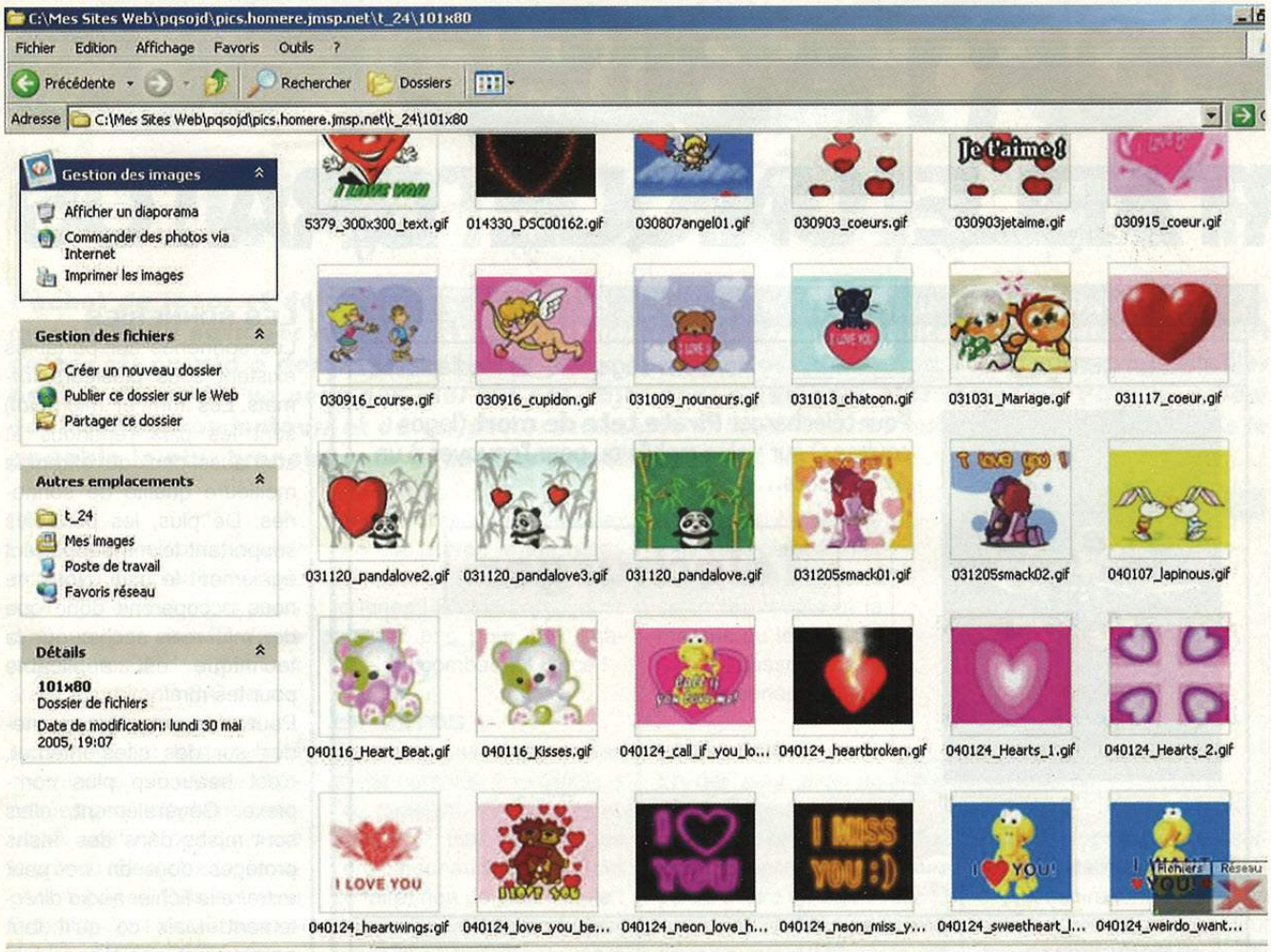
(voir image page suivante)

LES SONNERIES

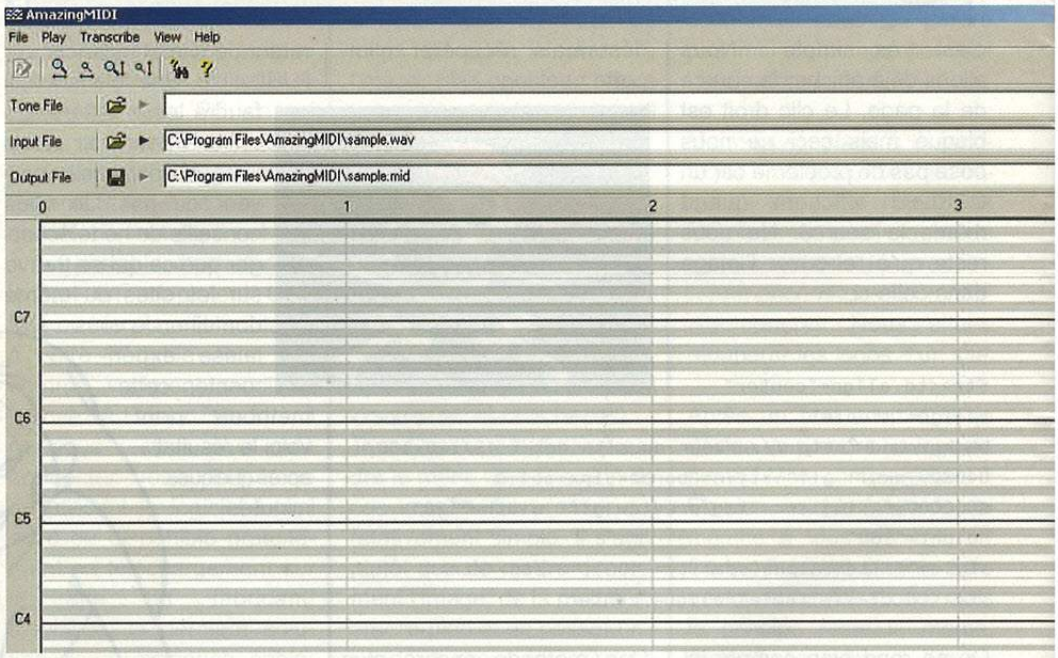
Les sonneries sur portables existent sous plusieurs formats. Les .mmf et .mid (midi) sont les plus répandus et sont aussi ceux qui offrent la meilleure qualité de sonneries. De plus, les portables supportant le mff supportent également le midi. Nous ne nous occuperons donc que des midi mais sachez que la technique est applicable pour les mmf.

Pour récupérer des sonneries sur des sites Internet, c'est beaucoup plus complexe. Généralement, elles sont mises dans des flashs protégés dont on ne peut extraire le fichier audio directement. Mais ce qu'il faut savoir c'est que les .mid et .mmf ne sont que des formats audios compressés pour portables. Nous n'avons donc qu'à compresser nos mp3
ou wav favoris pour en faire nos sonneries.

Pour convertir des wav en midi, il vous suffit d'utiliser



AmazingMidi. Vous sélectionnez votre wav en inputfile et le nom de votre fichier de sortie en midi comme ceci :



Il ne vous reste plus qu'à enregistrer…
L'url pour récupérer le logiciel : http://www.pluto.dti.ne.jp/~araki/amazingmidi/

La méthode est quasi identique pour les mp3. Il suffit de télécharger par exemple intelliscore sur : http://www.intelliscore.net/download.html ou tout autre logiciel de conversion et d'effectuer la même méthode que précédemment.

LE MOT DE LA FIN

Vous voilà donc fin prêt pour avoir le portable le plus customisé possible. Il ne vous reste plus désormais qu'à vous attaquer au firmware et autres logiciels internes pour tout finaliser mais là, ça devient plus compliqué. Allez jeter un ? il sur l'article qui explique comment créer un jeu sur son mobile ;)

ATTENTION, VOUS ETES SUR ECOUTE !

Ces derniers temps, les écoutes téléphoniques ont fait grand bruit. Avec l'affaire Bruno Gaccio, les écoutes illégales sont encore une fois repassées à la Une. Mais pensez-vous réellement que ces écoutes ne peuvent êtres faites que par la police ? Pas si sûr... Vous allez voir comment tous nos modes de communication préférés, en majorité sans fils, peuvent êtres abusés de manière très simple afin de pénétrer dans notre intimité. N'oubliez jamais, Big Brother is watching you !

LES TELEPHONES SANS FILS

Vous pensiez être à l'abris des oreilles indiscrètes lorsque vous utilisez votre téléphone sans fil ? Detrompez-vous, rien de plus facile que de mettre sur écoute ce genre d'appareils (encore plus simple pour écouter sur un babyphone). En effet, encore nombreux sont les appareils utilisant le mode analogique pour communiquer avec leurs bornes. Il suffit alors à l'intéressé de se munir d'un scanner de fréquences et de balayer la plage de fréquences réservée au téléphone sans fil jusqu'à ce qu'il tombe sur celle correspondant à votre téléphone. Ce genre de scanner est à la disposition de tous, en vente libre aussi bien sur des sites spécialisés que sur des sites grand public d'achats en ligne tel Ebay (une centaine d'euros).

Les scanners récents possèdent une fonction automatisant la recherche par balayage de fréquences ce qui simplifie énormément la tâche. Il faut savoir que les fréquences réservées aux téléphones sont connues de longue date et mises à la disposition de tous sur internet. De plus, la fréquence de votre téléphone est souvent inscrite au dos de celui-ci...
De quoi faciliter le travail d'un ami qui vous voudrait du bien...
Les appareils numériques sont beaucoup plus difficiles à écouter, c'est pourquoi nous vous les recommandons. Cependant, faites attention car de nombreux téléphones sont vendus comme étant analogiques et ne le sont pas forcément... Certains téléphones "cryptent" le signal en inversant les signaux, mais n'importe quel scanner haut de gamme décryptera la conversation automatiquement...

VOIP

Avec l'évolution des technologies en matière de communication internet, il est désormais possible au grand public d'accéder à des débits de connexion très élevés. Ainsi, on remarque l'arrivée sur le marché de nouvelles technologies de téléphonie reposant sur ces connexions, tel VoIP.
Qu'est-ce que le VoIP ? Sans entrer dans les détails techniques (voir l'article qui lui est destiné), il s'agit d'une technologie utilisant les protocoles internet permettant d'effectuer des appels aussi bien locaux que longue distance en utilisant le réseau internet au lieu des réseaux de téléphonie classiques, ou comme on l'entend dans les publicités de nos chers FAI : "le téléphone par internet".
Dès lors, du fait qu'elle repose sur les protocoles réseaux internet, elle se retrouve sujette aux mêmes types d'attaques. Ainsi, il est possible de capturer le trafic en sniffant ou bien en effectuant ce que l'on appelle un man in the middle par quelque méthode que ce soit, dans le réseau où se situe le téléphone et d'en enregistrer la communication.
On trouve depuis quelque temps ce genre de logiciels sur internet permettant de capturer puis d'analyser les données pour en reconstituer la discussion, le tout enregistré dans un mp3. Prenons par exemple CAIN (téléchargement gratuit sur : http://www.oxid.it/projects.html). La dernière version possède une fonction d'écoute et de reconstitution de la conversation. Lancez Cain, sélectionnez l'interface réseau, lancez le sniffer onglet VoIP et c'est parti. La discussion reconstituée et enregistrée dans un fichier format mp3 pour votre plus grand plaisir, je vous invite à aller voir tout le tutoriel sur le Net en vidéo à l'adresse http://www.iron-geek.com/i.php?page=videos/cainvoip1. Vous possédez une connexion wifi ?
C'est encore mieux ! En plus de sniffer vos mots de passe et d'utiliser votre connexion, le pirate pourra écouter vos appels. Il est très intérressant de noter que le VoIP tend à être de plus en plus utilisé dans les entreprises, tout comme le wifi...

GSM

Après toutes ces émotions, vous sautez sur votre téléphone portable, lui il est numérique et n'est pas relié au Net (quoique). En plus, le réseau GSM est protégé des écoutes par les divers algorithmes de cryptage. Il a été clairement établi par des scientifiques qu'il n'est pas possible de décrypter en temps réel une conversation. Néanmoins, il reste plusieurs attaques possibles concernant l'écoute des données sur le réseau, une fois celles-ci collectées et enregistrées.
L'accès à la partie du réseau comprise entre le BTS et le BSC est facile. Ce qui est plus dur dans ce type d'attaque est d'obtenir le matériel permettant d'écouter ces informations (seule la police en a le droit et les moyens) mais des sociétés louent cependant à des prix astronomiques ce genre d'appareils.
Il est possible aussi, pour les gens qui connaissent l'algorithme A5 et la clé Kc, de faire une fausse Station BTS et de faire croire à l'utilisateur à une connexion au réseau. Cette attaque (de type Man In the Middle) permet de récupérer toutes les informations désirées, en clair. Il est possible, pour ne pas se faire remarquer, d'envoyer par la suite les messages au réseau comme si de rien n'était. Cette attaque est donc très dangereuse car elle permet au fraudeur de récupérer toutes les informations voulues et même de les modifier.

Vous êtes toujours sûr de vouloir raconter vos plus grands secrets au téléphone ?

Il est aussi intéressant de signaler que de nombreuses caméras de surveillance sur IP sont disponibles en faisant une simple recherche sur Google. Les caméras de surveillance des bâtiments sont également très souvent sur wifi et très peu de matériel est nécessaire pour récupérer la vidéo de ces immeubles. J'ai par exemple pu récupérer la caméra d'un hangard se trouvant à 100 m de chez moi en installant un système pour partager mon lecteur DVD en wifi. Si le sujet vous intérresse, je vous conseille d'aller regarder sur internet, du côté du matériel d'espionnage : gsm espion, matériel d'écoute en tous genres, micro, etc. De quoi devenir vraiment parano...

BEST OF DU NET PIRAT'Z

Voici une sélection des meilleurs liens parus dans Pirat'z. Ces sites sont donnés pour information seulement. Du contenu potentiellement illégal pourrait s'y trouver suivant la législation de votre pays. Pour notre belle France, voir les articles du code de la propriété intellectuelle relatifs aux logiciels : www.legalis.net/legalnet/cpilog.htm

HACKING et SECURITÉ INFORMATIQUE

Vulnérabilité. Actualité en français sur le hacking et la sécurité : www.vulnerabilite.com

Packetstorm. Tous les exploits, outils, failles... en anglais : packetstormsecurity.nl

K-Otik. Toutes les vulnérabilités, en français : www.k-otik.com

Input Output Corporation. Une team qu'on l'aime bien : www.ioc.fr.st

Anonymat. Se cacher sur le net : www.anonymat.org

Stay Invisible. Si vous cherchez un proxy : www.stayinvisible.com

Ouah. Docs "spécialisées dans l'intrusion réseaux UNIX". Très technique : www.ouah.org

Phrack. L'e-zine de référence des hackers, en anglais : www.phrack.org

Zone-H. Actualité des activités pirates : zone-h.org

Madchat. Vision d'underground : www.madchat.org

NSA. Les espions américains qui nous surveillent : www.nsa.gov

DGSE. Les français qui surveillent les ricains : www.dgse.org

Dicofr.com. Un dictionnaire des termes techniques en informatique : www.dicofr.com

SAUVEGARDE et DEVELOPPEMENT

- Génériques

MegaGames. Une foule de cracks, de patchs, de trainers, de cheats, de tutoriaux et d'utilitaires sur toutes les plate-formes: www.megagames.com

GameCopyWorld. Cracks et utilitaires pour faciliter la sauvegarde : www.gamecopyworld.com

ConsoleDeJeux. tout ce que vous avez toujours voulut savoir sur vos consoles de jeux, sans jamais oser le demander : www.consoledejeux.info

- Copie (gravure, modchips, ...)

Files Forums. Forums dédiés à la sauvegarde et à la gravure : www.fileforums.com

JCInfos. Un autre forum où obtenir plein d'infos sur les puces consoles : jcinfos.com

Jeux et consoles. Bon site de vente pour les puces, consoles prémodifiées et autres accessoires : www.jeux-et-consoles.com

- Spécifiques à certaines machines

Programmer's tools. Tous les outils du programmeur Windows pour le reverse-engeneering : protools.cjb.net

Xbox Scene. Toute l'actualité de l'underground Xbox : www.xbox-scene.com

Xbox-Linux. Installez Linux sur votre Xbox : xbox-linux.org

PS2Ownz. Des infos et des forums bien remplis sur la PS2 : www.ps2ownz.com

Backup-Source. La sauvegarde sur PS2 et Xbox : www.backup-source.com

Guide copie Dreamcast. Et en français en plus : membres.lycos.fr/raptor83/dreamcast/copie.htm

XAVBOX. Les sites de Xavier sur la Xbox et la PS2 : www.xavbox.com et www.xavboxps2.com

Metagames-fr. Tout faire avec sa console : www.metagames-fr.com

HD loader. plus besoin de puces avec le hd loader hdloader.xavboxps2.com

ForumXboxPs2. Le forum sur toutes les puces de XBox et Ps2 : www.forum-xbox-ps2.com

TELECHARGEMENT et ACTU PIRATE

- Web

iSONEWS. La référence de l'actualité pirate : www.izonews.com

NFOrce. Tous les NFO, rien que les NFO : www.nforce.nl

Console-News. L'Isonews de la PS2 et de la Xbox: www.console-news.org

- Peer-to-Peer

Ratiatum. LE site français du P2P : www.ratiatum.com

Direct Connect. Logiciel de partage P2P original : www.neo-modus.com

Open-Files. Un site français sur le P2P en général et eDonkey, Overnet, eMule en particulier : www.open-files.com

- FTP, News et IRC

SmartFTP. Un client FTP gratuit : www.smartftp.com

newzBin. Traque pour vous les binaries postées sur les News : www.newzbin.com

mIRC. Le client IRC le plus répandu : www.mirc.com

Invision. Un mIRC bourré aux vitamines : invision.lebyte.com

ABANDONWARE et EMULATION

- Abandonware

Abandonware Ring. Recense les meilleurs sites traitant d'Abandonware : www.abandonwarering.com

Home of the Underdogs. Une référence de l'Abandonware que vous ne pouvez pas manquer : www.the-underdogs.org

Oldiesfr.com.. Un site moins fourni, mais en français : www.oldiesfr.com

- Emulation

Zophar's Domain. L'ancêtre est toujours là : www.zophar.net

Emu Unlim. Site très complet dédié à l'émulation : www.emuunlim.com

Linux Emu. L'actualité de l'émulation sous Linux : linuxemu.retrofaction.com

NGEmu. Un bon site d'émulation pour les consoles récentes : www.ngemu.com

Emu-France. Un site français très complet sur toute l'actualité de l'émulation : www.emu-france.com

Toudy. Un site bien sympa en français : www.toudy.com

Emulation64. Toute l'émulation N64 en français : www.emulation64.net

Pdroms. Des tas de roms freeware : www.pdroms.de

T-SHIRT PIRAT'Z GSM

22 euros
Frais de port compris

PIRAT'Z, 26 BIS RUE JEANNE D'ARC 94160 SAINT MANDE

Existe en plusieurs tailles : M, L ou XL

Nom : ..... Prénom : ..... E-mail : .....
Adresse : .....
CB : ..... / ..... / ..... EXP. le : .....

☐ *Chèque à l'ordre de Publia*
☐ *Mandat à l'ordre de Publia*

Frais de port compris

TOTAL A PAYER

Signature

PHSGSM1

Taille	Quantité